

CyberSecurity & Privacy

Training

Oct, 2019



Bell Pensioners' Group

Together, Protecting our Pensions and Benefits



Anthony English, Mariner Security
and Modified by Peter Dilworth, BPG

CyberSecurity & Privacy Events

Every day there are reports in the media about cybersecurity and privacy and these reports are typically in the following topic areas:

- [Data/Privacy Breaches](#) – confidential data is accessed by hackers or accidentally disclosed
- [Hacking](#) – an organization or individual is “attacked” by a hacker who accesses their computer(s) and/or data
- [Identity Theft](#) – personal information is stolen by a person who assumes their identity in order to steal from the victim’s bank accounts, use their financial credit, etc.
- [Nation-State Attacks](#) – a country or government uses trained hackers to attack the infrastructure or systems of another country for financial or military gain

Types of Attacks/Breaches

The ways that cyberattacks or data breaches can occur today are varied and evolve on a regular basis:

- **Ransomware** – software that is sent to a victim (often in an email) that looks harmless but encrypts your data and demands you pay a ransom to get your data back
- **Phishing** – fake emails that are sent to a victim to trick the victim into clicking on a link or sending personal or financial information
- **Vishing** – fake text messages that are sent to a victim to try to trick the victim in the same way as a phishing attack
- **Hacking** – this is typically a direct attack run across an Internet or public WiFi connection
- **Social Engineering** – this is when an attacker poses as someone they are not in order to gain your trust and then gain information from you.
- **Viruses or Malware** – viruses and malware can cause damage to data and computer systems

Phishing

Phishing is an attempt to trick the recipient of an email (or via telephone call - vishing) to do something that would provide the attacker with valuable information or resources. There are two types of Phishing:



Mass phishing – a mass fake email sent out to many recipients.



Spear phishing – a fake email is sent out to targeted recipient(s) and crafted to interest the target recipient(s).

Mass Phishing Example

From: Amazon <management@mazoncanada.ca> on behalf of Amazon
To: @sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

amazon.com[®]

Dear Client, ← Generic non-personalized greeting


We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

Sincerely, ← Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates

Spear Phishing Example

Ben Woelk

From: Edu Help Desk <info@pa.com>
Sent: Tuesday, September 08, 2015 3:16 AM
To: info@pa.com
Subject: [Suspected Spam] Edu Email Upgrade Against Spam.

Attn: Email User,

Due to the high risk of spam emails going on in the internet, we have decide to upgrade all educational email set by our admin panel, and access to your mailbox via our mail portal will be unavailable expect you upgrade your email account against fraudulent spam.

To upgrade and re-validate your mailbox, do click on the link to upgrade: [Upgradepage](#)

Thanks,
Educational Ad

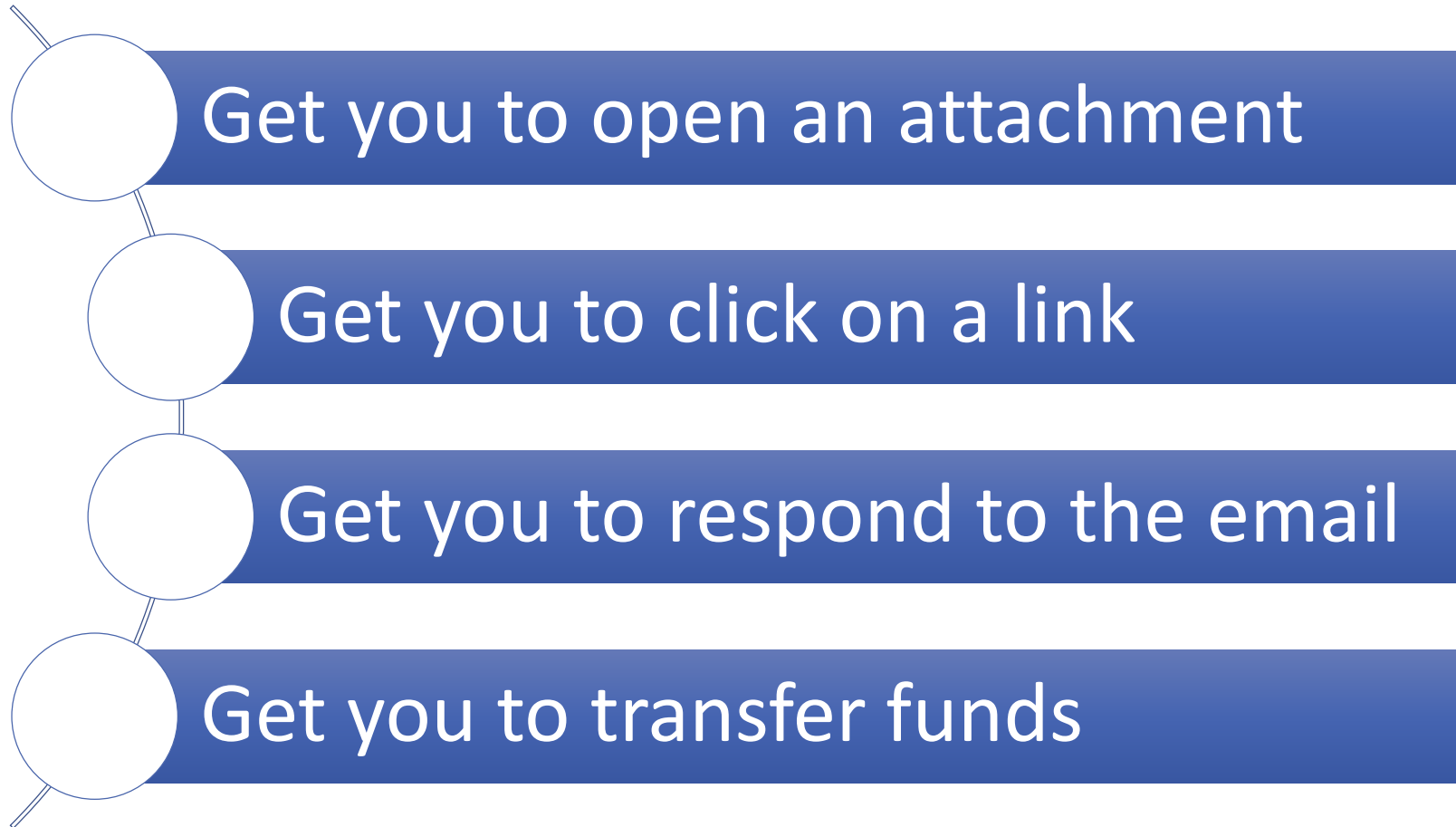
<http://www.designrepublic.cz/wp-content/advanced/cache/upgrade/account/webmail.php>
Click to follow link

Spelling

Generic addressee

Link goes to external site

Phishing – How They Trick You



How to Protect Yourself

- **Install an anti-virus** app like Symantec, BitDefender, etc.
- **Never open** an email or text that you did not expect to receive
- Do regular **backups** of your information
- Be sure to apply the **latest updates** to your computer, tablet, etc.
- **Avoid downloading** software from non-trusted web sites
- **Never trust a random phone call** that threatens you or asks for information
- If someone shows up asking you to let them in or give them access, **always default to "no"**. When in doubt, ask for ID
- **Never disclose personal information via email**, over the phone, or via text
- Always treat **other people's information as strictly confidential**
- **Never disclose personal information on social media** (e.g., vacation plans)
- **Use strong passwords** and change your passwords on a regular basis

Helpful Links



How to check to see if you are already hacked

Check the the following web site by entering your email address
(work or personal email):

<https://haveibeenpwned.com>

Online Security Tips

<https://www.shoutmeloud.com/5-tips-keep-yourself-safe-secure-surfing-internet.html>

https://www.f-secure.com/en/web/home_global/tips-for-safer-surfing