A Webinar on Cyber Security Best Practices and Security Awareness

November 2020

pwc

Agenda

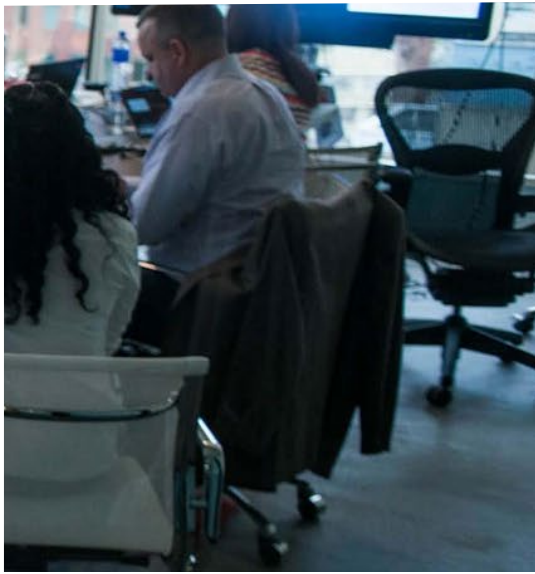
- Introductions
- Understanding the Threats
- Social Engineering
- Protecting Personally Identifiable Information
- Securing Devices
- Questions

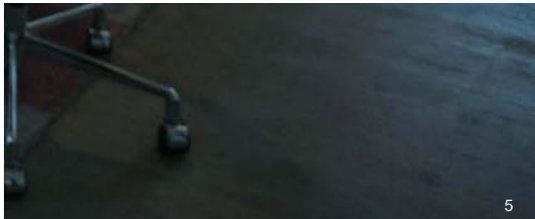
1 Introductions

Speaker

Andrew Plummer
PwC
BC Privacy Leader &
Cybersecurity Manager

2 Understanding The Threats





Remember: Information security is everyone's responsibility, not just IT

Cyber attackers understand that the easiest intrusion vector is you

- Phishing or planting infected USB drives are a few of the common ways methods used to exploit untrained employees
- No amount of technical controls can keep an organization 100% safe – security policies must foster a culture of **security awareness**

Data breaches can occur without any malicious actors

- Lost unencrypted laptops or accidentally sharing sensitive information on social media are incidents that can be considered breaches
- Your organization relies on you to report an incident when you see one

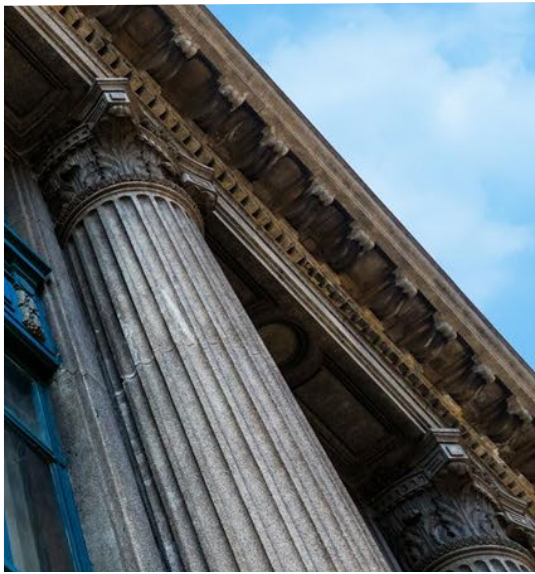
What can you do?

- ***Identify what you've got (crown jewels, PI, operational systems)***
- ***What's valuable (to you, and to outsiders)***
- ***How they're going to get it? Figure out where your risk lies***
- ***What can you do when you're small - be difficult***

Specific examples:

- ***Cloud is good,***
- ***Embed privacy and security into processes earlier,***
- ***Training + awareness,***
- ***Patching,***
- ***Two factor authentication,***
- ***Classify what you have,***
- ***Protect key information,***
- ***Delete what you don’t need,***
- ***Encrypt what you have.***

3 Social Engineering



Social engineering attacks

Social Engineering

Social Engineering has become one of the most widely used techniques for exploiting vulnerabilities. Cyber criminals use social engineering tactics because it is easier to exploit our natural instinct to trust than it is find out ways to hack the Organisation's network, servers and applications.

How does it happen:

- Attackers create a doppelganger account that is almost identical to the email address of the targeted individual, relying on the assumed trust between the victim and their email to facilitate the attack.
- Attackers use fake email Id's, text messages and fake phone calls on the targeted user or a group of users to exploit their accounts which in turn provide access to the internal network. All are designed to be appear normal and request a user to take action; by clicking a link, answering a question or sharing information about company or client.

How to prevent:

- Attackers employ a sense of urgency to make to make you act first and think later in phishing attacks. Be sure to take a moment to check if the source is credible or not.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Don't send sensitive information over the internet before checking a website's security.
- Take advantage of any anti-phishing features offered by your email client and web browser.
- Enforce multi-factor authentication (MFA).

Consequences of Successful phishing

All it takes is one employee to fall victim to a phishing attempt and allow hackers to successfully infiltrate cyber defenses.

Trojans

Hackers can use malware to exfiltrate sensitive information or sabotage critical IT systems.

Ransomware

Hackers can encrypt business data, making it unavailable for use, and demand payment in return for the data.

Spyware

Hackers can install malware that can keylog your keyboard input, monitor your internet activity, or activate your webcam and microphone

Compromised accounts

Hackers can use stolen usernames and passwords to gain restricted access to sensitive information such as firm strategy, client documents, personal data, etc.

Stolen identity

Hackers can use the personal information gained from the victim for identity fraud or further social engineering.

Wired money

Hackers can use financial information gained to wire money to untraceable accounts.

Identifying a Phishing Attempt

From: myaccount@amazoncanda.ca **[Validate the domain name]**

Subject: URGENT: Account Verification Required **[Be aware of the immediate action items. Do not proceed without verifying with respective authorities]**

Date: August 6, 2020 10:11:02 AM PST

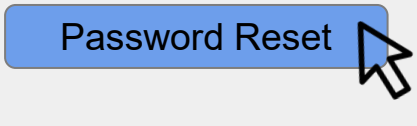
To: John Doe

Dear customer,

There has been some suspicious login attempts occurring through your account. In order to prevent further compromise to your account and personal information, we request you to reset your password through the link below within the next 48 hours otherwise your account will be frozen and terminated.

Thank you for your cooperation,

Your Amazon Team



[Hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed]

passwordreset2d4hk1.com

Types of Social Engineering Attacks

Email Phishing: malicious emails sent that are designed to deceive recipients into providing sensitive information, or clicking links/file attachments that install malware (e.g. viruses, spyware).

How to Identify and Prevent from Email Phishing

- Check for bad grammar
- Be wary of emails that play on your emotions
- For every email, verify the email address of the sender
- Do not click hyperlinks or download attachments from suspicious emails

Vishing ("voice" + "phishing"): phishing attempts that leverage voice technology such as landlines or mobile phones. Attackers often spoof their caller ID to appear as a legitimate phone number.

How to Identify and Protect from Vishing

- Use caution when answering unsolicited phone calls
- Be wary of phone calls that attempt to sell you something or demand payment
- Tell the caller you will call them back with their official number you have on hand.

SMiShing ("SMS" + "phishing"): phishing attempts that leverage SMS texting. Like vishing, SMiShing attackers may use spoofed phone numbers to send text messages.

How to Identify and Protect from Smishing

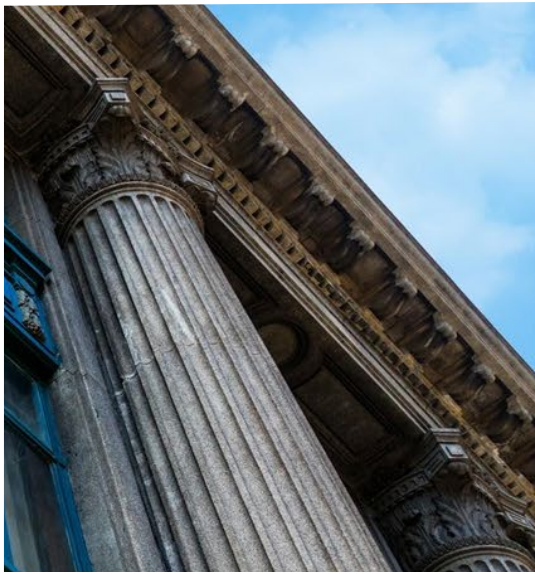
- Use caution when reading unsolicited text messages.
- Continue correspondence over official channels.
- Be wary of text messages from phone numbers that contain "5000" or are not actual phone numbers.

Spear phishing: phishing that focuses on small groups of people. Whale phishing is a method of phishing that targets individuals. Both are targeted and personalized to increase susceptibility.

How to Identify and Protect from Spear phishing

- Minimize the amount of information publicly available about you.
- Be cautious of strangers who attempt to connect with you via social media.
- Be aware that spear and whale phishing attempts may utilize emailing, calling, and texting conjointly.

4 Personally Information (PI)



Personally Information(PI)

PII is any data that can be used to identify a specific Individual. This Information floats around on internet and sometimes the information is publicly made available without considering the consequences. For Example, Social media profiles expose Individual names, Email IDs, Phone numbers which can be a threat if the information is used to target a specific individual or the company they work for. Businesses and consumers need to understand the risks and recommended security measures before releasing or storing any personal information.

Personally Identifiable Information includes names, contact numbers, Social Insurance Numbers, Passport documents etc. Other examples of PII include:

- Geolocations
- Biometrics
- Mailing Addresses
- Login Credentials
- Photographs and Personal Information in Social Media
- Medical records and Lab reports
- Patient information collected in Health care Providers Database

Best Practices to Secure PI for Organizations and Users

What Organizations can do to secure PI	What users can do to secure PI
• **Collect only what is required.** In most of the cases, PII is used for the verification process. For Example, SIN can be used to identify an individual, but afterward , the SIN it not necessary. In such cases, organizations should not store SIN as it increases their risk. • **Delete PII that is no longer needed.** Delete any PII that is outdated or no longer necessary so that it is not available to potential attackers. Make sure to follow a secure process for deletion and ensure that all copies and backups are deleted as well. • **Implement security measures based on the confidentiality of the PII.** Not all PII requires same level of protection. Identify the risk level and then implement security controls to prevent any data loss. Encrypting the data during the storage and in transit should be emphasized and access controls on mobile devices will mitigate the amount of risk to PII. • **Implement security measures based on the confidentiality of the PII.** Not all PII requires same level of protection. Identify the risk level and then implement security controls to prevent any data loss. Encrypting the data during the storage and in transit should be emphasized and access controls on mobile devices will mitigate the amount of risk to PII.	• **Be aware while providing sensitive information on websites and shared drives.** Users should remove PII from user entered information before submitting any application forms or online surveys. Do not post PII on internet (including social networking websites), shared drives that can be accessed by individuals who do not have a “need to know”. • **Be careful about sharing your social insurance number.** Users should only provide SIN number to only respective authorities when required. Validate and confirm whether you are providing this information to legitimate sources. • **Use strong passwords and creative security questions.** Do not use default passwords such as Password, 1234 etc. Use a strong password with a combination of letters, special characters and numbers to make sure it is difficult for someone to guess. Be creative while adding security questions to retrieve account information when you no longer remember the password. • **Browse Privately. Private browsing deletes cookies, temporary internet files, and browsing history after you close the window.** The best way to stay anonymous online is to hide your IP address using a web proxy, a VPN, or Tor, an open network that routes your traffic through a series of servers before sending it to your destination.

Using Social Media Safely To Safeguard Personal and Organization Data

Few tips on using social media :

Follow your company's social media guidelines. Remember to never post company information on social media sites without prior permission.

Always keep business accounts and personal accounts separate. Help prevent criminals from associating your personal life with your work life**.**

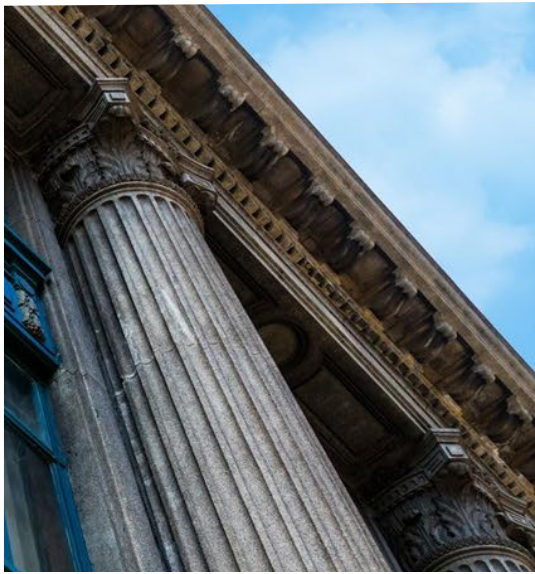
Define your privacy profile and settings to control the type of personal information you share. Controlling the information about you on the internet can reduce the amount of personal information criminals can use.

Risks with social media :

- User information is available for anyone who knows where to look.
- Network of known or connected peers, family members, or friends can be identified.
- Attackers can impersonate a known point-of-contact to gain additional information.
- What you put on the internet is there forever and can be propagated quickly.
- If you realize you put sensitive information on social media you want to redact – it may already be too late.

Social media can be a tool for cyber criminals to gain more information about you, or a source of an information breach if you're not careful of what you share.

5 Securing Devices



Keeping devices secured

A few tips on securing devices :

Lock your screen when you are away from your computer for a short amount of time. Locking your screen will prevent unauthorized individuals from accessing your laptop without your password.

Shutdown your laptop when no longer in use (e.g. end of day). If you need to store it overnight, secure safely in a locked cabinet, locker or file drawer.

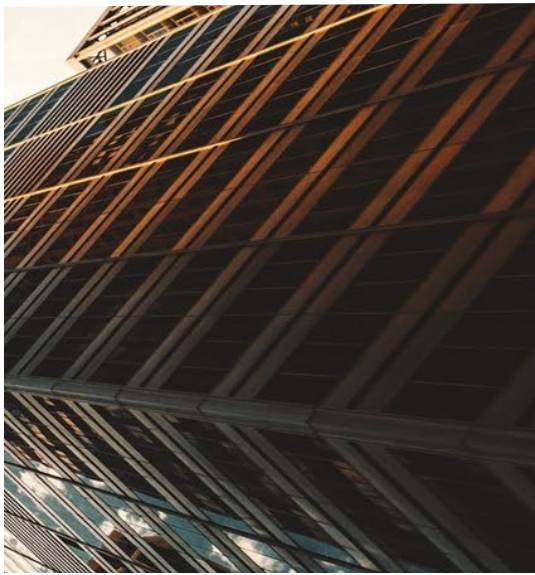
Do not share company-issued laptops and devices with family and friends. Access to sensitive data should be restricted only to yourself.

When working at a public location and stepping away from your laptop temporarily, secure laptops to a fixed point with a cable lock. Never leave devices at an unfamiliar location.

If you are leaving laptops or other devices in a car, secure everything out of sight and lock your car. Criminals may attempt to break into your car if they see valuable property in your vehicle.

Help protect sensitive information by keeping your devices safe from theft and unauthorized access.

6 In Conclusion



Main takeaways

Phishing is one of the top attack methods that organizations currently face – always double-check before clicking links or downloading attachments.
Employees with access to sensitive information are much more likely to be targeted for phishing/social engineering attacks – be wary of any stranger asking you for information.
Avoiding visiting risky websites and never ignore warnings from your browser.
Use sound business judgement at all time when using social media services.
When on-the-go, be sure to account for all of your devices and never write down passwords on sticky notes.
Be aware of your surroundings when working in public areas by using VPN connections and privacy screens.
Do not share your work devices, cell phones, tablets, or laptops with others, even your own family members.
Avoid using the same passwords for personal and professional accounts, and create long passwords with symbols, numbers, and lower/upper case characters.

PRIVACY LAWS AND CYBERSECURITY:
Understanding the Legal Framework and Best Practices

CLARK WILSON

Monica Sharma, Partner

Legal Framework for Cybersecurity

- Several laws impact cybersecurity
- Privacy Laws set out key obligations with respect to cybersecurity
- *Personal Information Protection and Electronic Documents Act* (Canada) or PIPEDA
  - does not apply where personal information is not collected in the course of "commercial activities"
  - can be tricky from a compliance perspective as some activities of a charity or not-for-profit could be a "commercial activity"

Legal Framework for Cybersecurity

- *Personal Information and Protection Act* (BC) or PIPA
  - does apply to charities and not-for-profit organizations in BC
- Cybersecurity is a key aspect of privacy compliance: holding personal information in compliance with the privacy laws, means holding it securely

Cybersecurity and the Privacy Laws

PIPA

"An organization must 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 risks." (PIPA, Section 34)

Cybersecurity and the Privacy Laws

PIPEDA

- PIPEDA contains 10 fair information principles
- Principles expand obligations in PIPEDA by including practical compliance aspects
- Principle 7 addresses cybersecurity squarely

Cybersecurity and the Privacy Laws

PIPEDA – Principle 7

4.7 Principle 7 — Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

Contd./ …

Cybersecurity and the Privacy Laws

PIPEDA – Principle 7 (cont'd)

4.7.3

The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

Best Practices for Cybersecurity

- Cybersecurity best practices involve considering the nature of personal information collected and determining the most secure methods to store and handle that information.
- There are several measures that can assist with complying with Principle 7 and PIPA's requirements
- Conduct an audit of the current cybersecurity status of the organization:
  - What and who is connected to your systems?
  - What programs are running on your systems?
  - What security programs and practices are in place to protect information?
  - Do you have programs to detect breaches?

Resources for Cybersecurity Compliance

Federal Privacy Commissioner
Securing personal information:
A self-assessment tool for organizations

Canadian Centre for Cyber Security
Baseline Cyber Security Controls for Small and Medium Organizations

Innovation, Science and Economic Development Canada
CyberSecure Canada Program

Repercussions for Non-Compliance with the Privacy Laws

- Investigations by Privacy Commissioners
- Fines
- Claims by individuals – several class actions for data breaches have been certified in Canada
- Reputational Harm and Loss of confidence of donors/members

Questions?

Andrew Plummer

PwC Canada

778 985 7780
andrew.x.plummer@pwc.com

Monica Sharma

Partner – Clark Wilson

604 643 3166
msharma@cwilson.com

Raman Johal

Partner – Clark Wilson

604 643 3145
rjohal@cwilson.com

Areet Kaila

Partner – Clark Wilson

604 643 3130
akaila@cwilson.com