First Nations Health Authority
Health through wellness

Information Security Awareness Training

Project & Risk Management Services

Innovation and Information Management Services

May 2016

Information Security Awareness

1. Introduction
2. Information Security Awareness
3. Objectives
4. Information Security Overview
5. Policy and Governance
6. Access Controls
7. Devices and Files
8. Security Threat Awareness
9. Security Outside the Office
10. Incident Reporting

Introduction

1. This course is mandatory training designed to provide First Nations Health Authority staff, contractors and others who have access to FNHA systems and networks with knowledge to protect information systems and sensitive information from internal and external threats.

2. This course fulfills the security awareness training requirements set out by the Office of the Information and Privacy Commissioner of British Columbia; the Personal Information Protection Act of British Columbia; the Federal Personal Information Protection and Electronic Documents Act; and ISO 27002 Code of Practice for Information Security Controls.

3. This course will take approximately 45 minutes to complete.

Purpose for IT Security Awareness Training

- Section 34 of the British Columbia Personal Information Protection Act (PIPA) requires FNHA to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risk.

- Though not specifically stated under PIPA, this also applies to the protection of personal health information as well as personal financial information.

FNHA Staff are the best line of defense…

- FNHA staff and contractors routinely access sensitive data like names, Social Insurance Numbers, Status Numbers, Personal Health Numbers, health records, and financial information in the performance of their job duties. Some of the systems and information may be considered highly sensitive if personal health information or personal identifiable information is involved.
- It is the responsibility of every member of FNHA to act responsibly and ethically when accessing FNHA information and information systems. Compliance with our policies, directives and procedures in addition to our legislated obligations is required by all.
- The security of a system is only as good as its weakest link. If even one person does not pay attention to security, the security of the whole system may be compromised.
- Good security standards follow the “90/10” rule:
  - 10% of security safeguards are technical
  - 90% of the security safeguards rely on the user (YOU!) to adhere to good computing practices

FNHA Staff are the best line of defense…

- ❖ As an example: The lock on your door is the 10%; the 90% is you checking that the door is closed, ensuring someone doesn't prop the door open, remembering to lock the door and keeping control of the keys so no one unauthorized has access.
- ❖ FNHA staff are critical to ensuring sensitive information systems and data are protected against unauthorized access and disclosure.

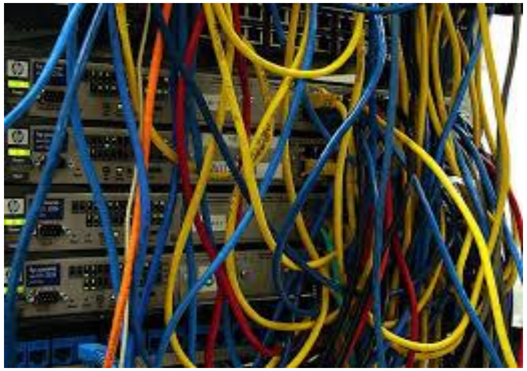
At the end of this course you will have the necessary knowledge to apply the learning objectives to your daily work.

Objectives

At the end of this course, you will be able to:

- Define information systems security;
- Identify regulations that mandate the protection of IT assets;
- Explain personal responsibility to protect information and information systems;
- Recognize threats to information systems;
- Identify best practices to secure IT assets and data in and out of the office; and
- Explain the proper procedure for responding to a suspected or confirmed security incident.

Information Security Overview



Did you Know?

- The average cost of a data breach in Canada is $5.32 million.

Source: Ponemon Institute 2015

- The black market rates for stolen medical records has surpassed financial records by 10 to 20 times.

Source: Infosec Institute 2015

- Canadian Anti-Fraud Centre reported in 2012 there were 17,009 incidents of identity theft and nearly $16 billion in losses; Halfway through 2014 there were over 10,000 victims and $4.7 billion in losses.

Source: CBC 2015

What is Information Security?

Information Security (IS) - Is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

- Information security is achieved through implementing technical (encryption), management (policies) and operational (clean desk) measures that are designed to protect the confidentiality, integrity and availability of information and information systems.
- The goal of an Information Security program is to **understand, manage** and **reduce the risk to information** under the control of the organization.

Key Security Concepts

There are three elements to protecting information:

1. Confidentiality – Information and resources can only be read or accessed by authorized parties.

2. Integrity – Assuring the reliability and accuracy of information and IT resources.

3. Availability – Defend information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users

Key Security Concepts

Confidentiality:

- Information and resources can only be read or accessed by authorized parties. This means access to the information is controlled with strong access controls e.g. complex passwords or a combination of security controls and the information is encrypted to protect confidentiality.

Integrity:

- Assuring the reliability and accuracy of information and IT resources. This means ensuring information and resources are accurate and consistent and can only be modified or deleted by authorized individuals.

Availability:

- Defend information systems and resources from malicious, unauthorized users to ensure accessibility by authorized users. This means, ensuring information systems and resources are available and accessible by authorized individuals when needed.

Example; Key Security Concepts:

Your ATM is a good example of an information system that must be confidential, available and have integrity.

- Imagine if your account was not kept ***confidential*** and someone else was able to access it when they approached the ATM. How much damage could be done?
- Imagine if every time you went to the ATM, the balance that is displayed was inaccurate. How could the poor ***integrity*** of your balance information adversely affect your account management?
- Imagine if your bank's ATM was rarely ***available*** when you needed it. Would you continue to use the bank?

The goal of an Information Security program is to understand, manage and reduce the risk to information under the control of the organization.

Key Security Concepts

Threats and vulnerabilities put information assets at risk.

- **Threats** – the potential to cause unauthorized disclosure, changes, or destruction to an asset.
  - Impact: potential breach in confidentiality, integrity failure and unavailability of information.
  - Types: natural, environmental, and man-made.
- **Vulnerabilities** – any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.
- **Risk** – the likelihood that a threat will exploit a vulnerability. For example, a system may not have a backup power source; hence, it is vulnerable to a threat, such as a power outage, which creates a risk.

Key Security Concepts

- **Controls** – policies, directives, procedures, and practices designed to manage risk and protect FNHA's IT assets.

- Common examples of controls include:
  - Security awareness and training programs;
  - Physical security, like guards, ID badges, and locking cabinets; and
  - Restricting access to systems that contain sensitive information.

Information Security Policy and Governance

Information Security Governance

- The purpose of information security governance is to provide a framework of policies, directives and procedures for which FNHA operates.
  - They define what FNHA does and how we do it;
  - They provide guidelines on what people should and should not be doing;
  - They provide transparency and consistency in the way we operate;
  - They ensures we know our legal obligations; and
  - They demonstrate our commitment to protecting information entrusted to us.
- IT Security policies, directives and procedures extend to all users who have access to FNHA systems and third party systems that contain sensitive or confidential information e.g. Panorama.
- All users should be familiar with FNHA's Information Security Policy and Acceptable Use Directive as a minimum requirement and any other policy, directive or procedure that is relevant to their job responsibilities.
- IT Security policies and directives can be found on the Bighouse under Resources > Corporate Policy Library > CIO – IIMS.

Information Security Policy and Governance

The table lists some sources of legislation and guidance that provide the governance for the protection of information and information systems.

Legislation	Standards
BC Personal Information Protection Act (PIPA)	ISO/IEC 27002; Code of practice for information security controls
Federal Personal Information Protection and Electronic Documents Act (PIPEDA)	Cobit5; Standards for governance and management of enterprise IT
	eHealth Conformance Standards

Access Controls

Protecting Sensitive Data

- ❖ Sensitive data includes documents and/or files which if compromised would have an adverse effect on FNHA Clients, employees or the organization. Users must be diligent in protecting sensitive data from unauthorized access, use, disclosure, modification or destruction.

- ❖ Sensitive data, in both electronic and paper format must be secured at all times. This means using only FNHA approved mobile storage devices that are encrypted and require a strong password and using locking cabinets or FNHA storage vaults for sensitive paper records.

- ❖ Sensitive data should never be sent via email over the public internet unless the information has been encrypted. Caution should also be observed prior to sending sensitive information via email internally. Even though the FNHA network is secure, you do not know who may have access to the email.

Access to Information Systems

- An “Information System” is any system that is used for storing, managing, using and gathering data and communications.
- FNHA has an obligation to ensure access to all systems and information is controlled and effectively administered and that only valid, authorized and authenticated users are permitted to access systems and information.
- The level of access (permissions) to information systems that a user should have is based on their role and must follow the premise of “need-to-know” and the principle of “least privilege”. What this means is that each user should only have the appropriate level of access to systems and information that they need to do their job, nothing more, nothing less.
- A rule of thumb is the more sensitive the information or greater the risk, the stricter the access requirements will be.
- For example, a user who needs to access a health information system or has a privileged account must use more than one authentication factor to verify their identity, such as “username and password” (factor #1) and a “security token” or “finger print” (factor #2). This is referred to as “two-factor” authentication; something you know and something you have. So if one factor is compromised it is useless without the other which ensures the confidentiality of the information system is maintained.

Passwords

- ❖ Having a strong password for your network account and applications is a basic protection mechanism. While it is tempting to create an easy or generic password that is easy to remember and that you use across all systems and applications, it is not a good practice because it is not secure.

- ❖ If your password should ever be compromised, the individual will have access to all systems and applications and information that you have access to. Having a strong and unique password for each system and application mitigates this risk.

Passwords

- The following explains how to create a strong password which is also defined in FNHA's security standards:
  - Passwords must be at least eight characters in length for general user accounts (e.g. Windows) and ten characters for administrator accounts and sensitive system accounts.
  - Each password should contain an upper case letter, lower case letter, number (0-9), and special characters (~!#$%^&*).
  - Note: The best location for special characters is inside the first and last characters to make it more difficult for password crackers to predict.
- A strong password only remains strong if it is changed regularly. Most systems will prompt you after a set period of time has elapsed to change your password. This ensures that it does not become stale and easier to compromise.
- If a system does not prompt you to change your password you should still follow FNHA standards noted above for creating passwords, as well as change it every 90 days.

Note: Do not reuse passwords

Password Protection

- ❖ Passwords should be protected in the same way you would protect your Social Insurance Number, bank account number and the keys to your home.
- ❖ You should **never** share your password for any reason or write it down and leave it in your work space where it can be discovered.
- ❖ As we are required to use more complex passwords it also becomes more difficult to remember them. One technique that can help you remember is to use a passphrase; using the initials of a song or phrase to create a unique password. For example; you may have a little ditty that sticks in your head like “take me out to the ball game!” (passphrase) which becomes “Tmo2tBG!” (unique password).
- ❖ DO NOT keep passwords near your computer or on your desk.

Password Protection

- If you must write down a password keep it in a secure place that only you have access to such as a locked drawer, your wallet or purse or a safe.
- If you suspect your password has been compromised, change it immediately.
- You should not use generic information that can be easily guessed, like your name, a family member's name, your pet's name, birthdates, phone numbers, favorite sports team or any common words found in the dictionary.
- You can review the User Identification and Access Management Directive and Password Standards for further information.

Proximity Cards & Keys

- Proximity cards (prox cards) use radio frequency identification (RFID) chips to reliably identify staff and grant access to FNHA facilities.

- Proximity cards contain information that is used to identify you and must be protected like a password.
  - Maintain possession of your prox card at all times.
  - If your prox card is lost or misplaced, report it to Corporate Services immediately.

- Keys to secure areas should be protected at all times.
  - Secure keys in a lockbox when not being used.
  - Use a sign-out sheet where appropriate.
  - Only copy keys to provide a back-up; keep it secure at an alternate location.

Devices and Files

Devices and Files

- Only devices owned and or approved by FNHA may be connected to FNHA systems.
- Use of personal devices for business purposes presents a risk to FNHA systems because the same level of diligence that FNHA maintains with the security of its devices and systems may not be followed by individuals with their personal devices.
- Using FNHA approved devices reduces the risk to FNHA systems being compromised by an infected personal device or from the unauthorized or inadvertent disclosure of sensitive or confidential information due to the loss or theft of a personal device that may contain FNHA information.
- For example, in 2016 an individual at another health authority connected their personal device to their organization’s network where it infected thousands of files with ransomware.

Devices and Files

- FNHA sensitive or confidential information should not be stored on your mobile devices or locally on the C:\ drive on your computer, or any cloud drive such as Drop Box, because it is not backed up by FNHA systems and we cannot guarantee confidentiality which could result in a breach of legislation if personal health information is being stored or traverses a foreign jurisdiction. In order to ensure FNHA information is backed up and secure, it must be stored on FNHA servers either using SharePoint or a network file share.

- When you are traveling you may not have access to the FNHA network and need to take electronic files with you. Do not store sensitive or confidential documents on your laptop or tablet any longer than necessary. When you reconnect to the FNHA network, move the files back to the network file share or SharePoint site.

- Note: Currently, the use of cloud storage services for FNHA business purposes has not been approved.

Devices and Files

- If you are travelling outside Canada, access to FNHA systems or provincial health information systems is not allowed.

- If you find a memory stick lying around or come across one in a parking lot, DO NOT connect it to any FNHA devices or any device you care about. Attackers today leave USB (memory) sticks laying around on purpose, banking on a basic behavior of people that we are curious and will plug in the memory stick to see what's on it and then their system is compromised. The only USB sticks that should be connected to FNHA devices are provided by FNHA's Service Desk team and have been approved by FNHA and are secure. If you find an unknown USB device, send it to the FNHA Service Desk for secure disposal.

- You can review the Acceptable Use Directive and IT Asset Management Directive for further information.

Physical Security

Physical Security

- There is a pretty good chance that during the course of your day you will be working with confidential or potentially sensitive information that is not for general disclosure. Whether you are in a shared office area or working remotely, it is important that you be aware of your surroundings and protect information from intentional or inadvertent viewing.

- When printing documents, sending a fax or expecting a fax, quickly retrieve the documents and do not leave them on the machine. Most multifunctional copiers/printers today have secure print functionality where your document will not print until you have entered a password that you set. This is a good practice in office environments where equipment is shared by different departments.

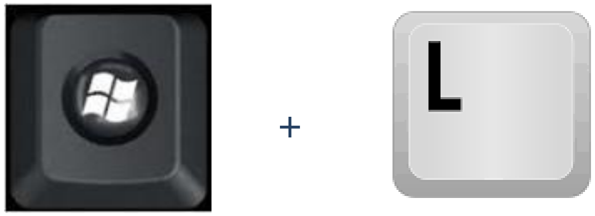
- If you leave your workspace unattended, put away any sensitive documents, keys or memory sticks so they can't be easily discovered and lock your computer, laptop or tablet. A quick way to lock your computer is to hold down the "Windows" key (on most keyboards it's beside the "Alt" key) and hit the "L" key.

- At the end of the day, tidy up and lock up because you don't know who will be in the workspace after hours.

- You can review the Physical Security Directive for further information.

Physical Security Tips

- Lock your workstation when you leave your desk or leave your laptop/mobile device unattended
  - Press the Windows Key and “L” (at the same time)



  - Press Ctrl-Alt-Del and “Lock Computer”
- Lock sensitive documents and materials in a file cabinet
- Dispose of sensitive materials appropriately
- Never share your access key, card or fob (where applicable)
- Always question unescorted strangers
- Always report incidents and suspicious activities

Security Threat Awareness

Security Threat Awareness

- The following information will provide you with a few examples of the kinds of threats that you may encounter and provide you with suggestions on how you can protect FNHA data and systems from harm.
- It is your responsibility to be aware, be alert and diligent. Always look for signs that external entities are trying to gain access to your PC and the FNHA network.
- Most threats are targeted, specifically with the hope that you will click on a harmful link, attachment, picture, video or icon in an email or webpage, including social media applications and in doing so, you risk launching a harmful program that may subject FNHA systems to malicious software.
- A very basic concept of online threat prevention is you control what you choose to click.

Cyber Crime

Cyber crime refers to any crime that involves a computer and a network. Offenses are primarily committed through the Internet.

- Common examples of cyber crime include:
  - Credit card fraud;
  - Spam; and
  - Identity theft.
- Health information and information system assets are a high value target.

Identity Theft

- ❖ Identity theft refers to the preparatory stage of acquiring and collecting someone else's personal information for criminal purposes.
- ❖ Techniques range from dumpster diving and mail theft to phishing and hacking.
- ❖ Today thieves use malicious software designed to acquire personal information.

Combat Identity Theft

- Use strong passwords to access FNHA's information systems;
- Do not disclose personal information unless you have the authority to do so;
- Prior to disclosing personal information, verify the recipient is who they say they are and has the authority to collect the information. Know how and why it will be used.
- Do not provide any more information than is required;
- Shred sensitive documents and mail containing personal information or use the confidential destruction bins.

Email Threats

- Email threats involve phishing, spoofs, hoaxes, malware and spam to just name a few. What all of these threats have in common is that they are designed to get you to click on an item like an attachment, link or picture which may result in you launching a harmful program or be directed to a harmful website which may compromise personal information or subject your FNHA device or the FNHA network to malicious software.

- If you cannot identify the source and attachments as being legitimate or are sure the links are safe by verifying the actual web address, you can logically conclude that this most likely an email threat.

- A quick way to validate a link is by hovering over it with your mouse and checking if the URL is a legitimate website.

- Even if the link is legitimate, it is good practice to copy the link into your browser rather than opening it within the email.

- You can review the Acceptable Use Directive for further information about appropriate use of FNHA email.

Appropriate Use of Email

- FNHA email accounts are provided for business use.
- Limited personal use is allowed.
- No other email services should be used for FNHA business unless authorized by IIMS or in the event of an emergency.
- Confidential or sensitive personal information should never be sent via email unless it is encrypted.
- Review the **Acceptable Use Directive** and **Communications (Network) Security Directive** for more information.

Social Engineering Threats

- **Social engineering** is classically defined as the art of manipulating and exploiting human behavior to gain unauthorized access to systems and information for fraudulent or criminal purposes.
- Social engineering attacks are more common and more successful than computer hacking attacks against the network Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn't normally take. Social engineering attacks can occur in person, over the phone, while surfing the Internet, and via email.
- Social engineers exploit the natural tendency of a person to trust another's word, rather than exploiting computer security holes.
- Common targets for social engineers are anything that will help them gain unauthorized access to systems and information for fraudulent or other criminal purposes.
- Some of the techniques social engineers use are shoulder surfing, hoaxes, tailgating and phishing.

Social Engineering Threats

Shoulder Surfing:

- ❖ Shoulder surfing is simply looking over someone's shoulder to gain information. The goal is to gain unauthorized information by casual observation and is most likely to occur in an office environment in order to learn someone's username and password. It can also occur remotely with the use of a camera.

Hoaxes:

- ❖ Hoaxes are often circulated through email that tells of a virus or other security threat that does not exist. Users may be encouraged to delete files or change their system configuration and in doing so, unknowingly compromise the system.

Tailgating:

- ❖ Tailgating is the practice of one person following closely behind another into a secure area without showing credentials.

Phishing Attacks

- Phishing is a social engineering scam whereby intruders seek access to your personal information or passwords by posing as a legitimate business or organization with legitimate reason to request information.

- Usually an email (or text) alerts you to a problem with your account and asks you to click on a link and provide information to correct the situation.

- These emails look real and often contain the organization's logo and trademark. The URL in the email **resembles** the legitimate web address. For example "Amazons.com".

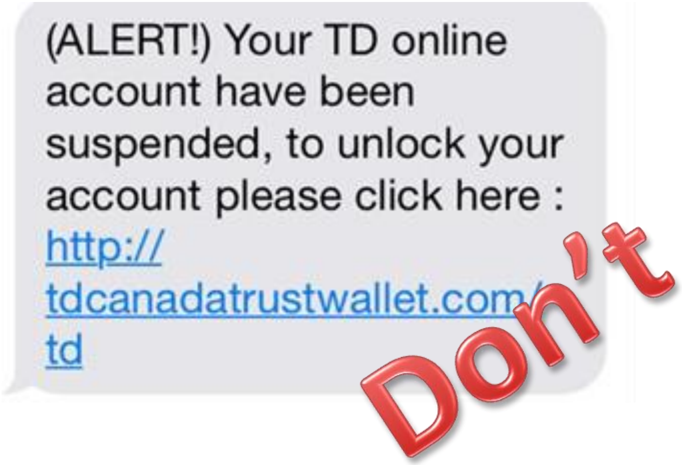
Spear phishing is an attack that targets a specific individual or business. The email is addressed to you and appears to be sent from an organization or person you know and trust, like a government agency or a professional association.

Whaling is a phishing or spear phishing attack aimed at a senior person in the organization.

Phishing Example

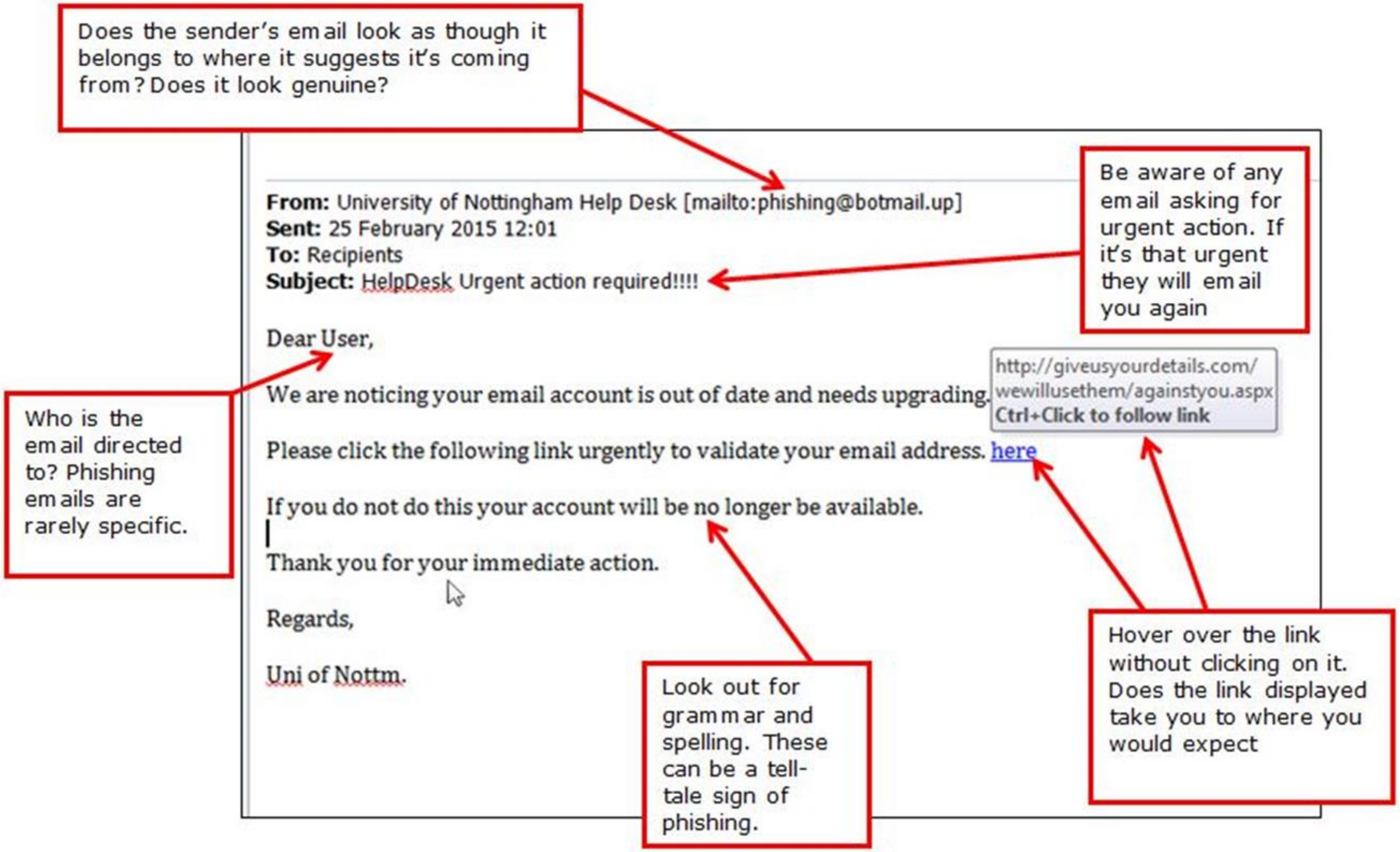
Phishing emails appear to be legitimate. Take a look at this real-life example.

- ❖ **Upcoming service fee adjustment**. An email appears to be a notice from your bank that it is adjusting fees for certain services related to your Chequing Account. In order to see a full list of the fee changes and how to avoid these fees you are instructed to download and complete an attachment to the email. The problem is, clicking on the attachment leads to a page where victims are asked to share sensitive information. If you receive such a message, just ignore it and delete it.



(ALERT!) Your TD online account have been suspended, to unlock your account please click here : http://tdcanadatrustwallet.com/td

Phishing Example



Does the sender's email look as though it belongs to where it suggests it's coming from? Does it look genuine?

From: University of Nottingham Help Desk [mailto:phishing@botmail.up]
Sent: 25 February 2015 12:01
To: Recipients
Subject: HelpDesk Urgent action required!!!!

Dear User,

We are noticing your email account is out of date and needs upgrading.

Please click the following link urgently to validate your email address. here

If you do not do this your account will be no longer be available.

Thank you for your immediate action.

Regards,

Uni of Nottm.

http://giveusyourdetails.com/wewillusethem/againstyou.aspx
Ctrl+Click to follow link

Be aware of any email asking for urgent action. If it's that urgent they will email you again

Who is the email directed to? Phishing emails are rarely specific.

Look out for grammar and spelling. These can be a tell-tale sign of phishing.

Hover over the link without clicking on it. Does the link displayed take you to where you would expect

Combat Phishing

- **NEVER** provide your password to anyone via email.
- Be suspicious of any email that:
  - Requests personal information;
  - Contains spelling and grammatical errors;
  - Asks you to click on a link; and
  - Is unexpected or from an individual, company or organization with whom you do not know or have a relationship.
- If you are suspicious of an email:
  - **Do not** click on the links provided in the email;
  - **Do not** open any attachments in the email;
  - **Do not** provide personal information or financial data;
  - **Do not** forward the email; and
  - **Delete** it from your Inbox.

Hoaxes

- Email messages that promise a free gift certificate to your favorite restaurant, plead for financial help for a sick child, or warn of a new computer virus are typically hoaxes designed for you to forward them to everyone you know.
- Mass distribution of email messages floods computer networks with traffic slowing them down. This is a type of distributed denial-of-service (DDoS) attack.

Combat Hoaxes

- Do not open emails from senders whom you do not recognize or if you are suspicious that the email could be a hoax.
- Try to verify the information before following any instructions or passing it along.
- Do not forward chain letters, email spam or broadcast messages.

…if it sounds to good to be true, it probably is.

Tailgating

- As previously noted, tailgating is when an unauthorized person follows closely behind an authorized person into a secure area.
- Physical security is an important information systems safeguard. Limiting physical access to information systems and infrastructure to authorized personnel diminishes the likelihood that information will be stolen or misused.

Combat Tailgating

- Never allow anyone to follow you into the building or secure area without his or her employee ID card.
- Be aware of procedures for entering a secure area, securing your workstation when you leave the office, and securing your workstation during emergencies.
- Do not be afraid to challenge or report anyone who does not display an ID card or visitor’s badge.
- Escort visitors to and from your office and around the facility.
- Do not allow anyone else to use your ID card for building or secure area access.
- Report any suspicious activity to Corporate Services.

Internet Threats

- Most internet threats are from malicious links that redirect you to harmful websites that trick the user into providing personal and sensitive information.

- When accessing external web sites, you need to be especially cautious of your activities to ensure FNHA systems and information are not compromised.

- Do not automatically click on internet links until you have absolute confidence in them. This includes pictures, videos, and navigational elements.

- For example, if a link indicates “Click Here”, rather than just clicking, hover your mouse over the link as previously mentioned and investigate the actual web address before you proceed.

- Applications that have not been approved by FNHA should not be installed on or accessed with FNHA devices.

Internet Threats

Malicious Software:

- Malicious software (a.k.a. Malware) come in the form of Viruses, Trojans, Worms and Spyware which can infect other programs, damage hard drives, erase critical information, take critical systems off-line, and forward data to external sites without your knowledge.

- Some signs of malware are;
  - Unusual items appearing on the screen (graphics, odd messages, or system error messages).
  - Corrupted or inaccessible program files.
  - Programs taking longer to start up, running more slowly than usual, or not running at all.
  - Increased number of pop-up advertisements.
  - Changed settings that can't be changed back to the way they were.
  - Web browser contains additional components that you don't remember downloading.

Internet Threats

Malicious Software:

- The anti-virus software that is running on your device protects against most malware, though should you suspect that your device has been compromised, take immediate action:
  - Close all files and programs
  - Document the symptoms you observed
  - Shut down your device and call the FNHA Helpdesk.

Internet Threats

Combat Malicious Software:

- Don’t click on links within emails from unknown sources (no matter how curious you may be).
- Don’t open attachments from unknown sources (malware can be embedded in PDF’s, Word Doc.’s Zip files and more).
- Be suspicious of free downloads from the internet (they may contain malware).
- If you believe your computer is infected, send an e-mail to the Helpdesk@fnha.ca or call 604.693.6647 or 1.855.913.2085

Internet Threats

Peer-to-Peer:

- Peer-to-Peer file sharing sites are inherently unsecure because they share everything on your computer with everyone by default and much of the activity is automatic and unmonitored. Some Peer-to-Peer programs are used to spread malware, contain spyware or use organizations file servers to store and forward information.
- Accessing Peer-to-Peer sites with FNHA devices is not allowed.

Pop-ups:

- Anyone who has browsed websites has experienced those annoying pop-up windows advertising something that you have no interest in. Today, those pop-ups are used for malicious purposes and although we have pop-up blockers, they do not always block ALL pop-ups.
- When you experience pop-ups always close them by clicking on the "X" in the upper right corner. Never click "yes", "no", "accept" or even "cancel", doing so could compromise your device with malicious software.

Internet Threats

Cookies:

- *A cookie is a text file that a website puts on your hard drive that saves information that you typed in like preferences or user name.*
- *Cookies can also be used to track your activities on the web.*
- *Cookies pose a security risk because someone could access your personal information or invade your privacy.*

Internet Threats

Combat Cookies:

- *Use cookies with caution.*
- *Confirm that web sites that ask for personal information are encrypted and the URL begins with "https".*
- *Note that there is an inherent risk anytime you enter personal information on a web site.*

Social Media Threats

- Social media threats are similar to email threats, postings on Facebook, LinkedIn, YouTube and others which may appear to take you to interesting content, funny videos, or connect you to other users and organizational sites of common interest. In reality, you may be clicking on links that launch malware or take you to sites other than the ones you expected.

- Some basic guidelines are:
  - Do not assume social networking sites are safe.
  - Do not click on links until you are sure they are legitimate. This includes pictures, videos, invitations to games and applications and navigational elements.
  - Be careful of postings and sites that ask to share personal or any other sensitive or confidential information.
  - Limit information you post on social media sites because criminals use the information to guess passwords or answer password reset questions.

You can review FNHA's Acceptable Use Directive for social media activities to ensure you are not putting yourself or FNHA systems and information at risk.

Security Outside of the Office

Did you Know?

- 30% - 40% of data breaches are caused by employees losing laptops, flash drives or other mobile devices.

Forrester Report and TechInsurance 2014

Travel

- Technology, telework, and job duties mean that many employees regularly work away from the office.

Be vigilant about protecting information and information systems outside of the office

Telework Threats

- Today more and more employees work remotely as a requirement of their job responsibilities or as a result of the organization supporting flexible work arrangements. No matter what the telework scenario, employees need to be aware of the risks to ensure safe computing practices.
- Assume when you connect to a non-FNHA wireless access point that it is inherently not secure and other individuals can potentially “see” your activity.
- Always use a VPN connection to launch a secure internet connection so that even with a public access point, you are able to work connected to the FNHA network with a greater level of security.
- If you are traveling outside Canada for work, it is not recommended that you connect to the FNHA network. Traversing the public internet from a foreign jurisdiction presents a risk even when using a VPN connection.
- In no circumstance should you ever access health information systems in British Columbia from outside Canada.
- Always be sure your laptop, tablet or other mobile devices are protected from unauthorized access, viewing or theft.

Mobile Computing and Teleworking

- ❖ When working remotely or teleworking, you need to be extra diligent with safeguarding FNHA devices and information. Only use FNHA devices to access FNHA systems or third party systems via the FNHA network. Appropriate measures have been taken to ensure the device is properly protected so it doesn't put systems at risk of being infected with malware or a virus.
- ❖ Be careful with your connections. Assume when connecting to a public wireless access point at the airport or hotel that it is inherently not secure and other individuals can potentially "see" your work activity. To reduce this risk and ensure a greater level of security, always use the VPN client on your desktop to launch a secure internet connection to the FNHA network.
- ❖ If you are using a cable connection, turn off the WiFi on your laptop or tablet so there isn't an additional "door way" into your device that can be exploited.
- ❖ Always be sure to protect your devices against unauthorized access, loss or theft. This also applies when working from home.
- ❖ Report a loss or theft of your laptop or other FNHA authorized mobile devices immediately to FNHA Helpdesk@fnha.ca or call 604.693.6647 or 1.855.913.2085

Security Incident Reporting

What is a Security Incident?

- A security incident is the violation either knowingly or accidentally, of FNHA security policies and procedures and/or standard security practices.
- As much as we try to prevent incidents through the use of technical, operational and management controls, incidents still happen. It is extremely important that if an incident is real or suspected that it be reported promptly so that it can be identified and contained.
- The reason for reporting real or suspected incidents promptly is to mitigate the risk of harm to FNHA and their clients or employees. The harm that could result from an incident could include:
  - Adversely affecting one or more individuals
  - Threats or hazards to the security or integrity of information in our control
  - Legal action
  - Loss of reputation
  - Negative media interest.

Common Incident Scenarios

- Security incidents often occur from the following scenarios:
  - Loss, theft or improper disposal of equipment, storage media or papers containing sensitive information.
  - Allowing an unauthorized person to use your credentials to access FNHA information or information systems.
  - Unauthorized or accidental access to information.
  - Unauthorized or accidental release, modification or destruction of data.

- In the event of a loss or theft of an FNHA device, notify your manager and the FNHA Helpdesk right away. For all other incidents contact the FNHA Privacy and Security Office who have documented incident reporting procedures that need to be followed.

Incident Reporting

- Report all security incidents to:

Helpdesk@fnha.ca
or call 26600, Option 2
604.693.6647, Option 2
1.855.913.2085, Option 2
&
Security@fnha.ca
or Manager, IT Security - 604.693.6791

- You can review the Privacy and Security Breach Management Procedures in the IIMS Policy Library on the Bighouse for further information or contact the Security Office at the number above.

Summary

You should now be able to:

- ✓ Define information systems security;
- ✓ Identify provincial and federal legislation that mandate the protection of IT assets;
- ✓ Understand personal responsibility to protect information systems;
- ✓ Identify best practices to secure IT assets and information in and out of the office; and
- ✓ Identify the correct way to respond to a suspected or confirmed security incident.

End