



Cybersecurity best practices guide



St. Lawrence
CEGEP CHAMPLAIN



Table of contents

- Introduction**..... 4
- Acknowledgment**..... 4
- Attackers and cybersecurity** 5
 - Types of attackers 5
 - Cyberattacks 5
- Phishing**..... 7
 - How do I identify a phishing email?..... 7
 - How can I protect myself from phishing? 8
- Ransomware** 10
 - The phases of an attack..... 10
 - Methods of infection 10
 - Consequences 11
- Social engineering**..... 12
 - Understanding Social Engineering..... 12
 - Recognizing a Social Engineering Attack 12
 - Avoid the pitfalls of social engineering 14
- Teleworking: A new era**..... 15
 - The risks of remote work..... 15
 - Advice on how to work remotely 15
- Password management** 17
 - Bad habits 17
 - How to better protect yourself..... 17
- Multi-factor authentication**..... 20
 - What is Multi-Factor Authentication (MFA)? 20
 - Best practices..... 21
- Mobile device usage and device security** 22

- Security tips for all devices 22
- Malware**..... 24
 - Types of malware 24
 - Common methods of infection 25
 - Signs of infection 25
 - What to do in case of infection 25
 - How can I protect myself from malware? 26
- Network security** 27
 - Connectivity and network type 27
 - Public Wi-Fi networks 27
 - Firewall 28
 - Best practices 28
- Information security** 29
 - Information classification and confidentiality 29
 - Personal information 29
 - Secure information handling 29
 - Threat to the security of information 30
 - Information security management strategy 30
- References** 32

Introduction

In our increasingly connected world, information security is paramount. While technology opens up many opportunities, it does not always guarantee security. As cyber threats increase in volume and sophistication, and as technology becomes indispensable to meeting the needs of individuals and society as a whole, it is imperative to strengthen cyber security and its reliability.

Information security is both a collective and individual responsibility, based on the recognition and implementation of a set of rights and responsibilities. It is also an organizational obligation, in accordance with the directives of the *Ministère de la Cybersécurité et du Numérique (MCN)*.

This Cybersecurity Best Practices Guide has been designed to provide you with the knowledge and tools you need to understand and face digital threats. It is intended to be read by all College employees in order to strengthen our security posture and protect our sensitive information. As you read through these pages, you'll learn about the different types of attacks we may face and best practices for preventing and responding to them.

Together, we can strengthen our digital defenses and ensure the security of our day-to-day operations. Thank you for taking the time to read and put the recommendations in this guide into practice.

Acknowledgment

The College would like to extend its gratitude to the Cégep de Saint-Jérôme for sharing its reference document, which contributed to the creation of this guide.

Attackers and cybersecurity

In the complex world of information security, there are many different actors and types of attacks that contribute to the growing complexity of online threats.

Types of attackers

Cybercriminals

- Motivated by financial gain
- Seeking to exploit system vulnerabilities to steal sensitive information or extort money

Insiders

- Can be employees or subcontractors
- Use their privileged access to compromise security and gain access to confidential data

State actors

- Hackers
- Hired by governments to target other nations in political or economic conflicts

Other

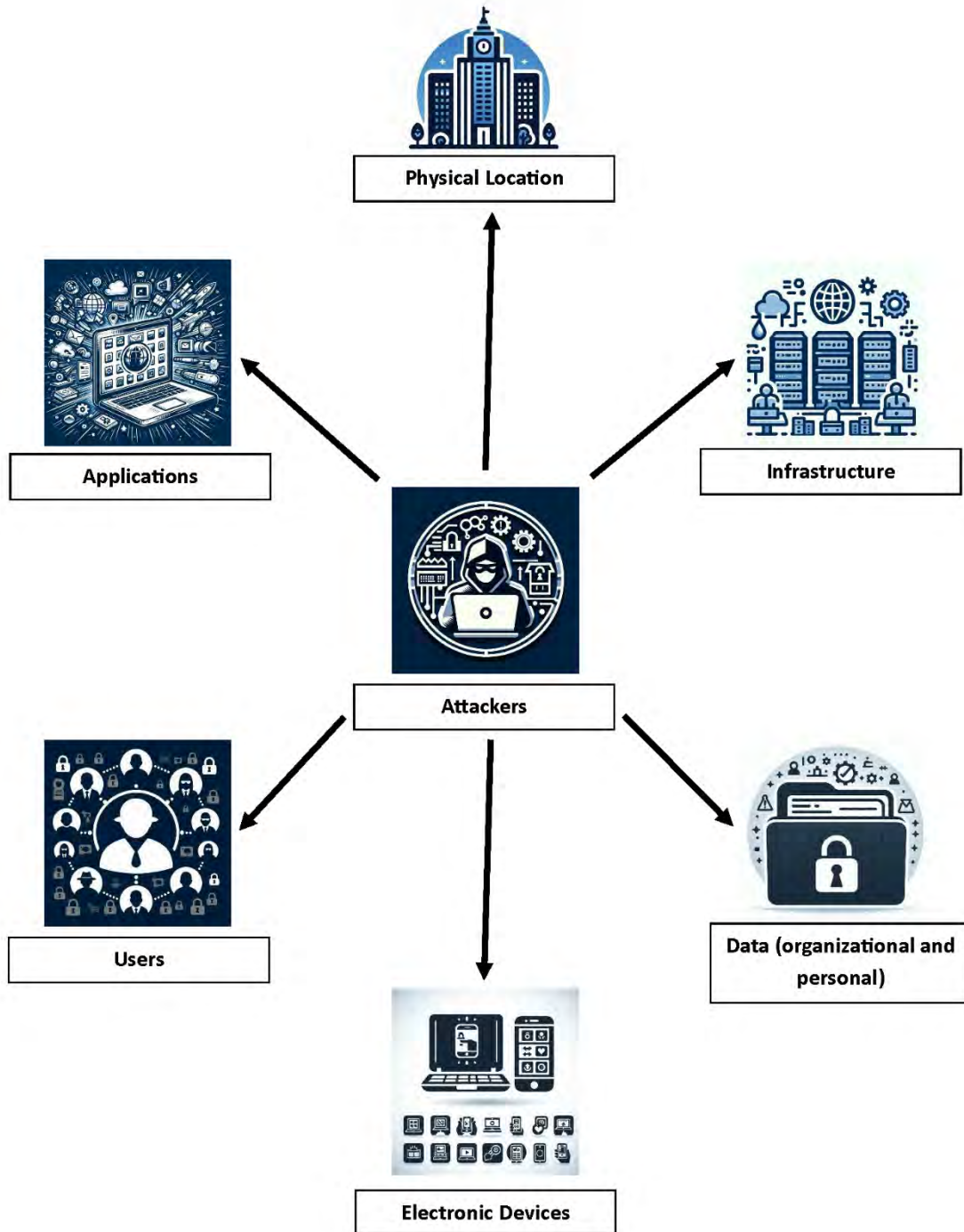
- Hacktivists, terrorists, or paid hackers
- Pose a serious threat to the security of IT systems

Cyberattacks

Cyberattacks¹ take many forms and target different elements of an IT system, such as users, websites, applications, electronic devices, software, network infrastructure, physical locations, and the data itself. These attacks are designed to alter, destroy, steal, or exploit information and disrupt or compromise the normal operation of a network.

It's important to recognize some common methods such as phishing, psychological manipulation known as social engineering, exploitation of vulnerabilities, use of malware, use of ransomware, and brute-force password attacks. These methods represent only a fraction of the many tools and techniques attackers use to compromise the security of IT systems. They are discussed in more detail in later sections.

¹ A cyberattack is a deliberate attempt to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system, or digital device.



Phishing

In today's ever-changing digital world, there's an insidious threat: online fraud, commonly known as phishing. Phishing is the practice of using fraudulent emails or text messages to trick users into performing unwanted actions, such as clicking on suspicious links, filling out dubious forms, or resetting sensitive passwords. These messages, disguised to look like legitimate communications from banks, companies, or even government agencies, are traps set by cybercriminals intent on stealing your personal information.

So why is this strategy so popular with cybercriminals? Simply because users are easier targets than infrastructure.

How do I identify a phishing email?

The most common forms of phishing are emails or text messages that appear to come from trusted sources, often creating a sense of urgency to get recipients to act without thinking.

Detecting errors

Phishing emails often contain grammatical errors and unusual sentence structure.

Request for sensitive information

Legitimate organizations will never ask for your personal information via email. If you receive emails asking for your personal information, it's important not to provide it and to report the message as potentially fraudulent. Here are some examples of sensitive information.

Connection identifier

- Username, password, etc.

Financial information

- Credit card number, bank account number, social security number, etc.

Personal information

- Date of birth, address, telephone number, passport number, etc.

Professional information

- Work login, access codes to internal company systems, etc.

Medical information

- Health insurance number, medical history, etc.

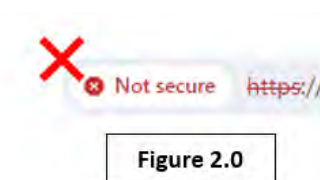
Alerts with warnings and consequences

Some emails are designed to give you a sense of urgency under the pretense that one of your accounts is being closed or a service is being blocked. It's important not to click on the links in these messages and to verify the information on the official site of the organization in question.

Urgent offer

Some messages are designed to lure users to a fraudulent site with a tempting offer that is about to expire. If you click on the link and accept the offer, the site will store your payment information for future scams. That's why it's important not to give your information to unknown companies.

Unsecured website



One indication that a website is potentially fraudulent is the absence of a secure certificate. If you click on a link in an email and the website address in the address bar is preceded not by a padlock (Figure 1.0) but by a warning message (Figure 2.0), it is critical that you never enter information that could be stolen.

How can I protect myself from phishing?

By recognizing the dangers of phishing and adopting vigilant online security habits, you can effectively protect yourself from this persistent threat in today's digital landscape.

Adopt a cautious attitude

Try to adopt a cautious and skeptical attitude toward any suspicious message. If you have the slightest doubt, do not click on links, fill out forms, or provide personal information. Simply reading or previewing an email is a low risk, although it is still a risk. The main risk is usually in the attachments and links.

Report message as phishing

There are features in email software that can be used to report fraudulent emails. If you think you've received a phishing email, after you open it, you can go to the toolbar, under the "Message" tab (Figure 3.0) and select the "Report Message" option (Figure 4.0). Once you've reported the email, there's no reason to keep it. You can delete it from your mailbox and then from "Deleted Items".



Figure 3.0

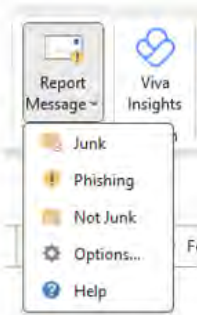


Figure 4.0

Contact your IT team or the College Information Security team



If you have any doubts or questions, please do not hesitate to contact your local IT team for assistance or the College Information Security Team (infosec@crcmail.net).

If you believe you have been the victim of a phishing attempt and have given out your personal information, don't panic, and most importantly, don't hide it. Report the incident and change any compromised passwords. If you have run suspicious software or files, shut down your computer immediately and wait for instructions from your local IT team or the College Information Security team.

Ransomware



Cybersecurity is a critical issue in today's digital world. Cybercriminals use a variety of methods to compromise the security of businesses and organizations, including the use of ransomware. This text aims to raise awareness and provide practical advice on how to protect against these attacks.

Ransomware has become one of the main business models of cybercriminal groups. They target businesses and other organizations and hold their data hostage for ransom.

The phases of an attack

An attack of this type generally has two distinct phases: preparation and execution.

Preparation

- ◆ **Illegal system access:** Criminals gain illegal access to a system through malware, phishing, or exploiting vulnerabilities.
- ◆ **Lateral movement:** Once inside the network, attackers move from one computer to another to take control of all systems.
- ◆ **Disabling backups:** Criminals look for backups and disable them to prevent data recovery after the attack.
- ◆ **Data exfiltration:** Private or confidential data is copied to remote servers, a process known as data exfiltration.

Execution

- ◆ **Data encryption:** Using specialized malware, all data is encrypted and rendered unusable without the decryption key.
- ◆ **Ransomware:** A ransom message appears explaining that the organization has been victimized by ransomware and providing instructions on how to pay the ransom.

Methods of infection

Ransomware can infect systems through a variety of methods, including phishing emails, malware downloads, and software vulnerabilities.

The importance of awareness

- ◆ **Understanding phishing:** Recognizing phishing attempts can help prevent ransomware attacks.
- ◆ **Frequent updates:** Keeping software up to date reduces the risk of vulnerabilities being exploited.

Consequences

Ransomware attacks can have devastating consequences for businesses and organizations.

- ◆ Loss of critical data and systems.
- ◆ Breach of data confidentiality.
- ◆ Threat of public disclosure of data.
- ◆ Financial and reputational risks.

Even if the ransom is paid, there is no guarantee of data recovery or confidentiality.

Conclusion

It's important to understand the risks associated with ransomware, and to adopt good information security practices to protect yourself. Raising awareness and implementing appropriate security measures are essential to reducing the likelihood of a successful attack.

Social engineering

Understanding Social Engineering



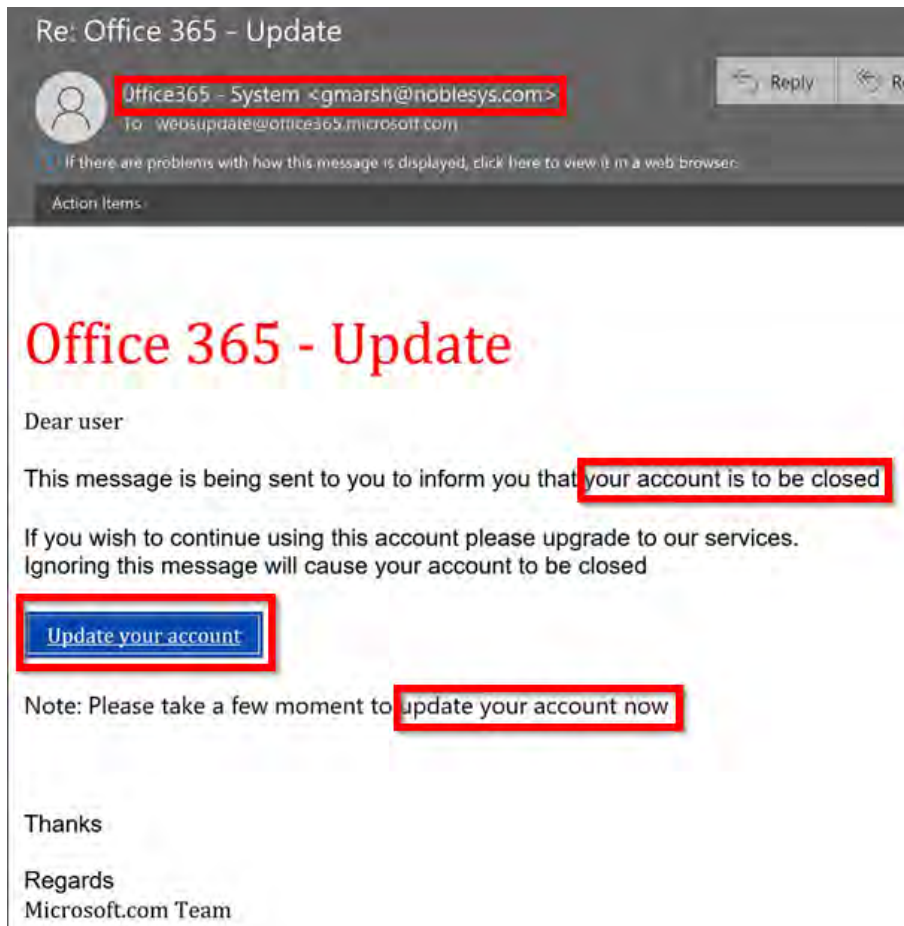
Social engineering exploits our natural tendency to trust and relies on people's good faith to gain access to sensitive information, whether personal or professional. This devious tactic can take many forms, including emails, text messages, or phone calls, often from supposed colleagues, friends, well-known companies, bosses, and so on. Subtly, cybercriminals use urgent language to lure their victims into impulsive action.

Recognizing a Social Engineering Attack

Manipulating emotions

Cybercriminals use fear and urgency to get people to take quick action, such as divulging sensitive information or transferring money.

For example, if you receive an email like this, **beware!**



Unusual friend requests

Hacked accounts often send suspicious messages to the victim's contact list. Be wary of non-personalized messages.

Offers that are too good to be true

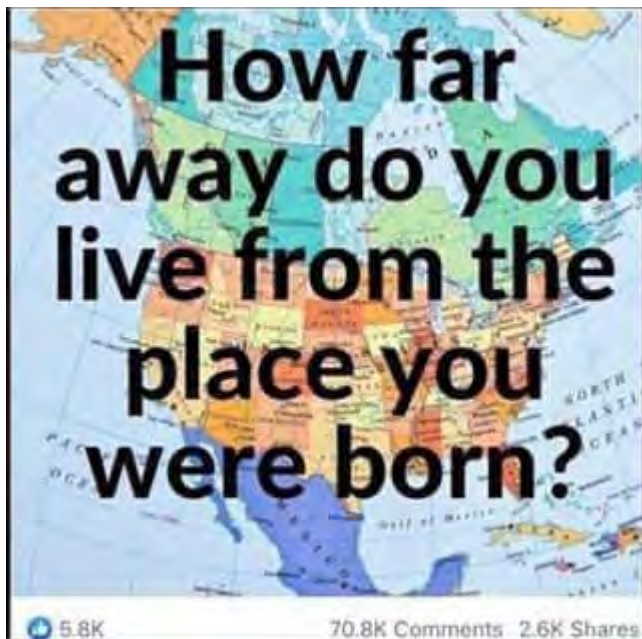
Scammers often lure people in with promises of quick wins or unrealistic benefits that should raise suspicion.

Innocuous questions

Answering innocuous questions can sometimes reveal sensitive information, such as passwords or security information.

It's common to come across seemingly innocuous posts on social networks, such as "Your birth date and favorite color will be your superhero name."

However, it is vital to understand that this information is often used to create passwords or security questions. Cybercriminals use these posts to obtain valuable personal information and use it for malicious purposes. Resist the temptation to participate in these activities, which can compromise the security of your online accounts.



Deepfake



Deepfake techniques use artificial intelligence to create fake content, such as videos or audio recordings, to mislead people about the authenticity of information.

You can watch this [video](#) to see an example of a deepfake.

Avoid the pitfalls of social engineering

Social engineering attacks are particularly insidious because they play on human traits such as curiosity and respect for authority. Here are some tips on how to protect yourself.

Verify the source

Assess the source of suspicious information. Check details such as email headers or spelling and consult official sources if necessary.

Get the information you need

Be cautious if the solicitor asks for sensitive information without adequate justification. A legitimate entity would normally have access to this information or provide proof of its identity.

Take time to think

Don't give in to the pressure of urgency. Take the time to verify the authenticity of the request by using alternative means of communication or asking for proof of identity.

Request identity verification

Before giving out confidential information, ask for proof of identity or check the references of the person requesting it. Don't blindly trust strangers, even if they seem well-intentioned.

Conclusion

By following these simple but important precautions, you can significantly reduce your risk of falling victim to a social engineering attack.



If you have any doubts or questions, please do not hesitate to contact your local IT team or the College Information Security team (infosec@crcmail.net) for assistance.

Teleworking: A new era

The global health crisis has profoundly changed the way we work, accelerating the use of telework. This evolution implies the need to access essential internal services, applications and information as if we were physically present in the office.

The risks of remote work

Physical access to devices

Vulnerability to theft

When devices are left unattended in public places or at home, they become vulnerable to theft or tampering by malicious individuals.

Handling

Eavesdropping

Network monitoring

Malicious individuals can monitor wireless network traffic to record online activity and retrieve passwords.

Traffic alteration

By infecting a mobile device with malicious code, an attacker can inject pirate traffic to disrupt data and gain access to the organization's network.

Advice on how to work remotely

Multi-factor authentication

Increase the security of your devices by enabling multi-factor authentication, which requires two different forms of identification, such as a password and a biometric.

Device monitoring

Precautionary measures

Never leave your equipment unattended, especially in public places, and immediately report any theft or loss to your local IT team or the College Information Security team (infosec@crcmail.net).

Responsiveness

Increase your awareness of the environment around you

Increased vigilance

Be aware of your surroundings and watch out for people around you who might compromise the confidentiality of your communications.

Regular updates

Importance of updates

Updates and patches mitigate security vulnerabilities and protect your devices from threats.

It's important to understand the importance of updates, as they guarantee the security of your devices, although installing them can sometimes be a source of stress and frustration. You can always visit the College to expedite the update process and receive further assistance from the IT Service Center.

Network security and public Wi-Fi

Wi-Fi security

When working from home, it's important to take steps to secure your Wi-Fi network. Change the default password provided by your service provider and choose a strong password or a phrase that's difficult to guess.

Be careful with public Wi-Fi

Whether you're at home, the library, or a café, make sure you're using a secure wireless network and avoid sending sensitive information over a public network. It's important to note that some malicious individuals create public Wi-Fi networks that look like legitimate establishments, allowing them to spy on the activities of users who connect. Avoid connecting to public networks or sharing sensitive information, including access to sensitive accounts, whenever possible.

It's your responsibility to ensure the security and maintenance of routers that are not managed by your organization, such as those you have at home. Like any other piece of equipment, routers will eventually become obsolete. End-of-life devices pose a security risk to your organization because their vendors typically stop updating and supporting them. Using out-of-date equipment exposes you to cyber attacks.

If you have any questions about your home equipment, we recommend that you contact your Internet Service Provider.



Conclusion

By following these tips, you can work remotely in complete security and keep your data and our organization's data safe.

Password management



In today's digital world, our passwords are the guardians of our online lives. They protect our personal information and sensitive data from cybercriminals who are always on the lookout. Unfortunately, many of us underestimate the importance of effective password management and often fall into risky habits that compromise our security. In this section, we'll explore the importance of password management, the risks associated with poor practices, and the steps everyone can take to strengthen their online security.

Bad habits

Bad habit	Description	Risks
Use the same combination	Reuse a password across multiple accounts.	If one password is compromised, all associated accounts are vulnerable.
Use weak passwords	Use simple, everyday passwords.	Easier for cybercriminals to guess.
Use passwords associated with personal information	Use of personal information (name, date of birth, etc.).	More likely to be guessed or discovered.

How to better protect yourself

Understanding threats

It's essential to be aware of the different methods cybercriminals use to compromise passwords, including phishing, brute force, stealing credentials from the Dark Web*, and more.



Did you know that?

*On the Dark Web, an underground online marketplace, cybercriminals trade and sell stolen information, including passwords. When a website is compromised in a data breach, user credentials, including passwords, can end up on the dark web. Cyber attackers use this information to fraudulently access users' accounts, compromising their online security. It's important to take steps to protect your passwords and prevent the risk of data compromise.

Best practices

Never share your password with anyone, never write it down on physical or digital documents that are accessible to anyone, never use the same password for multiple accounts, and avoid using weak passwords.

What is a complex password?

A complex password is a combination of lowercase and uppercase letters, numbers, and special characters, and must be sufficiently long, generally recommended 8 characters or more. The main goal is to make the password difficult for a malicious actor to guess by increasing the number of possible combinations.

Sample passwords	Complexity
Balloon80	Low
Bal!o0n80	Moderate
aj-E7Gf!&60!	Strong

Why use a complex password?

Our passwords are like digital keys that give us access to our online world. We have several for different accounts, but some have been the same for years. The problem? Cybercriminals know that many of us tend to choose passwords that are easy to guess or based on personal information. They use automated tools to try every possible password combination, and the simpler our passwords, the more vulnerable they are.

Use tools such as "[How secure is my password](#)" to assess the security of your passwords. Choosing a complex password is essential to reducing cybercriminals' chances of success and protecting your online information.



Use security methods

- ◆ Enable multi-factor authentication (MFA) if available.
- ◆ Use a password manager to store passwords securely.
- ◆ Use browser safes where appropriate.

Conclusion

Password management is a critical element of cybersecurity. By following best practices and using complex passwords, we strengthen the security of our personal and professional information online. Take steps now to protect your accounts and prevent cyberattacks.

Multi-factor authentication

Why passwords are no longer enough

Passwords have long been a first line of defense in protecting our services and systems. But as cyberattacks become more sophisticated, even complex passwords can be compromised. Here are some common methods used by cybercriminals:

- ♦ **Direct attacks on the system:** Stealing information from all users.
- ♦ **Targeted attacks:** Use of malware to log keystrokes and guess passwords.

If these attacks are successful, simple password-based authentication is not enough to protect users. This is where multi-factor authentication (MFA) comes in to strengthen security.

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication is a security method that overlays multiple authentication methods to strengthen access to a service or application. It is based on the use of two or more of the following categories:

Category	Examples
Something you know	Username, password, security questions, PIN
Something you have	Smart card, code sent by text or email, authentication application
Something you are	Retinal prints, fingerprints, photo ID cards

For authentication to be truly multi-factor, it must include elements from at least two different categories. This is why multi-factor authentication is often referred to as 2FA or two-factor authentication. They are similar, but 2FA is limited to two factors and MFA can have more than two.

Examples

Situation	Authentication methods	Category	MFA
Automatic teller machine (ATM)	Debit card + PIN	Something you have + know	Yes
Online connection	Username + password	Something you know + know	No
Secure online connection	Username + password + security code	Something you know + know + have	Yes

Common MFA methods

Method	Efficiency
Authentication application	Very high
Hardware token*	High
SMS verification	Moderate
Email verification	Low

* Tokens can be expensive and difficult to maintain. They are also more likely to be stolen or lost.

Watch out for bypasses!

Cybercriminals can sometimes bypass MFA using techniques such as:

- ♦ Impersonating a bank employee to obtain a verification code.
- ♦ Triggering multiple authentication requests to trick you into approving a fraudulent request.

Best practices

Avoid	To do
Never give MFA codes to anyone without verifying their identity.	Use MFA as much as possible.
Never approve a connection unless you are sure it belongs to you.	Keep your phone secure and out of the reach of people who could compromise your MFA.
	Use authentication applications instead of email or text messages when this option is available.

Conclusion

Multi-factor authentication is an essential technique for securing your online accounts against cyber attacks. By combining multiple authentication methods, you can significantly strengthen the protection of your personal and sensitive information.

Mobile device usage and device security

Understanding how to properly protect our devices is essential to avoid catastrophic consequences in the event of a cyber attack. This text provides practical advice on how to secure your mobile devices, both at work and at home.

On the job: Supported and Unsupported Devices



Supported devices: These are devices supplied and secured by the College to meet the organization's needs.

Unsupported devices: If you use your own devices, follow the best practices listed below to protect them from risk.

Security tips for all devices

Updates

Operating system and software updates are important because they improve security, correct issues, and add functionality.

Think before you text

Text messages can make you vulnerable to malware ²and data breaches. Take precautions:

- ♦ Do not give out personal information.
- ♦ Do not open attachments from unfamiliar sources.
- ♦ Avoid clicking on suspicious links.

Beware of untrustworthy applications

Download applications only from trusted sources, such as the App Store or Google Play. Before you install an application:

- ♦ Check the permissions you need.
- ♦ Research the application and read user reviews.

Protect and monitor your devices

- ♦ Lock your computer or mobile device when it's out of sight.
- ♦ Do not leave your computer unattended and keep it in a safe place.
- ♦ Don't let others use your work computer.
- ♦ Use a PIN, password, or fingerprint to protect your phone and avoid locking systems.
- ♦ Never connect unfamiliar peripherals to your computer. If necessary, bring the device to your local IT team.



² Malicious code, or malware, is a tool often used by cybercriminals to infect victims' systems and devices in order to steal their personal information.

Summary table of security best practices

Action	Why
Regular updates	Fix vulnerabilities and improve security
Precautions when sending SMS	Prevents malware and protects privacy
Download trusted applications	Reduce the risk of installing malicious applications
Device lock	Prevents unauthorized access in case of loss or theft
Avoid unfamiliar peripherals	Protects against malware hidden on external devices

Conclusion

Mobile device security is critical to protecting personal and sensitive information. By following these tips, you can significantly reduce the risk of cyberattacks and protect your sensitive information.

Malware



Malicious software (malware) is software designed to disrupt, steal data, or gain unauthorized access to a system. It is used by cybercriminals for a variety of reasons, including:

- ♦ Stealing personal information for identity theft.
- ♦ Financial theft.
- ♦ Controlling multiple computers to launch attacks.
- ♦ Mining cryptocurrency.

Types of malware

Software	Description
Virus	A virus injects itself into existing programs. It usually arrives in the form of an email attachment containing a malicious payload. Once the victim opens the file, the device is infected.
Trojan horse	Remote access Trojans allow hackers to take complete control of your computer. They disguise themselves as harmless applications to trick users into downloading them. Once installed, they can steal personal information, spy on your activities, or even launch attacks.
Spyware	Spyware collects personal information such as browsing history, passwords, screen shots, and keystrokes. Usually installed without your knowledge, these programs capture and transmit personal information.
Ransomware	Ransomware encrypts documents and demands a ransom. This type of malware installs itself on the victim's computer, encrypts files, and then demands a ransom to return the data to the user.
Adware	Adware displays unwanted advertisements, manipulates Internet traffic, and performs searches. They force users to see flashing ads or pop-up windows when they perform certain actions. Adware is often installed in exchange for a service, such as free use of a program.
Worm	A worm is a piece of software that reproduces itself on multiple computers over a computer network, such as the Internet. It has the ability to duplicate itself from one computer to another by exploiting security vulnerabilities in software or operating systems, without requiring user interaction to operate.

Fake antivirus software	Fake antivirus software is a ploy used by cybercriminals to make it appear that a computer or device is infected with malware in order to trick victims into purchasing a fake application. Cybercriminals use these programs and advertising manipulation to scare users into purchasing a fraudulent application.
-------------------------	---

Common methods of infection

- ♦ Open a phishing e-mail attachment or link.
- ♦ Download software from an untrusted source.
- ♦ Visit a compromised website.
- ♦ Plug in an unknown device (USB flash drive, external hard drive, etc.).
- ♦ Not updating your software or operating system.
- ♦ Use an unsecured wireless network.

Signs of infection

Common symptoms of a malware infection may include:

- ♦ Slow execution and poor performance.
- ♦ Browser redirects to unwanted sites.
- ♦ Infection alerts accompanied by requests to purchase solutions.
- ♦ Problems stopping or starting the computer.
- ♦ Frequent pop-up ads.

The more of these common symptoms you experience, the more likely it is that your computer is infected with malware. Browser redirects and numerous pop-up alerts claiming you have a virus are the best indicators that your computer has been compromised.

What to do in case of infection

Computer type	Actions to be taken
Personal computer	<ul style="list-style-type: none">♦ Turn off the computer and disconnect it from the network.♦ Contact your IT team.♦ Do not reconnect the computer to the network without authorization.
Work computer	<ul style="list-style-type: none">♦ Disconnect your computer from the Internet.♦ Run a full antivirus scan.♦ Change any compromised passwords.♦ Back up your files and reset your computer if necessary.

How can I protect myself from malware?

Protect your devices

- ♦ Keep your operating system and applications up to date.
- ♦ Never click on a link in a pop-up window.
- ♦ Limit the number of applications on your devices.
- ♦ Use a mobile security solution.

Use caution on the Internet

- ♦ Avoid clicking on unfamiliar links.
- ♦ Use only known and trusted sites.
- ♦ Beware of emails that ask for personal information.
- ♦ Avoid risky websites.

Beware of downloads

- ♦ Buy security software only from reputable companies.
- ♦ Use official app stores.
- ♦ Read app reviews before downloading them.
- ♦ Don't open email attachments from unknown sources.

Conduct periodic checks

- ♦ Run regular scans with your security software.
- ♦ Check your bank accounts and credit reports regularly.

Conclusion

Malware is a serious threat, but with vigilance and best practices, you can protect your devices and sensitive information from these attacks.

Network security

With the rise of remote work, it's important to understand the basic concepts of network security. This aspect of cyber hygiene is essential to protect information, ensure the security of shared data, and provide reliable access, network performance, and protection from cyber threats. Network security also protects against malware.

Connectivity and network type

Network connectivity

Computers can generally access the network in one of two ways:

- ♦ **Wi-Fi:** Wireless connection to the Internet and local networks.
- ♦ **Wired:** Uses Ethernet cables for fast, stable connection.

Network type

A computer can connect to different types of networks to access the Internet or the organization's servers:

- ♦ Home network
- ♦ Organizational network
- ♦ Mobile network using the access point function.
- ♦ Public Wi-Fi (hotel, restaurant, airport, etc.).

Public Wi-Fi networks

Public Wi-Fi networks are **dangerous** because they can be compromised or forged under the name of a legitimate organization. By using a compromised network, a cybercriminal can use it to read:

- ♦ Read unencrypted data sent from your computer to the Internet.
- ♦ Manipulate your network traffic to redirect you to a spoofed website.
- ♦ Attempt to intercept your encrypted communications and capture your passwords.

This part is extremely important. This is the most dangerous aspect of teleworking. As mentioned in the Telecommuting section, a malicious actor can set up a public Wi-Fi network and pose as a well-known organization. When this happens, a cybercriminal can gain access to a lot of confidential data, compromising both personal and organizational information.

To avoid these risks, it is important to:

- ♦ **Choose password-protected Wi-Fi networks:** Only use Wi-Fi networks that are password protected by the organization! **WARNING:** A malicious actor can still create a Wi-Fi network with the same name and password if this information is visible to all.
- ♦ **Avoid connecting to public networks that are not password protected:** Never connect to unsecured public Wi-Fi networks to avoid the risk of compromise.

Even if you're using a college-issued laptop, take the time to check the Wi-Fi source and make sure it's secure. **Your vigilance is the first line of defense against cyber threats.**

Firewall

Private networks, such as your home or college network, are protected by a firewall. If you connect a device to a private network, you run the risk of infecting systems on the network with malware.



Did you know that?

Firewalls control inbound and outbound network traffic according to predetermined security rules. They block unwanted traffic and are an essential part of everyday computing. Network security relies heavily on firewalls, especially those that focus on blocking malware and application-level attacks.

Best practices

Measurement	Description
Use of public networks	Avoid using public networks for work or sensitive activities such as banking transactions.
Securing home routers	<ul style="list-style-type: none">• Change your router's default password.• Use a separate guest network to provide Wi-Fi access to unsecured devices in your home.• If necessary, contact your Internet service provider for assistance.
Find out more	Ask the College about best practices for working remotely.

Information security

Information security refers to all the security measures put in place to protect information from unauthorized access, ensuring its confidentiality, integrity, and availability. Information is essential to any organization, and in the context of cybersecurity, the term encompasses all types of digital information, such as:

- ♦ Documents
- ♦ Business software
- ♦ Websites
- ♦ Social networks

Organizations are responsible for protecting their own information as well as the information entrusted to them.

Information classification and confidentiality

Organizations assign different levels of confidentiality to their information through a classification process:

- ♦ **Public information:** Publicly available (brochures, websites, etc.).
- ♦ **Internal information:** For internal use only (task lists, work papers, etc.)
- ♦ **Confidential information:** Disclosure of which could have serious consequences (student lists, employee files, etc.).

Personal information

Personal information is information that is specific to an individual, such as:

- ♦ Address.
- ♦ Telephone number.
- ♦ Online shopping history.
- ♦ Employee record.

This information can be used by unscrupulous organizations to commit fraud and identity theft. To reduce these risks, there are strict laws in place to protect personal information.

Secure information handling

Using secure file servers or document sharing applications (OneDrive, etc.) is critical to protecting your information. Work data should always be stored in organizational-approved locations.

Avoid	To do
Don't store your files on personal devices or in unauthorized locations.	Learn about the College's information security policy.
Don't hold on to large amounts of work without a backup.	Know the approved locations for document storage.
Do not share information with unauthorized parties.	Identify information that is subject to specific requirements.

Threat to the security of information

Databases are prime targets for cybercriminals, whether they are internal (employees, partners) or external (hackers, cybercriminals). Here are some common techniques used to compromise data security:

- ♦ **Phishing:** Using fraudulent emails to obtain sensitive information.
- ♦ **SQL injection:** Exploiting vulnerabilities in applications to gain access to information.
- ♦ **Unauthorized access:** Using elevated privileges to access unencrypted files.
- ♦ **Human errors:** Sharing passwords, configuration errors, etc.



Did you know that?

Human error is responsible for over 90% of data security threats and cyberattacks? In fact, the majority of security breaches are the result of human error. These mistakes can take many forms, including password sharing, configuration errors, phishing, weak password use, and carelessness.

Information security management strategy

Password management

- ♦ Use a password management solution to avoid reminders.
- ♦ Prefer secret phrases to traditional passwords.
- ♦ Enable multi-factor authentication (MFA).
- ♦ Change your passwords after a security breach.
- ♦ Avoid reusing secret phrases or passwords.

Software updates

Software updates fix vulnerabilities that cybercriminals exploit. Applying these updates regularly is essential to protecting your systems. The College is only responsible for software updates on provided devices. We strongly recommend that you update your personal laptop regularly, especially if you use it for work.

Conclusion

By following these guidelines and taking a proactive approach to data security, your organization can better protect its sensitive information from cyber threats and human error.

References

General

<https://www.cyber101.com/training>

<https://reseau.uquebec.ca/fr/nos-initiatives/centre-expertise-securite-information/guides>

<https://www.ibm.com/topics/cyber-attack>

Phishing

<https://www.getcybersafe.gc.ca/en/phishing>

<https://reseau.uquebec.ca/system/files/documents/se-proteger-contre-hammeconnage-v1-1-20230117.pdf>

Social engineering

<https://ia.ca/advice-zone/cybersecurity/social-engineering>

<https://www.proofpoint.com/us/threat-reference/social-engineering>

<https://www.fortinet.com/resources/cyberglossary/deepfake>

Teleworking

<https://www.cyber.gc.ca/en/guidance/telework-security-issues-itsap10016>

Password management

<https://reseau.uquebec.ca/system/files/documents/definition-mdp-v1-2-20240307.pdf>

Multifactor authentication

<https://www.cyber.gc.ca/en/guidance/what-multi-factor-authentication>

<https://reseau.uquebec.ca/system/files/documents/definition-mfa-v1-2-20240308.pdf>

The use of mobile devices and device security

<https://www.getcybersafe.gc.ca/en/secure-your-devices/phones-and-tablets>

Malware

<https://www.mcafee.com/en-ca/antivirus/malware.html>

Network security

<https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/>

Information security

<https://www.oracle.com/ca-en/security/database-security/what-is-data-security/>

<https://www.microsoft.com/en-ca/security/business/security-101/what-is-data-security>