CANADIAN CENTRE FOR CYBER SECURITY

Cyber Security for Healthcare Organizations: Protecting Yourself Against Common Cyber Attacks

UNCLASSIFIED

SEPTEMBER 2020 | ITSAP.00.131

As a healthcare organization, you work with highly sensitive information like personal health information (PHI), financial information, and research data, making you a high-value target for cyber threat actors. For example, PHI is more valuable on the black market than other types of personal information. It is used to create fake insurance claims, purchase medical equipment, or fill prescriptions that can be used or sold. Cyber security might be a new priority for you, but you don't have to be an IT expert to protect yourself from cyber threat actors. For more information on cyber security topics, visit the Canadian Centre for Cyber Security website: **cyber.gc.ca**

To get you started with cyber security, we have summarized some common methods that cyber threat actors use to steal personal health data and intellectual property or disrupt the operations of healthcare organizations:

RANSOMWARE

A type of malicious software that locks you out of your systems, devices, and files until you pay the threat actor. Even if you pay, you may not regain access or prevent data from being sold or leaked online. If you are a victim of ransomware, your critical processes may be slowed down or stopped, and you may lose access to research or patient information.

PHISHING

Threat actors try to trick (phish) people into sharing sensitive information or downloading malicious software. Be aware of emails, texts, or phone calls in which you are asked to provide personal information, open attachments, or click on links. Threat actors design these messages and phone calls to look and sound legitimate.

DENIAL OF SERVICE (DoS)

A threat actor floods a target (e.g. a server) with traffic to crash systems and make websites and internal services unavailable. Threat actors use this attack to disrupt services and research activities or distract you; while you're trying to recover, they may be trying to steal data. You may be vulnerable even if an attack is directed at one of your service providers.

PASSWORD SPRAYING

Threat actors use bots (Internet robots that perform repetitive tasks) and lists of common passwords to brute force attack (submit as many passwords as possible until the correct one is guessed) many accounts rather than just targeting an individual account. You put yourself at higher risk if you reuse a password for multiple accounts.

You can start to protect your organization's networks, systems, and information with three steps: start with cyber security awareness, make a threat actor's job more difficult, and secure your work environment. However, these are just some of the ways to combat cyber threats. For more information on cyber security topics and best practices, visit the Canadian Centre for Cyber Security website (cyber.gc.ca).

1 START WITH CYBER SECURITY AWARENESS

Take a proactive approach to security and increase your cyber security awareness through education and training activities.

Learn how to identify phishing attempts. Review some of the common characteristics of a phishing attempt, such as unfamiliar phone numbers or email addresses, spelling or grammatical errors, requests for personal information, threats, or offers that sound too good to be true.

Exercise caution when opening attachments or links. Think twice before opening an attachment or link. Attachments and links may look legitimate or harmless, but they may be malicious. Get in the habit of verifying that an embedded URL matches the link displayed in the email, typing URLs manually into a browser or search engine instead of clicking a link, and contacting the sender to verify that a request for information is legitimate.

Use additional resources. The Canadian Centre for Cyber Security website (cyber.gc.ca) has publications, blogs, and infographics on various cyber security topics, as well as alerts and advisories on relevant cyber security issues.

During the COVID-19 pandemic, the Cyber Centre has seen an elevated level of risk to the cyber security of Canadian healthcare organizations.

2 MAKE A THREAT ACTOR'S JOB MORE DIFFICULT

Even if you take precautions to protect yourself, a threat actor may still find a way to access accounts and information. However, you can make your devices and accounts more difficult to hack.

Use a unique passphrase or password for each account. If possible, use a passphrase instead of a password. A passphrase consists of a sequence of words and is easier to remember than the string of random characters required to create a complex password. Passphrases should include at least 4 words and be at least 15 characters long.

If sharing computers or devices, avoid selecting the 'Remember Me' or 'Save Password' option when logging into accounts. Always log out when you are done. If you need help remembering your passwords, consider using a password manager (either browser-based or stand-alone app). Be sure to protect your password manager with a strong master passphrase. If a threat actor can guess your master password, they have access to your stored passwords.

Enable multi-factor authentication (MFA). Don't just rely on your passphrase. Add an extra layer of security with MFA, which requires you to provide at least two different ways of validating your identity. For example, you might use a password and a fingerprint to unlock a device. You can usually find the option to enable MFA under your device or account settings. Using MFA is a step that you can take to protect your accounts and information if your password is compromised by phishing, brute force, or password spraying.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

3 SECURE YOUR WORK ENVIRONMENT

Whether working from a designated office or remotely, you can reduce the likelihood and the possible impact of a cyber attack by adopting a few habits.

Use a secure Wi-Fi network. When working remotely, avoid using public Wi-Fi networks. If you must use one, avoid sending sensitive information or logging into sensitive accounts. Using a virtual private network (VPN) is another way to protect information if you are using a public network. A VPN is a secure encrypted tunnel through which information is sent.

Protect your own Wi-Fi network by changing the default password that was given to you by your service provider. Consider creating a guest network to reduce the number of people who are using your main network.

Use protected domain name system (DNS) services, such as Canadian Shield, that actively block known-malicious websites when you try to connect to them.

Use trusted software and applications. When at work, only use software and applications that are approved. If you need new software or applications, contact your IT department. If you are downloading software and applications yourself, be sure to download them only from trustworthy vendors.

When you see update reminders for software and applications, don't ignore them. Updates ensure that bugs are fixed and security vulnerabilities are addressed so that you're not leaving yourself vulnerable to cyber threats. Run updates on your devices and applications as soon as you can.

Use security tools to support your efforts. Install anti-virus software on your computers, laptops, and mobile devices. Anti-virus software helps protect you against malware by scanning files and your system.

Protect your networks and systems with a firewall. A firewall is a security barrier that filters out known-bad traffic on your network.

For any tools that you are using, be sure to run updates regularly.

Back up your information. Backing up your information ensures that if anything were to happen, such as a natural disaster or a ransomware attack, you could still access critical information and systems, carry out research, and care for patients.

When backing up information, be sure to use storage media that your organization has approved (e.g. cloud-based storage, or physical storage media like USB keys or external hard drives). Consider the type of information you are backing up; sensitive information should be encrypted or protected with a password.

Manage accounts with security in mind. There are very few people who need access to everything. Ensure that only people who need administrative privileges have these privileges.

While it may be convenient to have a shared account with a password that multiple people know, you are introducing risks of a possible data or privacy breach. Ensure you have your own account and password.

LEARN MORE

The tips covered in this document are a great starting point. If you want to learn more about some of the key points identified, check out the following related publications, which are available on the Cyber Centre website (cyber.gc.ca).

Cyber Threats:

- Cyber Threats to Canadian Health Organizations (AL20-008)
- Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)
- Ransomware: How to Prevent and Recover (ITSAP.00.099)
- Protecting Your Organization Against Denial of Service Attacks (ITSAP.80.100)
- Have You Been Hacked? (ITSAP.00.15)

Best Practices and Tips:

- Best Practices for Passphrases and Passwords (ITSAP.30.032)
- Password Managers—Security (ITSAP.30.025)
- Rethink Your Password Habits to Protect Your Accounts from Hackers (ITSAP.30.036)
- Secure Your Accounts and Devices with Multi-Factor Authentication (ITSAP.30.030)
- How Updates Secure Your Device (ITSAP.10.096)
- Security Tips for Remote Work (ITSAP.10.116)
- Virtual Private Networks (ITSAP.80.101)