SECURITY AWARENESS

By Marc Gaudreau CISSP

GROUPE HELIOS

OBJECTIVES OF THE PRESENTATION

- Understand risks and threats
- Recognize threats (In doubt don’t open it)
- Basic preventive measures
- Risky behaviour

CYBER SECURITY RISKS

- Whether you're banking online, connecting with friends, sending emails, or checking out the real estate market in your area, the Internet has become an essential part of everyday life.
- What you may not know is that this amazing resource is also a breeding ground for criminal activity – where your every move can be monitored and your information compromised.
- But if you take the time to learn about the common threats and risks, online security and protecting yourself can be easy.

GROUPE HELIOS

COMMON THREATS TO BE AWARE OF

- BOTNETS
- HACKING
- MALWARE
- PHARMING
- PHISHING
- RANSOMWARE
- SPAM
- SPOOFING
- SPYWARE
- TROJAN HORSES
- VIRUSES
- WI-FI EAVESDROPPING
- WORMS
- Your life online

BOTNETS

- If you've never heard of a botnet, it's likely because they go largely undetected.
- **What they are:**
- A collection of software robots, or 'bots', that creates an army of infected computers (known as ‘zombies') that are remotely controlled by the originator. Yours may be one of them and you may not even know it.
- **What they can do:**
- Send spam emails with viruses attached.
- Spread all types of malware.
- Can use your computer as part of a denial of service attack against other systems
- Learn more about protecting your computer.

GROUPE HELIOS

HACKING

- Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities.
- **What it is:**
- The process by which cyber criminals gain access to your computer.
- **What it can do:**
- Find weaknesses (or pre-existing bugs) in your security settings and exploit them in order to access your information.
- Install a Trojan horse, providing a back door for hackers to enter and search for your information.
- Learn more about protecting your computer.

MALWARE

- Malware is one of the more common ways to infiltrate or damage your computer.
- **What it is:**
- Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and adware.
- **What it can do:**
- Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information.
- Reformat the hard drive of your computer causing you to lose all your information.
- Alter or delete files.
- Steal sensitive information.
- Send emails on your behalf.
- Take control of your computer and all the software running on it.
- Learn more about protecting your computer.

PHARMING

- Pharming is a common type of online fraud.
- **What it is:**
- A means to point you to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.
- **What it can do:**
- Convince you that the site is real and legitimate by spoofing or looking almost identical to the actual site down to the smallest details. You may enter your personal information and unknowingly give it to someone with malicious intent.
- Learn more about protecting your identity.

GROUPE HELIOS

PHISHING

- Phishing is used most often by cyber criminals because it's easy to execute and can produce the results they're looking for with very little effort.
- **What it is:**
- Fake emails, text messages and websites created to look like they're from authentic companies. They're sent by criminals to steal personal and financial information from you. This is also known as "spoofing".
- **What it does:**
- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.
- Learn more about protecting your identity.

RANSOMWARE

- **What it is:**
- Ransomware is a type of malware that restricts access to your computer or your files and displays a message that demands payment in order for the restriction to be removed. The two most common means of infection appear to be phishing emails that contain malicious attachments and website pop-up advertisements.
- **What it can do:**
- There are two common types of ransomware:
- Lockscreen ransomware: displays an image that prevents you from accessing your computer
- Encryption ransomware: encrypts files on your system's hard drive and sometimes on shared network drives, USB drives, external hard drives, and even some cloud storage drives, preventing you from opening them
- Ransomware will display a notification stating that your computer or data have been locked and demanding a payment be made for you to regain access. Sometimes the notification states that authorities have detected illegal activity on your computer, and that the payment is a [illegible] prosecution.

RANSOMWARE

- **What you can do:**
- Do not pay the ransom. These threats are meant to scare and intimidate you, and they do not come from a law enforcement agency. Even if you submit payment, there is no guarantee that you will regain access to your system.
- If your computer has been infected (i.e. you are unable to access your computer or your files have been encrypted), contact a reputable computer technician or specialist to find out whether your computer can be repaired and your data retrieved.
- In order to lessen the impact of a ransomware infection, be sure to regularly back-up your data with a removable external storage drive. It's possible that your files might be irretrievable; having an up-to-date backup could be invaluable.
- In order to report the incident, please contact your local police and the Canadian Anti-Fraud Centre at 1-888-495-8501 or http://www.antifraudcentre-centreantifraude.ca/
- Learn more about protecting your computer.

GROUPE HELIOS

SPAM

- Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people. Canada has a new anti-spam legislation that you can learn more about at www.fightspam.gc.ca
- **What it is:**
- The mass distribution of unsolicited messages, advertising or pornography to addresses which can be easily found on the Internet through things like social networking sites, company websites and personal blogs.
- Canada's anti-spam legislation applies to all commercial electronic messages. A commercial electronic message is any electronic message that encourages participation in a commercial activity, regardless of whether there is an expectation of profit.
- **What it can do:**
- Annoy you with unwanted junk mail.
- Create a burden for communications service providers and businesses to filter electronic messages.
- Phish for your information by tricking you into following links or entering details with too-good-to-be-true offers and promotions.
- Provide a vehicle for malware, scams, fraud and threats to your privacy.
- Find out more about email spam.

SPOOFING

- This technique is often used in conjunction with phishing in an attempt to steal your information.

- **What it is:**
- A website or email address that is created to look like it comes from a legitimate source. An email address may even include your own name, or the name of someone you know, making it difficult to discern whether or not the sender is real.
- **What it does:**
- Spends spam using your email address, or a variation of your email address, to your contact list.
- Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.
- Learn more about protecting your identity.

GROUPE HELIOS

SPYWARE

- **Spyware & Adware**
- Spyware and adware are often used by third parties to infiltrate your computer.
- **What it is:**
- Software that collects personal information about you without you knowing. They often come in the form of a 'free' download and are installed automatically with or without your consent. These are difficult to remove and can infect your computer with viruses.
- **What it can do:**
- Collect information about you without you knowing about it and give it to third parties.
- Send your usernames, passwords, surfing habits, list of applications you've downloaded, settings, and even the version of your operating system to third parties.
- Change the way your computer runs without your knowledge.
- Take you to unwanted sites or inundate you with uncontrollable pop-up ads.
- Learn more about protecting your computer.

GROUPE HELIOS

TROJAN HORSES

- A Trojan horse may not be a term you're familiar with, but there's a good chance you or someone you know has been affected by one.
- **What it is:**
- A malicious program that is disguised as, or embedded within, legitimate software. It is an executable file that will install itself and run automatically once it's downloaded.
- **What it can do:**
- Delete your files.
- Use your computer to hack other computers.
- Watch you through your web cam.
- Log your keystrokes (such as a credit card number you entered in an online purchase).
- Record usernames, passwords and other personal information.
- Learn more about protecting your computer.

VIRUSES

- Most people have heard of computer viruses, but not many know exactly what they are or what they do.
- **What they are:**
- Malicious computer programs that are often sent as an email attachment or a download with the intent of infecting your computer, as well as the computers of everyone in your contact list. Just visiting a site can start an automatic download of a virus.
- **What they can do:**
- Send spam.
- Provide criminals with access to your computer and contact lists.
- Scan and find personal information like passwords on your computer.
- Hijack your web browser.
- Disable your security settings.
- Display unwanted ads.
- When a program is running, the virus attached to it could infiltrate your hard drive and also spread to U external hard drives. Any attachment you create using this program and send to someone else could al with the virus.

GROUPE HELIOS

VIRUSES

- **How will you know if your computer is infected?**
- Here are a few things to check for:
- It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all.
- It takes a long time to launch a program.
- Files and data have disappeared.
- Your system and programs crash constantly.
- The homepage you set on your web browser is different (note that this could be caused by Adware that has been installed on your computer).
- Web pages are slow to load.
- Your computer screen looks distorted.
- Programs are running without your control.
- If you suspect a problem, make sure your security software is up to date and run it to checl If nothing is found, or if you are unsure of what to do, seek technical help.

GROUPE HELIOS

WI-FI EAVESDROPPING

- WiFi eavesdropping is another method used by cyber criminals to capture personal information.
- **What it is:**
- Virtual “listening in” on information that's shared over an unsecure (not encrypted) WiFi network.
- **What it can do:**
- Potentially access your computer with the right equipment.
- Steal your personal information including logins and passwords.
- Find out more about Wi-Fi networks.

WORMS

- Worms are a common threat to computers and the Internet as a whole.
- **What they are:**
- A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, doesn't damage or alter the hard drive and propagates by sending itself to other computers in a network – whether within a company or the Internet itself.
- **What they can do:**
- Spread to everyone in your contact list.
- Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies enormous amounts of lost revenue.
- Learn more about protecting your computer.

GROUPE HELIOS

YOUR LIFE ONLINE

- From emailing to social networking to shopping – the Internet is your connection to just about everything. That's why online safety should never be far from your mind.
- Email
  Risks associated with your email account.
- Banking and Finance
  Ways your private banking information could be compromised.
- Social Networking
  Protecting the personal information you share and avoiding scams.
- Mobile
  Attacks to your devices you may not know about.
- Shopping Online
  Staying aware of the risks of online shopping and bidding.
- Online Gaming and Entertainment
  Risks of online entertainment, games and contests.
- Downloading and File Sharing
  How to download safely.
- Voice over Internet Protocol (VoIP)
  The threats that come with online phone calls.

QUESTIONS ?

GROUPE HELIOS