BRITISH COLUMBIA | Ministry of Citizens' Services

Security 101 Guidebook

The Basics of Information Security in the Government of British Columbia

Information Security Branch
Ministry of Citizens' Services

Document Created October, 2012
Updated September, 2019

"It is the responsibility of every employee to protect government information"
Gary Perkins, Chief Information Security Officer

INTRODUCTION

Technology has become so much a part of today's society that almost every household in Canada has at least one computing device and computers in some form are part of most workplaces. In only the past several years in the BC government, software applications and e-business have been widely introduced to improve the delivery of services and programs to citizens. BC government workplaces have been continuously evolving to improve and enhance the ways in which employees and citizens interact. For BC government employees, access to the appropriate computing hardware, software and mobile devices has meant ongoing change and continuous learning. Changes have sometimes seemed so rapid and complex that employees have been concerned about learning all they need to know about the technology they now use every day.

Protection of the information in the care of the BC government will always be a priority. Citizens must have confidence that the government will protect their personal information and trust government's intention to use that information only as required.

Information security has grown more critical than ever before as technology has become more ubiquitous and more complex. Why? Because computer crime by cyber criminals has become one of the most important issues faced by all organizations and individuals. As new devices, software and apps are introduced, there are computer criminals around the world who work very hard to exploit any vulnerability they can find or create.

Why Have a Guidebook on Information Security?

After all, isn't security built into the devices and software we use? Don't the "techies" sit in BC government spaces somewhere taking care of that for us? Yes, and yes. The tech staff and contractors do a great deal of work to ensure the security of the entire government network and the data used every day. Year after year, however, research and experience have demonstrated that most data breaches in all types of organizations occurred because the people that use the information – the employees – were not given the guidelines and education they needed to recognize the simple actions they could take to prevent breaches. It has also found that some users do not apply these guidelines, thereby leaving the opportunity open for a data breach. Security researchers refer to employees as "the weakest link" in the security chain. Information security education and awareness is the most cost-effective form of data protection.

While information security has become more complex, the methods used by cyber criminals are known and can be combatted. The purpose of this Guidebook is to enable and empower BC government employees to protect the information in their care by describing the methods used by cyber criminals and what can be done. It was prepared by the Information Security Branch in the Office of the (Government) Chief Information Officer as part of the Information Security Awareness Program. This Guidebook provides an overview of the BC government policies on information security, describes security threats and risks, outlines employee roles and responsibilities, and offers security tips and best practices for all employees to follow.

This Guidebook is intended for employees handling government information, however, the security threats and tips described will generally also apply to the use of your home computer or the various types of mobile devices (e.g. laptops, tablets, e-readers and smartphones) available on the market. By becoming aware of the ways in which to protect information from those trying to obtain it, you can adopt a 'security state of mind' and reduce the likelihood of being a victim of cybercrime.

What is Information Security?

Information is an asset and the information that government collects, uses, maintains, stores, transmits and may eventually dispose of, is central to the work of every part of the government. The BC government is aware of its responsibility to protect that information and to ensure that the public has confidence in government's ability to protect the privacy and security of their personal information. This includes financial details, medical records, drivers' records and more.

Information security is about protecting information, software, and equipment from problems relating to disclosure, modification, interruption and disposal. With the information itself, requirements for privacy, confidentiality, integrity and availability must also be addressed.

What Kind of Information Do You Need to Protect?

As a government employee, you have access to a tremendous amount of information; therefore, the Office of the Chief Information Officer recommends that you become familiar with the contents of this Guidebook. In the BC government, there are three types of information that need to be protected: Personal, Confidential and Sensitive.

Personal Information:

Personal information means recorded information about an identifiable individual other than business contact information. Personal information can be about government employees, government clients or others and may be held by government or administered by service providers on behalf of government.

Personal information includes, but is not limited to:

- Name, address, telephone number, email address
- Race, national/ethnic origin, colour, religious or political beliefs or association
- Age, gender, sexual orientation, marital status
- Identifying number or symbol such as social insurance number or driver licence number
- Fingerprints, blood type, DNA prints
- Health care history
- Educational, financial, criminal, employment history
- Anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

Confidential Information:

There are various types of confidential information, but generally confidential information can be described as:

- Cabinet confidences (e.g., a briefing note to Cabinet or a Cabinet submission);
- Government economic or financial information (e.g., proposed budget before it is announced);
- Information harmful to intergovernmental relations (e.g., information received in confidence from another government);
- Third-party business information, where the disclosure of the information would harm the third party.

Sensitive Information:
Personal and/or confidential information are examples of sensitive information that, if compromised, could result in serious consequences for individuals, organizations or government. For example, personal information about an individual within a witness protection program is deemed as sensitive information because, if compromised, it could lead to serious harm to the individual. It also violates the requirements of the *Freedom of Information and Protection of Privacy Act*. Similarly, the architectural drawings of a correctional facility are examples of sensitive information because of the nature and function of the building and how the information could be used.

Who Looks After Information Security in the BC Government

The Office of the Chief Information Officer is the central office in government with responsibility for information security. This responsibility derives from Chapter 12 of the Core Policy and Procedures Manual (CPPM) and is implemented by the Information Security Branch. Specifically, Chapter 12.2.2 on Security states that the OCIO:

- Provides the overall strategic direction and policy for securing government's information technology infrastructure and government records including electronic information.
- Ensures that measures are established to assess compliance with IM/IT security policies, procedures and standards.

The Information Security Branch (ISB) developed an overall information security program which promotes a risk-based approach to information security that supports government in achieving its goals, and ensures programs, plans and processes are in place to appropriately manage information security risks to an acceptable level. The ISB has the following areas of concentration:

Security Awareness conducts education and awareness activities intended to create an awareness of current information security threats, risks and best practices for government and the Broader Public Sector by way of events, websites, weekly news and various types of materials in support of the protection of information.

Advisory Services provides subject matter expertise by way of consulting services across government on new technology and major initiatives. The Unit also manages government's information security program and Information Security Policy, conducts security audits or reviews as required, and develops and provides advice on information security standards and architecture.

Investigations and Forensics manages the investigation of detected or reported security incidents (actual and potential) to breaches of the Information Security Policy or other issues that may affect the confidentiality, integrity and availability of governments information or infrastructure. The unit leads investigations in Phishing, cyber/network attacks, endpoint investigation, suspicious behaviour, unauthorized data/system change, inappropriate/unauthorized system provisioning and credential misuse. The unit provides technical assistance and evidence collection services to CIRMO, BC Public Service Agency, BC Coroners Service, internal and external Compliance and Enforcement units and BC government Civil and Criminal Litigation groups.

Vulnerability & Risk Management provides the framework and support for information security compliance management, including providing tools and training to ministry information security staff to support the risk management process. The Unit manages government-wide information security assessment activities and key information security risks through tracking and reporting on all known security issues which pose a risk to government information.

Security Operations architects, designs, implements and supports a number of operational security services, including Firewall/Access Control, Content Filtering, Intrusion Protection, Application Scanning, Denial of Service protection, and a Security Information and Event Management (SIEM) service.

Access and Directory Management: The Access and Directory Management Services team provides the directory infrastructure and ID administration services for all Government staff and many Broader Public Service (BPS) organizations. The team also operates Government's web access management and single sign-on environment, enabling Government programs and BPS organizations to securely deliver their online services to citizens, businesses, and staff.

There are also IM/IT staff throughout the Office of the Chief Information Officer branches and Ministry Information Security Officers and numerous others in roles throughout government that support the protection of the government's information resources, as well as contractors and vendors that provide services on behalf of the government.

Employee Roles and Responsibilities in Relation to Information Security

Commitment: BC government employees are required to take an Oath of Employment and to abide by the Standards of Conduct. Both require that employees uphold the confidentiality of government information. These expectations are not unique – employers everywhere expect employees to respect the importance of the information they access on the job.

Adherence to Legislation and Policy: The *Freedom of Information and Protection of Privacy Act* and its Regulations are important for anyone working within the BC government and all public sector organizations within the province. In addition, BC government employees are responsible for complying with the Information Security Policy, other security-related policies and standards, information management policies, and approved standards and practices, while accessing government computers, mobile devices and other equipment, information and services.

Training Courses: All BC government employees are required to take a mandatory online training course – IM 117 Information Management: Access, Information Security, Privacy and Records Management, to learn what they need to know about privacy, security and records management.

There are a number of valuable online security and privacy courses provided by The Learning Centre of the BC Public Service Agency, including: *IM 113: An Overview of Information Security and You*, *IM 114: A Day in the Life; Information Security and You – Knowledge Check and IM 118: Information Security and Awareness: Supporting Employees in the Workplace*. There is also an *IM 500 Executive Role in Information Sharing* for excluded positions, from the Director to the Deputy Minister level.

Regardless of one's job duties or level within an organization, it is every employee's responsibility to learn more about information sharing, privacy and security by participating in these courses. All that is needed is your supervisor's approval. The courses are delivered online and can be taken at your convenience. For information and to register, go to the @Work BC government employees' site at https://gww.gov.bc.ca, Click on 'Tools and Resources' for the drop-down menu, then 'Learning System', where you can start your search.

Your contribution to ensuring and maintaining information security benefits every British Columbian, including you, as an employee and as a citizen who accesses and receives government programs and services.

What are Information Security Policies and How Do They Relate to You?

Policy is intended to enable progress by giving individuals the direction they need to properly and consistently accomplish work-related tasks. Information security policies document appropriate behavior, clearly describe what must be done, and outline what is or is not allowed.

As an employee, you need to know, understand, and follow government policies. In June of 2006, the British Columbia government adopted a comprehensive Information Security Policy (ISP) based on international standards, which applies to all employees and the work they do. The ISP (current version 4.0) is available at the OCIO Information Security Policy page.

https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy-and-guidelines

The ISP 4.0 (PDF) provides the foundation for the information security governance program, which includes standards, procedures, training and awareness material, all of which are used to protect government information and information systems. All employees need to be aware of their responsibilities to safeguard government information. The Information Security Policy supports security requirements in the *Freedom of Information and Protection of Privacy Act* and the *Information Management Act*.

What If There is an Information Security or Privacy Breach?

The BC government has a comprehensive Information Incident Management Process (IIMP) for responding to privacy and security breaches. An information incident (a broader term than "breach") occurs when unwanted or unexpected events threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, unauthorized alteration or destruction of information. An information incident can be especially serious when it is a privacy breach where the compromised data includes personal information such as names, birthdates, health or financial details, or social insurance numbers, or involves sensitive information such as Cabinet documents.

An all too frequent incident in offices everywhere involves employees clicking on a link or opening an attachment in a phishing email that was sent by a cybercriminal and intended to capture information or to download malicious code. A person can make a mistake out of curiosity or just being busy. The key to responding to information incidents is to act as soon as possible! You are responsible to report any actual or suspected (or accidental) information incident immediately to your supervisor. You or your supervisor must also immediately report the incident by dialing the Shared Services BC (SSBC) Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and selecting Option 3. You will then be contacted shortly by either the OCIO Information Security Investigations Unit or the CIRMO Information Investigations Unit, who will seek further details and will provide advice on next steps.

If there is a desktop computer, laptop or mobile device involved in the information incident – disconnect it from the network, do not shut it down; secure it until the situation has been reported and you receive information from the Investigations Unit.

The Information Incident Management Process policy document, Checklist, Easy Guide, Process for Responding and the Report Form all can be found at:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-breaches

Who Should You Contact Regarding Information Security?

Every ministry has a Ministry Information Security Officer (MISO) who is the single point of contact for information security issues and related concerns in their ministry. The MISO in your ministry has a good understanding of current information security threats, risks and policies and will know when it is appropriate to conduct Security Threat and Risk Assessments (STRAs) and Privacy Impact Assessments (PIAs) on projects or initiatives within the scope of your work.

As defined in the Information Security Policy (ISP) the Ministry Information Security Officer (MISO) is responsible for:

- Ensuring that standards/procedures to support day-to-day security activities are documented in compliance with the Information Security Policy;
- Coordinating information security awareness and education;
- Investigating reported information security events to determine if further investigation is warranted;
- Providing up-to-date information on issues related to information security;
- Assisting business areas in conducting Security Threat and Risk Assessments;
- Ensuring that each information system has a current System Security Plan;
- Providing advice on security requirements for information systems development or enhancements;
- Coordinating ministry information security initiatives with cross-government information security initiatives;
- Providing advice on emerging information security standards relating to ministry specific lines of business; and,
- Raising ministry security issues to the cross-government Information Security Advisory Committee, which is co-chaired by a MISO and a member of the Information Security Branch.

BC government employees can obtain the contact list of MISOs for each ministry at the following internal website https://intranet.gov.bc.ca/thehub/ocio/ocio-enterprise-services/information-security-branch/miso-contacts

While the OCIO is accountable for the strategic direction of IT across government, Deputy Ministers are accountable for ensuring that their ministries adhere to IT governance directions provided by the OCIO. This responsibility is usually delegated to a Ministry Chief Information Officer (MCIO). Each ministry has an MCIO, although some MCIOs have responsibility for more than one ministry. Generally, the MCIO:

- Reports to their respective ministry assistant deputy minister (ADM) accountable for IT, or directly to their Deputy Minister in the case of ADM-level MCIOs
- Is a member of the CIO council
- Maintains accountability for all ministry business and operational IT initiatives (i.e. those which do not have cross-government implications)
- Manages ministry information and technology, and all related support activities

To contact your MCIO, please see the MCIO contact list (PDF).

You may also contact the Information Security Branch directly at OCIOSecurity@gov.bc.ca to ask questions about information security or this Guidebook.

SECURITY THREATS AND RISKS
Cybercrime Goals and Methods

Cybercrime has become a massive business that is occurring all the time, all over the world, and mostly undetected. It is a very lucrative world-wide illegal business, operating in "the Underground Economy". No longer is cybercrime primarily a hobby activity for individual criminals seeking new computer challenges to earn some money and prove their prowess. Systematic cyber attacks are also conducted continuously every day by nation states – countries that are trying to gain economic, political or military advantage by obtaining critical information about another nation's intellectual property, infrastructure, economy and the personal information of its citizens.

Cybercrime operations function much like legitimate organizations, with sophistication that includes a hierarchy of management, worker recruitment and training, job descriptions, distributors, low level helpers and advertising on their own hidden networks. Criminal accounts can be created, perform an attack, and shut down without being detected. They also operate on a global level with servers and connections in many countries to avoid detection. Cybercriminals who want to operate on their own can easily and cheaply purchase, or rent, the hacking software and tools they require online. The option also exists to hire or outsource this business, much the same way as legitimate organizations.

It is very important for all employees, at every level, to understand the role that they constantly play in protecting information and the many types of devices we use. In fact, employees that are not aware of the ways they can prevent security breaches pose a potential risk to their employer. Users have been referred to as the "weakest link" in the security chain due to a lack of information or poor computer practices. Employee awareness has become an essential component of information security in all organizations world-wide, regardless of their business. Security researchers consistently emphasize that employee awareness must be part of every organization's security budget and priorities. Compared to technology hardware, firmware and software solutions, security awareness for users has the "biggest return on investment" because one user clicking on a malicious link or opening a corrupted attachment can initiate considerable damage to their own computer, or to their employer's systems and information resources.

Cybercrime Goals:
Cybercrime in general has two major goals: (1) to steal personal and sensitive information with the aim of committing identity theft/fraud or for some other gain, and (2) to install malicious code into a computer system that will continue to perform tasks and gather information without the knowledge of the owner. Cybercriminals are continuously creating new methods (and variations of existing methods) of infiltrating computers and networks to make money by stealing information and manipulating people, via social engineering, into unknowingly assisting them.

Their Goal #1: Identity Theft/ Identity Fraud

The Criminal Code of Canada recognizes that identity theft and identity fraud are two separate but related crimes. Identity Theft involves acquiring and collecting someone else's personal information for criminal purposes, while Identity Fraud is the actual deceptive use of the personal information, the identity, of another person, living or dead, without their knowledge or consent. The identity fraud often involves using someone's credit card for making transactions, selling their information in the underground economy, or actually setting

up a separate identity that can involve taking out loans, buying homes, buying goods and services, filing a fraudulent tax return or travelling over a period of time, under their victim's identity. It can take years of financial and emotional costs for a victim of identity fraud to undo the damage and restore their own credit rating.

Identity theft and fraud also includes a criminal fraudulently using your work or personal email address (and those of your contacts) to send out spam email that appears to come from you – referred to as 'spoofing'. This is extremely important for the protection of information. When a data breach captures the names and email addresses of online users, i.e. the Contacts, the attackers might not get the users' financial information, but they can still benefit by having their email addresses. Most people would not imagine that their home/personal email holds the key to unlocking much of their online identity, but it is from their email that people make online purchases, access websites, send and receive photos, make travel plans and share intimate information with family members and friends. As a BC government employee, it is essential that you do not share your work credentials – your IDIR logon account name and password – with anyone for any reason. (There are tools, called permissions, available to share your calendar, for example, without ever giving or receiving a co-worker's or supervisor's password.) The information provided here will let you know how to avoid having your work credentials stolen using the Internet.

Their Goal #2: Install Malicious Code or Malware

Malicious code is the term used to describe software (a computer program or application) designed to exploit, infiltrate or damage a computer system without the informed consent of the computer user. It is generally referred to as "malware" and includes computer viruses, worms, Trojan horses, rootkits, spyware, dishonest adware, and other unwanted software. Malicious code is typically distributed over the Internet, by email or via compromised web pages. A user can click on a link in a phishing email that results in the attacker planting malware on the computer that can continue working, sending information back to the attacker. Websites and online ads can also be corrupted or even substituted with a fake one, so that visiting the sites has the same impact – with malware installed on the user's device. Appendix A provides a list of common types of malware.

Cybercriminal Methods:

Following are descriptions of the major threats to information security used by cybercriminals that can occur not only at work but also on home computers and mobile devices. Every technology user should become familiar with these cyber threats and how to avoid them.

Ransomware

Ransomware is highlighted first here because it is a damaging form of malware that has exploded world-wide over the past two years, including targeting the BC government, as well as other governments, hospitals, medical clinics, financial institutions, universities, major corporations, critical infrastructure, small businesses, law enforcement agencies and individual users. Unlike some forms of malware, ransomware announces itself immediately to the user. It infects a computer or network and spreads rapidly to encrypt the data, displaying a message to the user demanding a ransom (often payable in bitcoin or other untraceable currency) to have their data decrypted and re-gain access. Many organizations have paid this ransom in the hopes of regaining control of their computers, particularly in hospitals where patient care has been brought to a complete halt. Once a computer has been infected with ransomware and the files encrypted, the user has only two choices: pay the ransom and get the decryption key from the attacker or shut down their computer/network and have the entire system re-installed using the most recent backup files. Security professionals strongly advise everyone to always back up your computer data to an external drive and keep it separate and unattached.

There are three ways that computers are commonly infected with ransomware:

(1) via Email – the individual receives an email with a malicious link or attachment. The email offers a software or system update, or even anti-virus clean-up tools, and when the user accepts, the malware infection begins, spreading quickly, and the user receives the ransom notice. The user has to click on a link or open an attachment to begin the infection process, which makes it entirely preventable.

(2) via Malvertising – the individual visits a legitimate site that displays infected third-party advertisements. This attack vector is currently causing security incidents among organizations globally. Attackers use online advertisements that will appear to be official, legitimate ads, but are loaded with ransomware, hence the name "malvertising". When the user clicks on the unsuspecting ad, the malware payload immediately encrypts everything in its path, including shared drives (A:\ through to Z:\). One of the main viruses in play is called CryptoWall, and its variants – it has been around for a long time, infecting systems around the world.

(3) via Zero-Day Exploit – the individual visits a legitimate or illegitimate infected website. This is the most concerning because it does not require any input from the user. A zero-day vulnerability is a flaw that leaves software, hardware or firmware defenseless against an attack that occurs the very same day the vulnerability is discovered. Such an attack is called a zero-day exploit, meaning that there are zero-days between the time the vulnerability is discovered and the first attack. The infected website contains a zero-day exploit, such as those known to affect Java and Flash, and simply opening the website that contains the ad will run the ransomware without the user knowing. Security researchers and attackers work full-time to find vulnerabilities – the good guys seek to have them patched before they can be exploited.

Social Engineering

Social engineering refers to manipulating others. Historically, people who cheat others for personal gain have always been part of society, unfortunately. Con artists, frauds, cheats, and social engineers rely upon the fact that other people are essentially trusting and considerate, and do not go through life being suspicious. People are likely to respond to offers that sound "too good to be true".

Social engineers use methods such as shoulder-surfing (looking at your monitor, your keystrokes or papers on the desk), mass marketing telephone calls and texts, or fraudulent emails to obtain sensitive details. Generally, it is easier for attackers to take advantage of people in this way, rather than trying to locate and exploit computer security vulnerabilities. Many large breaches of security in companies world-wide started by social engineering an employee, usually with a phishing email, into innocently providing information that gave the cybercriminals access. Social engineering has always been used to breach physical security. Many criminals have gained access to a secure workplace by fraudulently presenting themselves as workers, contractors or tradespeople that are supposed to be there, and were not asked to provide proof of their identity.

Be suspicious of unsolicited telephone calls or emails requesting personal, financial or account information, or information about the government's network, its employees or clients. Ask yourself if you should be giving out the information – it is better to tell the person you will call back, so you can talk to someone else about it and get another opinion or check for details. If you do call them back, ensure you look up the number of the organization and do not use the number they gave you or what is on the call display. Use your instincts (also called your "gut feeling") – if something just does not quite "feel right", don't give the person what they are seeking without getting confirmation. If you see someone in your work area that might not belong there, ask questions. If you are even slightly suspicious of someone, then do not provide access or information to that individual. Instead report the matter to your supervisor or manager, and if appropriate, also report them to building security personnel. Lastly, remember to always secure ('Lock') your computer when you walk away from it so that no one else can view or use your computer.

Phishing

The use of phishing email is a common type of online fraud, identified consistently for many years as one of the top Internet-based threats used for credit card fraud and identity theft. 'Phishing' attempts to trick people into disclosing credit card numbers, online banking information and passwords. The method involves sending a fake email that appears to come from a legitimate and reputable source, such as a bank or other financial institution, an online shopping company, or a Help Desk. The email asks the recipient to enter their financial information (credit or debit number and password) or their credentials (username or IDIR ID and password) due to a problem, thereby preying upon the person's concern about their personal accounts and information. The email usually says that there is a problem and that the reader must respond immediately to avoid an account being closed, or having a penalty imposed. The intention is to create fear and a spontaneous response.

The BC government firewalls are constantly being updated to block evolving phishing attempts and spam. Phishing emails are flagged, reported and investigated all the time, and alerts are given where feasible. Unfortunately, phishing email arrives in employees' inboxes despite these efforts, and because of this, some employees believe they must be legitimate emails. Making matters worse, most phishing/spam emails originate from the account of someone who previously was phished and that individual's legitimate-looking email address was used (spoofed) without their knowledge. This also happens when the attacker obtains a user's contact list and sends out phishing and spam emails that appear to come from familiar names.

While the government will continue to receive refined, legitimate looking phishing emails that make it through the government email firewall, try not to be the one to get caught by phishing! Be wary and take a moment to examine unsolicited emails. Does it make sense that you are receiving it? If you have nothing to do with finances in your job, then you should not receive an invoice. Does the name of the company match the email address of the sender? Hover your cursor over the links within the email to see if they show the same in the viewing box. If you still want to go to the link then instead of clicking on that link, you can copy and paste the link into a new browser window to see what comes up. As for suspicious attachments that you do not recognize, the best advice is to not open them. Opening the attachment can invite malware, including ransomware. The best thing to do with any suspicious email is to delete it.

One common example of phishing emails are when malicious actors pretend to be system administrators advising users that they have exceeded the space available on their computer. Other recent phishing emails appear as if they are from Canada Revenue Agency (CRA), PayPal, Canada Post, UPS, Apple or one of the banks. The emails urge the recipient to act now or there will be a negative consequence such as cancellation of their accounts. Some emails will offer a positive outcome, such as a prize for responding.

Besides emails, there are other methods of phishing to be aware of:

- Spear Phishing is the targeted version with attacks that are customized to the recipient, usually corporate executives, and include details only an insider would know, thereby gaining trust.
- SMS phishing or smishing uses cell phone or smartphone text messages.
- Vishing scams make use of Voice over Internet Protocol (VoIP) which allows people to talk over their computer lines (e.g., Skype or FaceTime). The criminals leave an automated message saying the person's credit card or account has been compromised, and to call a number for information. The caller ID can be altered to appear that it comes from a legitimate source.

Remember that there is no business reason for anyone in the BC government, including a Help Desk, or any financial institution or online account to contact you and ask you to provide name, account numbers, passwords or any other personal or financial information. Do not click on any links, and do not open attachments – these are vehicles for attackers to install malware. Do not respond in any way and delete the email. Also, do not click on 'Unsubscribe' as it lets spammers know they hit a live address. If you think the email might be valid, contact the company directly by phone. Never disclose your IDIR password to anyone! If you think you have inadvertently responded to a phishing email, do not worry about feeling embarrassed – in a busy workplace, it happens more often that one might imagine. Just contact the Shared Services BC (SSBC) Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 and select Option 3. Reporting a potential phishing attack is very important as it could prevent the spread of further emails or potential damage to the network.

Spam

Spam emails (the electronic version of 'junk' mail) represent the overwhelming majority of emails sent world-wide on any given day. There are constant reports of BC government employees receiving spam emails which have not been blocked by spam filters. Internet hoax/false emails are spam, as are offers of loans and mass marketing emails trying to sell goods at great prices that are counterfeit (e.g., prescription drugs without a prescription, designer goods such as purses, shoes and jewellery, and even anti-virus software and college diplomas). Spam emails are almost always offers that are "too good to be true", which should serve as a warning in itself. It is usually because of these claims, however, that people are fooled and robbed via spam emails. Spam writers understand human nature and psychology – they prey on people's good and trusting nature, and on their desire to get ahead in some way. Never click on links in these emails. Spam email should be deleted without opening, and never forwarded to others. (Use the Auto Preview or Reading Pane features in the View tab to peek at an email without opening it – a very useful and safe tool.)

Text Spam

As technology continues to evolve and offer more features for consumers, new threats and risks emerge. The rapidly growing popularity of hand-held devices has spawned "mobile marketing" using cell phones and smartphones. The success of this new mobile cybercrime, as with other forms of fraud, depends upon our naturally trusting nature and our tendency to be in a hurry, combined with using small screens in our hands. The results for the user can be unwanted charges on your bill, unwanted text messages, and the potential for your device to be infected with malicious code that can steal your information and continue to cause harm.

Text spam usually comes in the form of fun things like quizzes and games. Recipients respond to a text or enter a code, after which they become an unintended subscriber and can find "third party charges" for "premium services" that are outside of an unlimited or fixed incoming text plan. BC government employees have innocently texted a response on their work device that resulted in unauthorized charges on their bills. The charges can come repeatedly and cost anywhere from 10 cents to 25 dollars each time and show as premium services. If the price plan on your government-issued cell phone or smartphone includes text messaging, incoming text messages are free, however, these plans usually exclude premium messages (roaming, international, alerts, contests and promotions). If you do receive a spam message, simply text the 10 digit number of the received message to short code 7726 (SPAM) – this works for all cell service providers.

Another form of smartphone spam is a phone number with an unfamiliar area code or prefix. An automated message might tell the user to just hit a number to go to a website and receive some reward. Entering the number is the same as clicking on a link in a phishing email – it can result in the capture of your information, future charges on your bill, and possibly the installation of malicious code or malware on your device.

Internet Hoaxes

Internet Hoaxes are the email equivalent of old-fashioned chain letters (i.e., send this message to ten other people for good luck) and the unwanted junk mail sent in bulk through the postal system. These emails are successful because they are very manipulative and prey upon the trusting emotions of the victims. The goals in sending these emails are to install malicious code and/or to capture personal and financial information or the names and email addresses of the recipient's contacts when the email is forwarded.

Hoax emails contain messages that are typically untrue and commonly contain warnings about computer viruses or supposedly hazardous products or they present tragic stories or pleas for financial assistance. These emails always appear following a natural disaster anywhere in the world, soliciting money to help those affected, but have nothing to do with a legitimate aid organization. You might receive an email saying you have won a lottery or contest you did not enter or have a large inheritance in another country. They can even contain positive messages to pass along to inspire other people. Do not click on any links in these emails. In the BC government, it is a violation of Information Security Policy to forward these emails to other employees or to your personal contacts. (If you want to send financial aid following a natural disaster, contact the Red Cross and seek their advice.)

SECURITY TIPS & BEST PRACTICES FOR EMPLOYEES

Protect Your Workstation

The BC government network is protected by up-to-date anti-virus software that provides protection from the various forms of malware described in Appendix A, such as rootkits and botnets. Because this is being done by information technology specialists, you may not have to worry about this aspect of computer security at work. You should, however, 'Restart' your computer at the end of the day so the network can push any new updates, especially security patches or fixes, to your computer.

Lock your computer every time you leave your desk. This will prevent unauthorized users from accessing either your personal systems or the government network and prevent others from reading your screen. In some offices, you may be required to Log Off your computer when you are away from your desk. Ask your manager for clarification. Whenever possible, ensure your computer is powered up and connected to the network at the end of the day for system updates and patches.

*To **Lock** your computer:*

- *Click the **Start button** in the bottom left corner, click on the **fifth circle above the start button,** then choose **Lock***
  OR:
- *Press **Ctrl, Alt and Delete**, then choose **Lock this computer** from the list on your screen*
  OR:
- *Press the **Windows key and L key** to Lock your workstation*

Protect Your IDIR Account

Individuals require authorization in the form of an IDIR account to gain access to the BC government network. Your IDIR account is your government user ID (an abbreviation of your name) which in combination with your password provides a secure single sign-on that is unique to you. They are your "credentials" and you have responsibility for actions taken using those credentials. It is essential that you protect your IDIR ID/password combination. If someone gets this information, they have access to everything that you have access to, which includes the government network. Serious harm could come to the government and its assets, so treat the protection of this information very diligently.

Protect Your Passwords

User IDs and passwords are personal and confidential and must not be divulged to anyone, for any reason. Your password must be known only to you and be complex enough that it cannot be easily guessed. BC government Information Security Policy states that *you are not permitted to share your IDIR ID and password with anyone, not even your co-workers, support staff or manager*. The most common reasons given for sharing user ID and password information is to enable someone to access another employee's files, to act on their behalf, or to perform a task that has been delegated. Tools such as shared drives and permissions, are available to enable employees to properly delegate authority to another employee. These tools all have appropriate security controls and audit trails in place to protect you. Contact your Ministry Information Security Officer if you need direction.

As a BC government employee, if you ever receive a phishing email designed to trick you into providing your IDIR ID and password – delete it, as there is no business reason for anyone in the BC government to phone or send you an email asking for this information. You will never receive a legitimate email at work from 'Help Desk'. If such an email is addressed from another government employee, that person likely was a victim of a successful phishing attack. Do not contact that person.

There are some circumstances in which you should report a spam or phishing email:

- When it appears to come from a government source
- When it is threatening
- If you clicked on a link or attachment
- If you disclosed your IDIR ID and password

In these cases, spam/phishing emails should be reported as an Information Incident by calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866-660-0811 (available 24 hours a day) and selecting Option 3.

Always remember - you are accountable for all actions performed using your IDIR ID and password. It is your password – 'Keep it Secret' and 'Keep it Safe'. Do not write it down. If you are asked for the use of your password, or someone offers you their password to access their account, remind that person (including your 'boss') it is a security risk and a violation of the Information Security Policy. Don't be afraid to say 'No'. Tools are available for delegating.

Do not use your BC government password on your home computer or personal devices. It is security best practice to use different passwords for various accounts on your home computer and mobile devices, so that anyone obtaining your password will not have access to all your accounts. Criminals will try!

BC government network passwords automatically expire after 90 days. You will receive an automatic notification prompting you to change your password, beginning 14 days before it expires. If you do not want to

change your password at that time, you can close the notice, but you will receive further reminders and must change your password before it expires. You can also change your password at any time by pressing **Ctrl**, **Alt** and **Delete** and selecting **Change Your Password**. It is advised that you change your password after travelling with your BC government-issued devices (laptop, tablet or cell/smartphone), especially if you were out of the country.

When you create your IDIR password, follow these rules:

- Minimum length is 8 characters.
- Must contain at least one character from 3 of the 4 categories below:
  - English upper-case characters (A-Z)
  - English lower-case characters (a-z)
  - Base 10 digits (0-9)
  - Symbols ($,#,*,%).

More discussion on the importance of passwords can be found at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/password-best-practices

Protect Your Workplace

Developing and implementing security-conscious work habits will reduce the likelihood of someone seeing business information they should not. Security-conscious work habits include:

- Ensuring only documents required for current work are removed from file cabinets
- Covering up, filing or storing confidential or personal paper documents when visitors are present in the work area
- Clearing, changing or turning off the computer screen (e.g., minimize open windows) when people without authorization are close by
- Using privacy screens on your monitor to reduce the angle that your monitor can be viewed from by other people
- Locking your workstation when you are away from your desk so that sensitive information is not displayed, and no one can access your computer
- Not discussing confidential or personal client or business information in open work spaces or public areas
- Clearing desktops and work areas when you plan to be away from the office
- Securing documents and portable storage devices in a locked desk or file cabinet and storing the key in a safe place
- Ensuring that outgoing and incoming postal mail is appropriately secured
- Locking doors and windows
- Checking fax machines and printers to ensure that no confidential or personal information is waiting to be picked up

If you need to discard any personally identifiable information, or drafts of any confidential government documents, do not place them in an open recycling container. Use one of the locked records destruction bins provided in many offices for record shredding, or alternatively, use an office shredder (cross-cut shredders are preferable and many of these also shred compact disks).

Also be aware of people who walk through your work area. A popular and simple form of social engineering is for strangers to show up and talk their way into a secured office area or storage room by pretending to be authorized workers. Another popular way for outsiders to access a secure area is to 'tailgate' or follow someone through an entry point. If you do not recognize someone, do not hesitate to ask who they are and ask to see their credentials. It is easy to make the assumption that the person is there to meet with someone in your office premises. Don't be afraid to ask questions – it shows that you are security conscious!

GENERAL INFORMATION

Installing Software on Your Government Computer

BC government policy prohibits employees from installing unlicensed, unauthorized or non-work-related software onto their government-issued computers, laptops, tablets or mobile devices. Most government users are now using Windows 10 operating systems with some still remaining on Windows 7. For these two operating systems, some users within the government have local administrator privileges which permits them to load software and change system settings. Because some individuals have these privileges ministries and end users need to be aware of and manage the additional security risk. With this privilege comes the responsibility of the individual user to know and to practice safe computing behaviour and to follow government's policies and procedures.

Even though you may now be able to download software and apps, it is essential that there is no increased risk of data loss and exposure of information. Users still need to have ministry approval to purchase and download non-standard software (meaning not available from government), including apps on their mobile devices. Both a Privacy Impact Assessment (PIA) and a Security Threat and Risk Assessment (STRA) must be completed for any new applications (Apps). It is important to point out that employees are not allowed to install file-sharing software programs that allow users to share music and/or videos. For policies, procedures and guidance:

- The Appropriate Use Policy (PDF) establishes the policy requirements that all government employees must follow when accessing and managing government information and using information technology (IT) resources. This document is a must read for all BC government employees.
- The Application and Software Guide (PDF) is intended to provide employees with tips and tools that can be used when downloading applications and software to government-owned devices.

Using BC Government Email

It is advisable to make sure you double-check the email address and attachments before sending email. When in a hurry, it is easy to accidentally click on the contact name or the file name listed above or below the one you wanted. This type of accident has resulted in personal, confidential and sensitive information going to the wrong destination, causing embarrassment to government and the need for a formal information security investigation. Make it a habit to open, then close, the attachment, and check the intended recipient's name and email address before hitting Send.

You may be able to encrypt the information, so that if the email is intercepted, the information is not accessible. Personal or confidential information can be placed in an encrypted attachment, rather than in the text of the email, where an approved encryption service is available. Other options to consider are registered mail services or personal/hand delivery. For advice on using different methods of transmission contact your Ministry Information Security Officer (MISO).

Since the BC Government Directory, with employee names, phone numbers and email addresses, is posted on the government's public website (and available by doing a search on your name), employees may receive unwanted spam email in the form of phishing attempts, internet hoaxes or mass marketing (or from people who did a search and found out you work for the BC government). The spread of Internet hoaxes via email is one threat that you as an employee can stop. Do not forward hoax emails or chain letters to other employees or people you know outside of work. As mentioned previously, never click on a link or open an attachment in an unsolicited email. If you have any suspicions about an email, delete it without opening.

Employees can access their BC government Outlook account remotely to connect to Email, Calendar, Contacts and Tasks from any computer, including some mobile devices, using their web browser and their IDIR ID and password. Use https://summer.gov.bc.ca.

Some employees have used their government email to send work documents to their home email address, to work on the file at home. This is not a security best practice and is discouraged, as the email could be intercepted, and the potential risk for data loss is too high. There are safe and approved alternatives available, talk to your MISO.

Accessing Personal Email

As a government employee, you are allowed to access your personal email accounts (e.g., @shaw, @yahoo, @gmail) over the Internet while at work in order to conduct reasonable personal affairs and to help foster work-life integration. It is important to follow the Standards of Conduct and the Appropriate Use Policy (see below).

Using the Internet

You do have access to the Internet as a government employee, but this does not mean that you can have unlimited access to visit websites. You are not allowed to visit any website that has inappropriate material, such as sexual or violent content of any kind, racism, hate literature, or anti-government messages. Many of these types of sites are screened, and if an employee does attempt to visit one, a prominent "red screen" will appear on your monitor, saying that you are not permitted to view the site and access is blocked. If you think you will want to access non-work-related websites during work hours, you will find the rules on Internet use in the Appropriate Use Policy at http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/appropriate-use-policy

Cost of the average data breach to companies worldwide: $3.86 million (U.S. dollars)

Using Portable Storage/Mobile Devices

Portable storage devices are compact devices with storage capacity that can be attached to a computer. They include USB drives (also called thumb drives, memory sticks, or USB sticks), removable or external hard drives, laptops, tablets, netbooks, CDs and DVDs, portable digital assistants (PDAs), BlackBerrys, iPhones/iPods and other smartphones, game consoles, some e-book readers and other types of media players.

BC government information, including presentations, must only be stored on government-approved portable storage devices. Your office manager can arrange for the purchase of portable storage devices that will encrypt sensitive or personal information to ensure protection from data loss, compromise or unauthorized disclosure. Information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then the content fully deleted and wiped from the device.

New Mobile Devices must meet or exceed the published standard. An exemption to the standard may be applied for through the Office of the Chief Information Officer (OCIO) where it can be demonstrated that a new mobile device cannot reasonably be made compliant but does not pose an unacceptable security risk or conflict with OCIO strategic objectives. Devices acquired must have a supplier supported operating system that can be updated to the latest release. Mobile devices that are capable of storing confidential (personal and sensitive) information must be able to have adequate security controls enforced by a BC Government Enterprise Mobility Management (EMM) system (i.e. Mobile Device Management Service (MDMS)). If you want to continue using your existing mobile devices for work purposes, then they must be brought into compliance unless it can be demonstrated that the devices cannot store confidential (personal and sensitive) information.

Protecting Mobile Devices

You are responsible for protecting both the device itself and the information contained on the device. Every make and model of electronic device comes with built in safety and security features, outlined in a manual, usually available online from the manufacturer. It is the responsibility of the employee that is issued a mobile device to protect the information on it, by learning about the device itself and security best practices. Be very conscious of where the device is at all times. Remember that the device can connect to the government network and has a hard drive that stores government information. Always remember, do not leave any mobile device unattended. Whether your mobile device is in a work space or in your car, if you are not there, it can be stolen. Government-issued devices are regularly lost or stolen, with the number going up along with the increased use of mobile devices.

The Mobile Device Guidelines (PDF) provide employees with guidance on their use of mobile devices given current legal requirements, government policy, and best practices. This useful resource addresses the most commonly asked questions employees have about their mobile device setup, use and management. This document is a must read for all BC government employees using mobile devices.

If traveling to another country, preparation for departure must include adequate security awareness. Make sure to allow enough time before departure to study awareness information. To assist you in preparation there is the tip sheet for Work-Related, Government Approved Foreign Travel (PDF) which will provide you with guidance and strategies to protect government information, and maintain security of this information, when travelling with mobile devices on government business outside of Canada. For more information on traveling to other countries you can visit Global Affairs Canada and Travel Canada.

Reporting the Loss or Theft of Your Government Device

If the device is lost or stolen, follow the Information Incident Management Process and take action as soon as possible. You need to report the information incident immediately to your supervisor. The Information Incident Management Process was discussed at the beginning of this Guidebook (under What If There is an Information Security Breach, including a Privacy Breach). The documents, including the Report Form can be

found at https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-breaches. You will need to complete a General Incident or Loss Report (GILR) in accordance with Core Policy and Procedures Manual, Chapter L. The directions and the link to the GILR form, which is available online, are on the Risk Management Branch and Government Security Office website at http://gilr.gov.bc.ca/.

Protecting Information on Paper

While the emphasis in recent years has been on computer hacking and threats to electronic information security, theft of information in paper form continues to flourish. At the same time, it has been easy for people to become somewhat lax in their concern about the need to protect information on paper. As an employee, your responsibility to protect information on paper is more important than ever, as criminals create new ways to perpetrate theft and fraud, particularly identity fraud. In the BC government, many programs and services are paper-based, not computer based. They often record clients' personal information on documents such as application forms and may have copies of personally identifiable information attached, such as birth certificates.

If you need to discard any personally identifiable information, or drafts of any sensitive government documents, put them in a shredder (if employees do this themselves) or a shredder receptacle (if you have pick-up service from a company), rather than putting documents in a recycle container. If people other than employees come through your work area, cover any sensitive information when you walk away from your desk, in the same way that you would lock your computer. Do not leave client or business papers, or any confidential, personal or sensitive documents on a fax, photocopier, or multi-function device - retrieve it promptly. Contact your ministry Records Management Officers for other guidelines.
https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/government-records

Working Outside of the Workplace

Employees who need remote access to the BC government network while working outside of the office on a regular basis can have an account set up for this purpose. The most commonly used remote access options are DTS, RDC and VPN. The DTS (Desktop Terminal Service) can be used on your personal or government-issued (SSBC provisioned) device. You must download the CITRIX client for use of DTS on your personal device. If you need access to your email, use of Microsoft Office, access to corporate web services (Time and Leave, eForms) and access to shared files, DTS should be used. Virtual Private Network (VPN) allows your remote computer to connect securely to SPAN/BC network over a public network like a wireless hotspot or home network and access Government network resources that include your Exchange e-mail, applications and shared data. Finally, there is RDC (Remote Desktop Connection), which is an application that allows you to use your remote computer to access your primary @ work Gov't Provisioned Workstation. RDC must only be used over the Internet via a VPN enabled connection.
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/remote-access/remote_access_services_user_guide_2019.pdf for the complete list of remote access options.

Reference Guide to Many of the Policies Related to Information Security

Appropriate Use Policy:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/appropriate-use-policy

Information Security Policy:
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/isp_v4.pdf

Information Incident Management Process:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-breaches.
General Incident or Loss Report (GILR) Online Report Form: http://gilr.gov.bc.ca/

Other Resources
Office of the Chief Information Officer:
http://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/office-of-the-chief-information-officer (external) and
https://intranet.gov.bc.ca/thehub/ocio (internal)

Information Security: http://www.gov.bc.ca/informationsecurity (external) and
https://intranet.gov.bc.ca/thehub/ocio/ocio-enterprise-services/information-security-branch
(internal)

Legislation, Privacy and Policy Branch (for privacy legislation and information):
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy

Ministry Information Security Officers (MISOs)
https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy-and-guidelines/role-of-miso

Security News Digest is a compilation of global news stories about current security breaches, threats, and research, and is available online at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

Appendix A – Short Descriptions of Various Types of Malware

Viruses and Worms – A computer virus is a computer program that can copy itself and infect a computer. A virus that replicates by resending itself as an e-mail attachment or as part of a network message is known as a worm. Both can delete or change files or overload networks.

Trojans – A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do damage by installing a "backdoor", allowing outsiders to access and control your computer.

Keyloggers – A keylogger, sometimes called a keystroke logger or system monitor is a hardware device or small program that monitors each keystroke a user types on a specific computer keyboard (or an ATM or Interac/debit keypad), records everything that is typed (including passwords) and passes that information to outsiders (usually using Bluetooth or similar technology). Keyloggers can be purchased in retail stores and legally installed on home computers, for example, to monitor children's usage.

Spyware – Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put into a person's computer to secretly gather information about the user (such as what sites are visited) and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program on the computer.

Rootkits – A rootkit is a collection of tools (programs) that enables administrator-level access to a computer or computer network, and controls, attacks or gathers your information. They often run silently on computer systems and are generally not detected by anti-virus or anti-spyware software.

Botnet – A botnet is a number of computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie – in effect, a computer "robot" or "bot" that serves the wishes of a master Spam or virus originator. Most computers compromised in this way are home-based. Botnets are often installed because the user responds to a fraudulent request received via e-mail or opens an e-mail attachment. (Storm and Conficker are both botnets that received media attention for the large number of computers they infected around the world.) Security researchers consider botnets to be the greatest threat to security because they can be spread to such a vast number of computers world-wide, remain dormant without the knowledge of the user, and controlled by a central person at their will.

Back Door – A back door is a feature that programmers often build into programs to allow special privileges normally denied to users of the program, such as access to fix bugs. If attackers or others learn about a back door, the feature may pose a security risk.