RETAIL COUNCIL OF CANADA

RETAIL CYBERSECURE

MODULE 1

CYBER SECURITY FUNDAMENTALS FOR RETAILERS

Securing your devices, assets, and business.

A guidebook to help retail businesses
protect themselves against the impacts of cybercrime

RCC RETAIL COUNCIL OF CANADA

CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL

About Retail Council of Canada

Retail is Canada’s largest private-sector employer with over 2 million Canadians working in our industry. The sector annually generates over $85 billion in wages and employee benefits. Core retail sales (excluding vehicles and gasoline) were over $462B in 2022. Retail Council of Canada (RCC) members represent more than two-thirds of core retail sales in the country. RCC is a not-for-profit industry-funded association that represents small, medium, and large retail businesses in every community across the country. As the Voice of Retail™ in Canada, we proudly represent more than 143,000 storefronts in all retail formats, including department, grocery, specialty, discount, independent retailers, online merchants and quick service restaurants.

Retail Council of Canada acknowledges the support of The Ministry of the Solicitor General (Ministry), 2022-2024 Safer and Vital Communities (SVC) Grant.

Ontario

Contact Retail Council of Canada:

1881 Yonge Street, Suite 800
Toronto ON M4S 3C4
Telephone (toll-free): (888) 373-8245
E-mail: education@retailcouncil.org

Table of Contents

i. Introduction

For retailers operating today, the digitization of the industry, and the rest of the world around us, has resulted in boundless opportunities to connect with existing and potential customers, extend their reach and service, and maintain their relevance in an age of technological innovation and advancement. However, the current retail digital landscape is providing the perfect environment for those operating within the criminal world to prey on unsuspecting victims through the launch of a range of different cyberattacks.

By targeting websites, email addresses, social media accounts, and any other digital presence that a retailer has developed, cybercriminals seek those that they believe are vulnerable to attack. And, the prevalence and frequency of these attacks have only increased since the onset of the COVID-19 global pandemic. In fact, according to a recent Mastercard study, since the start of the pandemic, there has been a 600 per cent rise in cybercrime.

In light of the continued proliferation of this nefarious trend, it's critical that retailers, despite their size, format, or location, take the necessary steps to safeguard their operations in order to ensure that their devices, assets, and business are cyber-secure.

To help retailers achieve a safe and secure digital environment for their businesses to operate within, Retail Council of Canada has developed the Cyber Security Fundamentals for Retailers guidebook. Filled with a breadth of useful information, tips and best practices, it's a go-to resource meant to enhance any retailers' digital ecosystem, and protection against the threat of cybercrime.

The Impacts of Cybercrime:

- * The average cost of a data breach in Canada is $5.64 — $1-million more than global averages — with 99 per cent of victims agreeing the hack impacted their business operations.
- * The most common ramification reported as a result of a data breach was a loss of customer data, while more than a third said the hack strained their relationships with vendors or customers.
- ** Cybercrime and fraud cost Canadians more than $500-million in 2022 alone.

** according to Mastercard's 'Securing the digital economy' study.*

*** according to the RCMP data.*

ii. The Basics of Cyber Security

The first step for any retailer attempting to enhance its cyber security efforts is to ensure that it has – depending on the size of the organization – at least one individual who specializes in loss prevention and cyber security on staff to develop strategy and direction and to own the maintenance of the program. However, it's also important for other members of the leadership team to understand at least the basics of retail cyber security and the role is serves within their organizations.

What is Retail Cyber Security?

Retail cyber security refers to any and all efforts put forward by a retail organization, including technologies supporting a range of measures and practices, that are meant to defend against, or prevent altogether, the impacts of cyberattacks. Put simply, cyber security within a retail organization should serve to protect its systems, digital devices, applications, sensitive personal and business information, digital data, and assets against threats posed by cybercriminals, which may include computer viruses, ransomware attacks, and everything else in between.

What's the Goal of Retail Cyber Security Effort?

With the aim of protecting the retail organization against a range of cyber-threats, the most effective cyber security is often supported by three non-negotiable goals for success:

Maintaining confidentiality – Retailers are perpetually in possession of a breadth of important information, including records related to employees, clients or finances. This information should be kept confidential, and should only be accessed by others with permissions.

Upholding integrity – It's critical to keep all assets and information complete, intact and uncorrupted in order to uphold its integrity.

Ensuring availability – It's incredibly important to maintain the availability of all of the organization's systems, including networks and servers, services and information when required by the business or its clients.

How Can Retailers Maintain an effective cyber security program?

In order to ensure that an effective cyber security program and strategy can be put in place and executed going forward, a number of things are required of retailers and their cyber security teams on an ongoing basis:

Determining assets – Retail organizations will want to identify the assets that they wish to protect within their cyber security program, typically including assets owned or managed by the organization).

Identifying threats – It's critical to identify all potential threats and the estimated impacts caused to the assets as a result.

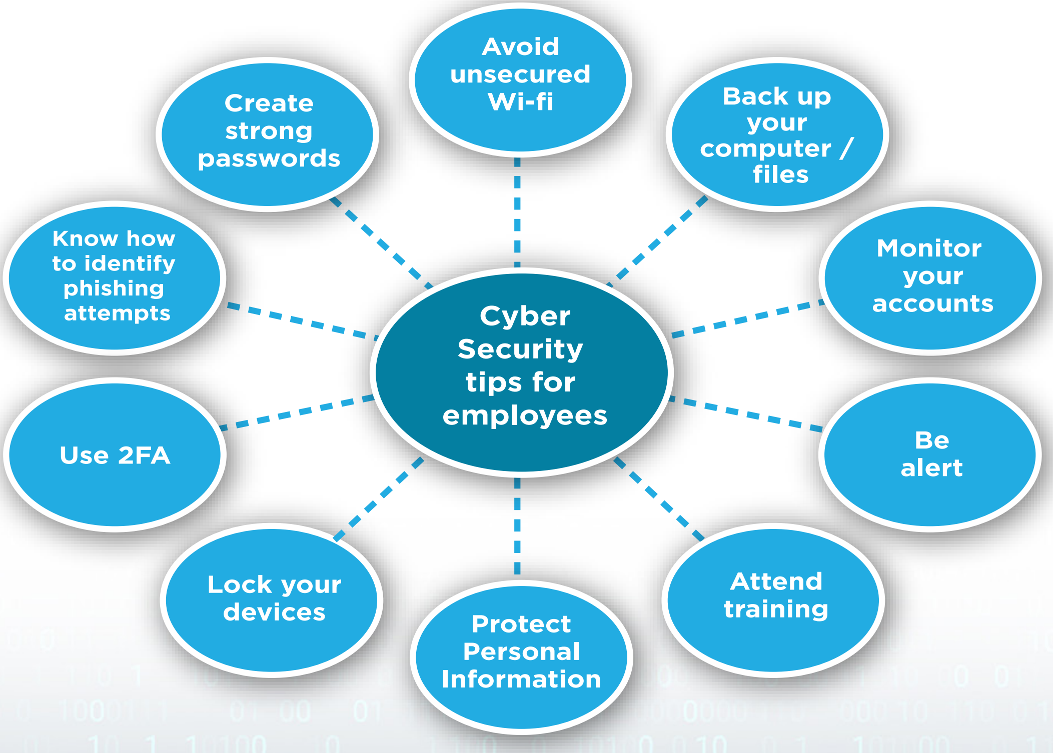
Developing safeguards – In response to the determination of assets and identification of potential threats, safeguards must be put in place in order to prevent or mitigate their impacts.

Continuous monitoring – Retailers can properly manage and assess the effectiveness of their cyber security programs through the constant and continued monitoring of the safeguards that have been put in place.

Speedy response – It's critical for retail organizations and their cyber security teams to act swiftly to incidents when they occur, in real-time, in order to maintain the effectiveness of their programs.

Tweaking and updating – It's also crucial for retail organizations to continuously tweak and update their systems and safeguards in order to properly respond to changes related to assets and threats.

Cyber Security for Employees:


Cyber Security tips for employees
Avoid unsecured Wi-fi
Back up your computer / files
Monitor your accounts
Be alert
Attend training
Protect Personal Information
Lock your devices
Use 2FA
Know how to identify phishing attempts
Create strong passwords

iii. Securing the Web

When it comes to securing the digital retail ecosystem, it makes sense to begin safeguarding the Internet and everything else Web-related. Given the amount of Web-based activity conducted by retail organizations and their staff, which can include the entering of personal and business information online, Internet browsing, and social media interactions, a holistic approach toward safeguarding assets must be taken.

Safeguarding Personal and Business Information

There are a number of different situations within a retail organization that might necessitate an employee to enter personal and/or business information online, including everything from work being conducted with clients and partners, to the filling out of newsletter and magazine subscription forms and office supply order forms. It often contains information that could include details, both private and confidential, revealing full names social insurance numbers, email addresses, phone numbers, physical addresses, banking information, as well as details related to a number of other assets and entities. And, every time this type of information is entered, there are distinct cyber-threats and associated risks involved.

In order to properly and effectively safeguard any retail organization against the range of threats posed by cybercriminals, it's imperative that their employees, from the executive suite to the customer service floor, understand the importance of Web security and the significance it represents for everyone involved. Cybercriminals prey on the vulnerable, and build their attacks on a foundation of personal and business information that they've collected by gaining illegal access to computers or systems. However, their potential impacts can be minimized if all employees within the organization adhere to a handful of simple best practices:

Legitimate and trusted – Ensure that all employees using company computers and devices understand the importance of only visiting and sharing information with legitimate and trusted websites.

Source verification – Before sharing any personal or business information with anyone, employees should first verify that the entity asking for it is a trusted and verified source.

Ask questions – Whenever anyone is asking for personal or business information, employees should ask plenty of questions as to the reasons why the information is needed. And, if the response provided does not suffice, employees should be empowered to refuse providing the requested information until further details are received.

Maintain safeguards – Despite the reasons that might be given, none can justify the removal or disabling of security measures or safeguards, such as anti-virus and malware protection software, that have been put in place on computers and networks by the organization.

Ensuring Safe and Secure Internet Practices

The extent to which retail organizations rely on the Internet and its capabilities to undergo routine day-to-day tasks is immense. From mundane emails and research to common purchasing activities, there are a number of reasons that require a retail organization and its employees to browse the Internet. Although the use of the Internet is inherent and widespread today, and is a part of the everyday operations of just about every retailer, it's an excellent idea for retailers to ensure that everyone within their organizations are exercising the right precautions when perusing the Web.

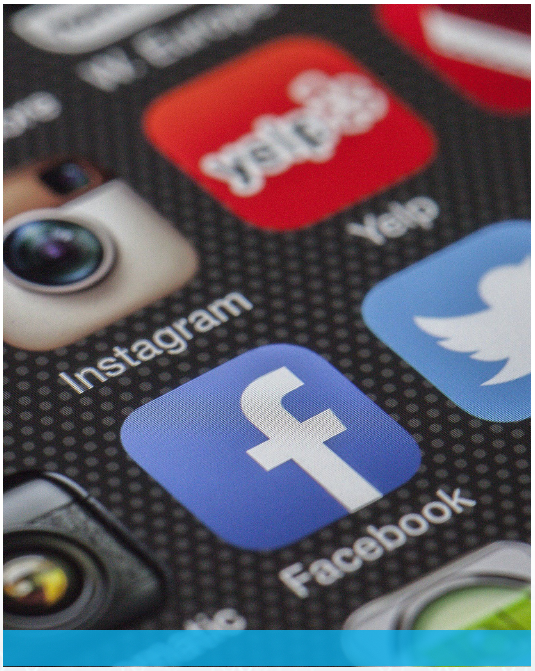
Policies and protocols – It's a very good idea for retail organizations to outline their expectations of their employees when it comes to Internet browsing activities and behaviour. To do this, retailers should develop their own internal Internet Usage Policy that clearly explains for employees the 'dos and don'ts' with respect to connecting to the Internet via the organizations' systems and devices.

Employee training – Once Internet policies have been developed for employees to follow, it's imperative to provide them with ample training related to the Internet Usage Policy.

Promote awareness – In addition to the amount of training that employees receive from retail organizations around their Internet Usage Policy, it should also be administered frequently in order to promote continuous awareness and understanding.

Implement site-rating tools – As an added precaution, retail organizations can easily equip employees' Internet browsers with a site-rating identification tool extension

Ensure safe searches – As part of their ongoing training, employees should be shown how to properly confirm that the URLs of the websites that they're visiting are safe and secure by using an Internet site-rating identification tool.



Establishing Social Media Protocols

Among all of the channels that have cropped up over the course of the past number of years, social networking websites such as Facebook, X, Instagram, Pinterest, and more, have perhaps proven to be the most influential, providing retail organizations with a range of customer engagement and marketing opportunities to build stronger relationships and a more robust brand. However, given the popularity of these sites, they're increasingly becoming targets for cybercriminals looking to take advantage of online vulnerabilities in order to pilfer personal and business information from computers and systems.

In light of this threat, it's incredibly important that retail organizations include social networking protocol and best practices within their Internet Usage Policy, outlining for employees the proper conduct that should be followed on these sites.

Designate social networking individuals – It's a good idea to identify and designate a small handful of individuals who will be responsible for the organization's social media activity. Activity should be limited to these authorized individuals.

Identify information to be shared – Retail organizations should clearly define the type of information that can be shared on social networking sites. This can be included within its Internet Usage Policy.

Do not include sensitive information – Employees should never include sensitive personal or business information within the organization's social media posts.

Be wary of social networking apps – It's wise for retail organizations and their employees to avoid using social networking apps, which are often developed and managed by third-party technology providers and may not be as secure as their websites.

Practice cautious communication – Whenever engaging with anyone on social networking sites, retail employees should exercise caution, especially when being asked to share or provide information about the business or any of its employees.

Review information before posting – It's always a great idea to be thorough when communicating on social networking sites. And that means reviewing information before its posted

It's also the policy of many retail organizations to allow their employees to check their own personal social media accounts while at work. If this is the case, they should be advised to follow the very same guides and best practices.

Protecting Against Social Engineering

As the means by which to perpetrate cyberattacks increase, so too does the level of manipulation with which they are deployed. And, as manipulative tactics go, social engineering is one of the most effective ways that information is obtained by cybercriminals. By tricking employees within the organization, cybercriminals are able to gain access to computers, systems and information.

Leveraging what little information they might already have at their disposal, they'll communicate with employees, either online, by email or over the phone, gaining their trust through seemingly honest behaviour. They'll often claim to be a client or partner of the company or close associates with one of the employees' colleagues. They may even attempt to offer manufactured "proof" of their "legitimate" connection to the business. Some may go as far as to impersonate a government official or other figure of authority, requesting information such as phone numbers or account information. In some instances, they may instruct individuals to open emails and attachments or to visit particular websites.

Because manipulation is the tactic, most victims are unsuspecting of the incident until it’s far too late, and only then begin to realize the very real fallout. In order to avoid these scenarios, and to properly protect the organization, its assets and people, retailers should ensure that their employees are aware of such scams and to be vigilant concerning these types of communications with outside sources.

Be on guard – It’s a good idea to advise all employees of the organization that they should be wary of any and all emails, phone calls and visits that they receive from individuals claiming to be connected in some way to the business or anyone working within it.

Ask for verification – Ask every individual requesting any type of information to verify their identity with official documentation.

Follow Web security best practices – Whenever in any kind of doubt with respect to proper protocol, employees should be advised to refer to all other best practices for conduct related to email, social networking, Internet activity, and other Web activity.

Defending Against Malware Attacks

Given the fact that the entire retail digital landscape and ecosystem is supported by, and connected to, an endless series of software, systems, programs and applications, the threats posed by malware are innumerable and, most often, highly disruptive and destructive.

What is malware?

Malware, or malicious software, is any nefarious software designed, developed and deployed with the intent to damage a system and/or illegally obtain information. And, because malware is meant not to be seen, it’s often able to reside among the operating systems of desktop computers, laptops, smartphones and tablets, without being detected or removed by security safeguards.

What types of malware exist?

There are a number of different types of malware. However, the most common, and arguably the most effective, is the ‘virus’, which is capable of infecting operating systems before making a copy of itself and infiltrating another device. However, there are a number of other types of malware that retail businesses and their employees should be aware of. They include:

Worms – Similar to viruses, worms spread independently, without the need to attach to other files or programs.

Trojans – Disguised as legitimate software, trojans trick users into installing them.

Ransomware – Encrypting files on a victim’s computer allows attackers to demand a ransom in order to grant access back.

Spyware – Designed to secretly collect information about a user's activities, typically without their knowledge or consent, spyware can capture keystrokes, monitor browsing habits, and collect personal information from the unsuspecting.

Adware – Displaying unwanted advertisements on a user's device, while not always malicious, adware can be intrusive and negatively impact system performance.

What's malware's purpose?

Most commonly originating from email attachments and website downloads, malware is designed to infiltrate operating systems within digital devices, infecting files, corrupting or deleting them altogether, allowing for the illegal capture of sensitive information.

What can retail organizations do?

Although malware is often incredibly effective in serving its purpose, there are a number of things that retail organizations can do in order to safeguard their businesses systems and digital information.

Anti-malware software – As a result of the proliferation of different types of malware, a range of anti-malware software now exists, providing users with the ability to scan all files that are incoming to the organization and block anything that it deems suspicious or that it suspects is embedded with malware.

Firewalls – Retail organizations may also want to install firewalls within their computers and systems in order to prevent connection to malicious and nefarious websites. In addition, many firewalls are also able to prevent many types of malware from even entering the system

Provide employee training – Along with the implementation of anti-malware software and firewalls, all employees within the organization should receive ongoing security awareness training.

Heed warnings – All employees within the organization should be aware of warnings on websites and emails of potentially malicious content, and heed those warnings fully.

Report alerts – If a report or warning is received by an employee from the anti-malware software implemented on a retail organization's computer or device, it should be immediately reported to a supervisor or manager.

Isolate suspicious emails and files – Employees should be advised to never open, forward or share suspicious emails or attachments with others.

Ensuring Proper Authentication Practices

When dealing with such large amounts of sensitive data and information, it's incredibly important that the authentication practices that have been designed by retail organizations are followed by all employees within the retail organization.

Passwords

Commonly used to protect a range of different accounts and systems containing a plethora of business information and tools, passwords are a necessary layer of protection within the retail digital ecosystem. However, if not used properly, passwords can become a vulnerability within businesses that expose them further to the threats of cybercriminals.

Maintain control and confidentiality – Ensure that employees understand the importance of keeping their passwords safe, secure, and unknown to others around them.

Avoid using weak passwords – Employees should avoid using easy-to-guess passwords that can enable others to gain access to their files and information.

Avoid using the same password – It should be made clear to all employees that, in addition to avoiding the use of easy-to-guess passwords, they should also avoid using the same password for every account and device.

Change password frequently – Passwords should be changed frequently by all employees to avoid complacency and reduce predictability.

Develop a policy – It might be a good idea for some retail organizations to develop a password policy that identifies for employees simple rules to follow when creating passwords.

Avoid common and simple – When creating passwords, employees should avoid the use of common phrases such as "password" or "enter", simple sequences of numbers such as "1234", and easy-to-guess personal names such as a child's first name.

Size matters – The more characters that are in a password, the more effective it is. So, be sure to create passwords that are at least eight characters long.

Combined strength – Passwords are also stronger when multiple types of characters (uppercase letters., lowercase letters, numbers, and special characters) are used in combination with each other.

Passphrases

For some retail organizations looking for a more enhanced form of security, the use of passphrases instead of passwords might be a smart consideration.

For instance, rather than using the password “G0bLUe!”, a passphrase such as “Thosewhostaywillbe-champions!” becomes that much harder to guess. In addition, acronyms can be used in place of longer phrases (i.e. “hailtothevictorsvaliantthechampionsofhtewest!” becomes “httvvtcotw!”), requiring fewer characters to be typed, but maintaining its effectiveness in protection and security.

Cybercriminals are constantly developing newer pieces of software designed to hack and guess passwords. In light of this, some retail organizations might want to consider using any one of a number of free online tools that demonstrate for users the relative strength or weakness of any given password or passphrase.

Two-Factor Authentication

Much more difficult to guess than passwords or passphrases are two-factor authentications, which have the ability to add a layer of complexity and security to any retail organization’s systems.

Essentially, as the name implies, two-factor authentication requires the person or system seeking authorization to provide two pieces of authentication – one factor is known by the person or system (like a password), and the second factor is something, permanent or temporary, that can be used to authenticate the person or systems identity (such as a fingerprint or temporary password).

As technologies continue to become more powerful and intuitive, and the capabilities of artificial intelligence and machine learning increase unabated, two-factor authentication is increasingly becoming a necessary implementation in order to enhance the protection and security of a retail organization’s assets, information and systems.

Reporting Incidents

If an incident of cybercrime occurs involving an employee within the organization, the employee should not hesitate to report it to supervisors and managers within the organization. If it’s suspected that the incident has compromised the business in any way, retail organizations should:

Report the Incident to Local Law Enforcement

Report the incident on the National Cybercrime and Fraud Reporting System here, alerting the Royal Canadian Mounted Police (RCMP), the National Cybercrime Coordination Centre (NC3), and the Canadian Anti-Fraud Centre (CAFC), in order to protect the organization today and help safeguard it against similar threats in the future.

iv. Securing Digital Communication

Most, if not all, communication between colleagues, associates and business partners today is conducted via email. However, as mentioned, email is increasingly being targeted by cybercriminals as a way by which to infiltrate retail organizations, computers, devices and systems in their quest for sensitive personal and business information.

In order to ensure the utmost in protection and security when working with email, all employees should be aware of the most common ways by which cybercriminals attempt to leverage email to their advantage.

Spam

Representing the vast majority of email communication that's sent over the Internet, Spam is email that has been sent unsolicited and without the recipient's permission, and is often disguised as product or service promotion or an offer that can be redeemed by clicking a link or visiting a website. By proxy, spam is incredibly intrusive and annoying to receive. However, if links are clicked or attachments are opened, malware is often downloaded onto the computer that it was accessed on, slowing down networks and servers, resulting in increased costs and |a downturn in productivity.

Retail organizations will want to ensure that their employees are mindful of the messages and emails that they're receiving and that they are cautious to identify possible spam messages.

Sender recognition – Employees should treat any communication that comes from an unknown sender with caution.

Spelling mistakes – In order to circumvent spam filters and other security features, cybercriminals will intentionally misspell words in the subject line of the email. Employees should not ignore this obvious flag.

Awkward phrasing – In addition to misspelled words, the body of the email communication will often contain awkward or unusual phrasing, indicating that the sender is perhaps not legitimate.

Be wary – If the email promises offers that seem too good to be true, requests that links within the message be clicked on, or asks for personal or business information, it's likely spam.

Phishing

An extremely pointed and specialized type of spam, phishing email communications are designed to look exactly like a legitimate message, and are often disguised as communication from a government agency, banking institution or other official organization. Often, these types of spam communication are painstakingly developed, sometimes using real logos, fonts, colour palettes, and imagery, and are indistinguishable from legitimate communication.

The purpose of phishing emails are similar to that of spam. However, their tactics are a little different. Rather than promote a service or product, phishing emails typically use either a helpful tone to engender trust, or intimidating messaging to create fear, each with the objective of eliciting a response or the clicking of a link.

The scope of phishing attacks is constantly expanding, but frequent attackers tend to utilize one of these four tactics:

Embedding links into emails that redirect users to an unsecured website requesting sensitive information.

Installing Trojans via a malicious email attachment or posing ads on a website that allow intruders to exploit loopholes and obtain sensitive information.

Spoofing the sender address in an email to appear as a reputable source and requesting sensitive information.

Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Ways to block phishing attacks:

Employees should always be suspicious of potential phishing attacks, particularly when they don't know the sender. Here are five best practices to follow in order to help make sure employees don't become helpless victims:

1. **Don't reveal personal or financial information in an email –** Make sure employees know not to respond to email solicitations for this information, including clicking on links sent in the emails.
2. **Check the security of websites –** This is a key precaution to take before sending sensitive information over the Internet. <http> indicates that the website has not applied any security measures, while <https> indicates that it has. With this in mind, employees should practice safe browsing habits while also understanding that websites that do not serve a legitimate business purpose are also more likely to contain harmful links.

3. **Pay attention to website URLs –** Not all emails or email links seem like phishing attacks, so employees may at times be lured into a false sense of security. Many malicious websites trick end users by mimicking legitimate websites. One way to figure out whether or not the website is legitimate is to look at the URL (if it's not hidden behind non-descript text). Employees may also be able to detect and evade the scheme by finding variations in spellings or a different domain (e.g.,.com versus .net).

4. **Verify suspicious email requests –** Contact the company the emails are believed to be from directly. If an employee receives an email that seems suspicious from a well-known company, such as a bank, reach out to the bank using means other than responding to the suspicious email address. It's best to contact the company using information provided on an account statement—NOT the information provided in the email.

5. **Keep a clean machine –** Utilizing the latest operating system, software and Web browser, as well as antivirus and malware protection, are the best defenses against viruses, malware and other online threats. Check with your management and IT department for approved and safe Web browsers.

What to do with phishing emails?

It's important to make employees aware of the prevalence of phishing scams and protocol concerning the way in which they report a suspicious communication. In most cases, employees should be instructed to avoid sending and sharing the message with anyone else, and instead save it in order to show a supervisor or manager. And, do not delete these types of suspicious messages, even after a supervisor or manager has been notified.

In addition, contact your IT security representative for your organization and inform them of the phishing email. IT security will want a copy of the email so that they can investigate and block the source. They will provide instructions for you to follow.

v. Securing Data

Within this ever-digitizing world, retailers are in possession of, and handling, an enormous amount of data at all times. Given the importance of the data that they're collecting every day to the growth of their businesses and optimization of their operations, it only makes sense that it be secured and protected as tightly as any other asset.

Why Back Up Data?

Backing up digital and physical files is a practice that helps to retain important data, and restore lost of damaged files. In addition, and perhaps most importantly, if executed properly and effectively at a regularly scheduled frequency, back up plans allow retailers to recover quickly and seamlessly in the event of a system crash, data corruption or other setback occurs.

Backing up Data

The most effective way for retailers to ensure the proper maintenance of data is to develop a back up plan for it – one which all employees of the company will abide by, adhering to a strict set of back up practices.

Back up frequently – Employees should be instructed to back up data regularly as per the back up plan, whether hourly or daily.

Physical storage – In conjunction with frequency, ensure that data is backed up in a number of different ways, including on physical hard drives, in order to add another layer of security.

Data destruction – Data that has not been backed up, which will be discarded by the company, should be thoroughly destroyed. Delete all digital files and shred all physical documents to avoid the potential of its use against the business.

Back Up Options

There are a number of ways by which data can be backed up by retail businesses, ensuring its short- and long-term security.

USB hard drive – Depending on the size of the business, portable or desktop USBs might serve as a suitable back up option.

Server – Ideally, data should be stored on the business' Local Area Network (LAN) and backed up automatically from there.

Online – Retailers can also choose to back up their data to the Internet, allowing third-party service providers to take care of backup and restoration.

Handling Sensitive Information

Given the amount of data that retailers are working with on a consistent basis, at least a portion of it can be deemed as sensitive, including personal employee information, as well as customer and financial data. As such, the mishandling of this data could result in unauthorized access to it, its loss, or manipulation and modification of it, and a range of damage to the business and its customers. In light of this, all employees should be versed in best practices related to the handling of sensitive data.

Restrict access – When data is not being used, whether digital physical files, it should be locked up with restricted access to a small number of employees, and secured by a combination of electronic and physical safeguards.

Label correctly – In order to ensure proper maintenance of sensitive data, files and documents should be properly labelled and stored accordingly.

vi. Securing Remote Access

A lot has changed within the North American business environment over the course of the past few years, with the popularity of remote access working among employees surging, and the adoption of these new work arrangements by companies everywhere increasing. It's proven to be a real boon for business, saving companies time and money, while boosting employee productivity. However, along with this evolution of work conditions and environment comes greater risks of exposure to cybercriminals and their digital schemes. Though, with the right controls in place and practices assured, much of the threat posed by cybercriminals can be allayed.

The Basics of Remote Computing

For retail businesses that have decided to grant their employees the benefits of working remotely, access to their networks will likely be provided via the Internet. And, although it proves to be an easy and efficient way to connect employees to their work, despite their location, connecting over the Internet is not considered a secure way to exchange information, providing cybercriminals with more opportunities than ever before to exploit weaknesses in digital policy and practice.

As a result, it's a good idea for retail businesses to use a secure Virtual Private Network (VPN) to connect employees to their networks, as they allow for the encryption of the connection, rendering communication and the transfer of information unusable to anyone aside from the person that the message was sent to.

It's advised by most to combine the use of a VPN with other safeguards and layers of protection mentioned throughout this guidebook, and that employees follow a set of best practices to ensure the security of remote access working.

Limit remote access to authorized employees with a clear business need. Access should only extend to the applications, information and services that are required for work to be performed.

Remote Access Agreement – All employees who enjoy remote access to do their work should be required to sign a Remote Access Agreement which outlines and highlights the related responsibilities and best practices.

Adjusting access – It's important to allow for the adjustment of remote access privileges in the event that responsibilities of individuals within the company change.

Assigned computers – It's a very good idea to provide employees with remote access with business computers that have been set up and enabled with the software and safeguards decided upon by the business to ensure greater security and control.

Label and record device information – Before assigning business computers and other devices to employees with remote access, they should all be labelled, with serial numbers recorded, in order to help track their configurations or with their recovery if they are ever lost or stolen.

Working From Home

The most common remote access arrangement is work-from-home. It's a simple and convenient way for employees to connect with their employer. However, if using a personal computer to do so, additional risks could be exposed, providing retail businesses and their employees with a few requirements to take care of in order to increase the security of work-from-home.

Restricting wireless access – All employees, when working from home on personal computers, should connect their computer directly to a router using an Ethernet cable, and connect the Ethernet cable to the modem, in order to prevent anyone outside of the network from listening to, or intercepting, communication.

Secure Wi-Fi – Employees should be advised to secure their Wi-Fi connection in order to prevent cybercriminals from gaining access to sensitive business information.

Change default network name – Employees working from home should change the default Wi-Fi network name and the router access password on the network router. This will allow for a more secure connection.

Network encryption – Network encryption should be turned on, preventing any intercepted communications and sensitive information from being used by cybercriminals.

Limited access – In addition to digital safeguards and security features, employees working from home on their personal computers should also be vigilant in taking physical precautions, limiting access to the computer that they do their work on.

Working While Travelling

The digitization of the world around us, combined with a new working reality, means that today's retail business is very much a portable one, allowing employees to work wherever and whenever they want, including while travelling and on-the-go from one destination to another. As a result, data and information housed within a retailers' digital ecosystem becomes that much more exposed to risk, requiring employees to exercise caution and to follow best practices when working while travelling.

Avoid questionable connections – When on the road, working from a hotel or airport, or anywhere in between, employees of retail businesses should always avoid using unknown or questionable Wi-Fi connections. Although they may be free, they are often not very secure.

Keep your devices close – Employees should never, ever leave their work devices, whether laptop, tablet or smartphone, unattended while working in a public workspace or anywhere else while on the road.

Protect confidential information – It's always a good idea for employees to protect any confidential or sensitive business information from being seen by those around them while working in public workspaces. Consider dimming the screen and sitting in an area where the screen cannot be viewed from any angle.

vii. Securing Digital Devices

Some of the more significant and important components and tools within the evolving digital retail ecosystem are the different devices that are leveraged by retail businesses and their employees in order to communicate, share information and collaborate on work. But, given the fact that each device represents one more possible entryway into a network or system, cybercriminals are increasingly targeting them in hopes of finding a breach. Therefor, it's becoming incredibly important for retail businesses to properly manage the use of these devices that are mobile and in frequent use.

Tablets and Smartphones

Some of the most common devices used by retail businesses and their employees, tablets and smartphones are unfortunately also some of the most targeted items for theft. And, if a tablet or smartphone issued by a retail business goes missing, it's susceptible to a number of negative outcomes, from damage and loss to the exposure to malware. And, worse, sensitive information and network tools can be vulnerable to misuse. In order to avoid the worst, there are a few things retailers will want their employees to consider.

Take precautions – It's important that employees understand that they should treat their tablets and smartphones with the same care and security precautions as they apply to other tools, like laptops and personal computers.

Systems access – Employee devices should be locked when not in use, and set up within the retailers' system to be accessed by password only, thereby protecting sensitive information, data, and network tools.

Safe and secure – While travelling, or on route from one destination to another, employees should ensure that proper safeguards are in place in order to protect the security of sensitive information contained within communications.

Portable Data Storage

Many retail businesses leverage the use of portable data storage devices, including portable hard drives and portable flash drives. They present a quick and easy way to transport large files and documents from one device to another. However, these devices also represent, yet again, another potential way by which cybercriminals can infiltrate a business' systems or networks. As a result, retail businesses and their employees should exercise precaution when using portable data storage devices.

Use existing safeguards – Most mobile devices today are equipped with security features, including anti-malware software, which should be enabled on each business-issued device.

Ensure encryption – All portable data storage devices should be encrypted to ensure that any and all information placed on it is protected and secured.

viii. Securing the Physical Space

Although the safeguards and layers of protection that will be put into place in order to secure the digital retail landscape, like authentication and encryption, are obviously necessary, the critical physical aspects of security can not be forgotten in order to ensure the utmost effectiveness of a retailer's cyber security efforts.

Out of sight – When employees are not at their physical work stations, any files, documents, CDs, USB memory sticks, or anything else that contain sensitive or confidential data and information should be put away and out of sight, including information about the business, personal information or customer information.

Lock up – Employees should always disable their computers whenever they leave their work stations. This can be done within most systems by entering a combination of keys. The computer can then be accessed again by its user by entering their password.

Avoid 'messy desk' mistakes

There are a number of other 'messy desk' mistakes that are commonly committed by employees which need to be addressed and avoided in order to limit the threat of cybercriminals.

Leaving computer screens on without password protection – Anyone passing by has easy access to all of the information on the open device. Be sure to lock down screen settings.

Placing documents on the desk that could contain sensitive information – It's best to keep these types of documents locked up in drawers and file cabinets.

Forgetting to shred documents before they go into the trash or recycling bin – Any document may contain sensitive information. It's best to shred everything rather than taking a risk.

Failing to close file cabinets – This makes it easy for someone to steal sensitive information and more difficult to realize a theft has occurred.

Leaving mobile phones and USB drives out in the open – These types of devices likely contain sensitive business or personal information and are easy to pick up quickly without being noticed.

Neglecting to erase notes on whiteboards – They often display confidential information concerning products, new ideas and proprietary business processes.

Leaving backpacks out in the open – There's often at least one device or folder with sensitive information inside everyone's backpack or bag.

Writing usernames and passwords on slips of paper or post-its – It's especially important to avoid doing this given the fact that usernames and passwords are typically used to log into more than one site.

Leaving behind a key to a locked drawer – This makes it far too easy for someone to come back later, perhaps after hours when no one is around, and access confidential files.

Displaying calendars in the open or on the screen for all to see – Calendars often contain sensitive dates and/or information about customers, prospects and/or new products. Keep them filed away or hidden from view.

Leaving wallets and credit cards out on the desk – This is more likely to impact the employee, but wallets may also possess corporate credit cards and security badges that should be kept safe and secure.

In today's fast-paced world in which employees are always on-the-go, too much time is required to determine whether or not documents, USB drives, devices, and other items contain sensitive information. The safest practice is to make sure everything is filed away, destroyed or locked up.

ix. Resources for Retailers

To help retail organizations further protect and safeguard their businesses from the threats of cybercrime, below is a list of additional resources to reference and access when needed:

Retail Council of Canada's Retail Cyber Secure Program:
https://www.retailcouncil.org/retail-cybersecure-program-rcc/

Canadian Centre for Cyber Security:
https://www.cyber.gc.ca/

Canadian Centre for Cyber Security - Alerts and Advisories:
https://www.cyber.gc.ca/en/alerts-advisories

Canadian Anti-Fraud Centre:
https://antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm

Government of Canada – Cyber Security:
https://www.canada.ca/en/services/defence/cybersecurity.html

RCC RETAIL COUNCIL OF CANADA CCCD CONSEIL CANADIEN DU COMMERCE DE DÉTAIL