SKILLS FOR SUCCESS
WORK READY YOUTH PROGRAM

DIGITAL WORKBOOK!

Skills Compétences
Canada

Acknowledgement

The Skills for Success Work Ready Youth Program - Workbook Series was developed by Skills/Competences Canada, with support from the Government of Canada.

Acknowledgement is given to Bow Valley College who were instrumental in developing the content of the workbooks.

For more information contact:
Skills/Competences Canada
294 Albert Street, Suite 201 | Ottawa, Ontario | K 1 P 6E6
Fax: (613) 691-1404 | Toll Free: 1 (877) 754-5226
https:// skillscompetencescanada.com/ en/

This document is distributed by Skills/Competences Canada

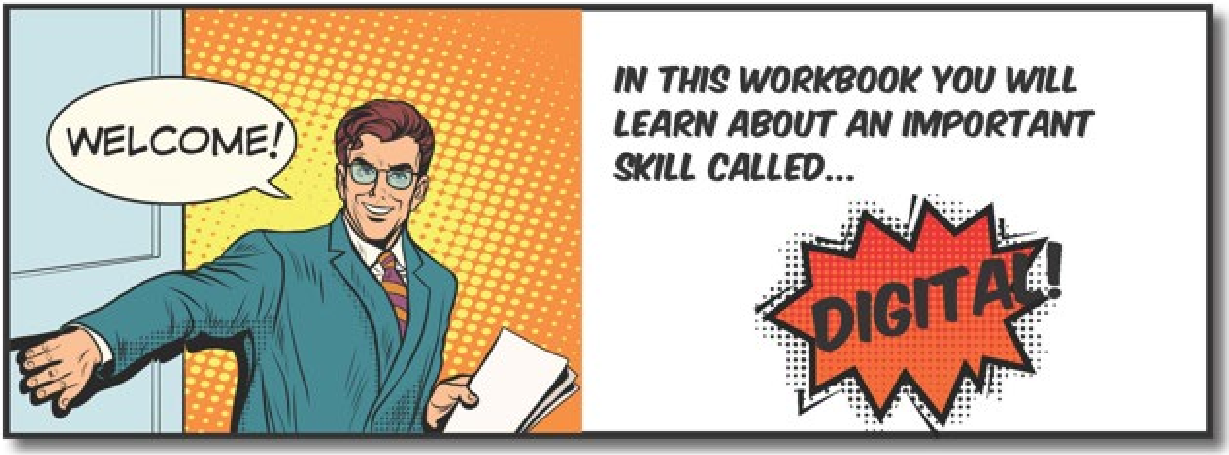
Funded in part by the
Government of Canada's
Skills for Success Program

Canada

DIGITAL

Use the table of contents to navigate through this workbook. Track your progress by putting a checkmark beside each topic you complete.

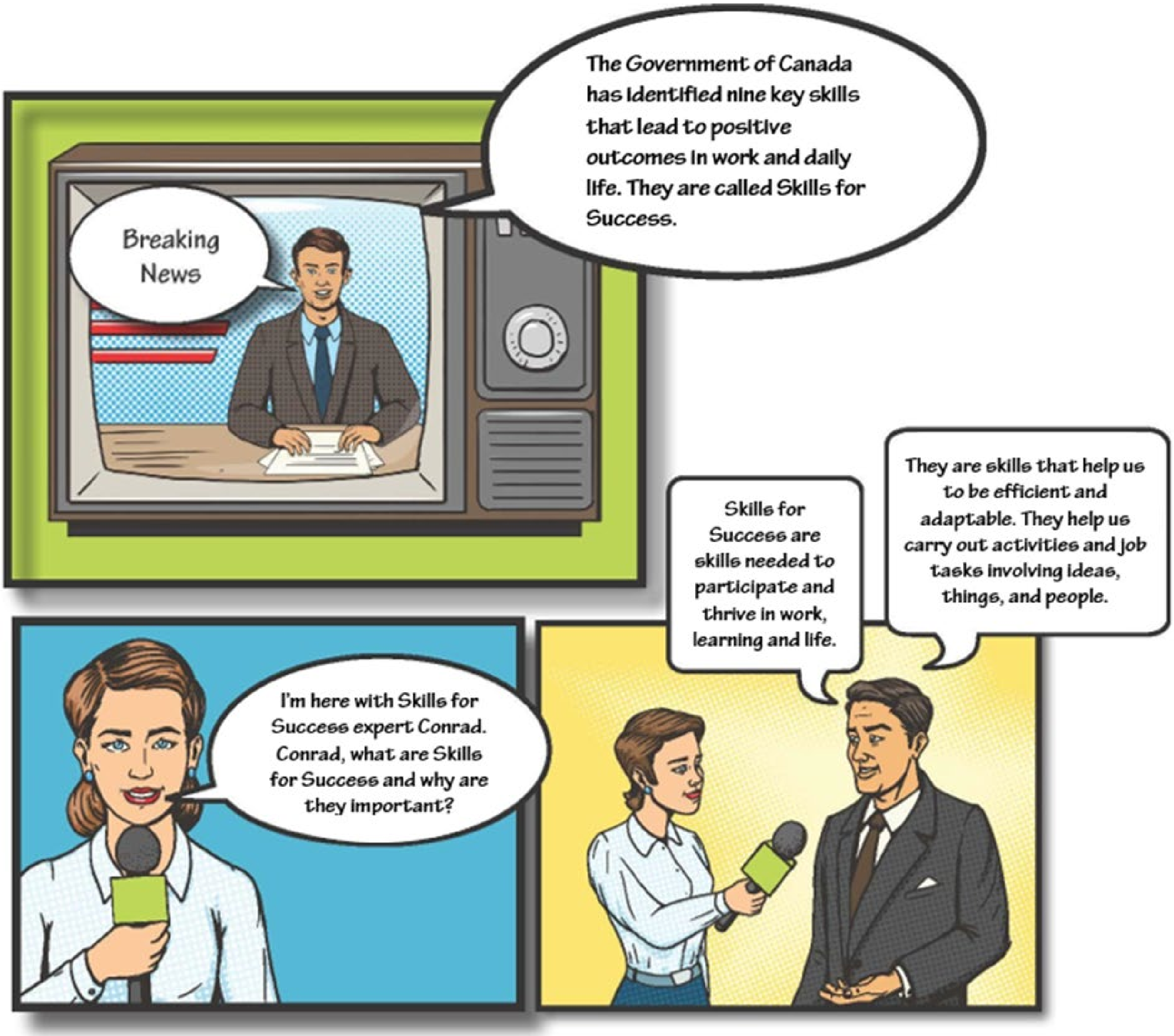
WELCOME TO THE SKILLS FOR SUCCESS WORK READY YOUTH PROGRAM


WELCOME!
IN THIS WORKBOOK YOU WILL LEARN ABOUT AN IMPORTANT SKILL CALLED...
DIGITAL!

Q: HOW DO I USE THIS WORKBOOK?

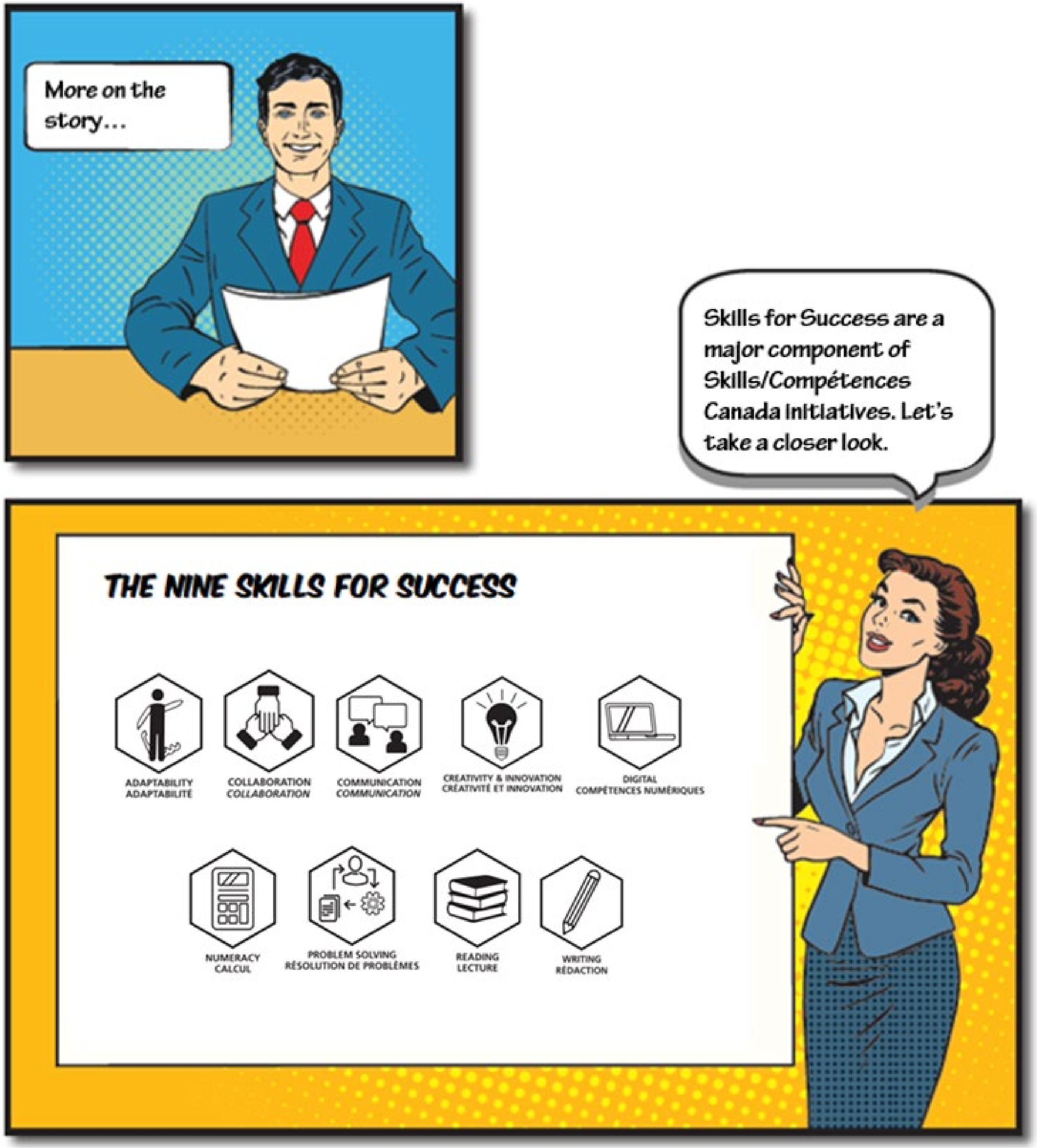
1. START BY REVIEWING THE INFORMATION AND FUN FACTS ABOUT DIGITAL AND SKILLS FOR SUCCESS.
2. PRACTICE YOUR SKILLS IN THE "WORKOUT" SECTION.
3. BUILD YOUR SKILLS IN THE "BOOSTER" SECTION.
4. IN THE ANSWER KEY SECTION, CHECK YOUR WORK FROM THE WORKOUT SECTION.
5. TRY THE ASSESSMENT QUESTIONS AT THE END TO GET AN IDEA OF HOW STRONG YOUR SKILLS ARE.

INTRODUCING THE SKILLS FOR SUCCESS


The Government of Canada has identified nine key skills that lead to positive outcomes in work and daily life. They are called Skills for Success.
Breaking News
I'm here with Skills for Success expert Conrad. Conrad, what are Skills for Success and why are they important?
Skills for Success are skills needed to participate and thrive in work, learning and life.
They are skills that help us to be efficient and adaptable. They help us carry out activities and job tasks involving ideas, things, and people.

SKILLS FOR SUCCESS ARE THE SKILLS ALL PEOPLE NEED FOR WORK, LEARNING AND LIFE. THEY FORM THE FOUNDATION FOR LEARNING OTHER SKILLS.

THE NINE SKILLS FOR SUCCESS



BUILDING SKILLS FOR SUCCESS

Think of a time you tried something new. It can be a sport, learning to code, learning to play an instrument. Maybe you were great at it right away, but most of us aren't. We practice so we get better. In the same way, you need to practice, to build your Skills for Success. To do this, you need to practice tasks, questions and problems related to the Skills for Success, starting with those at Entry level and working up to Intermediate and Advanced levels.

SKILLS FOR SUCCESS LEVELS		
Entry	Intermediate	Advanced
Practice needed	Ready to keep learning	Good to go!

Skills like muscles get stronger the more we use them and strengthening your Skills for Success will help you succeed in today's evolving work environment and in daily life.

WHAT DO THE LEVELS MEAN?

- Tasks, questions, and problems at Entry level are less difficult than those at the Intermediate and Advanced levels.
- People with skills at Entry level need to practice, to make their skills stronger. When you have skills at, or above, Intermediate level, you have skills that are strong enough to allow you to learn academic, technical, or job-specific skills.
- Employers like to hire workers who are efficient, capable learners because they know they are more likely to accurately solve problems, complete their work, learn new processes, and adapt to changes on the job.
- The skills are just as important in daily life. We all need to read information, fill out documents, make decisions about how much we can spend on things we want to buy, work, and communicate effectively with friends, family, teachers, and employers, and use computers and other digital technologies.

SKILLS FOR SUCCESS MATTER

SKILLS FOR SUCCESS ARE USED TO NAVIGATE OUR DAILY LIVES AND THE WORLD OF WORK, AND THEY ALLOW US TO KEEP LEARNING, SO WE DON'T GET LEFT BEHIND.

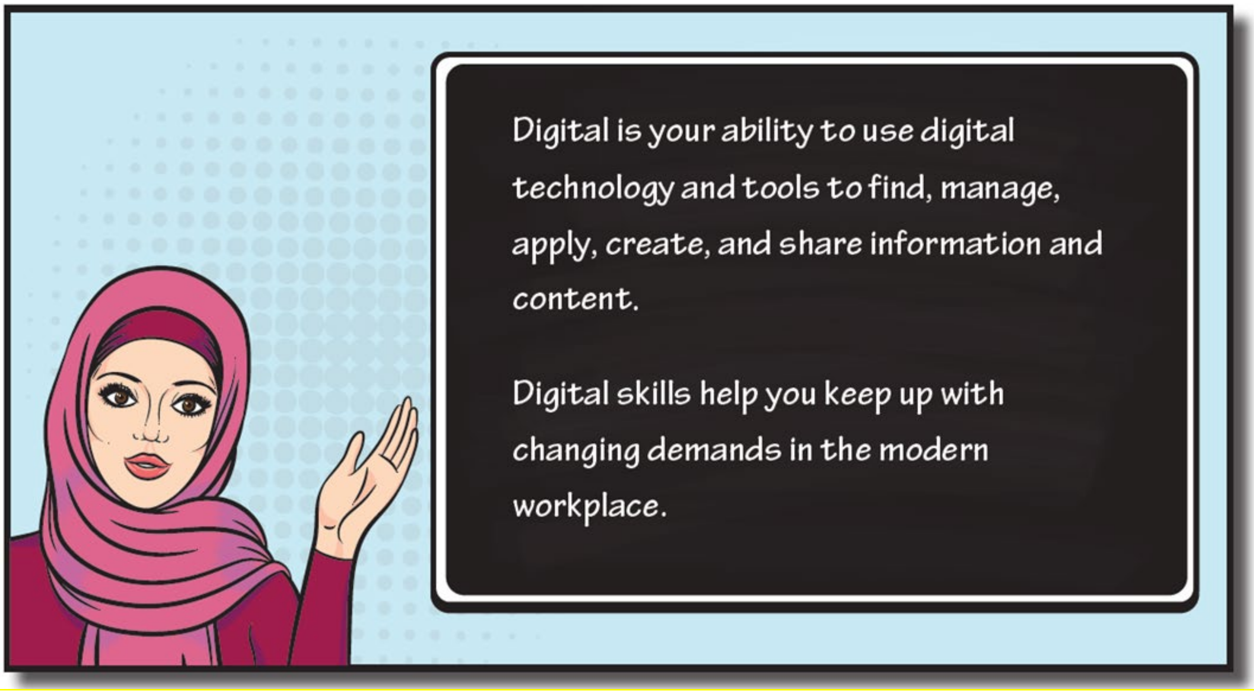
GIVE IT A TRY! MATCHING TASKS AND SKILLS

Look at the list below. What skills do you think you would need to complete each task? Write the abbreviation for any of the skills you think would be used to complete the task. One is started for you as an example. (*HINT: they all require more than one skill.*)

Task	Skills Used
Find information online to complete the set-up of a new iPhone.	
Apply online for a learner's license.	
Book concert tickets online.	
Help plan a fundraiser for your sports team.	
Make a plan to pay for the boots you want when they are more expensive than expected.	
Find an alternate way to travel when you can't use the car to go skiing.	
Text your coach to say you will be late for practice, and why, and how you will catch up on what you miss.	
Arrive at work early to learn the new customer payment system, from your boss.	NU,
Use an online transit schedule to get to your new job on time.	

Skills for Success	
ADA	Adaptability
COL	Collaboration
COM	Communication
C I	Creativity & Innovation
DIG	Digital
NU	Numeracy
PS	Problem Solving
RE	Reading
WR	Writing

GETTING STARTED WITH DIGITAL



Digital is your ability to use digital technology and tools to find, manage, apply, create, and share information and content.

Digital skills help you keep up with changing demands in the modern workplace.

ABOUT DIGITAL SKILLS

Every day you face new challenges at school or at work or in daily life. Many of these challenges require you use your digital skills. The word digital is an umbrella term that includes the tools you use (cellphones, tablets, etc.), the ways you create and manage information on those tools (software, apps, spreadsheets, etc.), and the knowledge you use to do all of those safely and securely.

There are many reasons "digital" is frequently in the spotlight. Here are a few of them. The world is so connected that news of what is happening is available almost instantly. Activities we do everyday – like shopping, using a telephone or doing our banking – increasingly require us to interact with digital technology. Technology is impacting every area of our lives, and the rate of digital change is speeding up.

A person born after 2001, is often called a "digital native", someone who was brought up during the age of digital technology and is therefore familiar with computers and the internet from an early age. But familiar does not mean you automatically know how to be a safe and smart user of that technology.

Remember, to use digital information and tools safely and securely, it is essential to be constantly aware of changes in technology and possible threats to privacy and security. Stay alert!

DIGITAL MAKES A DIFFERENCE

SKILLS FOR NOW & THE FUTURE

Digital technology has changed the way you find and share information, solve problems, and communicate with others. Most jobs now use digital skills, and you need them when you apply other skills such as reading, writing or numeracy.

https://srdc.org/project/research-report-to-support-the-launch-of-skills-for-success-structure-evidence-and-recommendations-final-report/#

YOUR DIGITAL SKILLS INCLUDE YOUR ABILITY TO UNDERSTAND AND APPLY ALL OF THE FOLLOWING CATEGORIES OF DIGITAL TOOLS AND PRACTICES.

DEVICES

Includes computers, tablets, phones, hand helds, and trade-specific tools.

TOOLS

Includes knowing when to use which software, apps, Artificial Intelligence (AI), etc.

DATA & INFORMATION

Includes knowing how to search for, evaluate, and organize digital data.

COLLABORATION

Includes using tools to communicate, collaborate and share information.

SAFE PRACTICES

Includes understanding and applying rules of privacy and security.

LEARNING

Includes the ability to keep up with rapid changes in technology to build on exisiting digital skills.

NOW GIVE DIGITAL SKILLS A TRY

Think about how you use your digital skills every day – whether at a job or in your daily life. Complete the following table with examples of how you complete digital tasks or practice digital safety related to each category either at work or in daily life: be as specific as you can. We've filled in examples from how a bricklayer uses their digital skills, to help you get started.

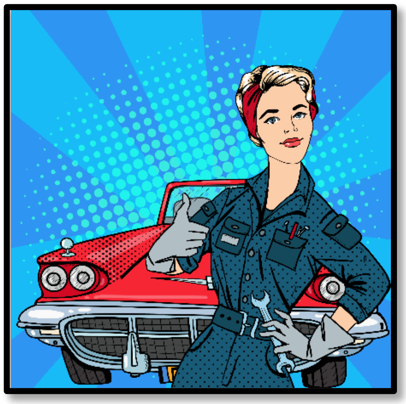
DIGITAL CATEGORIES	BRICKLAYER	YOU
Devices	*Uses digital measurement tools to accurately calculate area and required number of pavers.*	
Tools	*Uses emails to confirm expenses and texts to co-workers.*	
Information & Data	*Enters information in a spreadsheeted template to complete an estimate.*	
Collaboration	*Texts supervisor if they are running late or going to arrive early.*	
Safe Practices	*Enters a password to access the company accounting system to securely update client's personal information.*	

Learning	*Participates in online courses to update safety credential or learn about hardscaping with bricks.*	

DIGITAL SKILLS MAKE A DIFFERENCE

AT WORK

When you are working, your digital skills are an important factor in your success. Many skilled trade occupations that used to be considered primarily “hands on” now require advanced digital skills. For example, consider the diagnostic tools that automotive and heavy-equipment technicians use today, and the fact that schematic drawings are now mostly read on tablets rather than from rolls of paper blueprints. Your safety, productivity, and opportunities to advance will all be impacted by your digital skills.



AT HOME

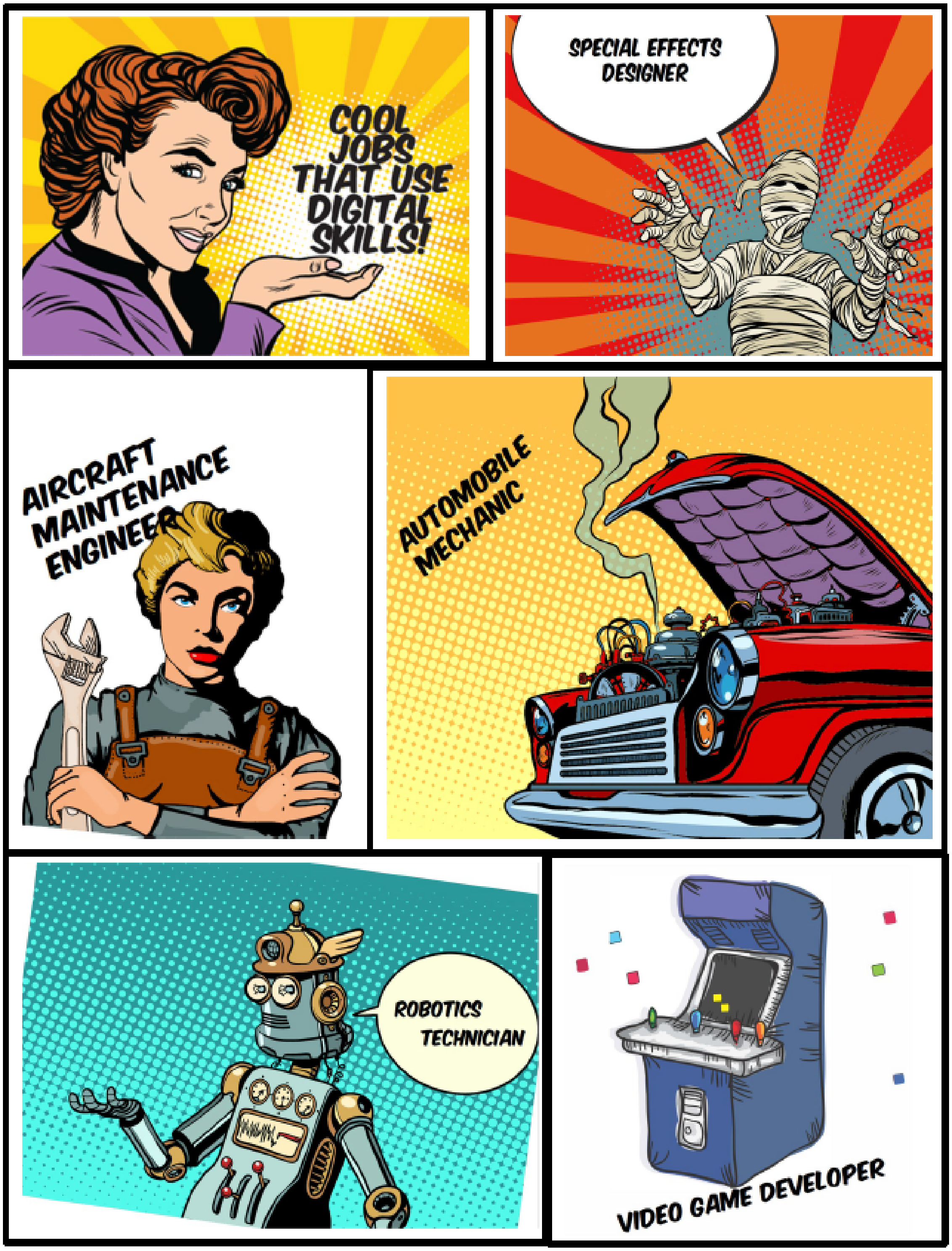
Our non-working life is impacted by our digital skills too. The way we communicate with others whether by text, email, or messaging apps all require us to use digital skills. Navigating digital tasks such as texting and making purchases online may seem easy to you, but making sure you complete those tasks securely is essential to protect your personal and financial security, and the privacy of those you are communicating with.

MEASURING DIGITAL SKILLS

Skill in digital is measured on three levels:

- Basic: You can use basic functions of familiar digital devices. You need guidance to find and evaluate the relevance and reliability of online information, and to engage in safe online practices.
- Intermediate: You can use a wider range of functions of familiar and unfamiliar digital devices, including customizing devices for specific purposes (e.g., download and use an app, set up macros to automate tasks). You can find and use relevant and reliable online information and engage in safe online practices.
- Advanced: You have in-depth knowledge of digital device operations and information technology systems. You can find and use relevant and reliable online information to improve digital processes, including enhancing your own online safety. You can assess future digital needs and keep your own digital skills up to date.

COOL JOBS THAT USE DIGITAL SKILLS



A DIGITAL LESSON...

About Apps

App is a short form of the word “application”. An application is a software program created to accomplish a specific task for a user or, sometimes, for another software program. Initially “app” referred mainly to mobile apps focused on one purpose or task, like checking the weather, taking notes, or completing calculations. Over time, the meaning of the term broadened and now it’s commonly used to refer to applications running on any type of device.

Mobile apps are convenient to use and very efficient. The personalized experiences they provide make them very attractive to users.

The Most Popular Apps in 2022

TikTok was the most popular app worldwide by downloads in 2022, maintaining its title for the fourth consecutive year. The video platform had 672 million downloads in 2022, with the company also doubling its annual revenue to $ 9.4 billion according to Business of Apps. https://www.visualcapitalist.com/cp/most-popular-apps-by-downloads/

AI Apps Are Gaining Popularity, Fast

In 2020 and 2021, many essential business apps including Zoom and Microsoft Teams grew quickly and saw massive success. While downloads for these apps fell in 2022, many other travel, food, and shopping-centered apps including Google Maps, McDonald’s, and Shein helped fill the void.

However, it was artificial intelligence (AI) apps, including Lensa AI and ChatGPT, that saw the greatest spike towards the end of last year. Could these same AI-infused apps help lead the pack in terms of downloads for the most popular apps of the future? https://www.visualcapitalist.com/cp/most-popular-apps-by-downloads/

A Useful Tip

Cleaning up your apps will make your phone easier to navigate, perform better, and also make it more secure. Old apps that no longer get updates or that you haven't updated in some time can create serious security flaws. consumercellular.com

A DIGITAL LESSON...

SHARING ON SOCIAL MEDIA

If you feel you must share news or information or chip in on online discussions, that can be useful or possibly even important. That sort of discussion is one thing it was originally envisioned social media would be very useful for. But if you do decide to chip in, do yourself and others who may read your posts a favour by taking the time to confirm that the information is accurate. Check with at least one other trustworthy source. The extra time you take could make the difference between a useful addition to an important discussion and adding to uninformed noise and chaos.

As Charlie Warzel, contributing writer for The Atlantic wrote, "Social media's greatest strength is thus its original sin: These sites are excellent at making you feel connected and informed, frequently at the expense of actually being informed,". https://www.theatlantic.com/technology/archive/2023/10/social-media-infrastructure-news-algorithms/675614/

DIGITAL MAKES A DIFFERENCE

THINK DIGITAL ISN'T A BIG DEAL? THINK AGAIN!

TWO KEY TAKEAWAYS FROM A SEPTEMBER 2020 REPORT BY THE CONFERENCE BOARD OF CANADA:

1. Improving digital skills will be the most important factor in adapting Canada's skilled trades to the future of work.

The report describes some of the ways digital technology is impacting trades and what the impacts mean for the specific skills apprentices and trades people need to develop.

Automotive tradespeople – service technicians, heavy-duty equipment technicians, auto body and collision technicians, and related motive power trades – are impacted by a shift toward more computerized systems and away from mechanical work. Compared with other large Red Seal trades, automotive service technicians report the largest impact of technological change in their workplace. The increasing use of digitalization in automotive trades mirrors the shift to electric, hybrid, and autonomous vehicles. Automotive service technicians are also expected to need human–machine interface skills to repair autonomous vehicles.

Manufacturing trades – Welders, machinists, industrial mechanics, and other industrial tradespeople – rely more and more on sophisticated technologies. They work with digital thermostats, digital control systems, sensors, digital measuring tools, and automation systems.

Construction trades – construction electricians, plumbers, carpenters, ironworkers, refrigeration and air conditioning mechanics, and other construction tradespeople – are impacted by a growing reliance on smart technologies, building information modelling, automation systems, and the Internet of Things, such as custom home lighting systems that are accessible via a smartphone.

Food service trades – cooks, bakers, and chefs – use digital apps and computerized systems in their daily work. Payroll and scheduling is more often done on apps, POS (point of sale) technology makes service faster, and orders are done on websites or through electronic chits.

2. Tradespeople will need seven core digital skills.

1. Technical
2. Information management
3. Digital communication
4. Virtual collaboration
5. Creativity
6. Critical thinking
7. Problem-solving in digital environments

ARE YOUR DIGITAL SKILLS READY?

DIGITAL SKILLS IN ACTION!

CHECK OUT THESE EXAMPLES OF REAL WORKPLACE TASKS THAT DEPEND ON DIGITAL SKILLS, FROM CAREERS YOU CAN READ ABOUT AT: SKILLSCOMPETENCESCANADA.COM

1. Refrigeration and air conditioning mechanics use databases to enter customer contract information and the model number of heating and ventilation systems installed. (Digital Basic Level)

2. Electrical installers search through internet websites and navigate several menus to locate technical data such as pin assignments on integrated circuit chips. (Digital Intermediate Level)

3. Automotive painters use electronic, hand-held wands to scan vehicle paint colours and determine paint colours and codes. (Digital Intermediate Level)

4. Cooks use spreadsheets to determine what quantities of each ingredient is required to make up 20 orders instead of 1 by using formulae. (Digital Intermediate Level)

5. Graphic designers use CAD (computer-aided design) software to produce computer animation in movies and games. For example, 2D and 3D animators use CAD to design buildings and rigid structures or the background scenes of games. (Digital Intermediate Level)

6. Electronic testers use computer-automated test software or computerized digital multimeters and oscilloscopes. (Digital Basic Level)

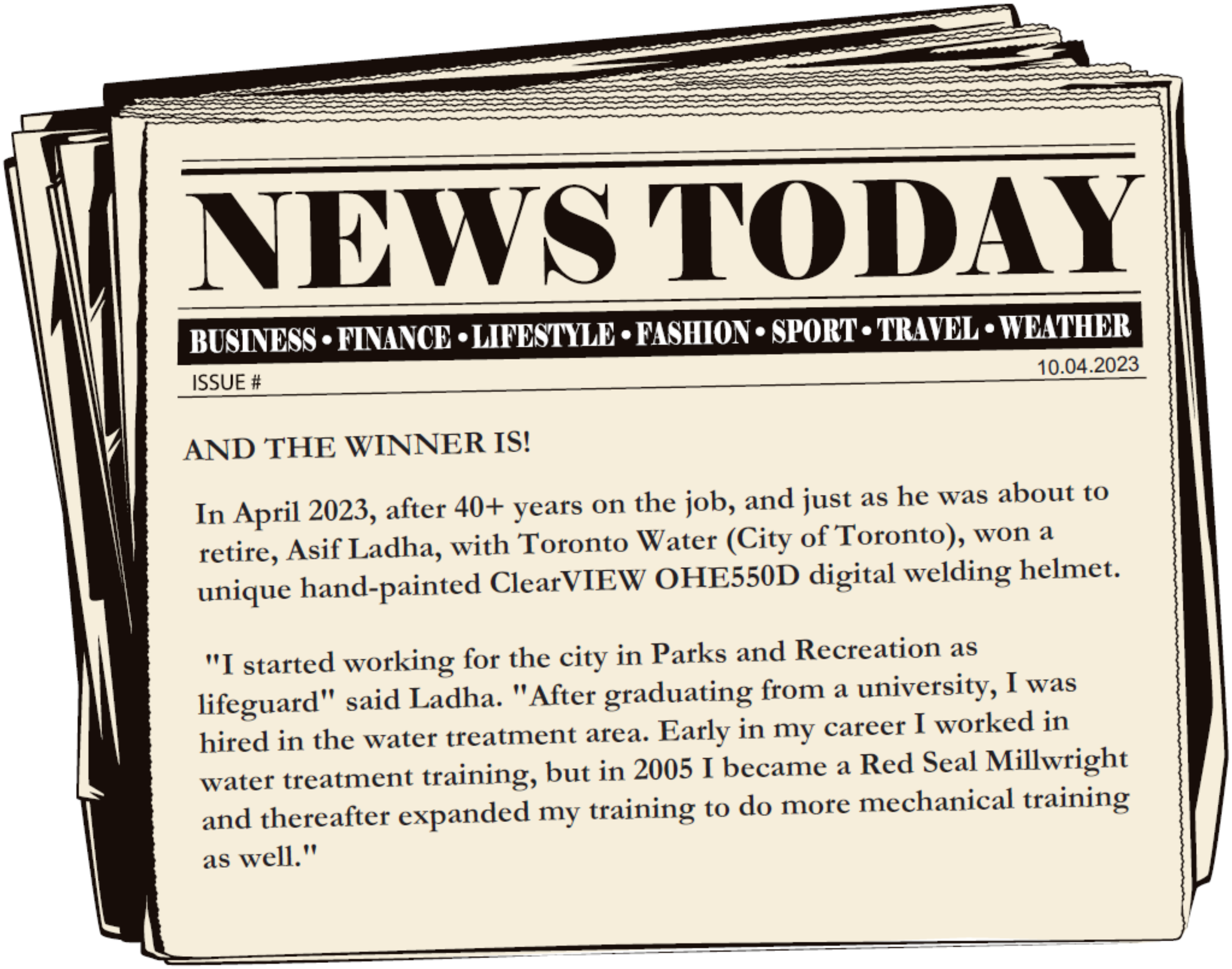
7. Welders input data and operate plasma cutting machines, orbital welders, and other computer-controlled equipment. (Digital Intermediate Level)

8. Carpenters use computer-controlled equipment such as total stations, smart levels and workplace alarm systems (Digital Basic Level)

9. Aerospace technologists use databases to optimize workflow, e.g., use corporate aircraft maintenance planning software to access the maintenance schedules required by manufacturers. (Digital Intermediate Level)

10. Web designers use graphics software to create banners, backgrounds, illustrations, animations, and other design elements for use in web sites. (Digital Advanced Level)

DIGITAL SKILLS IN THE NEWS!



NEWS TODAY

BUSINESS • FINANCE • LIFESTYLE • FASHION • SPORT • TRAVEL • WEATHER

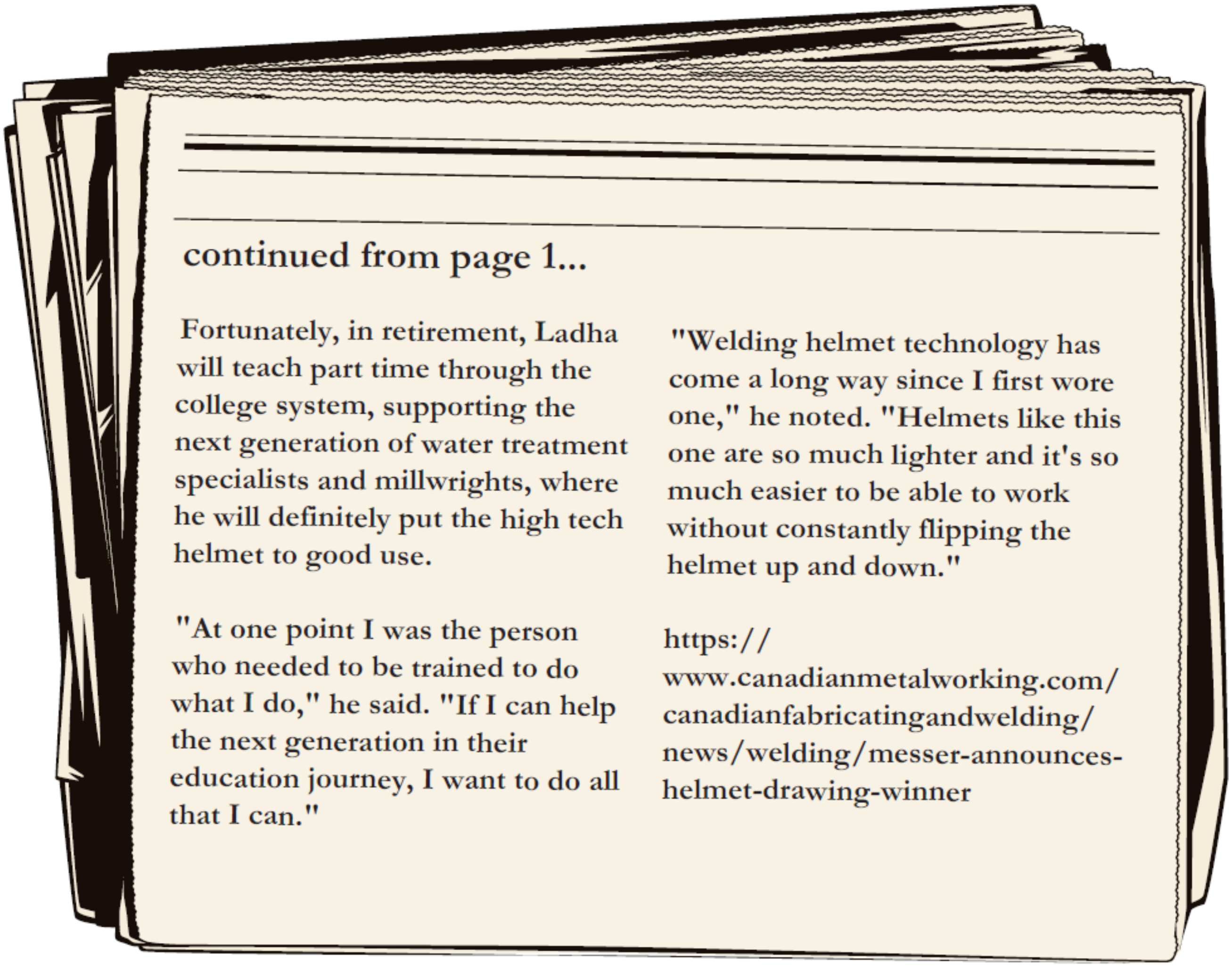
ISSUE #

10.04.2023

AND THE WINNER IS!

In April 2023, after 40+ years on the job, and just as he was about to retire, Asif Ladha, with Toronto Water (City of Toronto), won a unique hand-painted ClearVIEW OHE550D digital welding helmet.

"I started working for the city in Parks and Recreation as lifeguard" said Ladha. "After graduating from a university, I was hired in the water treatment area. Early in my career I worked in water treatment training, but in 2005 I became a Red Seal Millwright and thereafter expanded my training to do more mechanical training as well."



continued from page 1...

Fortunately, in retirement, Ladha will teach part time through the college system, supporting the next generation of water treatment specialists and millwrights, where he will definitely put the high tech helmet to good use.

"At one point I was the person who needed to be trained to do what I do," he said. "If I can help the next generation in their education journey, I want to do all that I can."

"Welding helmet technology has come a long way since I first wore one," he noted. "Helmets like this one are so much lighter and it's so much easier to be able to work without constantly flipping the helmet up and down."

https://www.canadianmetalworking.com/canadianfabricatingandwelding/news/welding/messer-announces-helmet-drawing-winner

DIGITAL SKILLS BITS AND BITES

DIGITAL SKILLS AT HOGWARTS

Passwords were used throughout Hogwarts Castle to restrict entry to certain areas such as House common rooms and teacher offices. Passwords in Hogwarts appeared to change on a frequent basis.

During Sir Cadogan's period of guarding the Gryffindor common room, he changed passwords so frequently that Neville Longbottom had to write them down. This list was snatched by Crookshanks and was given to Sirius Black, allowing him entrance.

Passwords were also used as a way to gain to access to the radio program Potterwatch, as a way to protect it from Death Eaters possibly listening. New passwords were introduced at the end of each broadcast, and could be used to listen to the next one. https://harrypotter.fandom.com/wiki/Password

THE AVERAGE PERSON HAS 100 DIFFERENT PASSWORDS!

According to Nordpass, the top 3 most used passwords are:

- Password (5 million users)
- 123456 (1.5 million)
- 123456789 (410K+)

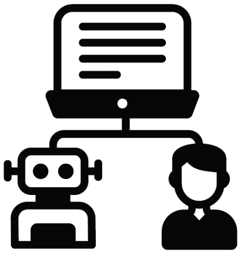
18% of employees share their passwords with others. Password sharing is a common mistake and can seriously compromise an organization's cyber security. But why do employees do this? Research has shown 42% of workers say they do it to more easily collaborate with team members, as well as 38% saying they share passwords because it is company policy. https://blog.entrustit.co.uk/6-facts-about-passwords-that-will-make-you-think

DIGITAL SKILLS BITS AND BITES

THE TURING TEST

gland
50
Final
ons m-config.
Pounds
This is only a foretaste of what is to come
and only the shadow of what is going to be
Alan Turing

The Turing Test was developed in the 1950s by Alan Turing, a British mathematician, computer scientist, logician, cryptanalyst, philosopher, and theoretical biologist after he had spent several years studying the concept of machine learning. Turing believed that a computer could be described as intelligent if it could imitate human responses under specific conditions. Or put another way, a computer was only intelligent if it could think.



Turing Test

The test involved 2 people: a questioner (A) and a player (B), and a computer (C) all in separate rooms. The questioner asks both players (one human and one computer) a series of written questions and tries to determine which player is the human and which is the computer. If the questioner fails to determine which player is which, the computer is declared the winner, and the machine is described as being able to think and has won the "imitation game".

Nominated or winning Oscars, Golden Globe Awards, Screen Actors Guild Awards and the People's Choice Award at the 39th Toronto International Film Festival, *The Imitation Game* is a highly successful 2014 thriller film based on the life of Alan Turing.

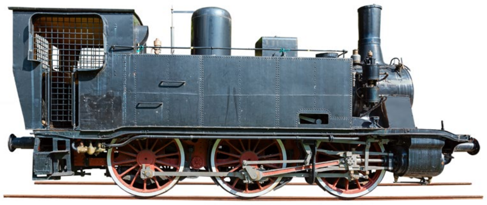
The film's title quotes the name of the game cryptanalyst Alan Turing proposed for answering the question "Can machines think?"

The subject of what happens when AI characters go rogue and turn against their creators has a long history in the movies including these terrifying and successful films.

- The Matrix
- 2001: A Space Odyssey
- The Terminator

DIGITAL SKILLS BITS AND BITES

REMEMBERING WHERE THE TRADES HAVE COME FROM



Hand or electrical tools that earlier generations of tradespersons used, are increasingly being replaced by digital versions in your generation. Respecting and appreciating how your trade developed is an important part of being a professional. The Canadian Museum of Making has collected machinery and tools that were built and used from 1750 to 1920 in Canada, Britain, the United States and Africa.

In addition to tools, the museum maintains a small collection of vehicles such as automobiles, trucks, motorcycles, steam tractors and horse drawn vehicles. All the tools and machines have been carefully preserved and restored to working order. The museum's goal is to create and maintain an accurate source of information about machines for all people who share their interest. The tools can be seen by visiting the museum in Calgary, Alberta and can also be viewed online in their Gallery of Collections pages https://museumofmaking.org/gallery/.

GEN Z AND PRIVACY

According to a blog post by Malwarebytes.com, Gen Z "*... care about privacy in a different way. ... Gen Z worries most about the exposure of their private information because of the chance of harassment, bullying, and lost friendships. In fact, when it comes to many privacy concerns that have a cybersecurity overlap, Gen Z cares less overall. According to our research, compared to 51 percent of non-Gen Z, 62 percent of Gen Z agreed or strongly agreed with the following statement:*

"I'm more worried about my private information being exposed online (e.g., embarrassing/compromising photos/videos, mental health, sexuality, etc.) than I am about typical cybersecurity threats (like viruses, malware etc.)."

https://www.malwarebytes.com/blog/personal/2023/11/what-gen-z-really-cares-about-when-it-comes-to-privacy?utm_source=iterable&utm_medium=email&utm_campaign=b2c_pro_oth_20231106_novemberweeklynewsletter_v1_169927472188&utm_content=person_with_their_long_hair

DIGITAL SKILLS BITS AND BITES

DO YOU HAVE CYBERCHONDRIA?

Cyberchondria is a form of illness known as an anxiety disorder. The term was coined in the early 2000s as a type of hypochondria connected to digital searches. Cyberchondria is defined as compulsively searching the internet for information about real or imagined symptoms of illness.

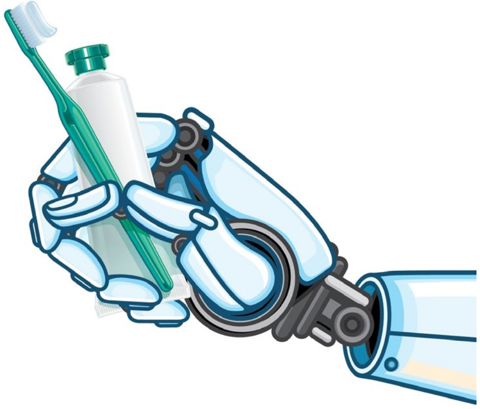
TECH HURTS

Do you get physical pain from overusing your tech? “Texting thumb”, “iPad hand” and “selfie elbow” are real physical injuries that many people, especially younger people, are increasingly reporting to their medical practitioners. All of these are variations on what are called repetitive stress injuries. As the name sounds, these injuries are caused by doing the same actions over and over again, sometimes 100s, or even 1000s, of times a day. Computers and smartphones can put us in unnatural positions for long periods of time. The important thing is to listen to your body and when you feel something hurts, stop doing it for a while.

DIGITAL SKILLS BITS AND BITES

OPEN YOUR MOUTH AND SAY, "AI?"

An AI toothbrush? The addition of AI is intended to make things better and now there is even a toothbrush that uses artificial intelligence to improve the way you brush your teeth. An AI toothbrush is programmed to take the data of thousands of lab-recorded brushing actions, combine it with your personal brushing style, and come up with recommendations to make your smile even whiter. You'll be alerted if you've missed spots when brushing, or if you're not brushing long enough. And, of course, there's a smartphone app so you can track your brushing progress.



PUT YOUR SKILLS FOR SUCCESS TO WORK!

GIVE YOUR SKILLS A WORKOUT. SKILLS, LIKE MUSCLES, GET STRONGER THE MORE WE USE THEM. BUILD YOUR SFS MUSCLES BY WORKING TO COMPLETE THE WORKOUTS. YOU CAN CHECK YOUR ANSWERS IN THE ANSWER KEY.

DIGITAL

Use the table of contents to navigate through this workbook. Track your progress by putting a checkmark beside each topic you complete.

1. SKILLED TRADES GO DIGITAL

The digital transformation in skilled trades means that workers in the trades require an expanded skill set. The two broad categories of digital tools in the trades are 1) tools used across many trades, and 2) tools specific to particular trades.

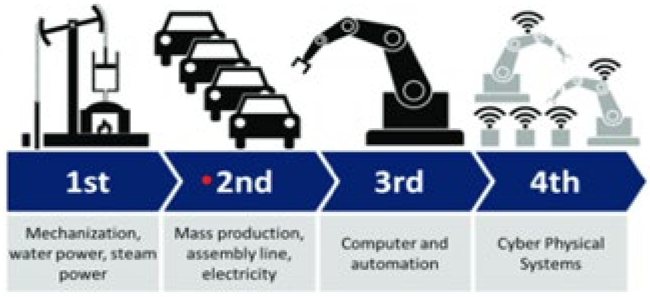
Digital tools across trades

Almost all trades use digital tools for scheduling, invoicing, and other software programs to speed up their paperwork. Smartphones and communication platforms such as Zoom and Slack allow for greater collaboration and problem solving among tradespeople, designers, and engineers. Schematic drawings used in many trades are now mostly read on tablets rather than from rolls of paper blueprints.

Digital tools specific to a trade

Examples of digital tools specific to trades include the diagnostic tools that automotive and heavy-equipment technicians use today and GPS-guided excavation that is routinely used in road construction and natural resource extraction projects.

This digital transformation is part of what's called the Fourth Industrial Revolution.


1st
Mechanization, water power, steam power
2nd
Mass production, assembly line, electricity
3rd
Computer and automation
4th
Cyber Physical Systems

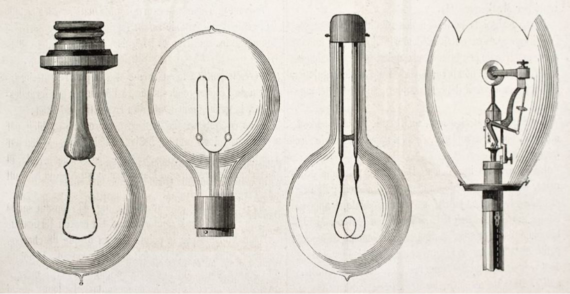
The four industrial revolutions. From the Wikimedia Commons. Christoph Roser at AllAboutLean.com licensed nder the Creative Commons Attribution-Share Alike 4.0 International license (Roser, 2015).

The Four Industrial Revolutions

The (First) Industrial Revolution

The first industrial revolution is commonly known as "the industrial revolution", or the "steam age". It is related to mechanization and the transformation from an agricultural to an industrial world. It began at the end of the eighteenth century. It was characterized by the introduction of water- and steam-powered machines in manufacturing. The steam engine, the textile industry, and mechanical engineering are its fundamental aspects. It lasted from the end of the 18th to the beginning of the 19th centuries. The year 1784, when the first power loom was built, is often cited as the start of this revolution.

The Second Industrial Revolution

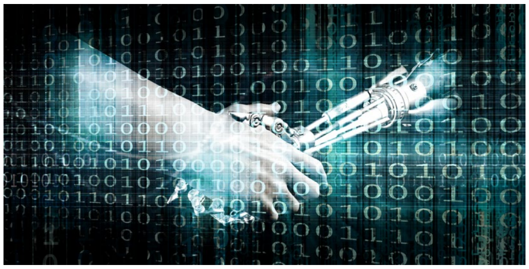


The second industrial revolution was also called the "electricity age" and introduced mass production of products. It was connected to the intensive use of electrical energy and occurred between the end of the 19th and the beginning of the 20th century (1870–1900). It was marked by the introduction of electricity and petroleum in mass production and by the development of railway and steel. The year 1870, when the first assembly line was used on a large scale in slaughterhouses, is sometimes cited as the start date.

The Third Industrial Revolution

The key feature of the third industrial revolution, or the "information age", was widespread digitization (computerization). It was the beginning of the first generation of information and communication technology (ICT) in industry. Also called "Industry 3.0", it started in the middle of the twentieth century, during the 1960s and overlapped with the new age of industrialization, the fourth industrial revolution. It is characterized by the use of electronics and information technologies in industry. The first programmable logic controller (PLC) brought the personal computer into commercial production in 1969.

The Fourth Industrial Revolution



The fourth industrial revolution, also called the "digital age", the digital revolution, or Industry 4.0, is characterized by the ability to connect real objects + people + virtual objects using a digital network. Its key element is the deep change in manufacturing systems through the integration of ICT, and the Internet of Things (IoT). Its starting point is the beginning of the 21st century. The fourth industrial revolution smoothly overlapped the third. Some researchers think that the term "evolution" is more appropriate than "revolution" for the ongoing changes because the main elements already existed and only some new developments were added. In either case, the major transformation is that production went digital.

Edited from https://www.researchgate.net/figure/The-four-industrial-revolutions-From-the-Wikimedia-Commons-Christoph-Roser-at_fig1_335581542

Check the Date!

18th century = 1701-1800

19th century = 1801-1900

20th century = 1901-2000

21st century = 2001-2100

Industry 5.0 is Coming!

Japan and the European Commission have identified a possible 5th revolution focussed not just on digital technology, but on how that technology can be used to improve society. For workers, Industry 5.0 means letting automation and robots do repetitive tasks while freeing them to do other things.

1. Using the information in the Four Industrial Revolutions article, complete the table to better understand what the major changes were in each of the revolutions. Enter a checkmark under the number of the revolution that matches each statement.
(*digital Intermediate level*)

INDUSTRIAL REVOLUTION DESCRIPTOR	1st	2nd	3rd	4th
Also called the electricity age				
Significantly changed the textile industry				
Also called the digital age				
Began in the middle of the 20th century				
Economy moved from agriculture to industry				
Assembly lines began				
Computer use began				

Machines powered by water and steam				
Evolved from the 3rd revolution				
Also called the information age				
Mass production began				
Occurred in 18th and 19th centuries				
Continues to impact trades in the 21st century				
Significantly changed the railroad industry				

Each of the four revolutions, or now evolutions, have brought significant changes both for skilled trades and for how you complete everyday activities. Research from Canada's Future Skills Centre, reports that tradespeople now need seven core digital skills:

- technical,
- information management,
- digital communication,
- virtual collaboration,
- creativity,
- critical thinking, and
- problem-solving in digital environments.

SKILLS AT WORK

Mike Bocsik is an auto repair technician with decades of experience running his own shop and another 12 years' experience as an automotive instructor teaching auto repair technician apprentices.

In his experience, today's students want to be fully engaged in what they're learning and are hungry for depth, detail, and information on up-to-date industry developments. https://www.cbc.ca/news/canada/skilled-trades-education-1.6773564 This includes information on changes in the digital tools they must use on the job.

For automotive repair technicians, digital competence means combining their vehicle knowledge with the ability to complete tasks like:

- Use a smartphone to take pictures of worn-out parts for customers to show why a part needs to be replaced or take a picture of a VIN number to accurately look up parts.
- Access and assess relevant information on online forums or YouTube to troubleshoot vehicle repairs.
- Interpret information from diagnostic tools and internet-based scanners.

Source: Future Skills Centre

Skills/Compétences Canda identifies digital as one of the top three Skills for Success needed by both automotive repair technicians and service mechanics, recognizing that vehicles today are becoming computers on wheels.

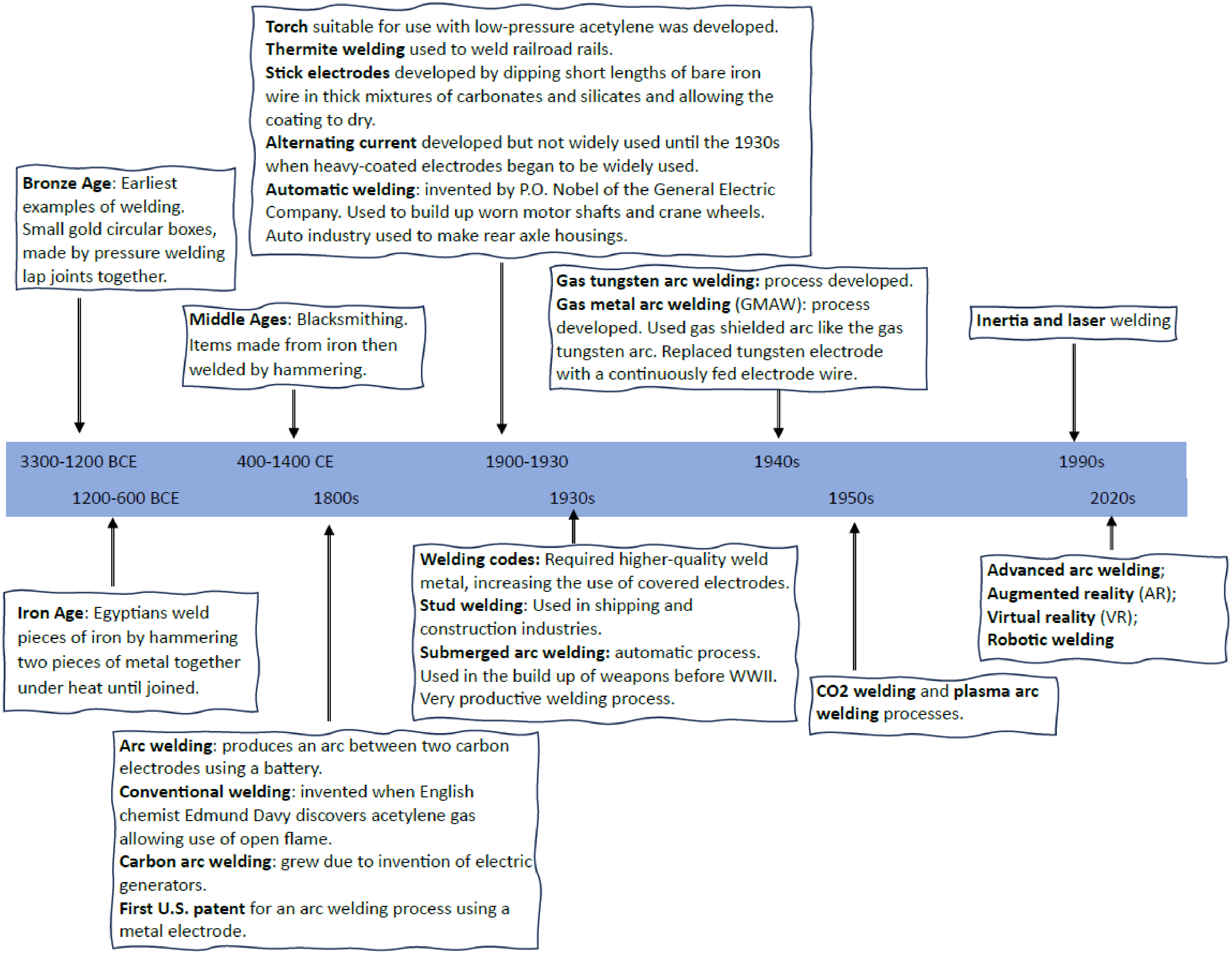
1. In the Task # column of the table, write the numbers of the work tasks that match the digital tools they are most often used for. One is done for you.
(digital Intermediate level)

Digital Tool	Task #	Work Task
Word processing		1. Take electrical energy readings.
Spreadsheet software		2. Complete repairs.
Communication software	8	3. Download data designed to regulate a vehicle's operating parameters.
Graphics software		4. Access data such as fault codes from onboard computers.
Databases		5. Write letters to insurance brokers to present the results of mechanical inspections.
Internet		6. Use graphics software incorporated into scan tools to access oscilloscope data displays such as signal values and ignition scope patterns.
Multimetre (can measure multiple electrical properties)		7. Take energy readings and troubleshoot faults.
Electronic equipment		~~8. Exchange e-mail with other technicians at other locations.~~
Scan tools such as oscilloscopes (displays electrical signals and shows how the signals change over time)		9. Retrieve repair information and technical drawings.

Laptops connected to digital logic control modules (programmable controllers that enable machines to perform processes without human intervention)		10. Participate in training courses and seminars offered by suppliers and employers.
Computerized equipment such as wheel alignment machines		11. Record and track billable hours.

Source: https://www.skillscompetencescanada.com/wp-content/uploads/2021/02/Automove-Service-PDF.pdf

WELDING DEVELOPMENT TIMELINE



3300-1200 BCE

Bronze Age: Earliest examples of welding. Small gold circular boxes, made by pressure welding lap joints together.

1200-600 BCE

Iron Age: Egyptians weld pieces of iron by hammering two pieces of metal together under heat until joined.

400-1400 CE

Middle Ages: Blacksmithing. Items made from iron then welded by hammering.

1800s

Arc welding: produces an arc between two carbon electrodes using a battery.
Conventional welding: invented when English chemist Edmund Davy discovers acetylene gas allowing use of open flame.
Carbon arc welding: grew due to invention of electric generators.
First U.S. patent for an arc welding process using a metal electrode.

1900-1930

Torch suitable for use with low-pressure acetylene was developed.
Thermite welding used to weld railroad rails.
Stick electrodes developed by dipping short lengths of bare iron wire in thick mixtures of carbonates and silicates and allowing the coating to dry.
Alternating current developed but not widely used until the 1930s when heavy-coated electrodes began to be widely used.
Automatic welding: invented by P.O. Nobel of the General Electric Company. Used to build up worn motor shafts and crane wheels. Auto industry used to make rear axle housings.

1930s

Welding codes: Required higher-quality weld metal, increasing the use of covered electrodes.
Stud welding: Used in shipping and construction industries.
Submerged arc welding: automatic process. Used in the build up of weapons before WWII. Very productive welding process.

1940s

Gas tungsten arc welding: process developed.
Gas metal arc welding (GMAW): process developed. Used gas shielded arc like the gas tungsten arc. Replaced tungsten electrode with a continuously fed electrode wire.

1950s

CO2 welding and **plasma arc welding** processes.

1990s

Inertia and laser welding

2020s

Advanced arc welding;
Augmented reality (AR);
Virtual reality (VR);
Robotic welding

DIGITAL DEVELOPMENTS IN WELDING

As the timeline on the previous page shows, the tools used in welding have significantly changed from the first basic hand tools and fire to the introduction of batteries, electrodes, automatic systems, and now digital developments using artificial intelligence (AI).

1. Complete the following statements using information from the timeline. (*digital Intermediate level*)

1. Carbon arc welding runs on ____________________ generators.
2. Stud welding was first used in the ____________________industry.
3. In ________________welding, the arc moves between two carbon electrodes.
4. There were three important developments in the ____________, the creation of welding ____________, stud welding and ____________________arc welding.
5. The first welding torch was developed between __________ and __________.
6. Railroad rails are welded using ____________________ welding.
7. Automatic welding was heavily used by the ____________________ industry.

Some of the most recent digital developments are advanced arc welding, augmented reality (AR) and virtual reality (VR), and robotic welding. Brief descriptions of each of these are below.

Advanced arc welding:

- Is corrosion resistant, making it perfect for chemical, nuclear, and toxic welding operations.

Augmented Reality (AR) and Virtual Reality (VR):

- AR makes training more visual, attractive, and educational. It also reduces the cost of materials used in training, moderates risk, and lets educators train more new welders at the same time. AR lets the user enter a real environment, touch and feel a real-life item and "augment" that item into a new shape, realistically changing its appearance. For example, using AR a welding student can take a plastic-based piece and interact with

it while it behaves as a carbon steel, stainless steel, or aluminum piece would when it's welded. It's very close to the actual welding experience, so trainees can see and feel a real-world welding environment using real welding equipment, such as a welding mask and welding torches.

- VR takes the user to a 100% computer-generated world where they can pretend to weld. The experience is like that of a video game.

Robotic welding:

- Connects people, machines, and smart technology. It refers to machines equipped with digital technology, including AI, being used alongside highly skilled human welders. Robotic welding is not about a humanoid robot using a blowtorch. It is about the need for Industry 4.0 technology advancement. The 4th industrial revolution will change the way manufacturing production is automated by using smart technologies.

Edited from: https://seaberyat.com/en/welding-technology-trends-2021-beyond/

2.

Underline the words or phrases in the Digital Developments in Welding article, that answer each question listed below.

(digital Intermediate level)

1. What are the advantages of AR?
2. Why is advanced arc welding so useful?
3. What can welder trainees do when using VR?
4. Why is AR such a valuable training tool?
5. How does AR impact costs and potential risks?
6. What does robotic welding refer to?
7. What is the anticipated impact on manufacturing of the 4th industrial revolution?

TOOL MUSEUMS

Remember the Canadian Museum of Making? It is just one example of museums around the world dedicated to showing the history and development of tools used in skilled trades.

Looking back 100, 50, or even 10 years, the tools that tradespeople use to do their jobs have significantly changed. Work that was once done by hand is now done working with tools that use digital information to monitor status and complete tasks. Consider the progression in carpentry from handsaws to table saws, to saws that can be programmed to complete accurate cuts 100s of times.
While the Museum of Making is working to preserve the tools of the past, work across almost all trades continues to move forward at lightening speed driven by digital transformation. The previous timeline shows the evolution of tools used in welding from the prehistoric times to the digital age and the article Digital Developments in Welding describes recent changes in more detail.

3. Using the information in the timeline and the Digital Developments in Welding article, imagine you have to describe the history of welding to someone. What are the 5 most important developments you would pick from the timeline? Write each development below and include why you think it is so important. Show what you believe is the most important as number 1. *(digital Intermediate level)* Answers will vary.

1.
Reason:
2.
Reason:
3.
Reason:
4.

Reason:
5.
Reason:

4. Now think about a trade you are interested in and how the tools used may have changed through time. Use your digital skills to search for information about the evolution of the trade from first records to the digital age. Visit at least 2 different websites to complete your research. Pick at least 5 interesting facts to complete the following.

(digital Intermediate level) Answers will vary

Trade Name: ____________________

Websites Visited:

1. ____________________
2. ____________________

Date of first recorded use of the trade: ____________________

Date of start of use of digital tools: ____________________

Interesting Facts:

1. ____________________
2. ____________________

3. ______________________________

4. ______________________________

5. ______________________________

KEEPING UP WITH CHANGE

The pace of change in the digital age is faster than at any other time in our industrial history. In addition to digital skills, Mike Bocsik, the automotive instructor we read about before, believes that no matter how long tradespeople have been working, they need regular, ongoing training to keep up with technological advancements — which arrive nearly every quarter for the automotive industry.

"If you let things stagnate, you're going to [fall] behind," he said. "It's super critical to continue with the upgrading and just move forward."
https://www.cbc.ca/news/canada/skilled-trades-education-1.6773564

New research from Athabasca University supports Mike Bocsik's position, finding that more than three-quarters of Canadian employees (77%) want to re-skill just to keep up with their job's changing needs, with digital skills being a top priority among 70% of respondents.
https://news.athabascau.ca/research/workplace-dynamics-study/

Review these tips for keeping up with the pace of digital change.

1. Ask questions. Digital tools are the same as all work tools; you need to know how they work to be able to use them efficiently and safely. If you don't know; ask.
2. Make sure any software you use is always the most up to date version. Download updates as soon as they are available or at least every 6 months.
3. Keep your digital tools safe, clean and secure. Spilled coffee is your phone's worst enemy.
4. Be certain the way you are using the tools is consistent with your employer's expectations and policies.
5. Read, either online or in print, articles in trade journals and blogs to keep up with what's coming.

1. For each digital tool in the table below, record whether and how long ago you completed the tasks identified. If you don't have the tools, interview someone who does. Record your answers using the ratings below then total your scores for each device.

Completed in last 6 months	3 points
Completed in last year	2 points
Completed more than a year ago	1 point
Never completed	0 points

(*digital Intermediate level*) Answers will vary

DIGITAL TOOL	TASKS					
	Updated software	Cleaned	Deleted unused files or apps	Learned to use new app or program	Updated or installed anti-virus software	Totals
Cellphone						
Laptop/Tablet						
Desktop						
Other digital tool(s)						
					Grand total	

Now rate your total score.

50-60 = Well done!

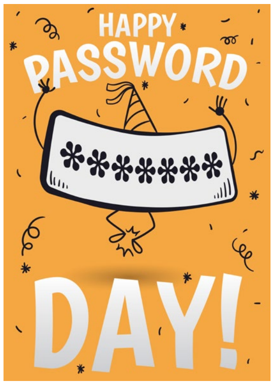
35-50 = Pretty good.

21 – 35 = You *really* need to work on it.

0 – 20 = High risk!

How did you do? Do you need to do some updating of your digital tools?

2. PASSWORDS AND CYBER SECURITY



Happy World Password Day!

Established in 2013 by Intel, World Password Day is observed on the first Thursday in May with the goals of raising awareness about the importance of good password hygiene and encouraging workers and individuals to recognize the role that strong passwords play in securing their digital lives.

How would you celebrate Password Day?

Passwords and password protection are a big deal! These days you need a password for almost everything that you do online. Whether it's for streaming services, social media accounts, or banking, many of us have dozens of passwords we use every day, and hackers are always looking for ways to guess what they are. Understanding and practicing excellent password hygiene is an important part of password protection.

Wait! Password hygiene? You've heard or oral hygiene to keep your teeth and gums strong, and handwashing hygiene to limit the spread of viruses, but what's password hygiene?

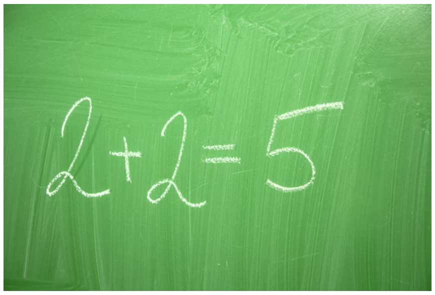
Simply put, password hygiene refers to the ways you create passwords and manage them to keep everything you do online safe.

Poor password hygiene is when you use one password for everything and tell your best friend what that password is.

Excellent password hygiene is when you create unique and complex passwords for different things you do online and keep those passwords safe and secure.

And like most things you do online, YOU are responsible for practicing excellent password hygiene at home, for class, and for your employer.

Hmm. Something doesn't add up. According to a LogMein survey, 91% of people know the risks of password recycling, but only 58% still always use the same password or a similar variation of that password for most of their online accounts.



1. Before you learn more about what you can do to practice good password hygiene, let's see what you're already doing right.
Complete the self-check by putting a checkmark √ beside each item you are already doing.
(*digital Intermediate level*)

#	ITEM	√
1	I change all my passwords every 2-3 months.	
2	I use different passwords for all my apps and accounts.	
3	I never include personal information in a password, like the name of my street.	
4	I never use consecutive numbers or letters in my passwords.	
5	I never reuse passwords.	
6	I never share my passwords.	
7	I never use my pet's name as a password.	
8	I never use the word "password" as a password.	
9	My passwords are always at least 12 characters long.	
10	My passwords always contain letters, numbers and symbols (&, *, @).	

Scoring

If you scored 8-10 checkmarks, you are a password pro!

If you scored below 8, you still have some work to do, and this workout will help.

What makes a great password?

According to Get Cyber Safe Canada, most people use passwords that are "okay". And that's because most apps and accounts require you to use passwords containing capital letters, numbers, and at least one special character. That's a good start but they can be better if you follow these tips.

1. A strong password should be at least 12 characters long, and the longer the better.
2. Using a complex combination of characters, numbers and symbols can help you protect your accounts.
3. Using any variation of "password" for your password is a bad idea. It's perhaps the most obvious password to crack, no matter how many random characters, numbers, or variations you use to spell it (for example, 123passw0rd765).
4. Use random strings of numbers in your password but don't use numbers (or letters) in sequence.
5. Don't use personal number sequences like phone numbers.
6. Don't use names of family pets or other personal information.
7. Don't use personal information like your full name or your address.
8. Do try a passphrase but mix up the word order.
9. Passphrases should be a bit longer than traditional passwords. Your passphrase should contain at least 4 different words and be at least 15 characters long.

1. Use the information in the tips to identify what's wrong with each of these passwords. Then update each password to make it stronger. (*digital Intermediate level*)

Password	What makes it weak?	Rewrite it so it's stronger.
Abcde3456789		
catschasemice		
MmFd386QR990		
X31mypasswordgh3$		

Beyond the Password

Many individuals and organizations are moving past using just passwords and passphrases by adding another layer of protection to logins. The most common form of added protection is multi-factor authentication (MFA). MFA adds extra steps to the login process that make your accounts and devices more secure.

MFA requires you to use a combination of two or more of the following factors to access your accounts:

- Something you know (e.g., a PIN (personal identification number), password or passphrase, answers to security questions; and/or
- Something you have (e.g., a smartcard, physical token, authenticator app, email or SMS (short message service): a form of text message that's sent from one device to another; and/or
- Something you are (e.g., a fingerprint, your face, or iris scan).

Adding MFA to your account is like adding a house or car alarm that requires you to enter a PIN to turn it off. It's an extra layer of protection from cybercriminals trying to break in. Even if they get through one layer (for example, by guessing your (weak?) password, they still need to get past a second, and possibly a third, barrier to access your account or the account of your employer or another business. It is a very good idea to set up MFA for your accounts whenever you can. Many organizations and businesses commonly do.

How does MFA work?

After you enter your normal login details (username and password), one or more of these things will happen.

1. You will receive an SMS either by text message, email, or voice mail, with a random, one-time password (OTP) that you must enter to confirm your identity so you can access or use an online service. (IMPORTANT: If you choose to receive an OTP by email, make sure that your email account itself is secure. This means that you should enable MFA for the email account you are using), *OR*

2. You will receive an OTP through an authenticator app. An authenticator app is a mobile application that generates a different random OTP every time you login. It is more secure than receiving a code by SMS. To use an authenticator app, you first need to download it to your device, *OR*

3. You must use one of your unique characteristics to authenticate your identity. This could mean providing one of the five most common types of biometric identifiers: fingerprints, facial recognition, voice, iris scan, or palm or finger vein patterns to access the device or mobile apps you need to access. Using biometrics as MFA is convenient because you can't misplace a part of yourself!

1. Write out the meaning of each abbreviation listed below.
(*digital Basic level*)

ABBREVIATION	MEANING
PIN	
SMS	
MFA	
OTP	

2. Multi-factor authentication requires you to connect who you are with something you know, and something you have to provide an extra layer of digital security.
Identify each factor listed below as either:

1. Who you are.
2. What you know.
3. What you have.

(*digital Intermediate level*)

FACTOR	#
PIN	
Fingerprint scanner	
Hardware token	
Smart card	
Security questions	
Voice recognition	
SMS	
Iris scanner	
Application-based authenticators	
Facial recognition	
Passwords and passphrases	

3. When have you had to use MFA? For banking? For shopping? For work? Other? Name up to three of the situations and describe the steps you have had to take in each case. Haven't used MFA yet? Interview someone who has.
(*digital Intermediate level*)

Situation: ______________________________

Steps:

Situation: ______________________________

Steps:

Situation: ______________________________

Steps:

Is password protection really that big a deal?

SOMETHING AS SIMPLE AS MFA VERIFICATION CAN PROTECT YOU FROM:

- **100% OF AUTOMATED BOTS**
- **96% OF PHISHING ATTACKS**
- **76% OF TARGETED ATTACKS**

Yes. Yes, it is. It's a big deal for both you and any employer you may work for.

Cybercriminals don't just target large corporations and organizations to gain access to their data systems, obtain sensitive information and demand ransoms. Small businesses have become equal if not bigger targets for cybercrime hackers. In fact, 71% of small to medium enterprises (SME) have reported experiencing at least one cyber-attack according to the Canadian Internet Registration Authority (CIRA). And that small or medium-sized business, could be one that you work for. Sometimes it happens because an SME may be sub-contracting work from a larger company. Here's a real-life example.

> In 2020, a Canadian construction company that's won millions of dollars' worth of contracts with the military and other federal departments was hit by a ransomware attack. Ransomware attacks involve hacking into a company's system – often via a weak

password or through a phishing scam – to install malicious software to damage the company's computer system and then demanding a cash payment to undo the damage. In this attack the hackers stole 60 GBs of data.

Because the company had won almost 50 federal contracts between 2006 and 2015 worth a total of over $ 400 million, the RCMP were heavily involved in the investigation. Commenting on the investigation, the president of the Canadian Association of Defence and Security Industries, said "When we look at the major hacks that have occurred, especially on the defence side, where you know fighter aircraft information was stolen — it wasn't stolen from the prime contractor, it was stolen in a tiny, tiny shop supplying widgets". https://www.cbc.ca/news/politics/ransomware-bird-construction-military-1.5434308

The reality is, even if you are a worker in a small widget manufacturing company, your mistake could lead to a much bigger attack. Research shows that small businesses are more vulnerable to cyberattacks because they usually don't have the security resources and cybercrime training for employees that larger businesses have so they are less able to protect themselves against cybercrimes.

Employers you may work for will have policies and procedures in place to keep their company's data secure and you will be expected to follow them closely. If you don't, you could get fired.

One of the best ways that employers can keep their online information safe is to require employees to take regular cyber security training. Below is an outline of common elements of employee cyber security training programs.

What is commonly included?

- Password management
- Email security
- Securing your equipment
- Cyber safety practices and expectations specific to the company

When do you take the training?

- When you are hired
- Every few months after that

How is the training offered?

- Online or in person or a combination of the two
- As part of your regular work hours

1. In the scenario that follows, Martin has been working in manufacturing for a long time but is a new employee at DIGICAN, a manufacturing company that practices a high level of digital security. This is new for Martin and he's already having a hard time with some of the practices. Martin blames the technology and says it's the employer's problem and not his responsibility. Read what happened his first day and highlight anything you think he could have done differently.
(*digital Intermediate level*)

On day 1 Martin was excited to get to know his way around the shop so he was late for his security briefing. By the time he got there the trainer had another meeting and so he gave Martin some written instructions and rescheduled the training for 3 days later. Martin followed the instructions to login to the company system. He created a password (Martin123456) and immediately wrote it down so he wouldn't forget. He wrote it on a post it and stuck it to his workstation. The instructions then said to create an online HR profile. Martin used the same password again, so he'd never forget. While creating his profile, Martin saw there was a new email with the subject line CONGRATULATIONS. He didn't recognize who it was from but that was expected, as he was new and didn't know anyone. He assumed it was a welcome message and clicked on a link in the message which made his screen turn red and locked the computer down. Martin closed the computer, didn't tell anyone, and went to see if he could get fitted for his PPE.

Message Security

One of the most important cyber security topics for employees is message security. Message attacks don't need to figure out how to crack your password. When you respond to an email or text message attack, you open the door for the hacker.

A significant number of cyberattacks are launched via message techniques known as phishing, or related techniques known as smishing, spear phishing and whaling. Cyber criminals use these types of messages to try to steal sensitive information from people by pretending to be legitimate senders like the person's bank or a colleague. One of the most common ways to send an attack is via email.

DON'T TAKE THE BAIT!

Phishing: any message that has been deliberately faked to make it look like it's from an authentic sender.

Smishing: any phishing message sent through SMS (also known as a text message).

Spear phishing: tailored messages sent to one person or a small group of people, making it a much more targeted approach.

Whaling attacks: spear phishing aimed at senior executives or high-profile victims.

Like all aspects of cyber security, recognizing and preventing phishing-type attacks is a shared responsibility. Employers are responsible for training employees in how to spot and fight phishing. Employees are responsible for putting that training into action.

There are clues that an email might be a phishing attack.

1. Phishing attacks often use urgent or threatening language. Look out for messages pressuring you to respond quickly, especially if the request is odd.
2. Suspicious attachments and links. Look out for links with unfamiliar URLs and attachments with odd file names or file types (like an .exe) that you didn't ask for, especially from a suspicious sender. Do not click on them.
3. Strange sender email addresses. A message might be from a bank but when you hover over the email from "Accounts Department", the sender's address is actually "max@cx3bancor.com"
4. Requests for sensitive or personal information. Look out for links directing you to login pages and requests regarding your personal information (like someone asking for your account password).
5. Typos and poor design. Look out for incorrect email addresses, suspicious links and any unusual spelling or grammar errors, as well as inaccurate or blurry logos, or corporate emails with formatting issues.

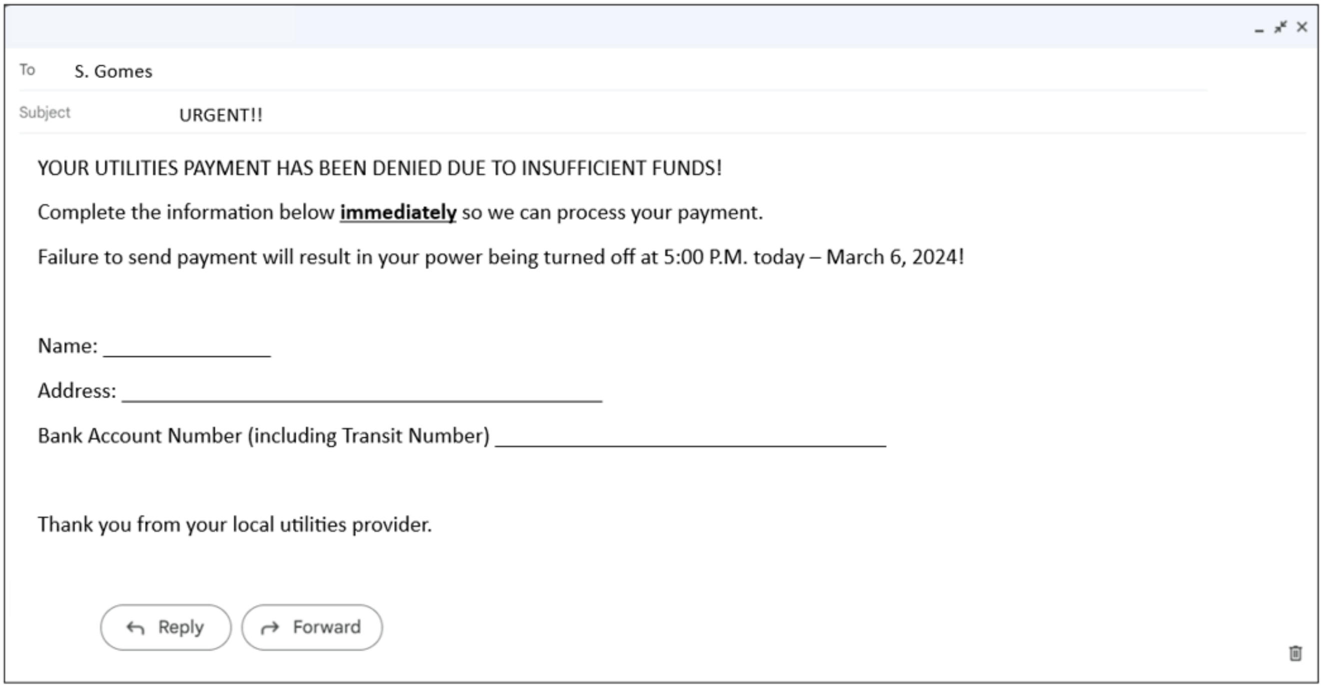
If you do click on something in a message that turns out to be a phishing attack, remember:

- Don't panic!
- Don't pretend it didn't happen!
- Don't turn off your computer!
- Don't forward the message to anyone else in your organization (this includes IT!).

There are some important things you can do:

- Contact your IT department or supervisor immediately and let them know what happened.
- Your IT department will probably ask you to:
  - Change your password.
  - Enable MFA if possible.
  - Take more security training so it doesn't happen again.

1. In each of the email messages on the next page, highlight 3 clues that indicate it might be a phishing attack.
(*digital Intermediate level*)



To S. Gomes

Subject URGENT!!

YOUR UTILITIES PAYMENT HAS BEEN DENIED DUE TO INSUFFICIENT FUNDS!

Complete the information below **immediately** so we can process your payment.

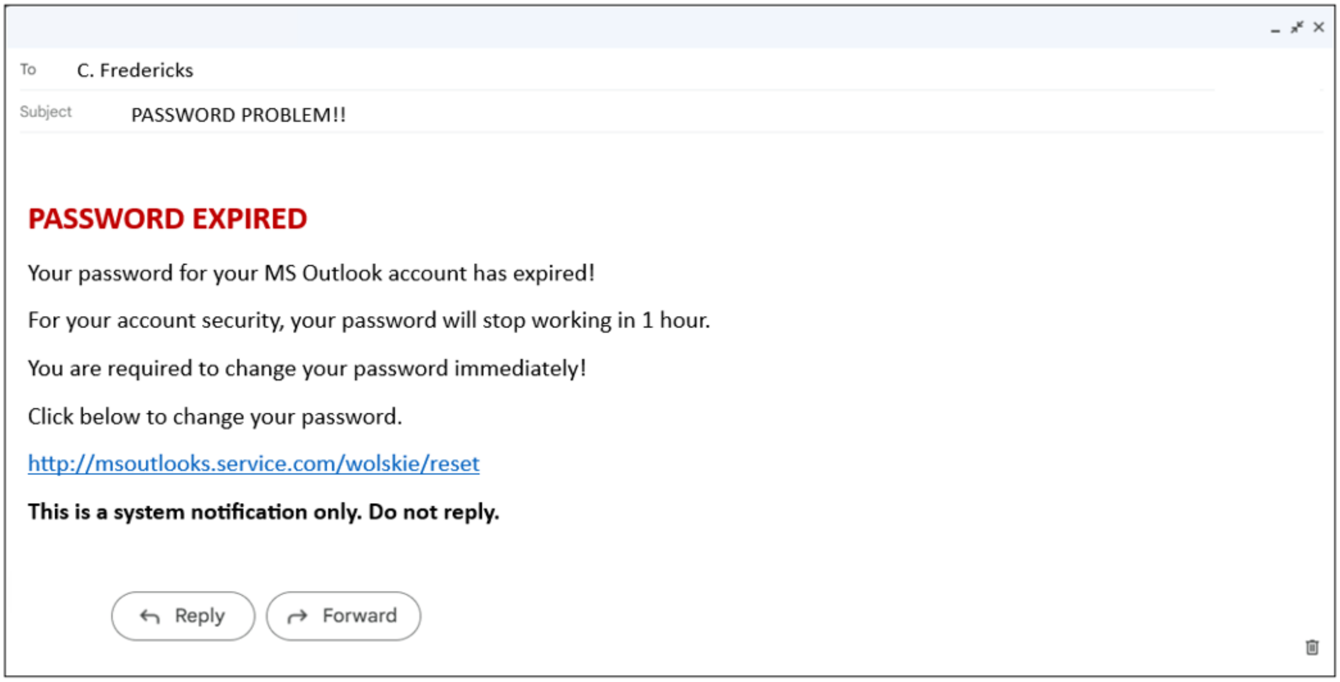
Failure to send payment will result in your power being turned off at 5:00 P.M. today – March 6, 2024!

Name: _______________

Address: ____

Bank Account Number (including Transit Number) ____________________________________

Thank you from your local utilities provider.



To C. Fredericks

Subject PASSWORD PROBLEM!!

PASSWORD EXPIRED

Your password for your MS Outlook account has expired!

For your account security, your password will stop working in 1 hour.

You are required to change your password immediately!

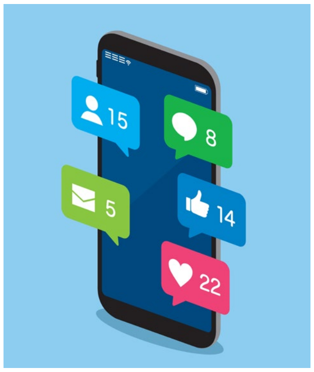
Click below to change your password.

http://msoutlooks.service.com/wolskie/reset

This is a system notification only. Do not reply.

3. SOCIAL MEDIA SMARTS

Social media includes any online platform that you use to create and share data to build or expand your social networks. Think social media is just for fun? WRONG! Social media is also an important tool for you to get and keep a job. What you post on social media can make a potential employer or volunteer organization think you are a perfect fit for their company, apprenticeship, or opportunity, or that they definitely don't want to work with you. It's all up to you.



You are responsible for the content of your online information.

You are responsible for keeping your online information private and secure.

Think those responsibilities aren't important? Think you know everything about social media because you've been using it forever? So did a college football player on what should have been the best night of his career. Read the story below.

The Heisman Trophy is awarded every year to the top college football player in the US. In 2018, the same night it was awarded, the media reported on several negative tweets that the winner had written years before when he was still in high school. Posting on Twitter (X), the player used homophobic slurs to refer to his friends. He apologized several times and said it was meant as a joke but media all around the world carried the story and his reputation was damaged. While the original tweets were finally deleted, you can still search for and read the story online.

And, before you think that social media mistakes only happen to young people, read this one.

A contractor for Chrysler Automobiles posted an obscene tweet on the Chrysler brand's official account. His Twitter (X) post read: "I find it ironic that Detroit is known as the #motorcity and yet no one here knows how to (expletive) drive." It was meant to appear on his personal account, but he mistakenly sent it to the Chrysler brand's feed while he was stuck in traffic on the highway. He lost his job, and his tweet was part of the reason Chrysler didn't renew its contract with his (former) employer. "As a Detroiter, it was cool to know the work I was doing was part of this larger comeback for Detroit and the Big Three," he told the Detroit Free Press. "I poured all my heart and soul into that. It's unfortunate it's all being overshadowed by 140 characters."

1. Use the information from both situations to complete the table.
(*digital Intermediate level*)

	Football player	Chrysler contractor
What social media platform did they use?		
What type of media did they post? (video, comment, etc.)		
What did people who saw the post think was wrong?		
What happened to the person who did the posting?		
What could each person tweeting have done to avoid the problem.		
Do you think the reaction to the football player's tweet was fair? Why or why not?		
Do you think the reaction to the contractor's tweet was fair? Why or why not?		

Whether you think the reactions and punishments were fair or not is interesting, but the fact is they happened. The good news is there are things you can do to prevent making these sorts of mistakes and project a positive online identity.

Let's start with how you use social media.

2. Review the list of popular online platforms below and put a ✓ beside each one you use. Add any others that are not in the list in the blank rows. Then fill in the remaining columns for the ones you selected.
(*digital Intermediate level*)

Platform	✓ if you use	# times a week you post something	# times a week you comment on or share someone else's information
Facebook			
Instagram			
Twitter / X			
YouTube			
LinkedIn			
Snapchat			
TikTok			
Total posts/comments/shares per week			
Total posts/comments/shares per year			
Total number of pieces of information shared between grade 8 and graduation			

Even if you post just once a day, that's 365 posts a year, or 1,825 pieces of information between grade 8 and high school graduation. That's a lot of information about you, what you think and what you like and don't like that is out there on the internet.

Things that are posted to the internet can be there forever. Even if you delete something, if someone else has already shared it, it's still out there. Controlling who can see your posts before you decide to post them is very important. That's where privacy settings come in.

Social media platforms (apps and web pages) come with free privacy settings that give users some control over who can view the information they post.

The most basic privacy settings are public and private.

1. Public means that anyone with access to the platform can view your posts.
2. Private means that a limited group of people, for example people you've identified as "friends", can view your information.

It's a good idea to review your privacy settings often. Figure out how to adjust the settings on different apps and for different audiences according to what you post.

Controlling your privacy settings means that even if you post something that you might regret, you can at least limit who will see it. It also means that you can limit the information that strangers have access to and so reduce the chances of being hacked and having personal information stolen.

But it's important to remember that while privacy settings help keep your online identity safe in most cases, they are not foolproof. A determined hacker may still access information you shared online that you want kept private among friends.

The Office of the Privacy Commissioner of Canada (OPC) has published advice for Canadians on how to set and adjust privacy settings. Helpful tips include:

- Before you automatically click "accept", read privacy policies to learn what personal information is collected and the privacy controls available. If you're not comfortable, don't sign up for it.
- Explore what an app's default settings are and adjust as needed.
- Look for options to turn off location-based settings or limit tracking to only when you're using the service.
- Don't login to one app automatically from another. Set up a new identity.
- Don't share personal information like your phone number.
- Do look for options that allow you to delete your history on a regular basis.
- Don't think of your settings as something you do once and forget about. Many sites regularly modify their settings' options, so review them frequently. There's also value in going back to evaluate your settings to make sure you're still comfortable with your previous decisions.

1. Understanding how privacy works online, and regularly checking your settings, are two of the most important things you can do to keep your identity safe.

Mark each statement below as true or false. If the statement is false, rewrite it so that it is true. (The first one is done for you.)
(digital Intermediate level)

Privacy settings provide total protection. TRUE **FALSE** *Privacy settings do not provide total protection*
Sharing personal information online, like your address, is safe. TRUE FALSE
Privacy settings can be changed. TRUE FALSE
Privacy settings are a good way to keep information private. TRUE FALSE
Public means everyone on the social media site can see what you post. TRUE FALSE
Logging in to one app from another is fast and safe. TRUE FALSE
Once you read a privacy policy you don't need to read any updates. TRUE FALSE
Privacy settings cost extra. TRUE FALSE

« ZUT! ILS VOLENT D'ABORD MA VÉRITABLE IDENTITÉ, PUIS MON IDENTITÉ SECRÈTE ! »

" DANG, FIRST THEY STEAL MY IDENTITY, THEN THEY STEAL MY SECRET IDENTITY! "

https://www.priv.gc.ca/en/about-the-opc/publications/illustrations/

Now that you know why privacy settings are important to help protect your online identity, let's check and see how well you are using them and where you might need to improve.

1. Complete the self check by putting a ✓ in the box that best describes how often you complete each task. Then total the ✓ in each column.
(*digital Intermediate level*) *Answers will vary.*

Privacy Self Check

How often do you do each of the following?	On a schedule	When I think I of it	Never
Review your current privacy settings			
Check who can see your posts			
Review your profiles			

Update your friends list			
Restrict logging in from third-party apps			
Add a calendar reminder to review your settings again			
Read the privacy policy, including updates, of all apps you use			
TOTALS			

To be privacy smart, all your checks should be in the first column. How did you do? What can you improve?

To stop employers or others from viewing content you don't want them to see, you might decide to make everything private, or even to have no online identity at all.

Unfortunately, according to research this is a bad idea as not having any digital presence has the potential to make organizations suspicious and limit opportunities for the positions you are interested in, so, post but post smart.

One of the quickest things you can do to check your online identity is to regularly "google yourself". Searching your own name shows what others see when they do the same thing. Experts say it's a good idea to google yourself at least three times a year. When you search your name, you should expect to see images and posts that you remember posting but you may be surprised to see what else comes up that you didn't post.

1. Follow these steps to google yourself and answer the questions.
(*digital Intermediate level*) *Answers will vary.*
Enter just your name in the Google search bar. How many results did you find?

Now enter your name in quotation marks and the city or town you live in. How many results now?

2. To complete the next questions, search at least the first 3 pages of results.
(*digital Intermediate level*) *Answers will vary.*

What is one result you found that you remember posting?

What is one result you found that you didn't know what there?

Looking at all the results, list 5 words that you think describe "you" according to this search.

Looking at all the results, is there anything you wish was not there?

Did you know that Google results are customized to each user? They are, so now that you have completed the activity, it's a good idea to have someone else Google you to see what they find that may not have been included in your search results.

What does your social media say about you?

While some provinces and territories have legislation that prohibits employers from using digital background checks in hiring, many still do, and digital checks may be freely used to decide on promoting or firing employees after they've been hired.

Digital background checks are also done for some apprenticeship and post-secondary admissions decisions and by some volunteer organizations. Many post-secondary institutions use social media to identify students who appear to know how to responsibly balance fun with their schoolwork. Volunteer organizers are looking for people who are as passionate as they are and know how to share their passions and lives in a respectful manner online.

According to a 2023 article in the BC newspaper, the Times Colonist:

"Post-secondary institutions in Canada all have their own criteria for admissions. The University of British Columbia, for example, doesn't assess social-media behaviour, and says if an incoming student were to post inappropriate content on a school-administered social-media site, the school would respond on a "case-by-case basis," and that the school reserves the right to deny admission.

The university's advice is that prospective students should conduct themselves online with the assumption that any post, even a private one, could be used against them.

Applicants to the university should also keep in mind that offers of admission can always be taken away. "Anything you share has the opportunity to affect your reputation and important decisions in one's life," according to a UBC spokesman. "It remains a real wild card in the admissions process."

1. So, exactly what does this policy mean? To ensure you understand what they're saying match the synonyms to the words from the article.
(*digital Intermediate level*)

FROM THE ARTICLE	SYNONYM
Wild card	
Post-secondary institutions	
Case-by-case	
Assess	
Criteria	

<u>SYNONYMS</u>
Individually
Standards
Something unpredictable
Evaluate
Colleges and Universities

2. **Complete each sentence with "does" or "doesn't" to make it true.**
(*digital Intermediate level*)

The university ________________ check applicant's social media.

The university ________________ check enrolled students' social media.

The university ________________ believe students are responsible for what they post.

The university ________________ treat every case the same.

3. **Now consider some of your own social media. Imagine you are applying for an apprenticeship, a new job, or a promotion. What impression would you want the person interviewing you to get from your online identity? Write your ideas in the space below.**
(*digital Intermediate level*)

____

____

____

4. Pick one of the social media accounts you use most often. Use the ideas you wrote down as your criteria to review at least four posts you have made recently. Decide whether you should leave the post up or delete it. The post can be a comment, photo, or link: anything that clearly came from you. Remember to check not only your original post, but what has happened to it since. What comments or links are now associated with the post? Are you comfortable with them? Do they meet the criteria you identified? Record your results in the table below.
(*digital Intermediate level*)

Post 1

____

Decision:

____

Reason:

____

Post 2

Decision:

Reason:

Post 3

Decision:

Reason:

Post 4

Decision:

Reason:

The good news is that you can also use social media not only to present yourself the way you want to be seen, but also to identify employers and opportunities where you would like to be considered.

Even small companies use social media to let potential customers know more about them and the services they provide. Some companies use their social media channels to share what it's like to work for the company. This helps them to attract people who are the best fit and can help you determine if the company is the right fit for you.

Doing social media research is particularly important when you are actively looking for a job or trying to find out more about the industry you would like to work in.

1. Pick a company that you think you'd like to work for that has at least one active social media account linked to their website. Popular company accounts are Instagram and Facebook. Identify the company and then answer questions about 3 of their posts.

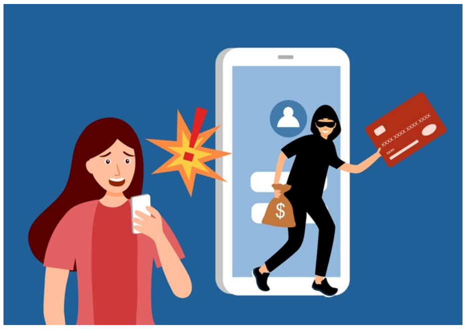
(*digital Intermediate level*)

Company name	
Website	
Type of social media account	
Post 1 What is it about?	
What does it make you think about the company?	
Does it make you feel you could work there?	
Post 2 What is it about?	
What does it make you think about the company?	
Does it make you feel you could work there?	
Post 3 What is it about?	
What does it make you think about the company?	
Does it make you feel you could work there?	

4. DIGITAL MONEY SENSE

THE COST OF CONVENIENCE

There's no doubt that the ability to move money online makes life easier. Paycheques are automatically deposited in personal bank accounts. Bills are automatically deducted when scheduled so there's never a missed payment or an interest charge. And being able to press "pay now" from your favourite comfy chair means that ordering almost everything you want is just a click away.



Of course, all that speed and convenience come at a cost. Sometimes that cost is real money and other times it may be a loss of equally valuable personal data.

But hey, you're a "digital native." You've been clicking and texting almost since before you could walk. No one's going to scam you online; right?

Unfortunately, that's not true. In fact, research confirms that younger people are the ones most likely to be the victims of online fraud.

- In Canada, older Canadians (55+) are among the least likely to report having knowingly been victimized by fraud or scams at some point in their lifetime (31% vs. 50% aged 18-54). By comparison, almost two-thirds (63%) of younger Canadians (aged 18-34) admit that they've knowingly been the victim of fraud or scams at some point. (IPSOS 2023)
- In the US in 2022, people under the age of 20 lost $ 101.4 million to online scams, according to a recent study from cybersecurity startup Social Catfish, which cited figures from the Federal Bureau of Investigation's Internet Crime Report. (CNBC 2023)
- In the UK, people between the ages of 16-34 are significantly more susceptible to being scammed and account for over half of the scams experienced in the UK. (local.gov.uk 2023)

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ipsos.com/sites/default/files/ct/news/documents/2023-02/CPA%20Fraud%20Survey%20Factum%202023_1.pdf

The good news is that, like everything you do online, there are steps you can take to protect your money movement and to recognize scammers trying to take advantage of you. So, let's get started!

FRAUDS AND SCAMS

The most common ways that people are cheated online are through frauds and scams. Many people use the words frauds and scams interchangeably, but while their meanings are similar, they are not exactly the same.

Fraud involves someone (a hacker) stealing your information (usually financial) such as credit card or bank account numbers, without your knowledge that it is happening.

Scams trick you into knowingly providing personal information through tactics such as phishing emails, fake social media accounts, and too-good-to-be-true offers.

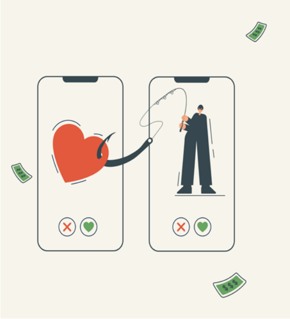
Online frauds and scams are a huge problem as they can inconvenience or even destroy your financial, personal, and professional life.

1. Fill in the blanks so the sentences make sense.
(digital Intermediate level)

In a ________________, a hacker __________________ information, usually ________________________.

In a ________________, you are usually __________________into giving ___________________________ information.

COMMON TYPES OF SCAMS



According to the Office of the Canadian Ombudsman for Banking Services and Investments (OBSI), the most common types of online scams in Canada involve romance, employment, and online shopping.

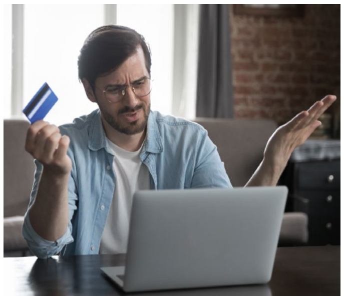
Romance scams often take place through online dating sites or other social media. The scammer creates a fake online profile often using a stolen identity. They often pretend to have a prestigious job that forces them to travel a lot. This means they can later say that is what makes it hard to meet in real life.

The scammer then identifies someone who seems eager to make a connection and charms them online until they feel they are part of a real relationship. Once the scammer gains the trust of their victim, they tell them they need to borrow a small amount of money for an emergency. The amounts get larger and larger until in many cases, the scammer borrows a very large amount, and the victim loses everything when the scammer disappears.

Employment scams often appear on job boards, social networking sites like Facebook and Twitter (X), or the targets of such scams may receive unsolicited emails from supposed employers. The scammer often pretends to be a legitimate company and offers the victim a "too-good-to-be-true" job that pays well and can usually be done from home. The offer makes the victim feel important.

In this scam victims willingly send requested personal information like their social insurance numbers, photo government IDs, or bank account numbers so their pay auto-deposit can be set up. The "new hire" may be asked to receive and re-send money to other people in the "company". They may be asked to repay money because their pay was incorrectly calculated. Or, they may have their entire identity stolen.

Online shopping is the third of the big scam types. Rip-offs from purchasing items online is one of the most common frauds affecting teenagers and young adults.



When you are buying, fraudulent sellers may offer products but never deliver after you pay.

When you are selling, fraudulent buyers might send you a fake cheque or money order or fraudulent cash app transfer. Sometimes they might overpay using one of the fake payment types and then ask you to send them the difference or a complete refund.

Safe online shopping isn't all that different than when you're buying from a physical store that you're familiar with. Stick to businesses you know and trust, especially for larger purchases like electronics, gadgets, and gift cards.

If you do find yourself shopping on a new website, however, there are a few things you can look for to make sure you don't get scammed:

Don't save your credit card information in your web browser.

- While it might save a few seconds, saving your credit card information in your browser means that anyone that has access to your device or accounts can make purchases with your card. This gets even scarier if cyber criminals compromise or hack your device.

Check your bank accounts and credit card statements regularly.

- If you're making purchases online, it's important to check your statements frequently to make sure you aren't getting scammed. If you're paying by debit card, remember to check the account it is connected to. If you do see suspicious or unexpected charges on your statements, get in touch with the bank or credit card company right away.

Edited from: https://www.obsi.ca/en/news/online-scams-are-cheating-a-growing-number-of-consumers-out-of-their-savings.aspx

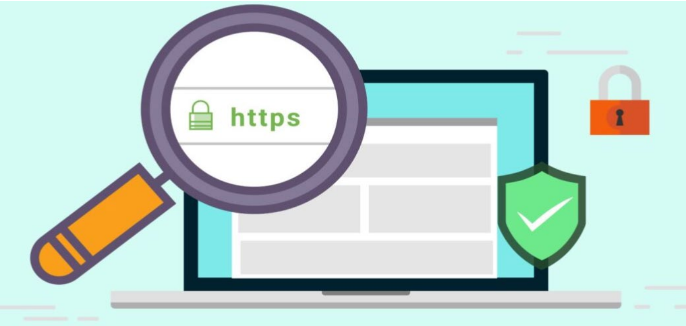
1. Using the information you just read, put an X in the columns to match each technique with the type of scam it's used in most often. Note, different scams may use the same techniques.
(*digital Intermediate level*)

TECHNIQUE	ROMANCE	EMPLOYMENT	SHOPPING
Gains your trust			
Too good to be true			
Send fake money transfer			
Requests personal ID			
Urgent			
Don't send what was promised			
Makes you feel important			
Unusual payment type			
First contact is through social media			

2. Based on the information in the text box, which of the listed images or words when displayed on a website tell you it's safe to shop there with your credit card? Check all that apply.
(*digital Intermediate level*)

Safe website shopping

1. A green checkmark
2. The word secure
3. The word buysafe
4. A lock symbol
5. A red checkmark
6. The word http
7. The word ccsafe
8. The word https
9. The word safe
10. The word SSL



Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed. You'll know if the site has SSL because the URL for the site will start with HTTP**S**—instead of just HTTP. An icon of a locked padlock will also appear, typically to the left of the URL in the address bar or the status bar down below; it depends on your browser. HTTPS is standard now even on non-shopping sites, enough that Google Chrome flags any page without the **S** as "not secure."

3. Check at least 2 websites that you have bought things from and answer the following questions for each one.
(digital Intermediate level) Answers will vary

Website 1

Company name: ____

Website URL: ____

Does the payment page begin with https? Yes ___ No ____

Does the payment page have a padlock icon? Yes ____ No ____

Have you saved your credit card information in the site? Yes ____ No ___

(If yes, consider deleting it now.)

Website 2

Company name: ____

Website URL: ____

Does the payment page begin with https? Yes ___ No ____

Does the payment page have a padlock icon? Yes ____ No ____

Have you saved your credit card information in the site? Yes ____ No ___

(If yes, consider deleting it now.)

RECOGNIZING ONLINE SCAMS

In addition to checking websites when you are making payments, watch for these signs indicating that something could be a scam:

- The contact is unexpected.
- It seems too good to be true – a discount or offer much better than you'd expect.
- You're asked to provide personal information.
- You're asked to make a payment of any kind.
- You're asked to make a payment in an unusual and specific format (e.g., wire transfer, bank order).
- You've been asked to do something quickly or you will miss the deal.

1. Read each scenario and identify at least 3 clues in each of them that should have helped the victim recognize the situation as a scam. Write your answers in the spaces provided. (*digital Intermediate level*)

Scenario 1

At the last minute, Karrie wanted to by two tickets to a weekend summer music festival that the official website said was sold out. She found someone online that had two available for $150 each. She thought that was a really good deal and agreed to send $300 via PayPal. The seller said he preferred gift cards because he'd been scammed before and now knew it was "safer" than PayPal. He also said he was really sorry he couldn't go but he urgently needed to sell the tickets so couldn't hold them while she decided. Karrie thought it was strange, but the guy seemed nice so agreed and bought three $100 gift cards online and sent him the information. The cards were redeemed and then he instantly blocked her on Facebook. No tickets, no refunds, and no way to find him.

List at least 3 clues

____

____

____

Scenario 2

Devrin had just started their first real job out of school and wanted to buy their parents a present to thank them for their help over the years. Devrin knew the family BBQ was getting older so had been looking for a deal online. They found a website that was offering brand name BBQs at ridiculously low prices. The site said they were a new business, and the low prices were part of their opening specials so was a "limited time offer". The only condition was you had to apply for and pay for it on the company credit. The card rate was very competitive at only 2.9%. Devrin did an online search for the company and couldn't find any bad reviews so went ahead and signed up for the card on the company website and used it to pay for the BBQ. A week later they received an email saying that due to supply chain issues the BBQ was delayed, but as it was not the company's responsibility, they were sorry but there could be no refund. Devrin immediately went back to the company website, but it was gone. And, as the BBQ never arrived, so was their money.

List at least 3 clues

Scenario 3

Alix met her partner Seamus through Facebook. They texted and chatted online for several months, and the relationship became more serious over time. Seamus said he was based in Ireland, but he was ready move to Canada to see where the relationship could go. He sent his flight information to Alix and told her he'd already shipped his things. The day of the flight Alix got a call from a customs agent saying the shipment had arrived but there were funds owing. Customs had tried to reach Seamus but of course couldn't as he was in transit. Alix's number was on the shipment as the Canadian contact, so they tried her. Customs explained if the funds weren't paid immediately, they would be returned to Ireland at Seamus' cost. Alix wanted to help so paid the balance owing by wire transfer as instructed in the amount of $3,355.99. She had loaned Seamus small amounts of money before which he'd always paid back so wasn't worried.

When Alix arrived at the airport that evening to meet Seamus, he didn't show up. When she tried to text him, there was no answer and his Facebook profile disappeared. After a few days Alix realized she'd been scammed. She asked her bank to recall the payment, but the money had already been moved and they were unsuccessful.

List at least 3 clues

WHY DO SCAMS WORK?

There are 2 main reasons that scams work.

1. People are in a hurry.
2. Scammers are smart and know how to manipulate people.

The amount of digital information that comes at you everyday is enormous. Not only has digital technology made doing many everyday things easier, but it's also made them faster. That makes us feel we need to be faster, that we need to respond right away. Feeding into that, according to malawarebytes, 70% of messages analysed, that were connected to a scam, contained some kind of "Hurry up please" messaging. Research confirms this increase in volume and speed has had a very negative effect on the length of our attention spans reducing them to shorter than 8 seconds! Reduced attention span means people rarely look at all the details of any message.

So given the volume, speed, and short attention span, with everyone using their mobile phone for banking, shopping, booking appointments etc., it is easy to see a text or email from a scammer and believe it is legitimate.

Scammers are smart. Most scammers are not the stereotypical geek sitting in their parent's basement. They may work as part of sophisticated networks of people working together. Working alone or with others, they not only understand that people have short attention spans and how to use weaknesses in digital technology to their advantage, but they understand a lot about how people think, and they use it against them. This is called psychological manipulation, and it can work on anyone.

Scammers are very good at manipulating people to get what they want, such as getting you to reveal personal information or convincing you to give them money. They do this by using tactics that take advantage of normal human tendencies and feelings. Scammers know that most people want to feel valued and avoid things that are unpleasant, so they will imply that you should:

- Trust someone because they seem likable.
- Trust someone because they say you're special and they like you.
- Do the same things that others are doing so you don't have to be afraid of missing out.
- Obey an authority figure.
- Avoid punishment or embarrassment.
- Want something because it is scarce and not everyone can have it.
- Act fast because it's urgent or time sensitive.

1. Check all the statements that apply.
(*digital Intermediate level*)

SCAMS WORK BECAUSE:	√
People are stupid	
People want to get a good deal	
People use cellphones	
Scammers are smart	
People like to feel special	
People don't get enough email	
Scammers know how to manipulate people	

2. Mark the statements below as true or false.
(*digital Intermediate level*)

STATEMENT	TRUE	FALSE
Typical attention spans are 8 minutes.		
FOMO is a real cause of scams.		
Any aged person using the internet can be scammed.		
Psychological manipulation doesn't work.		
Some people are scammed because they are lonely.		
Only 7% of email scams are urgent.		
Some people are scammed because they think they're smarter than other people.		

WHAT IF YOU ACCIDENTALLY PAY A SCAMMER?

If you accidentally pay a scammer there are things that you can and should do right away. While you may not always get your money back, by reporting, you can help to make sure that someone else doesn't fall for the same scam.

1. Tell somebody!
   a. Scamming is a crime! Gather all information about the fraud. This includes documents, receipts, copies of emails and/or texts. Report these to the police, especially if you lost money.
   b. Report to the anti-fraud centre or competition bureau.
   c. Notify the website or online marketplace where the fraud took place.
   d. Tell your bank or financial institution and credit card company.

2. How did you lose the money? The type of payment method you used has an impact on what you should do next.
   a. Did you pay with your credit or debit card? Always report any fraudulent charges on your card to your bank and ask for a reversal.
   b. Did you pay using a gift card? Contact the company that issued the gift card right away and tell them about the scam. Keep copies of any gift cards and their receipts for reference purposes.
   c. Did you send a wire transfer through your bank? Report the transfer to your bank as soon as possible. Have them direct you through the process that has to be followed to reverse a wire transfer.
   d. Did you use a money transfer app? Contact the app company responsible and report the scam. Find out if they have a policy that will allow you to reverse the payment to get your money back.
   e. Did you pay with cryptocurrency? If you used a centralized exchange, report the scam to them and ask if they are able to reverse your payment.

1. Match the type of payment used with where you should report it if you are ever scammed. Some answers may be used more than once.
(*digital Intermediate level*)

Payment type	Report scam to…
Money transfer app	
Credit card	
Wire transfer	
Gift card	
Cryptocurrency	

The exchange

Your bank

The company

The app owner

SCAMS AT WORK

Recognizing online scams and frauds at work is just as important as in your personal life. If you communicate online for work, you must follow all employer policies on digital communication. This is true when emailing or texting coworkers and customers but especially true if part of your job is to make online purchases for your employer or share financial information online. Consider this case.

A mid-size transportation company received an email from one of their suppliers. The supplier said that the bank had updated the account information for them to receive payments and included the account number. They asked if payments could now be directed to the new account and apologized for the inconvenience. The email included an invoice of what they'd supplied that month as well as the prior email trail between the company and the supplier. Everything was a perfect copy of the invoices they'd received before, so the transportation company sent the payment of over $80,000 to the new account and never thought much about it. Unfortunately, the real supplier never received it the payment.

Turns out the scammers had hacked into the supplier's IT department to access old emails and account information and create a false invoice. Because the scammers were using the supplier's real email address but had some way to intercept and hide the company's emails, the supplier never received those either. The company didn't find anything out until the supplier contacted them via phone to ask about why the invoice hadn't been paid.

This was a very sophisticated scam, and the only real clue was that it was about a change in banking information. The best way to avoid this would have been for the employer to have a policy that said, whenever banking details are involved, you must contact the supplier directly using a second, reliable mode of communication, like a known phone number, to verify the request.

Edited from: https://www.scamwatch.gov.au/protect-yourself/real-life-stories/scam-victims-tell-us-their-stories/business-email-compromise-our-business-lost-190-000-when-our-suppliers-email-was-hacked

HOW TO LEARN MORE

Competition Bureau Canada
Bureau de la concurrence Canada
THE LITTLE BLACK BOOK OF SCAMS
Canada

The Government of Canada recognizes online frauds as a big problem for individuals and business.

Check out these sites for the most up-to-date information on what scams are out there and how to keep yourself safe.

- Competition Bureau of Canada: The Little Black Book of Scams 2nd. Edition – available in multiple languages. https://ised-isde.canada.ca/site/competition-bureau-canada/en/little-black-book-scams-2nd-edition
- Get Cyber Safe. https://www.getcybersafe.gc.ca/en
- Canada Revenue Agency: scams and frauds. https://www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html

5. USING AI

The World of AI

One of the biggest developments in digital technology is artificial intelligence (AI). The use of AI technology is growing at a phenomenal rate and things people thought of as science fiction just 10 years ago, like self-driving cars, are actually happening today. Chances are AI is already part of your daily life and likely going to become a bigger part of your personal and work experiences. Like most digital technologies AI is neither good nor bad; it all depends on how you use it.

AI SNAPSHOT

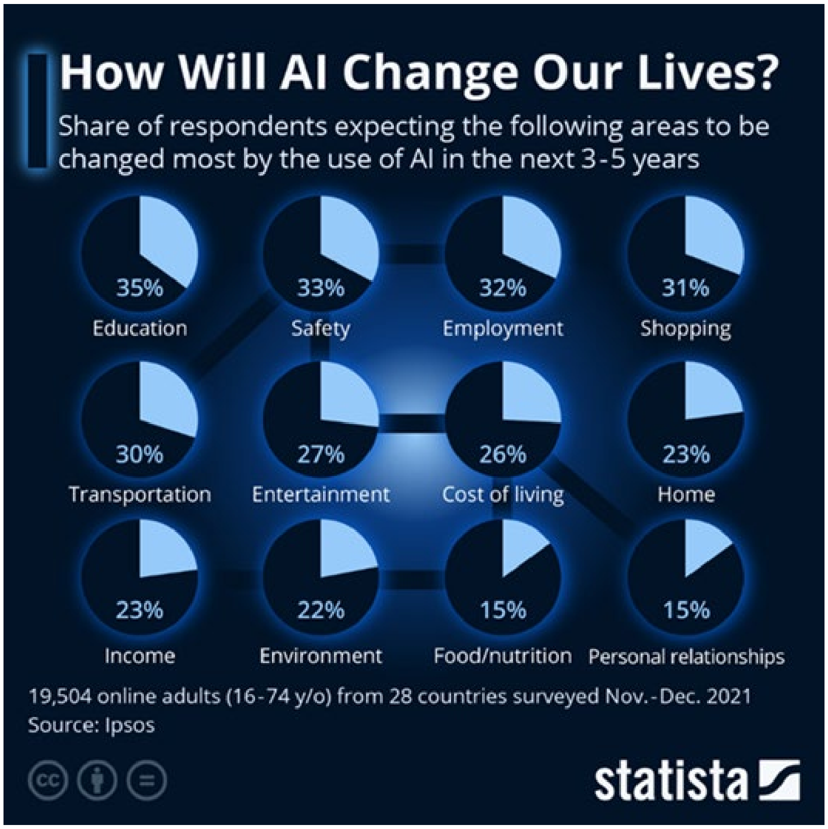
- AI is short for artificial intelligence and is the science of making machines that can think like humans. AI makes machines "smart".
- In the 1950s, computer scientist Alan Turing created the first big test to see if machines could have intelligence. The first recorded use of the term AI was at a conference in 1955.
- AI uses "algorithms" which are sets of rules programmed by humans into computers. AI can adapt these algorithms, so they become smarter and faster the more they are used and the more data they analyze. This is how computers "learn".
- In Canada, the use of AI is a federal responsibility and in October 2023 the government issued a voluntary code of conduct for the use of generative AI systems that includes a commitment to transparency and avoiding bias. Generative AI includes products like ChatGPT and other systems that can create things (generate them) like text, images, music, or video. This recommended code covers all types of businesses.

SMART THINKING!

SMART tech is powered by AI. SMART is the acronym for "**S**elf-**M**onitoring, **A**nalysis and **R**eporting **T**echnology", but the technology is also usually described as being "smart" because it actually makes things like phones and other tech smarter.

So, in what part of life do people think there will be the greatest change as a result of the use of AI?

1. This chart shows which areas of life consumers around the world expected to change the most due to the increased use of AI between 2021 and 2026. Use the information in the chart to answer the questions.
(*digital Intermediate level*)



https://www.statista.com/chart/29229/areas-of-life-most-expected-to-change-by-the-use-of-ai/

What is the area where most people think there will be the greatest change?

____

What is the area where you think there will be the greatest change? Provide a reason for your answer.

____

____

____

What is the area where most people think there will be the least change?

____

What is the area where you think there will be the least change? Provide a reason for your answer.

____

____

____

WHAT DO YOU ALREADY KNOW ABOUT AI?

You may not have a self-driving car, but if you have asked Alexa what time the movie starts or used a Snapchat filter to change your profile pic into a cartoon, you are already using AI.

Read how Morgan uses AI every morning.

Every morning when Morgan wakes up, they reach for their smartphone, hold it up to their face to log on and see what happened while they slept. They click into social media, scroll the first few posts, and check any new friend requests. They check their smartwatch to see how they slept and their calendar to see what meetings they have. They search for the fastest route to get to a building they've never been to before, see there's road construction, and send their co-worker a text letting them know the recommended detour and how much extra time they'll need. That's a lot of AI, all before getting out of bed.

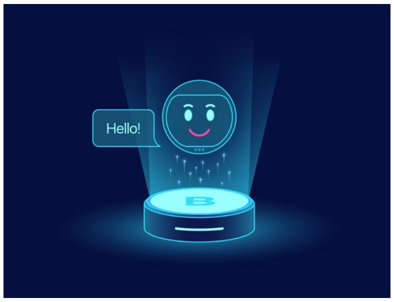
1. List all the types of AI you think Morgan used before getting out of bed. Check your answers on the next page.
(*digital Intermediate level*)

Here's the list of AI Morgan used that morning. How many did you get?

- Smartphone: Morgan's smartphone is powered with AI. That's what makes it "smart".
- Face recognition: FaceID uses AI biometrics and machine learning algorithms to compare the scan of your face with what it has stored about your face to determine if the person trying to unlock the phone is really you.
- Personalized recommendations: AI works to decide which posts you see when, so that your social media is personalized to your past interests, so you'll spend more time on it.
- SMART tools: Smartwatches use AI to track biometrics advising when there are changes in your health.
- GPS: Maps apps use AI to track real time routes and events.
- Writing tools: Emails and text communications are enhanced by AI tools like Grammarly and predictive text.
- Anti-virus software: AV software uses AI to block spam and ensure your messages arrive safely.

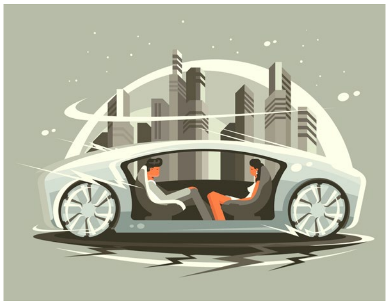
Here are a few more examples of everyday AI in more detail with an advantage and disadvantage for each.

VIRTUAL ASSISTANTS



Smart assistants like Amazon's Alexa, Apple's Siri, and Google Assistant employ AI technologies to interpret voice commands, answer questions, and perform tasks. These assistants use natural language processing and machine learning algorithms to understand user intent, retrieve relevant information, and carry out requested actions.

- Advantage: Provides fast answers to basic questions. Usually very accurate.
- Disadvantage: Virtual assistants are always "listening". There are privacy risks concerning what they do with that data. (You can learn more about privacy in the Workout: Passwords and Cyber Security.)



COMMUTING TO WORK

Self-driving cars rely heavily on AI for perception, decision-making, and control. Using a combination of sensors, cameras, and machine learning algorithms, these vehicles can detect objects, interpret traffic signs, and navigate complex road conditions autonomously, enhancing safety and efficiency on the roads. Google maps and other travel apps use AI to monitor traffic to give you real-time traffic and weather conditions as well as suggest ways to avoid gridlock.

- Advantage: GPS in phone and car apps is a huge time saver and its voice features mean drivers don't have to just rely on information on screen.
- Disadvantage: Today self-driving vehicles are very expensive and prone to accidents. But they are getting cheaper and safer.

RECOMMENDATIONS FOR STREAMING AND SHOPPING

Online shopping is another way many people are exposed to artificial intelligence regularly. The retailers' AI algorithms track what you buy, and what other people who the AI thinks are like you buy, to provide recommendations when you visit their sites. Streaming services work the same way. The companies' recommendation engines are powered by AI and use your past viewing history to deliver suggestions for what you might want to watch (including genres, actors, time periods, etc.). Its tool gets as specific as when you were watching and what you usually like to watch during that time. In fact, 80% of what we're watching is driven by Netflix's recommendations.

- Advantage: You easily see products and movie suggestions that may interest you.
- Disadvantage: May convince you to purchase items or rent movies you had no intention of buying.

1. Think of 2 types of AI that you use and write them down with what you think is an advantage and a disadvantage for each one. Do not repeat the advantages and disadvantages mentioned in the previous article.
(*digital Intermediate level*) *Answers will vary.*

AI #1: ______________________________

____

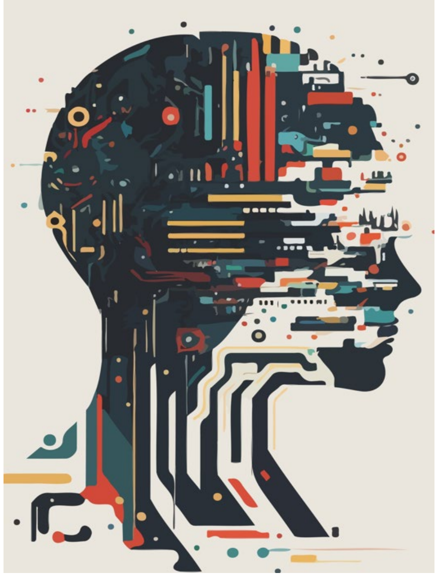
____

AI #2: ______________________________

____

____

AND THEN THERE'S THE NEWEST KID ON THE BLOCK – ChatGPT!



In 2023, even people who didn't know anything about artificial intelligence, suddenly knew about ChatGPT. Since it was introduced to consumers in 2022 as a free download, ChatGPT has been a really big thing. So, what is it?

The name ChatGPT is the acronym for Chat Generative Pre-trained Transformer. It's a very intelligent chatbot (a computer program designed to simulate conversation with human users, especially over the internet). It's designed to provide natural and fluid responses to humans. The chatbot is built on machine learning technology, which means it can adapt to different situations and interactions to deliver a more personalized and effective experience.

ChatGPT doesn't just provide answers like virtual assistants do. It customizes those answers with layers of human emotions and experiences. For example, users can ask ChatGPT to write wedding vows that are "sincere and heartfelt" or obituaries that are "serious but with a little old-fashioned humour". Of most interest to instructors and learners, ChatGPT can write school assignments such as papers that "describes the history of carpentry hand tools in Canada using the 5-paragraph essay model that sound like they're written by a grade 9 student."

High-school teachers, post-secondary instructors, parents, and learners all have questions about the use of ChatGPT, questions that include:

- Plagiarism: Does ChatGPT encourage students to cheat?
- Ethics: Does ChatGPT encourage students to think it's okay to use other people's ideas?
- Misinformation: How does ChatGPT know if the information its sharing is true?
- Biases: Does ChatGPT pass on the biases of the people who are using it?

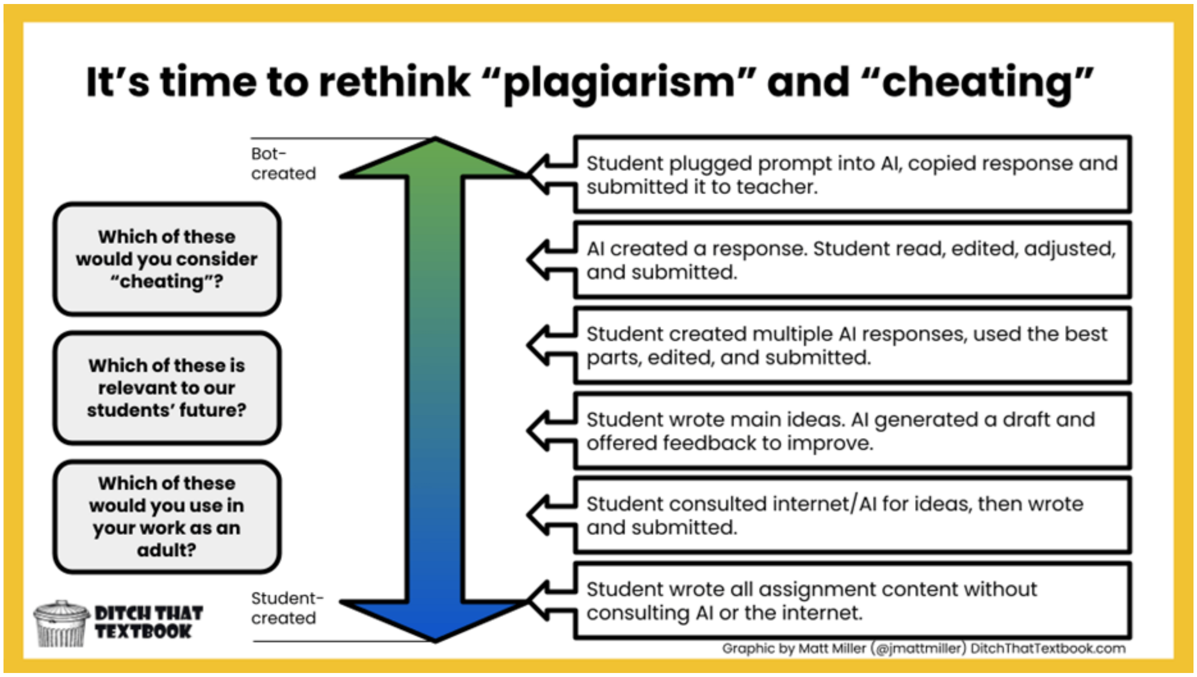
2. It's important to know what different words mean in the context of AI. In the table on the next page, match each word with what you think is the best definition, by drawing a line between them.
(*digital Intermediate level*)

WORD
Plagiarism
Ethics
Misinformation
Bias
Cheating

DEFINITIONS
False or inaccurate facts.
Predictions or outputs that favour or discriminate against specific groups of people.
When a person presents some type of work as their own creation when, in reality, it isn't their work.
When a person does something dishonest in academic or professional work that misrepresents what they understand or can do, giving them an unfair advantage.
A set of moral principles that are followed by people who are generally thought of as good.

Schools and post-secondary institutions will likely have their own definitions of plagiarism and cheating and perhaps the emphasis will be on encouraging ethical use of the technology rather than on restricting its use. Maintaining good ethics is an important part of being a student and being a working professional.

3. Look at the graphic on the next page created for teachers about how students use AI like ChatGPT. Which of the actions on the right do you think are cheating? (*digital Intermediate level*) *Answers will vary. Sample answer provided.*



It's time to rethink "plagiarism" and "cheating"

Bot-created

Which of these would you consider "cheating"?

Which of these is relevant to our students' future?

Which of these would you use in your work as an adult?

Student-created

- Student plugged prompt into AI, copied response and submitted it to teacher.
- AI created a response. Student read, edited, adjusted, and submitted.
- Student created multiple AI responses, used the best parts, edited, and submitted.
- Student wrote main ideas. AI generated a draft and offered feedback to improve.
- Student consulted internet/AI for ideas, then wrote and submitted.
- Student wrote all assignment content without consulting AI or the internet.

DITCH THAT TEXTBOOK

Graphic by Matt Miller (@jmattmiller) DitchThatTextbook.com

https://ditchthattextbook.com/ai/

4. Write 3 simple rules you think would be useful for helping students understand when they can use ChatGPT and for making sure it is used ethically.
(digital Intermediate level) Answers will vary. Sample answers provided.

5. Consider this real-life use of AI reported in Toronto Life Magazine and answer the questions that follow.
(*digital Intermediate level*)

In February of 2023, a student in earth and environmental sciences at the University of Toronto went with his class on a field trip to High Park. Afterward, the professor gave students a soil sample from the mucky bottom of Grenadier Pond and instructed them to write a paper on the sediment, linking it to events in Toronto history. The student was stumped: the sedimentary record didn't seem to line up with the historical one. Roughly 25 centimetres from the top of the sample, he saw what seemed to be a layer of black tar, which he dated to the early 1970s. But what could have caused it?

He searched the university databases in hopes of uncovering a regional event—a fire, say, or a major construction project—that might explain the sedimentary change, but nothing came up. In desperation, he wrote up a description of the soil sample and prompted ChatGPT to interpret it. The bot responded in seconds, linking the tar in the sample to the construction of the Queensway thoroughfare in the 1950s.

At first, the solution seemed absurd to the student—the timing made no sense—but he soon realized it was correct. In his original analysis, he'd misdated the soil sample, attributing sediment from the postwar construction boom to events 20 years later. ChatGPT had corrected the mistake.
https://torontolife.com/deep-dives/chatgpt-ai-cheating-revolutionizing-university-education/

What digital tool did the student use in addition to ChatGPT?

___

What did the student write into ChatGPT?

___

What is the mistake ChatGPT corrected?

___

___

Do you think the student was cheating or did they use ChatGPT ethically? Include a reason to support your answer. (*Answers will vary. Sample answer provided.*)

___

___

CHEATING OR SMART TECH?

- 1960s: Handheld calculators introduced, and schools worry it's cheating.
- 1970s: Calculators encouraged in class for basic math.

- 2001: Wikipedia created, and schools worry it's cheating.
- 2010: Wikipedia is a great place to start.

- 2022: ChatGPT created, and schools worry it's cheating.
- Today: While it is still very early in the development and integration of AI, it seems likely that it will become an accepted part of how learners at all levels conduct research and undertake assignments. Perhaps the emphasis will be on encouraging ethical use of the technology rather than on restricting its use.

ADVANTAGES OF AUTOMATION AND AI IN THE TRADES

Automation is the use of technology to perform tasks without human intervention. This can include anything from simple machines like conveyor belts to complex robots and computer systems that can perform a wide range of tasks repeatedly.

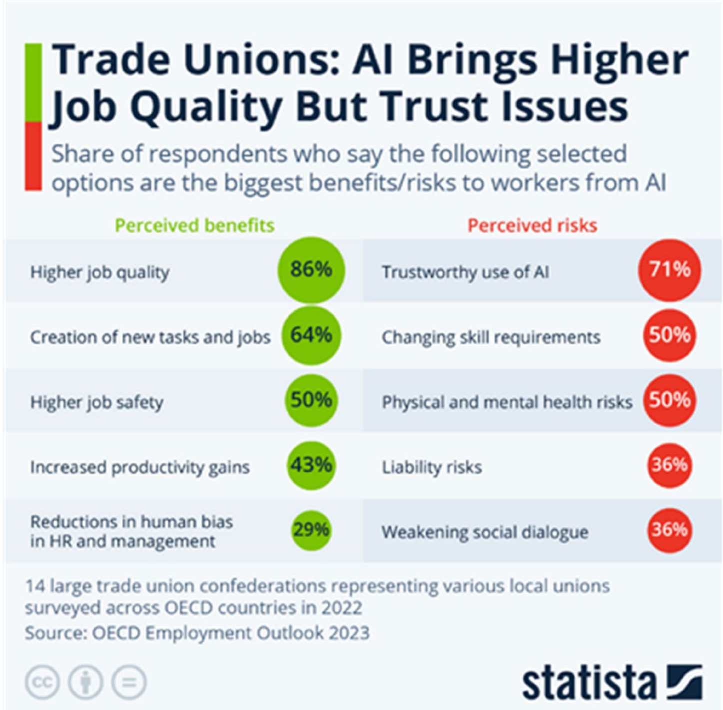
With automation, workers set up machines to repeat the same tasks over and over again. However, the machines can't do anything else.

With the addition of AI, humans can program those machines so that they detect when things are going wrong, figure out how to fix things, learn from those experiences, improve their function, and report the changes back to humans. AI can enhance automation when the two work together. When that happens, there are significant benefits. For example, two of the biggest disadvantages of automation have been that machines cannot handle complex tasks or correct for errors. Adding AI capability and custom programmed algorithms creates technology that can make decisions and correct errors.

An example of AI in the trades is the use of robotics. Robotics is a division of science and engineering which designs, develops, manufactures, and operates robots. These robots are intelligent machines that are designed to perform different kinds of tasks. Robots come in different shapes, forms, and sizes and their level of intelligence and sophistication varies.

There's no question that AI is having a significant impact on how the work of skilled tradespersons is done. As AI is used for more tasks, many wonder if AI will replace those workers. The idea that workers can be replaced by machines is not new. The use of automation has been part of production and manufacturing processes since the first industrial revolution. The work of skilled tradespersons has been changed by automation, but they are still in high demand.

Organization for Economic Cooperation (OECD) researchers surveyed 14 large trade union confederations across OECD countries to better understand current thoughts about the future of AI in their workplaces.



Trade Unions: AI Brings Higher Job Quality But Trust Issues

Share of respondents who say the following selected options are the biggest benefits/risks to workers from AI

Perceived benefits		Perceived risks	
Higher job quality	86%	Trustworthy use of AI	71%
Creation of new tasks and jobs	64%	Changing skill requirements	50%
Higher job safety	50%	Physical and mental health risks	50%
Increased productivity gains	43%	Liability risks	36%
Reductions in human bias in HR and management	29%	Weakening social dialogue	36%

14 large trade union confederations representing various local unions surveyed across OECD countries in 2022
Source: OECD Employment Outlook 2023

statista

https://www.statista.com/chart/30441/biggest-benefits-risks-in-the-workplace-from-ai/

As the chart shows, a majority of respondents said that the adoption of AI could improve job quality for workers - perhaps through effective collaboration between workers and AI. This could result in a reduction of working time to complete a task allowing a possible focus on more interesting tasks and increased work autonomy. At the same time, the survey data showed that many working within the trade unions sphere consider AI to be creating new tasks and jobs, such as the roles of data analysts, computer engineers, scientists, and network experts.

AI IN DIFFERENT TRADES

AI is creating new jobs and modernizing traditional trade jobs by introducing cutting-edge technologies and machines. With better technology, jobs become smoother and easier and faster to accomplish. AI can help suggest the best processes and products for a job and relieve people of labour that could be too strenuous to be safe for a person, such as lifting heavy machinery. It can also help with making it easier to conduct maintenance work assisting workers by showing them exactly the problem area, so that they don't need to deconstruct an entire appliance.

Examples of AI complementing the work of skilled tradespersons include:

Manufacturing

- Airbus developed an AI system to analyze aircraft performance data to predict when parts might need to be replaced or serviced, increasing safety, and reducing maintenance costs.

Agriculture

- John Deere, a manufacturer of farm equipment, uses AI and machine learning to analyze soil samples and other data to help farmers make better decisions about when and where to plant crops resulting in better crop yield.

Construction:

- In the construction industry, AI is already being used to automate tasks such as surveying, scheduling, and project management, improving efficiency and reducing costs.

Warehouse Robots

- A famous example of human and robot collaboration is Amazon's warehouse robots that work alongside staff in its fulfillment centers. These robots have one job – to bring items to human pickers so they can be packaged and labeled for dispatch. They do this by moving entire shelving units and are programmed to watch out for humans so they will not collide and cause accidents. While the existing robots are limited to working in certain designated areas, a newer model currently being trialed, nicknamed "Bert," will be able to safely navigate anywhere on the factory floor.

1. Answer the 3 questions below.
(*digital Intermediate level*)

What is the most significant difference between automation and AI?

Based on the information in the article, write down one benefit of using AI in each of the sectors listed.

- Manufacturing: ____
- Construction: ____
- Agriculture: ____

What will the new warehouse robot be able to do that current robots can't?

____

2. The perceived benefits and risks of AI in the workplace as noted in the OECD research are listed below. Are there other benefits and/or risks you would have included? Enter them in the spaces provided. Then number the benefits and risks in the order *you* think they will have the greatest impact. (1 = most impactful.)
(*digital Intermediate level*) *Answers will vary.*

BENEFITS	Order #
Higher job quality	
Creation of new tsks and jobs	
Higher job safety	
Increased productivity gains	
Reductions in human bias in HR and management	

RISKS	#
Trustworthy use of AI	
Changing skill requirements	
Physical and mental health risks	
Liability risks	
Weakening social dialogue	

6. DIGITAL HEALTH

NOTE:

This workout is designed to describe, and have you think about, how the ways in which you access digital information at school, at work, or in the community might impact your health – physically and mentally.

Some digital health impacts, especially mental health impacts, are very personal and very complicated. In those cases, you need more than the information in this workout; you need friends and trusted adults, including, possibly, professionals, to help you sort things out.

If you have completed the Passwords and Security workout you will have read about digital hygiene. The ideas of hygiene and health are similar, but when this workout talks about your digital health, it means your physical and mental health.

The digital revolution has changed everything. It makes many things easier and more creative, but we also need to think about how using digital tools impacts not just the ways we live and work, but what that impact is on our health and how we feel.
The digital world also provides an endless amount of health-related information. And, like all other aspects of the digital transformation, it's important to know how to use it safely.

DR GOOGLE. PAGING DR GOOGLE.

The term "Dr. Google" emerged in the early 2000s when people started using the powerful search engine to self-diagnose. According to *The Conversation*, by 2013, more than half of Canadians polled said they used Google search to self-diagnose. In 2020, 69% of Canadians used the internet to search for health information, and 25% used online sources to track their fitness or health. During the covid pandemic, virtual medical care, self-monitoring, and online self-diagnosis became even more common.

Being able to search for health-related information on your own can be empowering. If you do not have easy access to health care or if you feel unheard, it can feel empowering to be able to gather your own information – but it still usually needs to be discussed with a health professional. Some of the problems identified with self-diagnosis are:

- exaggerating symptoms and missing the actual problem.
- delays in starting the needed treatment.
- increases in stress, anxiety, and depression.
- self-diagnosis often results in poorer outcomes.

1. Read the article on the next page, *Limiting the Risks of Self Diagnosis,* about the possible downsides of relying on the internet for health information and then use the words in the bubbles to complete the statements.
(*digital Intermediate level*)

1. Look for websites that are ________________________ by health or government agencies.
2. A misdiagnosis can ________________________ getting proper treatment.
3. Many serious diseases can have ________________________ symptoms.
4. ________________________ is a common problem when getting health information from social media sites.
5. Only use the internet to ________________________ mild health conditions.

diagnose

moderated

delay

mundane

misinformation

LIMITING THE RISKS OF SELF DIAGNOSIS

The kinds of conditions that search engines diagnose best are mild like a cold or the flu. While it is important that you are informed as a patient, and there are cases where people with mysterious illnesses have found solutions on the internet, using Dr. Google to self-diagnose also comes with risks.

Using the internet to self-diagnose can lead to a misdiagnosis and delay the correct diagnosis. Many serious diseases also have mundane symptoms. For example, stomach pain can be caused by issues relating to the stomach, appendix, gallbladder, spleen, bowel, liver, and gynecological issues. Or it may just be a sign that you ate too much. For people self-diagnosing, it becomes easy to be convinced there is something serious going on and become anxious. Instead of just using broad web searches, it's better to use more reliable sites that are offered by medical schools, government health agencies, and disease-specific organizations like the Canadian Cancer Society that are moderated by healthcare professionals.

Even when reliable sites are included, it's possible to go deep into Cyberchondria Wonderland. The more websites consulted, the more likely it is to happen. Forums, unmoderated chat rooms, and social media can contain personal experiences that went wrong or are incomplete increasing your anxiety. Anything can be posted, and it can be difficult to separate fact from fiction.

Whether the diagnosis is correct or incorrect, there can be adverse consequences when people self-treat. If they are fortunate, the only consequence will be wasted time and money on treatment that doesn't work. If not, the treatment could make their condition worse and/or result in significant side-effects or complications.

A further risk to digital self-diagnosis is the "footprint" you leave every time you visit a website. Many unreliable sites use tools to track visitors to their websites. Your personal data and volunteered medical information may be collected or even sold. You can limit this risk by never "subscribing" or entering any personal information into a site.

2. For each of the risks listed in the table, identify at least one action you can take to reduce the risk.
(*digital Intermediate level*)

RISK	ACTION
Following inaccurate information	
Loss of personal information	
Increasing your anxiety level	
Delay in getting the medical care you need	
Wasting time and money on false cures	

LET'S GET PHYSICAL

Overuse of digital technology can have several negative impacts on your physical health. These include head, neck and back pain, eye and hearing health, as well as poor sleep, obesity and a tendency not to exercise. Fortunately, there are precautions you can take to reduce or even prevent these impacts.

Looking down at an electronic device for long periods can lead to neck and back pain, as well as pains in elbows, wrists, and hands. In addition, laptop and smartphone usage can involve people sitting in positions consistent with poor ergonomic function and body position. As well as back pain from computer use, often caused by poor gaming posture or computer posture, there have also been reports of "selfie elbow" or "texting thumb" caused by technology overuse. Pain in these parts of the bodies is called musculoskeletal pain (referring to muscles and bones).

What is "ergonomics"?

Ergonomics can roughly be defined as the study of people in their working environment. More specifically, an ergonomist (pronounced like economist) designs or modifies the work to fit the worker, not the other way around. The goal is to eliminate discomfort and risk of injury due to work. The term comes from the Greek words ERGON (work or labour) + NOMOS (natural laws).

Tips to prevent or reduce musculoskeletal pain:

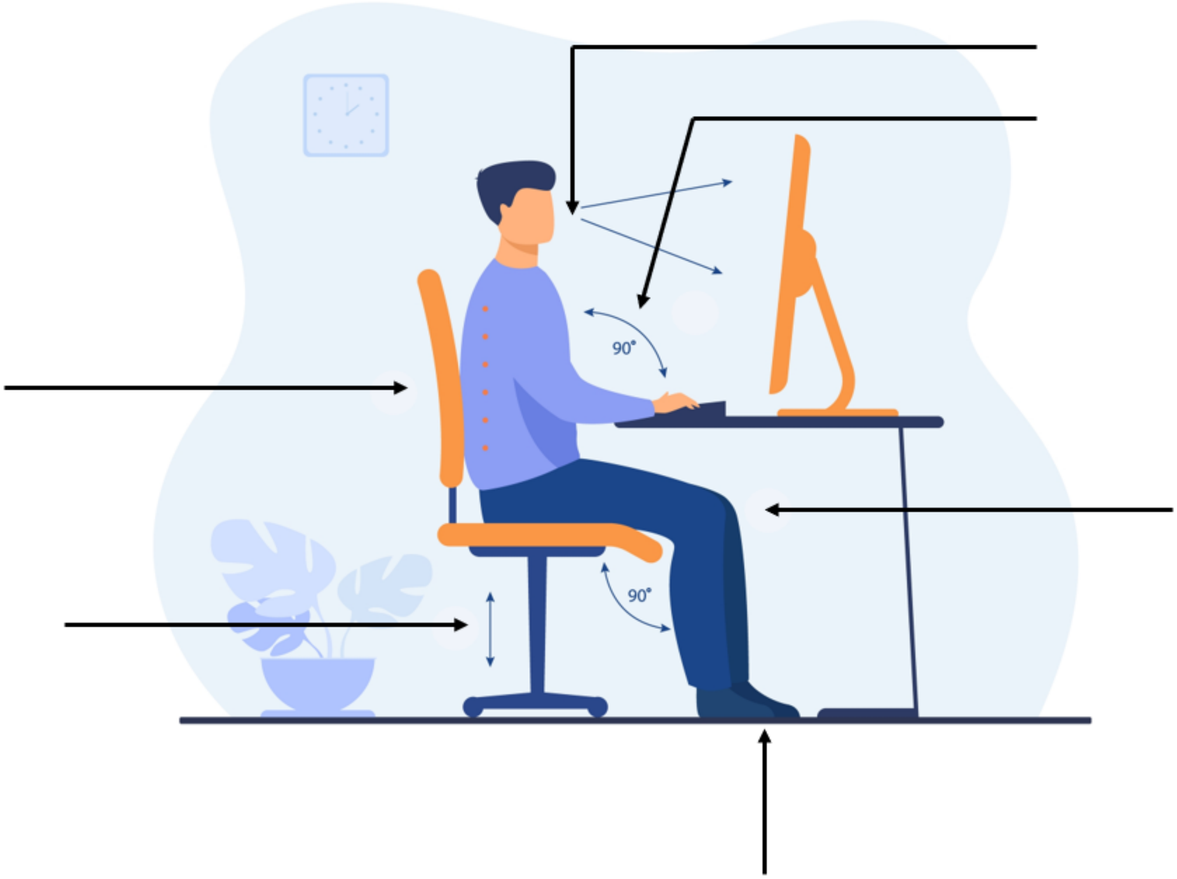
- Be mindful of your posture when using different devices:
- Use proper sitting posture at the computer by ensuring that your desk, seat, and screen set-up is optimized. Seat height should be set so your knees are at 90° to the floor when your feet are flat on the floor. Your elbows should also be at 90° to your body. Your back should be straight and touching the chair back.
- Instead of holding your phone in your lap, you can minimize neck problems by holding it out in front of you. Positioning the device so it is in front of your face with your head sitting squarely on your shoulders is helpful to your neck.
- If texting with your thumbs causes pain, try using other fingers to text or use a stylus.
- Schedule regular short screen breaks. Set a timer for every 20-30 minutes to get up, stretch and walk around for a few minutes. This will help not only reduce muscle pain and eye strain but also stress.

Digital eye strain is one of the most reported symptoms of too much screen time. Signs of digital eye strain include dry eyes, redness around the eyes, headaches, blurry vision, and even pain in the neck and shoulders.

Tips to prevent or reduce eye strain:

- When working at a desk, the top of the monitor should be at your eye level and the distance from your eyes to the monitor should be 45-70 cm.
- Make sure to blink. When we stare at digital devices, we can blink less frequently, leading to dry eyes. If dry eyes bother you, eye drops could help.
- Reduce overhead lighting to minimize screen glare.
- Increase text size on devices so you can read comfortably.

1. Use information from the Let's Get Physical article to label the image to show which ergonomic precautions the person is taking to prevent musculoskeletal and eye strain issues. (*digital Intermediate level*)



Hearing protection is another important part of protecting your digital health.

Hearing loss can happen when you're around loud sounds a lot. The World Health Organization says that 1.1 billion young people worldwide might hurt their hearing by listening to music too loudly via headphones, earphones, or earbuds.

Think about it from a work perspective. In some skilled trades your work requires you to be around loud noises generated by machinery. On those job sites hearing protection is an important and necessary part of your PPE (personal protective equipment). Think of protecting your hearing in the same way when listening to music or streaming media.

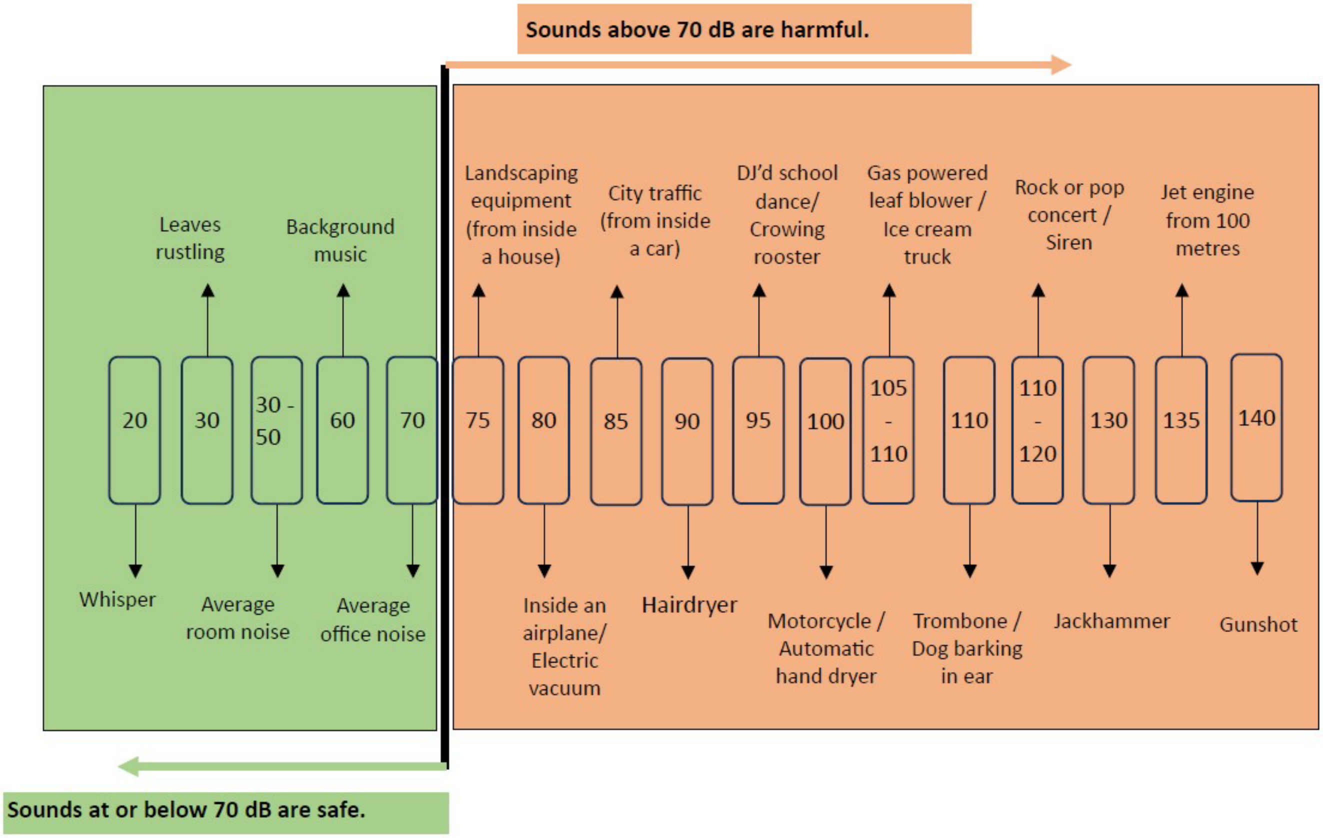
Tips to prevent or reduce hearing loss:

- Choose headphones that sit outside the ear instead of ear buds that go in the ear. This provides extra space that helps protect your hearing.
- Try using noise-canceling headphones, which use special waves to block out outside sounds.
- Experts suggest listening at no more than 85 decibels (dB) for no more than 8 hours each day is the maximum "safe level" for workplace noise exposure.

Decibels are the unit of measurement for sound. Their abbreviation is db. Sounds at or below 70 dB are considered safe for our hearing. That's the sound of a normal conversation between two people. Consistent noise above 70 dB will damage hearing over time.

2. Use the information in the noise levels diagram on the next page to answer the questions. (*digital Intermediate level*)

1. What is the difference in decibels between hearing landscaping equipment outside or from inside a house? __________
2. Does taking a flight potentially harm your hearing? Circle your answer. YES NO
3. What is the threshold for safe sounds? __________
4. How many dBs above the safe level is a hair dryer? __________
5. Other than a plane, what is the loudest transportation noise? ________________
6. What's the difference in decibels between a powered hand dryer and hair dryer? __________


Sounds above 70 dB are harmful.
Leaves rustling
Background music
Landscaping equipment (from inside a house)
City traffic (from inside a car)
DJ'd school dance/ Crowing rooster
Gas powered leaf blower / Ice cream truck
Rock or pop concert / Siren
Jet engine from 100 metres
20
30
30 - 50
60
70
75
80
85
90
95
100
105 - 110
110
110 - 120
130
135
140
Whisper
Average room noise
Average office noise
Inside an airplane/ Electric vacuum
Hairdryer
Motorcycle / Automatic hand dryer
Trombone / Dog barking in ear
Jackhammer
Gunshot
Sounds at or below 70 dB are safe.

Sleep

Getting enough sleep is vital for your body to work well. Healthy Living Canada recommends that up to age 17 you should get 8 to 10 hours of good sleep a night, and between 18 and 64 you should get 7 to 9 hours on a regular basis. Poor quality sleep, or not enough sleep, has been linked to depression and many chronic health problems, including heart disease, high blood pressure, and obesity.

Using a laptop, tablet, or smartphone right before bed, can make it hard to fall asleep. That's because the blue light from these devices can make you more awake and mess up your body's sleep schedule.

Some people think they need their screens to wind down (not true). If this is you, do something passive like listening to music, reading an e-book, or watching TV. Avoid interactive activities like playing video games or chatting on social media. Doing interactive stuff is more likely to mess with your sleep than passive things.

Tips to encourage good sleep habits:

- Stop using your smartphone, laptop, and tablet at least an hour before bedtime. Reading a book is more likely to help you relax than looking at social media.
- Make the screen as dark as you can at night. Some e-readers let you change the screen color to white words on a black background. Many devices also have a 'night-time mode' that's easier on your eyes before bed.
- If you can, keep screens out of your bedroom.
- Create a relaxing routine before bed that doesn't involve screens. It will help you chill out before going to sleep.

3. In addition to managing your digital devices, there are other things you can do to improve your sleep quality. Use the information you just read and the infographic from Public Health Canada, on the next page, to answer the questions.
(*digital Intermediate level*)

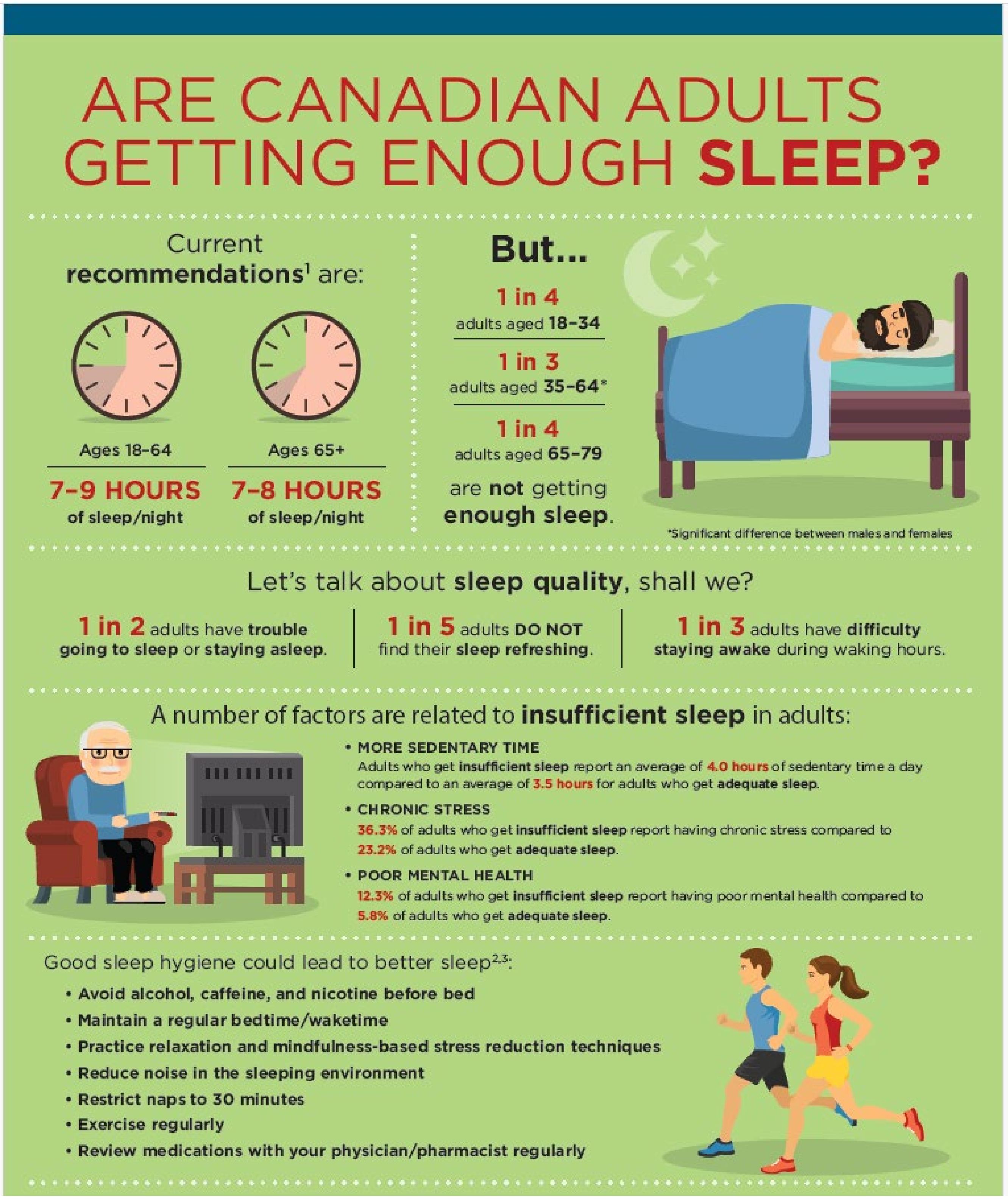
1. What percentage of adults under the age of 35 are not getting enough sleep? __________
2. What percentage of adults have trouble staying asleep? __________
3. What percentage of adults might fall asleep during the day? __________
4. For your age, how many hours of sleep should you get each night? __________
5. How many hours sleep do you get? __________
6. If you get fewer than the recommended number, identify 2 changes you could make.

____

____

____

____



ARE CANADIAN ADULTS GETTING ENOUGH **SLEEP?**

Current **recommendations**[1] are:

Ages 18-64	Ages 65+
7-9 HOURS of sleep/night	**7-8 HOURS** of sleep/night

But...

1 in 4 adults aged **18-34**

1 in 3 adults aged **35-64***

1 in 4 adults aged **65-79**

are **not** getting **enough sleep**.

*Significant difference between males and females

Let's talk about **sleep quality**, shall we?

1 in 2 adults have **trouble going to sleep** or **staying asleep**.

1 in 5 adults **DO NOT** find their **sleep refreshing**.

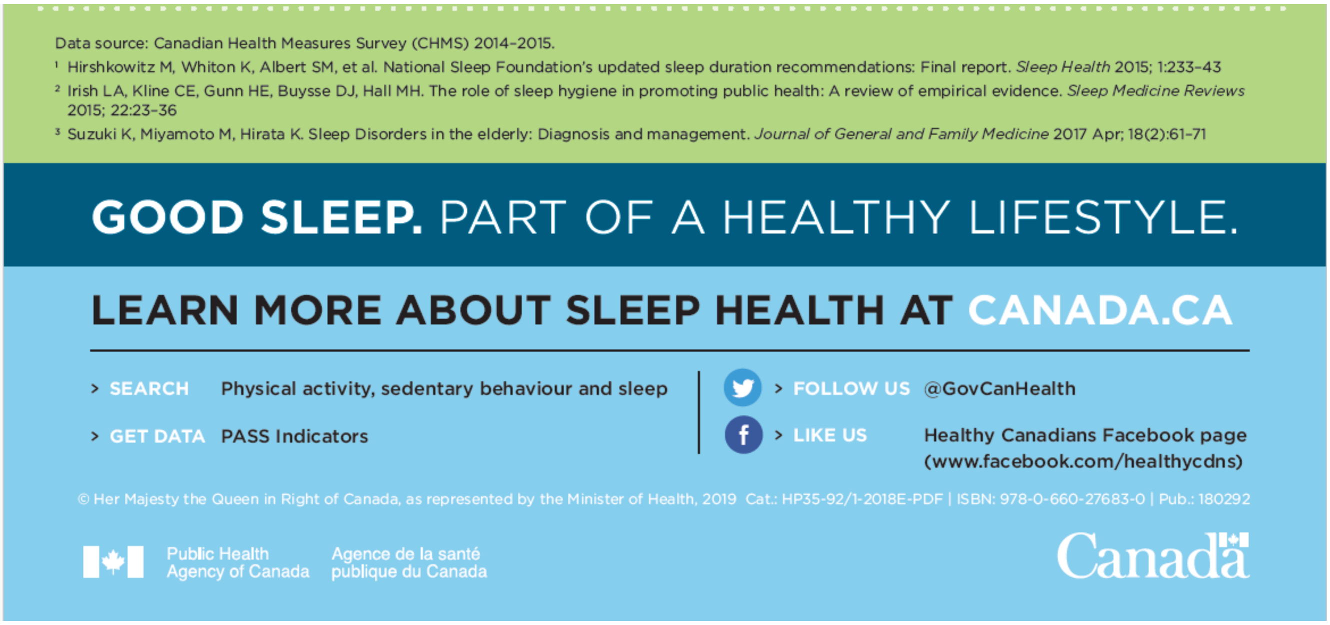
1 in 3 adults have **difficulty staying awake** during waking hours.

A number of factors are related to **insufficient sleep** in adults:

- **MORE SEDENTARY TIME**
  Adults who get **insufficient sleep** report an average of **4.0 hours** of sedentary time a day compared to an average of **3.5 hours** for adults who get **adequate sleep**.
- **CHRONIC STRESS**
  36.3% of adults who get **insufficient sleep** report having chronic stress compared to **23.2%** of adults who get **adequate sleep**.
- **POOR MENTAL HEALTH**
  12.3% of adults who get **insufficient sleep** report having poor mental health compared to **5.8%** of adults who get **adequate sleep**.

Good sleep hygiene could lead to better sleep[2,3]:

- **Avoid alcohol, caffeine, and nicotine before bed**
- **Maintain a regular bedtime/waketime**
- **Practice relaxation and mindfulness-based stress reduction techniques**
- **Reduce noise in the sleeping environment**
- **Restrict naps to 30 minutes**
- **Exercise regularly**
- **Review medications with your physician/pharmacist regularly**



Data source: Canadian Health Measures Survey (CHMS) 2014-2015.

[1] Hirshkowitz M, Whiton K, Albert SM, et al. National Sleep Foundation's updated sleep duration recommendations: Final report. *Sleep Health* 2015; 1:233-43

[2] Irish LA, Kline CE, Gunn HE, Buysse DJ, Hall MH. The role of sleep hygiene in promoting public health: A review of empirical evidence. *Sleep Medicine Reviews* 2015; 22:23-36

[3] Suzuki K, Miyamoto M, Hirata K. Sleep Disorders in the elderly: Diagnosis and management. *Journal of General and Family Medicine* 2017 Apr; 18(2):61-71

GOOD SLEEP. PART OF A HEALTHY LIFESTYLE.

LEARN MORE ABOUT SLEEP HEALTH AT CANADA.CA

> SEARCH Physical activity, sedentary behaviour and sleep

> GET DATA PASS Indicators

> FOLLOW US @GovCanHealth

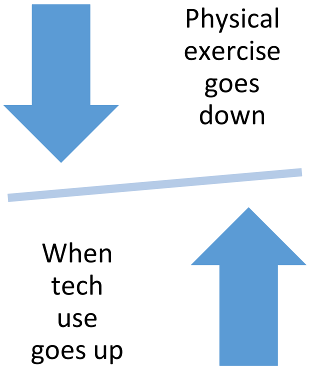
> LIKE US Healthy Canadians Facebook page (www.facebook.com/healthycdns)

Public Health Agency of Canada Agence de la santé publique du Canada

Canada

Lack of physical exercise

Research confirms there is a correlation between the amount Canadians use their digital technology and the amount of physical exercise they get. A correlation is when one thing directly impacts another. In basic terms the correlation here is:



Of course, there are exceptions. Many people use digital apps like pedometers to count their steps or track other kinds of exercise they do, and that tracking can encourage them to increase the amount of activity they get. Some people use smartphones or GPS-devices for outdoor physical activities like geocaching.

But as a rule, the more we use our devices, the less likely we are to get physical exercise and that's a problem. Canadian teens and young adults need a minimum of 60 minutes of physical activity every day to reach and maintain good health. According to the World Health Organization, only 3 in 10 of North American high school students get that much exercise.

- Examples of moderate-intensity physical activity include walking quickly, skating, bike riding and skateboarding.
- Examples of vigorous activity include running, basketball, soccer and cross-country skiing.
- Examples of muscle-strengthening activities include doing push-ups and sit-ups, lifting weights, climbing stairs, and riding a bike.
- Examples of bone-strengthening activities include running, walking, yoga and jumping rope.

4. Complete the following self-assessment from Health Canada to see how your physical activity level measures up.
(*digital Intermediate level*) *Answers will vary.*

Do you complete these activities?	Yes	Not yet
Some exercise for 60 minutes a day		
If yes, what do you do?		
Vigorous activity 3 x a week		
If yes, what do you do?		
Muscle or bone strengthening exercise 3 x a week		
If yes, what do you do?		
More than 2 hours a day online? (outside of school or work)		
If yes, how can you reduce that number?		

5. Define the following terms found in this workout in your own words.
(*digital Intermediate level*)

Ergonomics: ____________________

____

Interactive: ____________________

____

Cyberchondria: ____________________

____

Musculoskeletal: ____________________

____

Decibel: ____________________

____

Precautions: ____________________

____

Correlation: ____________________

____

PPE: ____________________

____

MENTAL HEALTH IS HEALTH

There's a growing awareness that our mental health deserves the same attention as our physical health. And once again, we find that there can be positive and negative effects on our mental health when we use digital tools depending on how and how much we use them.

Digital tools make connecting with family and friends easier and allow us to feel connected to people, even those we don't see often in real life. Being connected makes people feel less lonely or isolated. Digital technology also makes information available to everyone with access to the internet making it easier for people to learn about mental health and seek help.

In the same ways, the impact of social media on mental health is particularly significant. On one hand, it can foster connections, boost self-esteem, and cultivate that sense of belonging. However, it also has the potential to generate considerable stress, create a pressure to compare yourself to others, and contribute to feelings of sadness, isolation and even depression, and be a place where cyberbullying can happen. Using social media mindfully is crucial to managing its effects on mental well-being.

What is cyberbullying?

Cyberbullying is the use of computers, smartphones, or other connected devices to embarrass, hurt, mock, threaten or be mean to someone online. It is a serious problem that affects young people every day. (Government of Canada)

Cyberbulling is real and it's a serious problem.

According to Public Safety Canada, 3 in 10 Canadian teenagers say they have been bullied online. If you are being cyberbullied, remember that you are not alone and there are things you can do to stop it and prevent it from happening again.

- Break off contact: Do not respond.
- Protect yourself: Use privacy settings and change passwords often.
- Get help: Tell someone you trust what happened, whether that's a parent, a teacher, or a friend.

https://www.canada.ca/en/public-safety-canada/campaigns/cyberbullying/cyberbullying-youth/what-to-do-if-you-re-being-cyberbullied.html

FINDING A BALANCE

As we keep saying, digital tools are not "good" or "bad". What matters is the way we use them. The key to managing the impact of technology on physical and mental health is striking a balance between the benefits and negative effects. Here are some great tips from Citizen Advocates (https://citizenadvocates.net) that can help:

1. Set boundaries: Establish limits on screen time, particularly before bed, to improve sleep quality.
2. Unplug: Take regular breaks from technology to reduce stress and improve mental clarity. Find activities that are tech-free such as walking or reading.
3. Practice mindful use: Be intentional about your technology use. Consider setting specific goals for your time spent online, such as only checking e-mail or social media at designated times.

4. Seek out in-person connections: Prioritize face-to-face interactions with friends, family and colleagues. Engage in social activities that do not involve technology.
5. Seek help when needed: If technology use is impacting your mental health, seek support from a mental health professional.

1. Underline the best solution for each example of the negative impact of too much technology. (*digital Intermediate level*)

Can’t sleep	A. Go for a morning walk.
	B. Disconnect from all tech 30 minutes before bed.
Experiencing cyberbullying	A. Tell a responsible adult.
	B. Ignore it; they’ll stop eventually.
Have constant neck pain	A. Try holding your phone higher than your lap.
	B. Stop using earphones.
Are constantly checking your phone	A. Schedule physical activity.
	B. Schedule set times to check messages.
Feeling isolated and depressed	A. Talk to a friend or counsellor in person.
	B. Tell a new friend online how you feel.

2. Read the story of Juno and then complete the table to identify 3 negative impacts she’s experiencing and a possible solution for each. (*digital Intermediate level*)

Juno is a 17-year-old high school student. By day, she tackles endless online classes, messages her friends, and relies on AI-powered study tools. By night, she dives into the virtual world, attending online events and hanging out with friends in virtual spaces.

While it may seem like Juno is thriving in this digital-centric lifestyle, behind the glowing screens, she grapples with feelings of anxiety, loneliness, and the constant pressure to always be "on." She posts to multiple platforms many times every day and constantly refreshes her phone to see if the content is liked or if she’s gained new followers. She experiences constant neck and back pain, her eyes ache, and she rarely gets a good night’s sleep. She panics when there's a lag in her internet connection and feels down when her phone is silent. She scrolls late into the night and keeps her phone under her pillow when she finally falls asleep. It's a struggle for her to maintain her sanity without being glued to her phone.

NEGATIVE IMPACT	POSSIBLE SOLUTION

BUILD YOUR SKILLS FOR SUCCESS!

IN THIS SECTION OF THE WORKBOOK, YOU CAN GIVE YOUR SKILLS A BOOST BY REVIEWING SOME SKILLS FOR SUCCESS BASICS.

DIGITAL

Use the table of contents to navigate through this workbook. Track your progress by putting a checkmark beside each topic you complete.

1. ONLINE PRIVACY AND CYBER SECURITY

PB & J

Just like peanut butter and jam, online privacy and cyber security are good on their own, but so much better when they come together. Used well, privacy and security practices are very effective at preventing intrusions by bad actors into the online worlds of individuals and businesses.

Online privacy refers to your right and responsibility to control how much information is seen, who sees it and how it is seen, when you are connected to the Internet.

Cyber security refers to the protection of digital data stored in electronic devices. It includes the use of best practices for preventing unauthorized access to data and the management of situations in ways that reduce the impacts of unauthorized access.

ONLINE PRIVACY	CYBER SECURITY
Online privacy practices protect your personal data in daily life and at work from individuals and organizations that want to steal your data for criminal purposes. Personal data, also called personal information or personally identifiable information, is any information connected directly to you.	Cyber security practices protect digital data from external threats that are perpetrated on the internet. Effective cyber security practices within organizations help keep personal data secure. Digital data is information presented electronically in a format or language that machines can read and understand.

EXAMPLES OF COMMON CYBERATTACKS AND DATA BREACHES

- Identity theft, fraud, extortion
- Malware, phishing, spamming, spoofing, spyware, trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service attacks (DoS)
- Password sniffing
- System infiltration
- Website defacement
- Instant messaging abuse
- Intellectual property (IP) theft

There are many ways to protect your personal online privacy in daily life and at work, and many ways for individuals like you and for organizations/businesses to prevent cyber security breaches. Some of the most useful practices are described in the lists of tips that follow.

BEST PRACTICES YOU SHOULD USE TO PREVENT PERSONAL DATA BREACHES

- Always use strong passwords.
- Use multi-factor authentication (MFA) whenever possible.
- Never share passwords or login credentials.
- Ensure your social media accounts contain very little personally identifiable information.

- Use anti-virus software.
- Check the security of websites before accessing them. For example, does the address start with https (secure) or http (not secure)?
- Turn off tracking on mobile devices. This increases your level of privacy, but you will see fewer personalized ads and search suggestions.
- Don't open or click on links in texts or emails that come from sources you don't recognize.
- Choose stricter privacy settings when the option exists on a website.
- Check text or email addresses before sending any messages or attachments that contain personal data to avoid accidentally sending to the wrong person or organization.
- Never leave personal private documents, or documents controlled by your employer, visible on a computer screen. They can be copied, read, or photographed by unauthorised persons.

BEST PRACTICES YOUR EMPLOYER MAY USE TO PREVENT CYBER SECURITY BREACHES

- Has a cyber security policy.
- Keeps software and hardware up to date.
- Installs anti-virus and anti-malware software on all computers.
- Keeps anti-virus and anti-malware software up to date.
- Requires multi-factor authentication (MFA).
- Provides privacy and security training to employees.
- Regularly tests employees by sending fake attack emails.
- Manages access to data so only those who need it can see it.
- Doesn't keep any more data than is needed.
- Regularly backs up data.
- Encrypts all data including email.
- Has a cyber-breach response plan in place and update it regularly.

2. A BRIEF HISTORY OF PASSWORDS

History shows you that passwords – in the form of spoken codes, watchwords, or passphrases – have been used for thousands of years to gain access to a place, a group, or an object. Most spoken passwords changed frequently so the information, things, or places they were protecting would be kept safe.

Today, rapidly evolving technology makes it even more important to use passwords and password systems that are up do date and regularly changed. You need to evolve as the technology evolves. The farther you get left behind, the more you're opening yourself up to identity theft or a serious data breach.

While it's interesting to look back and see how we got here, the most important thing to remember is to continue to look forward.

BEFORE COMPUTERS

Spoken passwords have been around since there was spoken language. If you didn't know the password, or secret word, you weren't allowed access. Examples include:
"Open sesame!" (in 1001 Nights by Galland)
"Long live the king!" (in Hamlet by Shakespeare)
"Watchwords" used by armies in ancient Rome and changed daily

The first record of a biometric identification system (one that is specific to parts of a person's body) was in the late 1800s in Paris, France. Alphonse Bertillon developed a method of taking and recording specific body measurements for the classification and comparison of criminals.

Fingerprinting followed in the 1880s and was used both to identify criminals and as a form of legal signature on contracts.

AFTER COMPUTERS

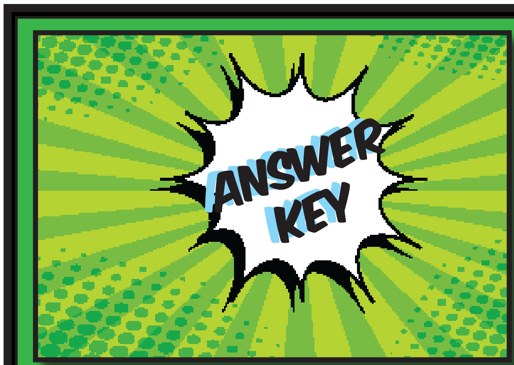
Today, digital passwords, passphrases and other forms of uniquely personal information have evolved to do the same things as early spoken and physical forms.

	PASSWORD EVOLUTION
Passwords	The first recorded use of a digital password was at MIT (the Massachusetts Institute of Technology) in 1961. Basic passwords were usually just a word. Then organizations started to add a number, then special characters, and capital letters.
Passphrases	A passphrase is a password that is composed of a sentence or combination of words, preferably with some special characters and numbers thrown in to make it more complex. A long or randomly constructed passphrase takes much more time to crack than a single password. For example, the website BetterBuys estimates that a randomly constructed password like j9@vAg7$ would take over ten years to crack.
Password Managers	A password manager is not a person. It is a digital tool that stores and retrieves all your passwords in an encrypted cyber vault that can only be opened by your master password, which acts as the decryption key. Without the key, your other passwords remain encrypted and safe from hackers. Password managers can be accessed online through a web platform or on your mobile devices through an app.
MFA	Introduced in the early 2010s, MFA, or multi-factor authentication, is a process that adds another layer of security to your or an employer's devices and accounts. Authentication of your right to access is validated by using a combination of different factors including something you know (e.g., a password), something you have (e.g., a physical token), or something you are (a biometric). MFA requires both a password and the additional verification(s) to access your devices or accounts. Two-factor identification is a type of MFA.

Digital Biometrics

Important dates in biometric digital access (access that uses body parts) include:
1980: the National Institute of Standards and Technology developed a speech group to study and push forward the processes for speech recognition technology.
1991: First use of facial detection technology making real time recognition possible.
1994: The first iris recognition algorithm was patented.
2013: Apple included fingerprint identification to unlock the iPhone, beginning the wide acceptance of biometrics as a means of authentication.
Today, facial and voice recognition, and fingerprints are the most common biometrics used to provide digital access.

Looking to the future, many security experts predict that what we think of as passwords today (combinations of letters, numbers, and symbols) will no longer exist.



ANSWERS FROM THE SFS WORKOUTS!

IN THIS SECTION OF THE WORKBOOK, YOU CAN CHECK YOUR ANSWERS FOR THE SKILLS FOR SUCCESS WORKOUTS YOU COMPLETED!

DIGITAL

Use the table of contents to navigate through this workbook. Track your progress by putting a checkmark beside each topic you complete.

0. MATCHING TASKS AND SKILLS

USE THE ANSWERS BELOW TO CHECK YOUR WORK.

Suggested responses are below. You may have thought of more/other Skills for Success for getting the job done.

Task	Skills Used
Find information online to complete the set-up of a new iPhone	RE, DS, PS
Apply online for a learner's license	RE, WR, PS
Book concert tickets online	DS, RE, PS
Help plan a fundraiser for your sports team	NU, PS, COM, COL, CI
Make a plan to pay for the boots you want when they are more expensive than expected.	PS, NU, RE
Find an alternate way to travel when you can't use the car to go skiing.	COM, COL, CI
Text your coach to say you will be late for practice, why, and how you will catch up on what you miss	DS, WR, PS, COL
Arrive at work early to learn the new customer payment system, from your boss	NU, COL, COM
Use an online transit schedule to get to your new job on time	PS, NU, DS

1. SKILLED TRADES GO DIGITAL

1. Using the information in the Four Industrial Revolutions article, complete the table to better understand what the major changes were in each of the revolutions. Enter a checkmark under the number of the revolution that matches each statement. (*digital Intermediate level*)

INDUSTRIAL REVOLUTION DESCRIPTOR	1st	2nd	3rd	4th
Also called the electricity age		✓		
Significantly changed the textile industry	✓			
Also called the digital age				✓
Began in the middle of the 20th century			✓	
Economy moved from agriculture to industry	✓			
Assembly lines began		✓		
Computer use began			✓	
Machines powered by water and steam	✓			
Evolved from the 3rd revolution				✓
Also called the information age			✓	
Mass production began		✓		
Occurred in 18th and 19th centuries	✓			
Continues to impact trades in the 21st century				✓
Significantly changed the railroad industry		✓		

Skills/Compétences Canda identifies digital as one of the top three Skills for Success needed by both automotive repair technicians and service mechanics, recognizing that vehicles today are more like computers on wheels.

1. In the Task # column of the table, write the numbers of the work tasks that match the digital tools they are most often used for. One is done for you.
(*digital Intermediate level*)

Digital Tool	Task #	Work Task
Word processing	5	1. Take electrical energy readings.
Spreadsheet software	11	2. Complete repairs
Communication software	8	3. Download data designed to regulate a vehicle's operating parameters.
Graphics software	6	4. Access data such as fault codes from onboard computers.
Databases	9	5. Write letters to insurance brokers to present the results of mechanical inspections.
Internet	10	6. Use graphics software incorporated into scan tools to access oscilloscope data displays such as signal values and ignition scope patterns.
Multimetre (can measure multiple electrical properties)	1	7. Take energy readings and troubleshoot faults.
Electronic equipment	4	~~8. Exchange e-mail with other technicians at other locations.~~
Scan tools such as oscilloscopes (displays electrical signals and shows how the signals change over time)	7	9. Retrieve repair information and technical drawings.

Laptops connected to digital logic control modules (programmable controllers that enable machines to perform processes without human intervention)	3	10. Participate in training courses and seminars offered by suppliers and employers.
Computerized equipment such as wheel alignment machines	2	11. Record and track billable hours.

Source: https://www.skillscompetencescanada.com/wp-content/uploads/2021/02/Automove-Service-PDF.pdf

DIGITAL DEVELOPMENTS IN WELDING

1.

Complete the following statements using information from the timeline.
(*digital Intermediate level*)

1. Carbon arc welding runs on electric generators.
2. Stud welding was first used in the shipping industry.
3. In arc welding, the arc moves between two carbon electrodes.
4. There were three important developments in the 1930s: the creation of welding codes, stud welding and submerged arc welding.
5. The first welding torch was developed between 1900 and 1930.
6. Railroad rails are welded using thermite welding.
7. Automatic welding was heavily used by the automotive industry.

2.

Underline the words or phrases in the Digital Developments in Welding article, that answer each question listed below.
(*digital Intermediate level*) Answers are shown as highlighted text.

1. What are the advantages of AR?
2. Why is advanced arc welding so useful?
3. What can welder trainees do when using VR?
4. Why is AR such a valuable training tool?
5. How does AR impact costs and potential risks?
6. What does robotic welding refer to?
7. What is the anticipated impact on manufacturing of the 4th industrial revolution

DIGITAL DEVELOPMENTS IN WELDING

As the timeline shows, the tools used in welding have significantly changed from the first basic hand tools and fire to the introduction of batteries, electrodes, automatic systems, and now digital developments using artificial intelligence (AI). Some of the most recent digital developments are advanced arc welding, augmented reality (AR) and virtual reality (VR), and robotic welding. Brief descriptions of each are below.

Advanced arc welding:

- is corrosion resistant, making it perfect for chemical, nuclear, and toxic welding operations.

Augmented Reality (AR) and Virtual Reality:

- AR makes training more visual, attractive, and educational. It also reduces the cost of materials used in training, moderates risk, and lets educators train more new welders at the same time. AR lets the user enter a real environment, touch and feel a real-life item and "augment" that item into a new shape, realistically changing its appearance. For example, using AR a welding student can take a plastic-based piece and interact with it while it behaves as a carbon steel, stainless steel, or aluminum piece would when it's welded. It's very close to the actual welding experience, so trainees can see and feel a real-world welding environment using real welding equipment, such as a welding mask and welding torches.

- VR takes the user to a 100% computer-generated world where they can pretend to weld. The experience is like that of a video game.

Robotic welding:

- Connects people, machines, and smart technology. It refers to machines equipped with digital technology, including AI, being used alongside highly skilled human welders. Robotic welding is not about a humanoid robot using a blowtorch. It is about the need for Industry 4.0 technology advancement. The 4th industrial revolution will change the way manufacturing production is automated by using smart technologies.

Edited from: https://seaberyat.com/en/welding-technology-trends-2021-beyond/

2. PASSWORDS AND CYBER SECURITY

1. Use the information in the tips to identify what's wrong with each of these passwords. Then update each password to make it stronger.
(digital Intermediate level)

Password	What makes it weak?	Rewrite it so it's stronger. Sample answers shown.
Abcde3456789	*It uses numbers and letters in sequence.*	djFyGi0496745 Random assortment of numbers and letters. Some capitalized.
catschasemice	*It uses words in a sequence that makes sense and passphrases should be at least 4 words and minimum 15 characters.*	micecucUm_bersstacit Used words not usually associated spelled cats backwards at end. Added underscore.
MmFd386QR990	*It doesn't include any symbols.*	Mm_Fd38**6Q%R990 Added underscore, asterisk and percent symbol
X31mypasswordgh3$	*It uses the word password.*	X31nFiugSpodkg3$ Used random letters. Added capitals.

1. Write out the meaning of each abbreviation listed below.
(*digital Basic level*)

ABBREVIATION	MEANING
PIN	*personal identification number*
SMS	*short message service*
MFA	*multi-factor authentication*
OTP	*One-time password*

2. Multi-factor authentication requires you to connect who you are with something you know, and something you have in order to ensure an extra layer of digital security.
Identify each factor listed below as either:

1. Who you are.
2. What you know.
3. What you have.

(*digital Intermediate level*)

FACTOR	#
PIN	2
Fingerprint scanner	1
Hardware token	3
Smart card	3
Security questions	2
Voice recognition	1
SMS authentication	2
Iris scanner	1
Application-based authenticators	3
Facial recognition	1
Passwords and passphrases	2

3. When have you had to use MFA? For banking? For shopping? For work? Other? Name up to three of the situations and describe the steps you have had to take in each case. Haven't used MFA yet? Interview someone who has.
(*digital Intermediate level*) Answers will vary. Sample answers shown.

Situation: Banking

Steps:
Enter user ID and password.
Select either email or text message to receive OTP.
Enter OTP to access account.

Situation: Employer's computer system

Steps:
Enter user ID and password.
Select either email or text message to receive OTP.
Enter OTP to access to account.
Note: Required to change password every 3 months.

Situation: Government website for personal tax information

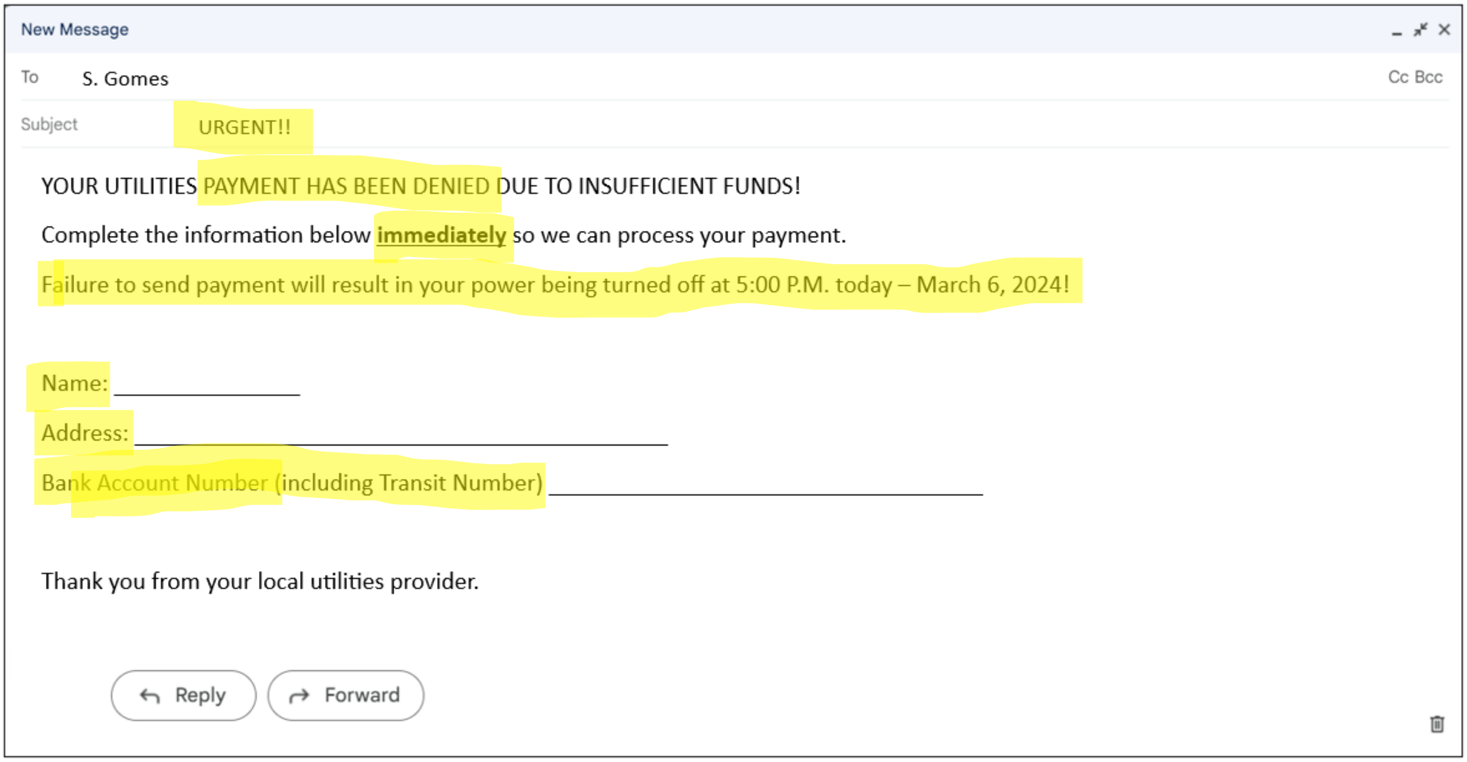
Steps:
Enter user ID and password.
Provide answer to security question.
Choose whether to receive OTP via text or voice.
Enter code to access account.

1. In the scenario below, Martin has been working in manufacturing for a long time but is a new employee at DIGICAN, a manufacturing company that practices a high level of digital security. This is new for Martin and he's already having a hard time with some of the practices. Martin blames the technology and says it's the employer's problem and not his responsibility. Read what happened his first day and highlight anything you think he could have done differently.
(*digital Intermediate level*)

On day 1 Martin was excited to get to know his way around the shop so he was late for his security briefing. By the time he got there the trainer had another meeting and so he gave Martin some written instructions and rescheduled the training for 3 days later. Martin followed the instructions to login to the company system. He created a password (Martin123456) and immediately wrote it down so he wouldn't forget. He wrote it on a post it and stuck it to his workstation. The instructions then said to create an online HR profile. Martin used the same password again, so he'd never forget. While creating his profile, Martin saw there was a new email with the subject line CONGRATULATIONS. He didn't recognize who it was from but that was expected, as he was new and didn't know anyone. He assumed it was a welcome message and clicked on a link in the message which made his screen turn red and locked the computer down. Martin closed the computer, didn't tell anyone, and went to see if he could get fitted for his PPE.

1. In each of the email messages below highlight 3 clues that indicate it might be a phishing attack.
(*digital Intermediate level*)

Any 3 of the possible answers shown.



To S. Gomes

Subject URGENT!!

YOUR UTILITIES PAYMENT HAS BEEN DENIED DUE TO INSUFFICIENT FUNDS!

Complete the information below **immediately** so we can process your payment.

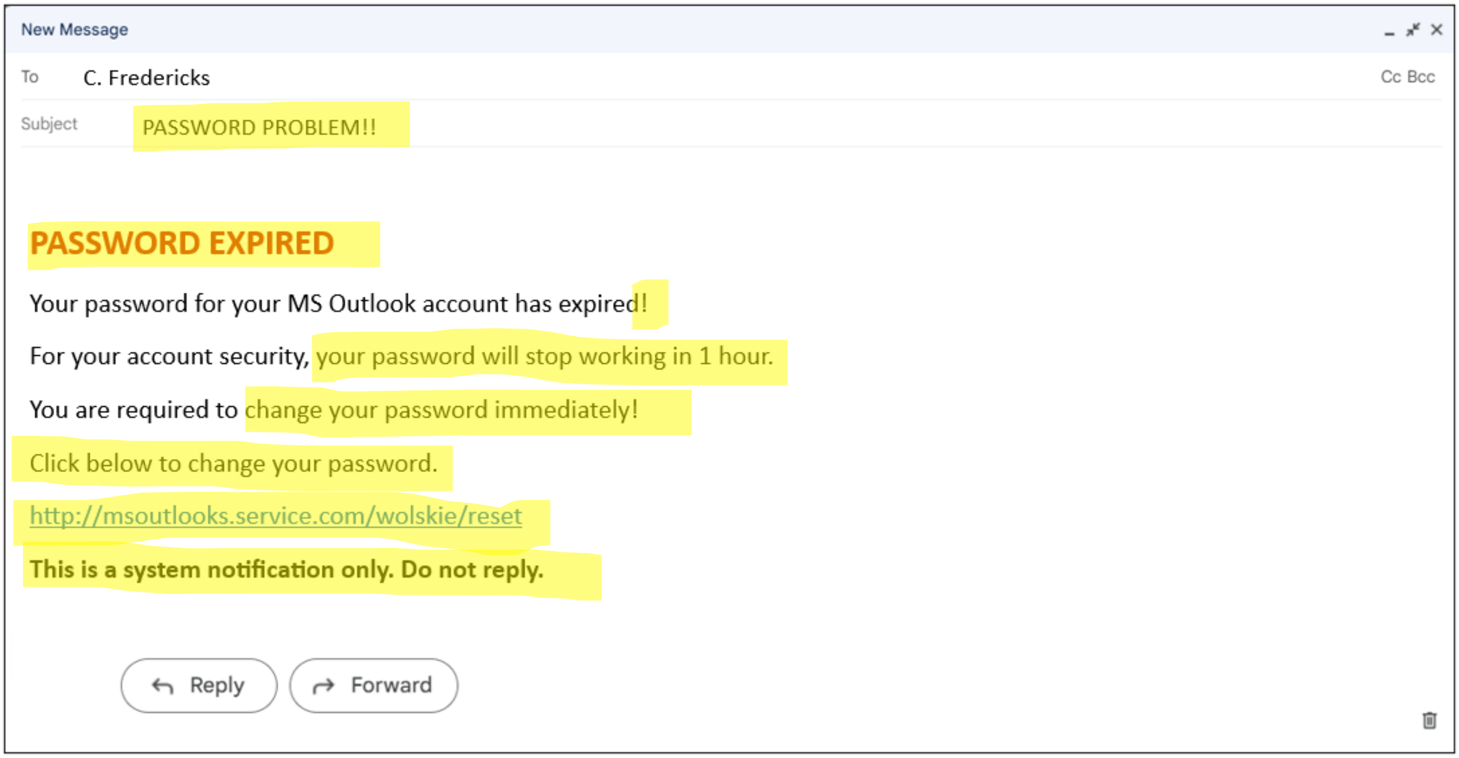
Failure to send payment will result in your power being turned off at 5:00 P.M. today – March 6, 2024!

Name: ______________

Address: ____

Bank Account Number (including Transit Number) ________________________________

Thank you from your local utilities provider.



To C. Fredericks

Subject PASSWORD PROBLEM!!

PASSWORD EXPIRED

Your password for your MS Outlook account has expired!

For your account security, your password will stop working in 1 hour.

You are required to change your password immediately!

Click below to change your password.

http://msoutlooks.service.com/wolskie/reset

This is a system notification only. Do not reply.

3. SOCIAL MEDIA SMARTS

1. Use the information from both situations to complete the table.
(digital Intermediate level) Answers should be similar to those shown.

	Football player	Chrysler contractor
What social media platform did they use?	Twitter (X)	Twitter (X)
What type of media did they post? (video, comment, etc.)	tweet	tweet
What did people who saw the post think was wrong?	Used homophobic language.	Used obscene language.
What happened to the person who did the posting?	Reputation was damaged.	Lost their job.
What could each person tweeting have done to avoid the problem.	Cleaned up his social media before he started college.	Checked to be sure he was posting to the correct account and not used an obscenity.
Do you think the reaction to the football player's tweet was fair? Why or why not? Answers will vary.		
Do you think the reaction to the contractor's tweet was fair? Why or why not? Answers will vary.		

2. Review the list of popular online platforms below and put a √ beside each one you use. Add any others that are not in the list in the blank rows. Then fill in the remaining columns for the ones you selected.
(*digital Basic level*) *Answers will vary. Example shown.*

Platform	✓ if you use	# times a week you post something	# times a week you comment on or share someone else's information
Facebook	√	3	2
Instagram	√	6	5
Twitter / X	√	5	8
YouTube			
LinkedIn	√	1	3
Snapchat			
TikTok			
Total posts/comments/shares per week		15	18
Total posts/comments/shares per year		780	936
Total number of pieces of information shared between grade 8 and graduation		3,900	4,680

1. Understanding how privacy works online, and regularly checking your settings, are two of the most important things you can do to keep your identity safe.
Mark each statement below as true or false. If the statement is false, rewrite it so that it is true. (The first one is done for you.)
(digital Intermediate level) Answers will vary. Examples shown.

Privacy settings provide total protection. TRUE **FALSE** *Privacy settings do not provide total protection.*
Sharing personal information online, like your address, is safe. TRUE **FALSE** *It is not safe to share personal information like your address online.*
Privacy settings can be changed. **TRUE** FALSE
Privacy settings are a good way to keep information private. **TRUE** FALSE
Public means everyone on the social media site can see what you post. **TRUE** FALSE
Logging in to one app from another is fast and safe. TRUE **FALSE** *It may be fast, but it is not safe to login to one app from another.*
Once you read a privacy policy you don't need to read any updates. TRUE **FALSE** *You need to read privacy policy updates.*
Privacy settings cost extra. TRUE **FALSE** *Privacy settings do not cost extra.*

1. So, exactly what does this policy mean? To ensure you understand what they're saying match the synonyms to the words from the article.
 (*digital Intermediate level*)

FROM THE ARTICLE	SYNONYMS
Wild card	Something unpredictable
Post-secondary institutions	Colleges and Universities
Case-by-case	Individually
Assess	Evaluate
Criteria	Standards

2. Complete each sentence with "does" or "doesn't" to make it true.
(*digital Intermediate level*)

The university doesn't check applicant's social media.

The university does check enrolled students' social media.

The university does believe students are responsible for what they post.

The university doesn't treat every case the same.

4. ONLINE MONEY SENSE

1. Fill in the blanks so the sentences make sense.
(*digital Intermediate level*)

In a __fraud__, a hacker __steals___ information, usually __financial___.

In a ___scam___, you are usually ___tricked___ into giving ____personal___ information.

1. Using the information you just read, put an X in the columns to match each technique with the type of scam it's used in most often. Note, different scams may use the same techniques. (*digital Intermediate level*)

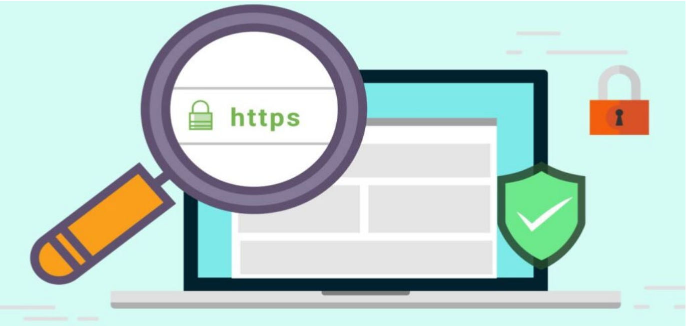
TECHNIQUE	ROMANCE	EMPLOYMENT	SHOPPING
Gains your trust	X	X	
Too good to be true		X	
Send fake money transfer			X
Requests personal ID		X	
Urgent	X	X	
Don't send what was promised			X
Makes you feel important		X	
Unusual payment type			X
First contact is through social media	X		

2.

Based on the information in the text box, which of the listed images or words when displayed on a website tell you it's safe to shop there with your credit card? Check all that apply.
(*digital Intermediate level*)

Safe website shopping

1. A green checkmark
2. The word secure
3. The word buysafe
4. A lock symbol
5. A red checkmark
6. The word http
7. The word ccsafe
8. The word https
9. The word safe
10. The word SSL



Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed. You'll know if the site has SSL because the URL for the site will start with HTTP**S**—instead of just HTTP. An icon of a locked padlock will also appear, typically to the left of the URL in the address bar or the status bar down below; it depends on your browser. HTTPS is standard now even on non-shopping sites, enough that Google Chrome flags any page without the **S** as "not secure."

1.

Read each scenario and identify at least 3 clues in each of them that should have helped the victim recognize the situation as a scam. Write your answers in the spaces provided. (digital Intermediate level) Answers will vary. Sample answers shown.

Scenario 1

At the last minute, Karrie wanted to by two tickets to a weekend summer music festival that the official website said was sold out. She found someone online that had two available for $150 each. She thought that was a really good deal and agreed to send $300 via PayPal. The seller said he preferred gift cards because he'd been scammed before and now knew it was "safer" than PayPal. He also said he was really sorry he couldn't go but he urgently needed to sell the tickets so couldn't hold them while she decided. Karrie thought it was strange, but the guy seemed nice so agreed and bought three $100 gift cards online and sent him the information. The cards were redeemed and then he instantly blocked her on Facebook. No tickets, no refunds, and no way to find him.

List at least 3 clues

Seller said they needed to sell right away - sense of urgency

Was asked to make a payment in a specific way

Unofficial reseller

Scenario 2

Devrin had just started their first real job out of school and wanted to buy their parents a present to thank them for their help over the years. Devrin knew the family BBQ was getting older so had been looking for a deal online. They found a website that was offering brand name BBQs at ridiculously low prices. The site said they were a new business, and the low prices were part of their opening specials so was a "limited time offer". The only condition was you had to apply for and pay for it on the company credit. The card rate was very competitive at only 2.9%. Devrin did an online search for the company and couldn't find any bad reviews so went ahead and signed up for the card on the company website and used it to pay for the BBQ. A week later they received an email saying that due to supply chain issues the BBQ was delayed, but as it was not the company's responsibility, they were sorry but there could be no refund. Devrin immediately went back to the company website, but it was gone. And, as the BBQ never arrived, so was their money.

List at least 3 clues

Price too good to be true

Limited time offer - sense of urgency

Was asked to make a payment is a specific way

Scenario 3

Alix met her partner Seamus through Facebook. They texted and chatted online for several months, and the relationship became more serious over time. Seamus said he was based in Ireland, but he was ready move to Canada to see where the relationship could go. He sent his flight information to Alix and told her he'd already shipped his things. The day of the flight Alix got a call from a customs agent saying the shipment had arrived but there were funds owing. Customs had tried to reach Seamus but of course couldn't as he was in transit. Alix's number was on the shipment as the Canadian contact, so they tried her. Customs explained if the funds weren't paid immediately, they would be returned to Ireland at Seamus' cost. Alix wanted to help so paid the balance owing by wire transfer as instructed in the amount of $3,355.99. She had loaned Seamus small amounts of money before which he'd always paid back so wasn't worried.

When Alix arrived at the airport that evening to meet Seamus, he didn't show up. When she tried to text him, there was no answer and his Facebook profile disappeared. After a few days Alix realized she'd been scammed. She asked her bank to recall the payment, but the money had already been moved and they were unsuccessful.

List at least 3 clues

Call from Customs – unexpected contact (also, Customs never calls)

Immediate payment required – sense of urgency

Previous requests for money

Gained her trust

1. Check all the statements that apply.
(*digital Intermediate level*)

SCAMS WORK BECAUSE:	√
People are stupid	
People want to get a good deal	√
People use cellphones	
Scammers are smart	√
People like to feel special	√
People don't get enough email	
Scammers know how to manipulate people	√

2. Mark the statements below as true or false.
(*digital Intermediate level*)

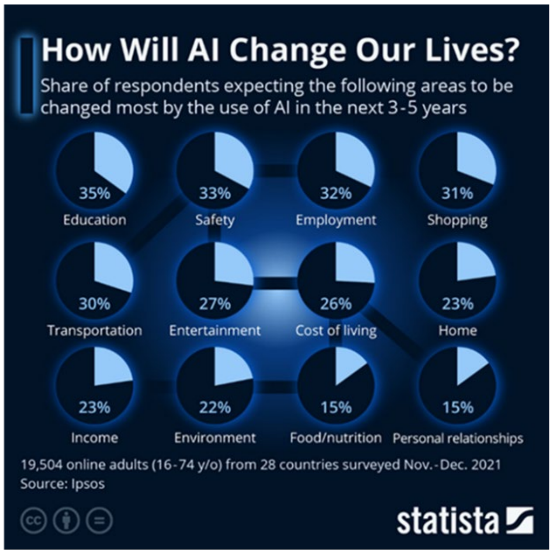
STATEMENT	TRUE	FALSE
Typical attention spans are 8 minutes.		√
FOMO is a real cause of scams.	√	
Any aged person using the internet can be scammed.	√	
Psychological manipulation doesn't work.		√
Some people are scammed because they are lonely.	√	
Only 7% of email scams are urgent.		√
Some people are scammed because they think they're smarter than other people.	√	

1. Match the type of payment used with where you should report it if you are ever scammed. (*digital Intermediate level*)

Payment type	Report scam to…
Money transfer app	the app owner
Credit card	your bank
Wire transfer	your bank
Gift card	the company
Cryptocurrency	the exchange

5. USING AI

1. This chart shows which areas of life consumers around the world expected to change the most due to the increased use of AI between 2021 and 2026. Use the information in the chart to answer the questions.
(digital Intermediate level)



What is the area where most people think there will be the greatest change?

Education

What is the area where you think there will be the greatest change? Provide a reason for your answer.

Answers will vary

What is the area where most people think there will be the least change?

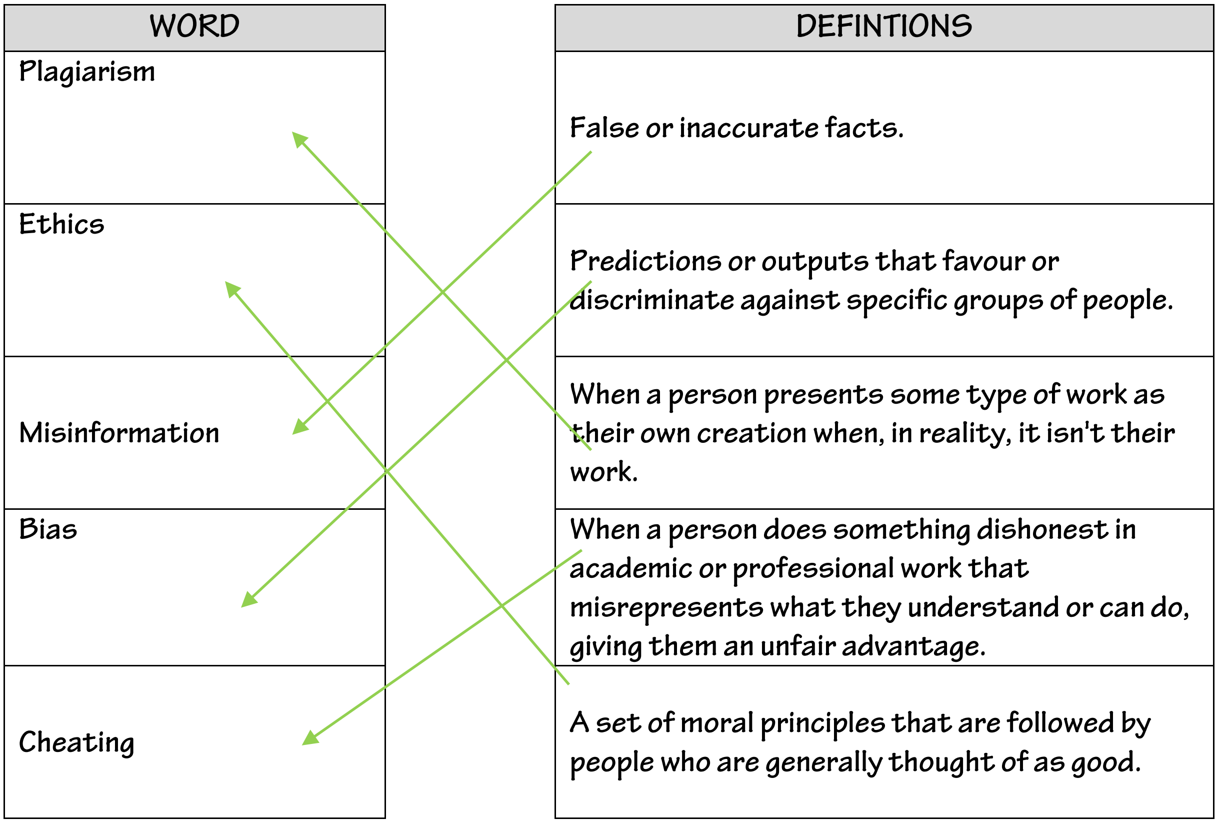
Food/Nutrition and Personal Relationships

What is the area where you think there will be the least change? Provide a reason for your answer.

Answers will vary

2.

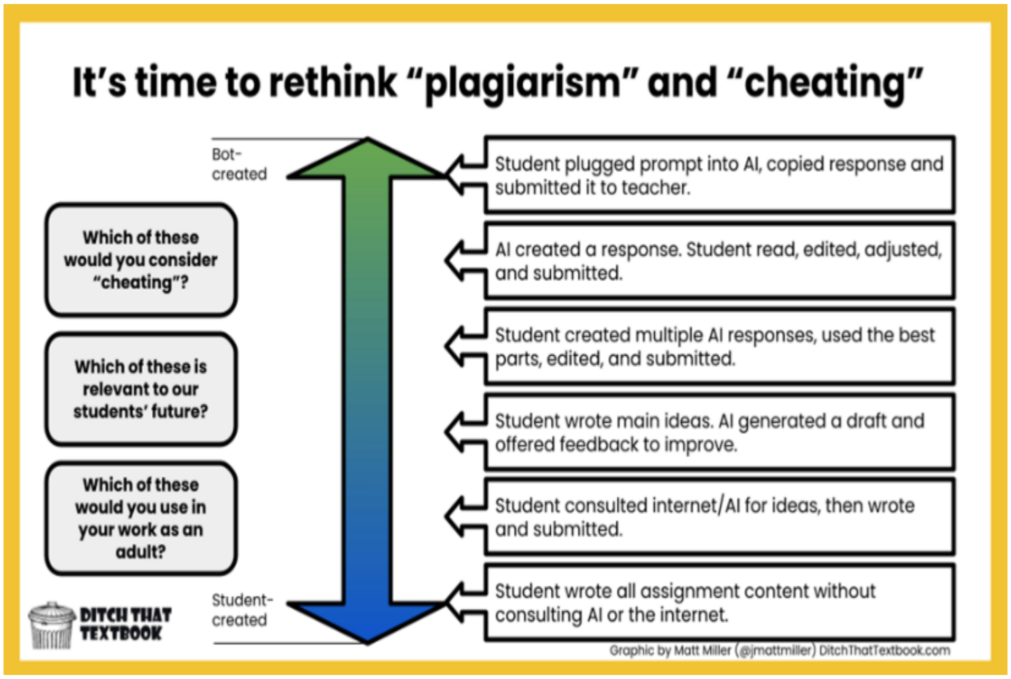
It's important to know what different words mean in the context of AI. In the table on the next page, match each word with what you think is the best definition, by drawing a line between them.
(*digital Intermediate level*)



WORD	DEFINTIONS
Plagiarism	False or inaccurate facts.
Ethics	Predictions or outputs that favour or discriminate against specific groups of people.
Misinformation	When a person presents some type of work as their own creation when, in reality, it isn't their work.
Bias	When a person does something dishonest in academic or professional work that misrepresents what they understand or can do, giving them an unfair advantage.
Cheating	A set of moral principles that are followed by people who are generally thought of as good.

3.

Look at the graphic on the next page created for teachers about how students use AI like ChatGPT. Which of the actions on the right do you think are cheating?
(*digital Intermediate level*) *Answers will vary. Sample answer provided.*



It's time to rethink "plagiarism" and "cheating"

Bot-created

Which of these would you consider "cheating"?

Which of these is relevant to our students' future?

Which of these would you use in your work as an adult?

- Student plugged prompt into AI, copied response and submitted it to teacher.
- AI created a response. Student read, edited, adjusted, and submitted.
- Student created multiple AI responses, used the best parts, edited, and submitted.
- Student wrote main ideas. AI generated a draft and offered feedback to improve.
- Student consulted internet/AI for ideas, then wrote and submitted.
- Student wrote all assignment content without consulting AI or the internet.

Student-created

DITCH THAT TEXTBOOK

Graphic by Matt Miller (@jmattmiller) DitchThatTextbook.com

https://ditchthattextbook.com/ai/

Sample answer

Perhaps only the first in the list of actions, in which the student took what AI presented, copied it verbatim and handed it in as their own work, would be considered cheating. In all the other actions the student interacted with the text to understand and revise it or chose not to use AI.

4. Write 3 simple rules you think would be useful for helping students understand when they can use ChatGPT and for making sure it is used ethically.
(*digital Intermediate level*) *Answers will vary. Sample answers provided.*

1. Use it to improve your work, not create it.
2. Use it to check grammar and spelling.
3. Use it to provide good examples.
4. If you think you have used it too much, you are probably right.
5. Don't believe everything it writes is true.

6. *Make sure you can answer questions about what ChatGPT has written for you.*

5.

Consider this real-life use of AI reported in Toronto Life Magazine and answer the questions that follow.
(*digital Intermediate level*)

What digital tool did the student use in addition to ChatGPT?

Databases

What did the student write into ChatGPT?

A description of the soil sample.

What is the mistake ChatGPT corrected?

The date of the tar layer was from the 1950s not the 1970s.

Do you think the student was cheating or did they use ChatGPT ethically? Include a reason to support your answer. (*Answers will vary.*)

1.

Answer the 3 questions below.
(*digital Intermediate level*)

What is the most significant difference between automation and AI?

Automation can only repeat tasks it is programmed to do. AI can be programmed to detect when things are going wrong, figure out how to fix things, learn from those experiences and improve their function.

Based on the information in the article, write down one benefit of using AI in each of the sectors listed.

- Manufacturing: *increase safety or reduce costs*

- Construction: *improve efficiency or reduce costs*
- Agriculture: *help farmers better plan or improve crop yield*

What will the new warehouse robot be able to do that current robots can't?

Move around the factory.

6. DIGITAL HEALTH

1.

Read the article on the next page, Limiting the Risks of Self Diagnosis, about the possible downsides of relying on the internet for health information and then use the words in the bubbles to complete the statements.
(digital Intermediate level)

1. Look for websites that are *moderated* by health or government agencies.
2. A misdiagnosis can *delay* getting proper treatment.
3. Many serious diseases can have *mundane* symptoms.
4. *Misinformation* is a common problem when getting health information from social media sites.
5. Only use the internet to *diagnose* mild health conditions.

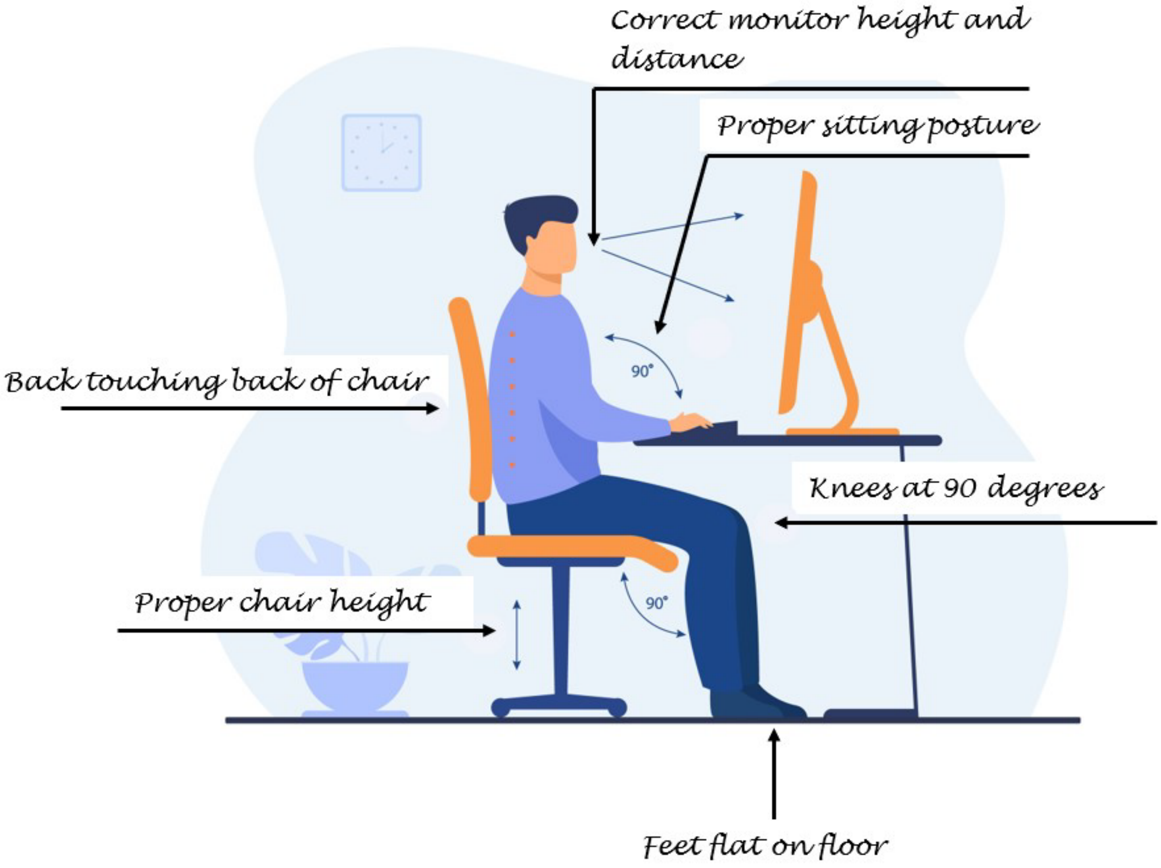
2.

For each of the risks listed in the table, identify at least one action you can take to reduce the risk.
(digital Intermediate level) Answers should be similar to those in the answer key.

RISK	ACTION
Following inaccurate information	*Check website authors/owners.* *Look for reliable organizations.*
Loss of personal information	*Don't enter information into health websites.* *Don't subscribe.*

Increasing your anxiety level	Limit the number of websites you look at. Only look at reliable sites. Consult a medical practitioner.
Delay in getting the medical care you need	Use internet searches for minor ailments only. Consult a medical practitioner.
Wasting time and money on false cures	Only look at reliable sites.

1. Use information from the Let's Get Physical article to label the image to show which ergonomic precautions the person is taking to prevent musculoskeletal and eye strain issues. (*digital Intermediate level*)



2.

Use the information in the noise levels diagram on the next page to answer the questions. (*digital Intermediate level*)

1. What is the difference in decibels between hearing landscaping equipment outside or from inside a house? 35
2. Does taking a flight potentially harm your hearing? Circle your answer. [✓ YES] NO
3. What is the threshold for safe sounds? 70
4. How many dBs above the safe level is a hair dryer? 20
5. Other than a plane, what is the loudest transportation noise? Siren
6. What's the difference in decibels between a powered hand dryer and hair dryer? 10

3.

In addition to managing your digital devices, there are other things you can do to improve your sleep quality. Use the information you just read and the infographic from Public Health Canada, on the next page, to answer the questions. (*digital Intermediate level*)

1. What percentage of adults under the age of 35 are not getting enough sleep? 25%
2. What percentage of adults have trouble staying asleep? 50%
3. What percentage of adults might fall asleep during the day? 33%
4. For your age, how many hours of sleep should you get each night? 7 to 9 hours
5. How many hours sleep do you get? __________ *Answers will vary.*
6. If you get fewer than the recommended number, identify 2 changes you could make. *Answers will vary.*

5.

Define the following terms in your own words.
(digital Intermediate level) Answers should be similar

Ergonomics:

the study of people in their working environment

Interactive:

when two or more things work together

Cyberchondria:

a type of anxiety order related to searching illnesses on the internet

Musculoskeletal:

referring to muscles and bones

Decibel:

a unit of measurement for sound

Precautions:

actions taken to prevent problems or injuries

Correlation:

when one thing directly impacts another

PPE:

personal protection equipment

1. Underline the best solution for each example of the negative impact of too much technology. (*digital Intermediate level*)

Can't sleep	A. Go for a morning walk.
	B. Disconnect from all tech 30 minutes before bed.
Experiencing cyberbullying	A. Tell a responsible adult.
	B. Ignore it; they'll stop eventually.
Have constant neck pain	A. Try holding your phone higher than your lap.
	B. Stop using earphones.
Are constantly checking your phone	A. Schedule physical activity.
	B. Schedule set times to check messages.
Feeling isolated and depressed	A. Talk to a friend or counsellor in person.
	B. Tell a new friend online how you feel.

2. Read the story of Juno and then complete the table to identify 3 negative impacts she's experiencing and a possible solution for each. (*digital Intermediate level*) *Answers will vary. Sample answers shown.*

NEGATIVE IMPACT	POSSIBLE SOLUTION
feelings of anxiety, loneliness, and the constant pressure to always be "on."	*Spend more time with people in real life.* *Schedule breaks from her phone.* *Talk with a mental health professional.*
rarely gets a good night's sleep	*Remove the phone from under her pillow.* *Leave the phone out of the bedroom.* *Do something off-screen before bed.*

experiences constant neck and back pain, her eyes ache	Review ergonomic tips for posture and reducing eyestrain. Take mini breaks from sitting and being on-screen

SKILLS FOR SUCCESS
WORK READY YOUTH PROGRAM

SFS ASSESSMENT!

DIGITAL

Use the table of contents to navigate through this workbook. Track your progress by putting a checkmark beside each topic you complete.

1. DIGITAL SKILL TESTING QUESTIONS

TRY THE 14 QUESTIONS BELOW THEN CHECK THE ANSWER KEY TO SEE HOW WELL YOU DID.

1. According to this description, which statement is correct?

Japan and the European Commission have identified a possible 5th revolution focussed not just on digital technology, but on how that technology can be used to improve society. For workers, Industry 5.0 means letting automation and robots do repetitive tasks while freeing them to do other things.

During Industry 5.0:

a) Robots will replace all workers.
b) Robots will make workers' jobs more interesting.
c) Workers will replace some robots.

2. Match the work tasks with the digital tools they are most often used for by writing the number of the task beside the correct tool.

DIGITAL TOOL	TASK #
Databases	
Communication software	
Word processing	
Spreadsheet software	
Internet	

TASKS

1. Complete safety report.
2. Compare materials costs with different suppliers.
3. Calculate impact of 15% increase in materials.
4. Inform supervisor you're running late.
5. Check product availability.

3. In the context of digital tools and processes, MFA stands for:

a) Multi-factor access
b) Multi-factor authentication
c) Multi-factor admission

4. What are the 3 factors most often used in MFA?

a) Who you are, what you want, what you know
b) What you know, what you have, where you are
c) What you have, what you know, what you are

5. Mark each statement as true or false.

a) Privacy settings provide total protection. T F
b) Sharing passwords when working on the same project is safe. T F
c) Emails marked "important" are always safe. T F

6. Which type of scam could this be?

Marc receives a message via FB in response to a post they shared about a new tech start-up launching in Montreal. The sender says they work for the company and thank Marc for sharing the post. They then invite Marc to click on a link to sign up to be included in the first round of interviews which means Marc would get an interview before anyone else.

a) Shopping
b) Employment
c) Romance

7. If you think you've been the victim of a phishing scam at work, what is the first thing you should do?

a) Turn off your computer.
b) Delete the email.
c) Tell your supervisor.

8. Check √ all devices and applications that use AI.

Electric drill	
Laser welder	
Safety vest	
GPS	
Smartphone	
Eye wash station	

9. It's important to know what different words mean in the context of AI. Match each word in the table with what you think is the best definition, by drawing a line between them.

WORD
Plagiarism
Ethics
Misinformation
Bias
Cheating

DEFINITIONS
False or inaccurate facts.
Predictions or outputs that favour or discriminate against specific groups of people.
When a person presents some type of work as their own creation when, in reality, it isn't their work.
When a person does something dishonest in academic or professional work that misrepresents what they understand or can do, giving them an unfair advantage.
A set of moral principles that are followed by people who are generally thought of as good.

10. Why is MFA useful?

a) It makes it safe to share passwords.
b) It makes it easier to log in.
c) It adds another layer of digital protection.

11. Ergonomics is:

a) the study of the ego
b) the study of peoples' physical working environment
c) the natural laws of physical work

12.

Check √ all the suggestions that can help you avoid discomfort or injury from working with digital technology.

Sit with your knees at a 90-degree angle.	
Always use your thumbs to type messages on your phone.	
Hold your phone in your lap when texting.	
Take regular short breaks from screens.	
Set your monitor up so the top is at eye level.	
Keep lighting bright.	

13.

Cyberchondria is:

a) A fear of cyborgs

b) A fear of serious illness based on internet searches of symptoms

c) A reasonably reliable way to determine if you have a cold or the flu

14.

Match each example of a possible negative impact of too much technology with an effective strategy to reduce the impact.

EXAMPLE	STRATEGY #
Experiencing cyber bullying	
Neck hurts	
Can't sleep	
Feeling isolated	

1. Stop screen time 30 minutes before bed.
2. Plan an activity with a trusted friend in person.
3. Monitor how you are holding your phone.
4. Tell an adult you trust.

2. DIGITAL
SKILL TESTING QUESTIONS
ANSWER KEY

HOW DID YOU DO ON THE 11 QUESTIONS?

1. According to this description, which statement is correct?

Japan and the European Commission have identified a possible 5th revolution focussed not just on digital technology, but on how that technology can be used to improve society. For workers, Industry 5.0 means letting automation and robots do repetitive tasks while freeing them to do other things.

During Industry 5.0:

b) Robots will make workers' jobs more interesting.

Digital – Intermediate Level

2. Match the work tasks with the digital tools they are most often used for by writing the number of the task beside the correct tool.

DIGITAL TOOL	TASK #
Databases	*2 or 3*
Communication software	*4*
Word processing	*1*
Spreadsheet software	*2 or 3*
Internet	*2 or 5*

TASKS

1. Complete safety report
2. Compare materials costs with different suppliers
3. Calculate impact of 15% increase in materials
4. Inform supervisor you're running late
5. Check product availability

Digital – Intermediate Level

3. In the context of digital tools and processes, MFA stands for:

b) Multi-factor authentication

Digital – Intermediate Level

4. What are the 3 factors most often used in MFA?

c) What you have, what you know, what you are

Digital – Intermediate Level

5. Mark each statement as true or false.

a) Privacy settings provide total protection. T [✓ *F*]

b) Sharing passwords when working on the same project is safe. T [✓ *F*]

c) Emails marked "important" are always safe. T [✓ *F*]

Digital – Intermediate Level

6. Which type of scam could this be?

Marc receives a message via FB in response to a post they shared about a new tech start-up launching in Montreal. The sender says they work for the company and thank Marc for sharing the post. They then invite Marc to click on a link to sign up to be included in the first round of interviews which means Marc would get an interview before anyone else.

b) Employment

Digital – Intermediate Level

7. If you think you've been the victim of a phishing scam at work, what is the first thing you should do?

c) Tell your supervisor.

Digital – Intermediate Level

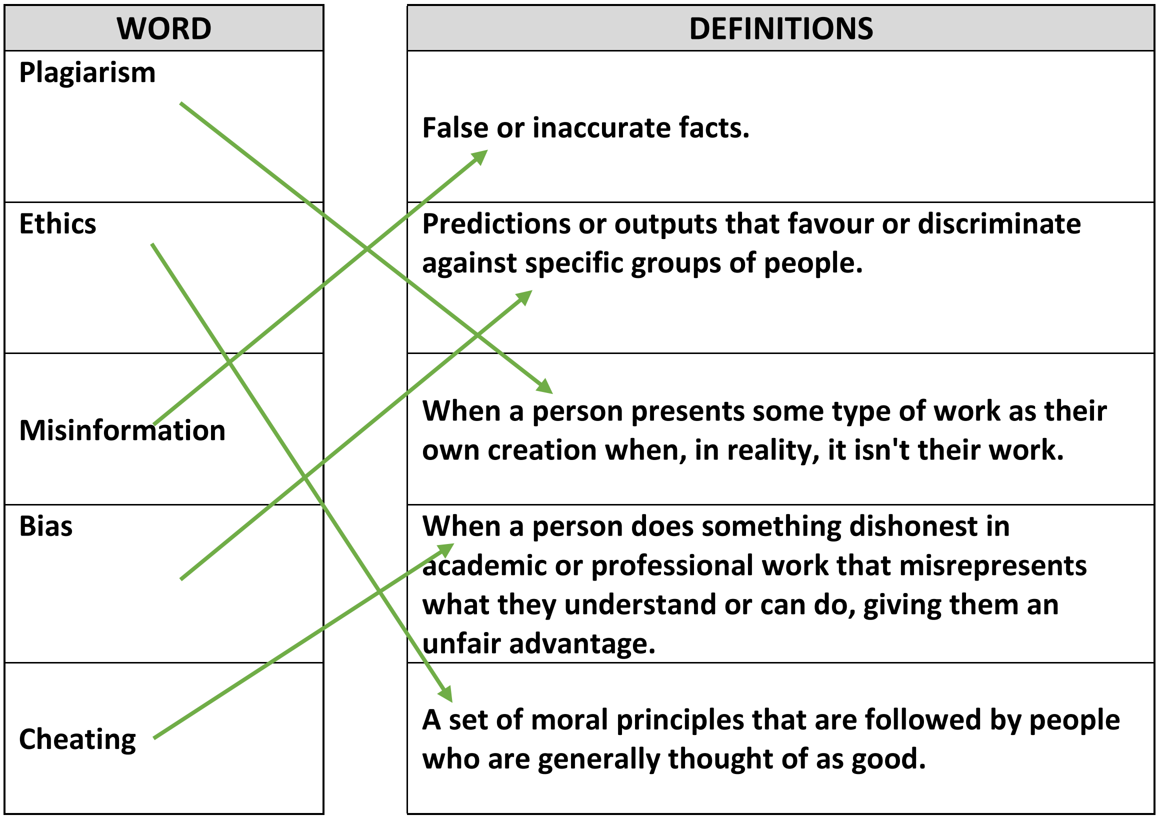
8. Check √ all devices and applications that use AI.

Electric drill	
Laser welder	√
Safety vest	
GPS	√
Smartphone	√
Eye wash station	

Digital – Intermediate Level

9. It's important to know what different words mean in the context of AI. Match each word in the table with what you think is the best definition, by drawing a line between them.

Digital – Intermediate Level



WORD
Plagiarism
Ethics
Misinformation
Bias
Cheating

DEFINITIONS
False or inaccurate facts.
Predictions or outputs that favour or discriminate against specific groups of people.
When a person presents some type of work as their own creation when, in reality, it isn't their work.
When a person does something dishonest in academic or professional work that misrepresents what they understand or can do, giving them an unfair advantage.
A set of moral principles that are followed by people who are generally thought of as good.

10. Why is MFA useful?

c) It adds another layer of digital protection.

Digital – Intermediate Level

11. Ergonomics is:

b) the study of peoples' physical working environment

Digital – Intermediate Level

12. Check √ all the suggestions that can help you avoid discomfort or injury from working with digital technology.

Digital – Intermediate Level

Sit with your knees at a 90-degree angle.	√
Always use your thumbs to type messages on your phone.	
Hold your phone in your lap when texting.	
Take regular short breaks from screens.	√
Set your monitor up so the top is at eye level.	√
Keep lighting bright.	

13. Cyberchondria is:

b) A fear of serious illness based on internet searches of symptoms.

Digital – Intermediate Level

14. Match each example of a possible negative impact of too much technology with an effective strategy to reduce the impact.

Digital – Intermediate Level

EXAMPLE	STRATEGY #
Experiencing cyber bullying	4
Neck hurts	3
Can't sleep	1
Feeling isolated	2

1. Stop screen time 30 minutes before bed.
2. Plan an activity with a trusted friend in person.
3. Monitor how you are holding your phone.
4. Tell an adult you trust.

How did you do?

Enter the number of answers that you got correct. ________/14

11 -14 correct: Good work! You've mastered the fundamentals, and your skills might be quite quickly increased with practice.

8 - 10 correct: Keep at it! Your skills need to be improved, but some of the fundamentals are in place. It might be possible to improve reasonably quickly.

<7: Your skills definitely need practice.