Cyber Security & Policy #83:Information Technology and Mobile Devices

Township of Southgate and Cyber Security

Purpose

- The purpose of this training is to outline Policy #83 Information Technology and Mobile Devices as well as gain better understanding of cyber security

- The purpose of the policy is to outline the acceptable use of information systems and computing equipment at The Township of Southgate. These rules are in place to protect Council members, employees and the Township of Southgate. Inappropriate use exposes the Township of Southgate to risks including malware attacks, compromise of network systems and services, loss of confidential information, and legal issues .

What is Cyber Security?

- Cyber Security is the practice of protecting systems, networks and programs from digital attacks.
- This includes implementing (and using) technologies, processes and practices to protect our systems (ie our Policy)

What is Cyber Risk?

- Cyber Risk is any threat that can harm an organization or company through its technology
- Any devices connected to the internet are at risk
- Technology is a big component of the workplace and leaves risk of leaking sensitive information

How to Prevent Cyber Attacks

- Employees are the most targeted for Cyber Attacks because they generally have access to sensitive information and with so many employees, the odds are eventually one of them will be tricked
- Know what they can look like
- Be familiar with and follow Township of Southgate Policy #83 Information Technology and Mobile Device Policy.

What does a Cyber Attack Look Like?

What do Cyber Attacks Look Like?

There are 2 types of attacks

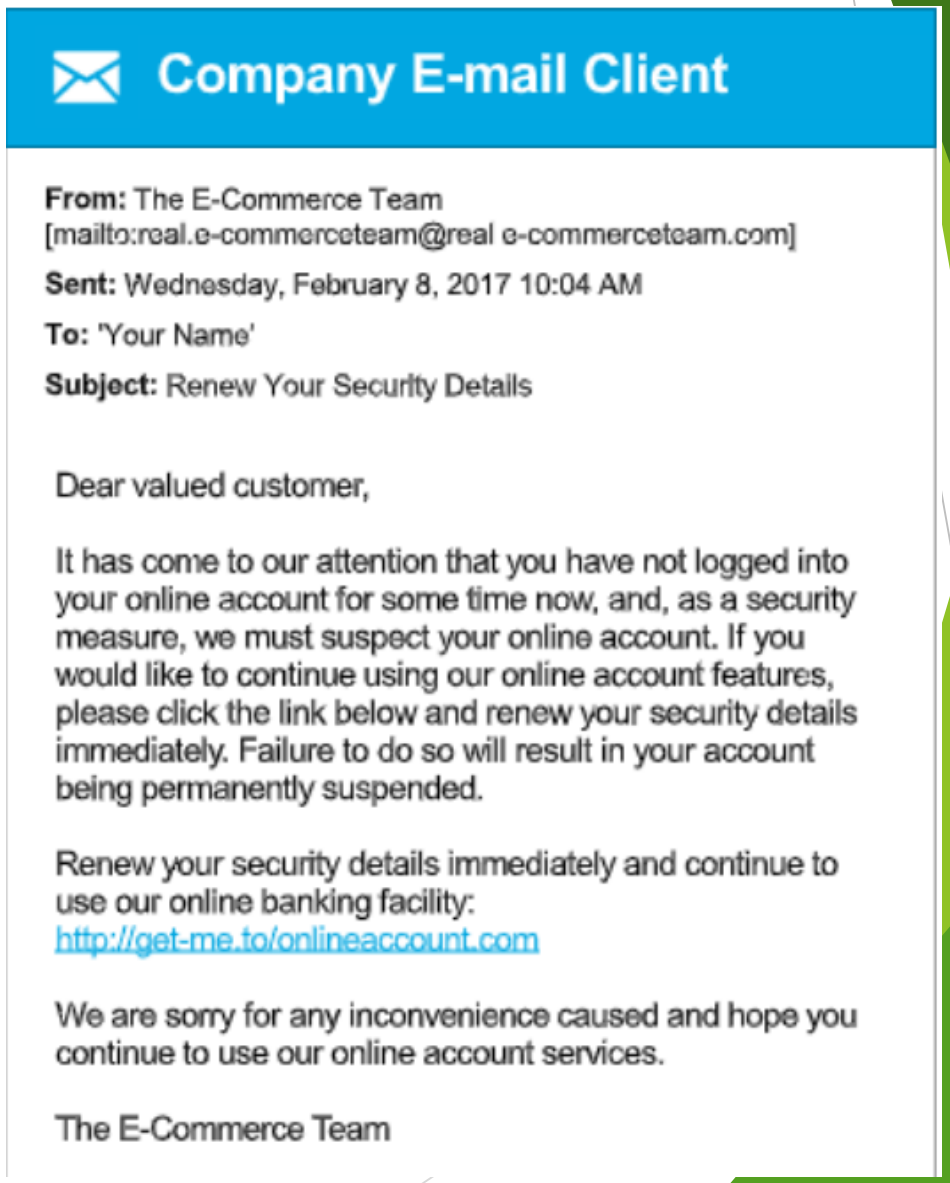
- **Go After the Technology Directly**
  - Use computer viruses and/or code that steal data, corrupt files or hold company's files for ransom
  - These can be introduced through:
    - Hyper Links on websites or in an email
    - Email attachments
    - Software downloads
  - These often look like legitimate attachments or links to real websites. Sometimes the website looks legitimate.
- **Attack IT Systems through the employees who use them. Also known as "Social Engineering"**
  - Definition of Social Engineering: the use of deception to manipulate individuals into divulging confidential or person information that may be used for fraudulent purposes

Recognizing Cyber Attacks

- Tips on how to spot a Phishing Email
  - Check the URL of the link by hovering over and confirm it is the same as the link shows and does not include any suspicious names or spelling mistakes
  - The message includes poor grammar or spelling
  - The message asks for sensitive information such as passwords, account numbers, etc.
  - You were not expecting the email
  - In the email it gives a password for the attachment
  - Check the email address; if the email appears to be from someone you know but seems suspicious check the address matches one they have used before OR call the person to confirm they actually sent the email

Recognizing Cyber Attacks

This link would send you to a website that looks legitimate and would ask you to enter a username and password and possibly answer security questions. This information would then be recorded and used to gain access to your account on the actual website.



Company E-mail Client

From: The E-Commerce Team
[mailto:real.e-commerceteam@real e-commerceteam.com]

Sent: Wednesday, February 8, 2017 10:04 AM

To: 'Your Name'

Subject: Renew Your Security Details

Dear valued customer,

It has come to our attention that you have not logged into your online account for some time now, and, as a security measure, we must suspect your online account. If you would like to continue using our online account features, please click the link below and renew your security details immediately. Failure to do so will result in your account being permanently suspended.

Renew your security details immediately and continue to use our online banking facility:
http://get-me.to/onlineaccount.com

We are sorry for any inconvenience caused and hope you continue to use our online account services.

The E-Commerce Team

Recognizing Cyber Attacks

- Pretexting is another method of social engineering
- Pretext is a made-up scenario to convince a person to give information that the perpetrator is not allowed to know (usually login credentials or financial data)
- This could be a person calling or emailing and impersonating someone that requires information.
- An example would be someone saying they are from our IT support and ask for your username and password. They will tend to make up consequences to make you feel pressure.

Tips:

- If something is questionable – don't do it. Contact Kayla or our IT Support to confirm
- If it appears to be coming from someone you know but you aren't sure – contact that person via phone to double check

Policy # 83

Policy #83: Information Technology & Mobile Device Policy

- The purpose of the policy is to protect all of us and the Township
- The Policy applies to all Township of Southgate devices, employees (including Council) and contractors
- Acceptable Use
  - Outlines what actions are not to be done
  - Personal internet use must adhere to all usage policies
  - Online File Sharing is to be approved by IT support prior to use
  - Email usage policy includes not sending unsolicited emails, harassment, chain letters or similar messages
  - Social Media standards when posting on behalf of the Township
  - Remote Access is not permitted without authorization
  - Reporting security incidents

Policy #83: Information Technology & Mobile Device Policy

- General Provisions
  - Lock devices and use strong passwords and PINs
  - Do not install unauthorized software or apps from untrusted sources
  - Do not modify configuration settings
  - Report lost or stolen devices immediately
  - Keep your devices secure and do not leave unattended
  - Backup your data
  - Keep your system updated
  - Log out of sites after use
  - Do not send personal information via text or email
  - Be careful what you click

What to do if Cyber Attack happens?

- If you suspect something has happened, contact IT Support immediately and Kayla

- If you need to wait for them for any reason, disconnect your device from the internet/wifi until they have been in touch with you.

Questions?