Information Security – Best Practice Guidelines

Introduction

Although OTN has taken a number of measures to ensure confidentiality, integrity, and availability of the data hosted on its infrastructure, protection of Personal Health Information (PHI) is ultimately a joint responsibility between OTN and its users. While OTN has deployed a combination of Administrative, Technical and Physical safeguards to protect the data at transit and at rest, once the data leaves OTN's network, it is up to the user to ensure that the information remains protected from unauthorized access, modification, and disclosure.

This document provides a set of security best practices that users of OTN services are expected to follow. Adherence to these guidelines will minimize the risk of unauthorized disclosure, modification, and/or destruction of sensitive or business-critical data.

Secure Internet Browsing

The Internet has changed the way we live and do business. It provides convenient access to information and the ability to perform work from virtually anywhere in the world. Unfortunately, the Internet is also a host to security threats that can put your information at risk. Seemingly reputable sites may contain malware or the sites themselves can be counterfeit – phishing sites posing as the real thing to lure you into disclosing information. Follow these guidelines to protect your information and system online:

- Update Web browsers regularly – choose "Yes" when browser programs (Chrome, Firefox, IE, Safari) prompt you to update
- Increase your browser security settings
- Look for signs of an encrypted (TLS/SSL) Web page when exchanging sensitive information – key identifiers include a URL that begins with "http***s***" and a padlock icon in the browser status bar (location will vary based on the browser)
- Avoid questionable Web sites
- Think before you click – never click on links in messages from people you don't know
- Beware of phony websites – these sites may have an address that is very similar to a legitimate site, but differs slightly by a letter
- Only download software from sites you trust - carefully evaluate software before downloading it
- Always "log out" and close the browser when finished using an online service
- Disable automatic password-save features in the browser and software you use to access the internet.
- Do not perform sensitive tasks in public areas, such as airports, coffee shops, or business lounges where there is an opportunity for strangers to see over your shoulder
- Do not use public terminal computers that you don't control to transmit sensitive information - these may have key loggers and other network spying tools installed designed to capture information.

Email Security

There are many reasons to be wary of emails that seem suspicious. Some emails might be phishing scams designed to trick you into divulging personal information, while others might contain viruses and other malicious software designed to infect your system. If an email looks suspicious, don't risk your personal information by opening or responding to the message. Here are some tips to help protect yourself against common email threats:

Approach Links in Email Messages with Caution.
Links in email messages can often take you to fake sites that encourage you to provide personal information or infect your computer when clicked.
Before you click a link, make sure to read the target address by hovering your mouse pointer over the link to ensure that the URL point to the correct destination.

Example of a malicious link hidden behind what appears to be a safe URL:

Do Not Open Attachments from Unknown or Unexpected Senders.
Attachments might be malware that downloads to your machine when you open the file. If you don't know who the attachment is from, or if you weren't expecting it, DO NOT OPEN THE FILE!

Do Not Reply to Messages asking for Personal Information.
OTN and most other reputable organizations will never use email to request that you reply with a password, OHIP, SIN or any other personal information.

Password Security

Passwords provide the first line of defense against unauthorized access. The stronger and more complex your password, the more protected your information will be from hackers and malicious software. Most people use passwords that are based on personal information and are easy to remember. However, that also makes it for an attacker to guess or "crack" them. To protect yourself and your information, you'll want to create a password that is long, strong, and difficult for someone else to guess while still keeping it relatively easy for you to remember.

Choose a Strong Password
A strong password is one that is difficult for others to guess. It can be made more difficult to guess by being longer and random looking. A strong password should:

- consist of ***at least 8 characters***; and
- contain a combination of ***uppercase*** and ***lowercase letters***, ***numbers*** and ***special characters.***

There are various strategies to make choosing and remembering passwords easier. For example:

1. Select a word that is 8 characters or longer (e.g. ***chocolate***)
2. Capitalize the first letter → ***Chocolate***
3. Add a punctuation mark at the end → ***Chocolate!***

4. Replace any letters that "look like" numbers with the corresponding numerical values → ***Ch0c01at3!***

The result is a strong, hard to guess password that is still easy to remember.

(Note: This example is provided here for illustrative purposes only. Do not use this exact password when signing up for OTN Services – select a unique password that is known only to you.)

Protect Your Password
Generating a strong password is only the first step. Although difficult to guess, it may still end up in the wrong hands if it is not sufficiently protected. Following rules should be followed to minimize the risk of unintentional password disclosure:

- ***Do not*** share your password with anyone. This includes trusted colleagues, family members, and friendly support technicians. There is no valid reason to disclose your password to anyone. If you ever forget this rule, change your password immediately.
- ***Do not*** write down your password and store it where it is easy to find. If you feel that you must write down your password, keep it in a safe place (e.g. your wallet).
- ***Do not*** type your password on computers that you do not control. Computers in public places like Internet cafes, airport lounges, computer labs, hotels or conferences may have keystroke loggers installed, and are thus unsafe.
- ***Do not*** under any circumstance provide your password in response to an email request. Such "phishing" scams are very common and no matter how legitimate looking, will result in your password in the hands of cyber-criminals.
  Do not use the same password for all applications. Consider what would happen if the password and personal information you just used to sign up for a free daily horoscope run by a gang of cyber-criminals is also the same password you use for online banking account.
- ***Change*** passwords with access to confidential information (e.g. Personal Health Information) regularly and at least every 3-6 months

Mobile Equipment Security

Mobile devices such as Smartphones, Tablets, and Tablets can be easily lost or stolen due to their small and compact size. Loss of a mobile device will not only result in the loss of the data, but it may also potentially lead to unauthorized disclosure of this information, if the phone or the tablet ends up in the wrong hands.

Guard your phone as you would a wallet – do not leave it unattended at any time and keep it locked and out of sight when not using it.
Think of the mobile device and protect it the same way you would your wallet. Leaving it unattended and in plain sight will attract potential thieves and opportunists with a readily available target. Whenever finished using the mobile device keep it in your pocket or otherwise lock it in a drawer or a safe.

Do not interfere with or disable the security features of your device.
Most mobile devices come equipped with various security features to minimize the risk of unauthorized disclosure, modification, or destruction of personal information. "Jailbreaking" or "rooting" a smartphone or otherwise interfering with the mobile device's security features will increase the risk of a breach.
In particular, mobile devices should always:

- Be secured with a PIN or a password
- Lock automatically after a period of inactivity

- Have malware protection installed
- Be up to date and have the latest versions of the software installed
- Have encryption enabled

Workstation Security

Despite rapidly increasing popularity of mobile devices, workstations remain a popular and widely adopted option to conduct work and business, particularly in the healthcare field. The following practices will help prevent breaches and increase the security of your workstation:

- Stay up-to-date with Operating System (Windows, Linux, OS X) software patches and updates
- Install Anti-Virus and Anti-Spyware Software keeping updates current
- Enable Firewall Software
- Use strong passwords to protect access to the workstation
- Use secure system configuration (including browser settings) based on recommendations from the vendor
- Configure the system to automatically lock after a few minutes if not in use
- To prevent power failure related interruptions, connect your workstation to an Uninterruptible Power Supply (UPS)
- Ensure that any sensitive data stored locally on the hard drive is encrypted
- Make periodic backup copies of data, especially if this data is essential to business functions
- Ensure physical security of workstations and related peripherals (disks, USBs, etc.)

Please contact OTN's Information Security Department should you have any questions:
Information Security - Ontario Telemedicine Network
105 Moatfield Drive, Suite 1100, Toronto, ON M3B 0A2
Email: security@otn.ca | Tel: 416-446-4110

Care. Connected.