CyberSecurity & Privacy

Training

Oct, 2019

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

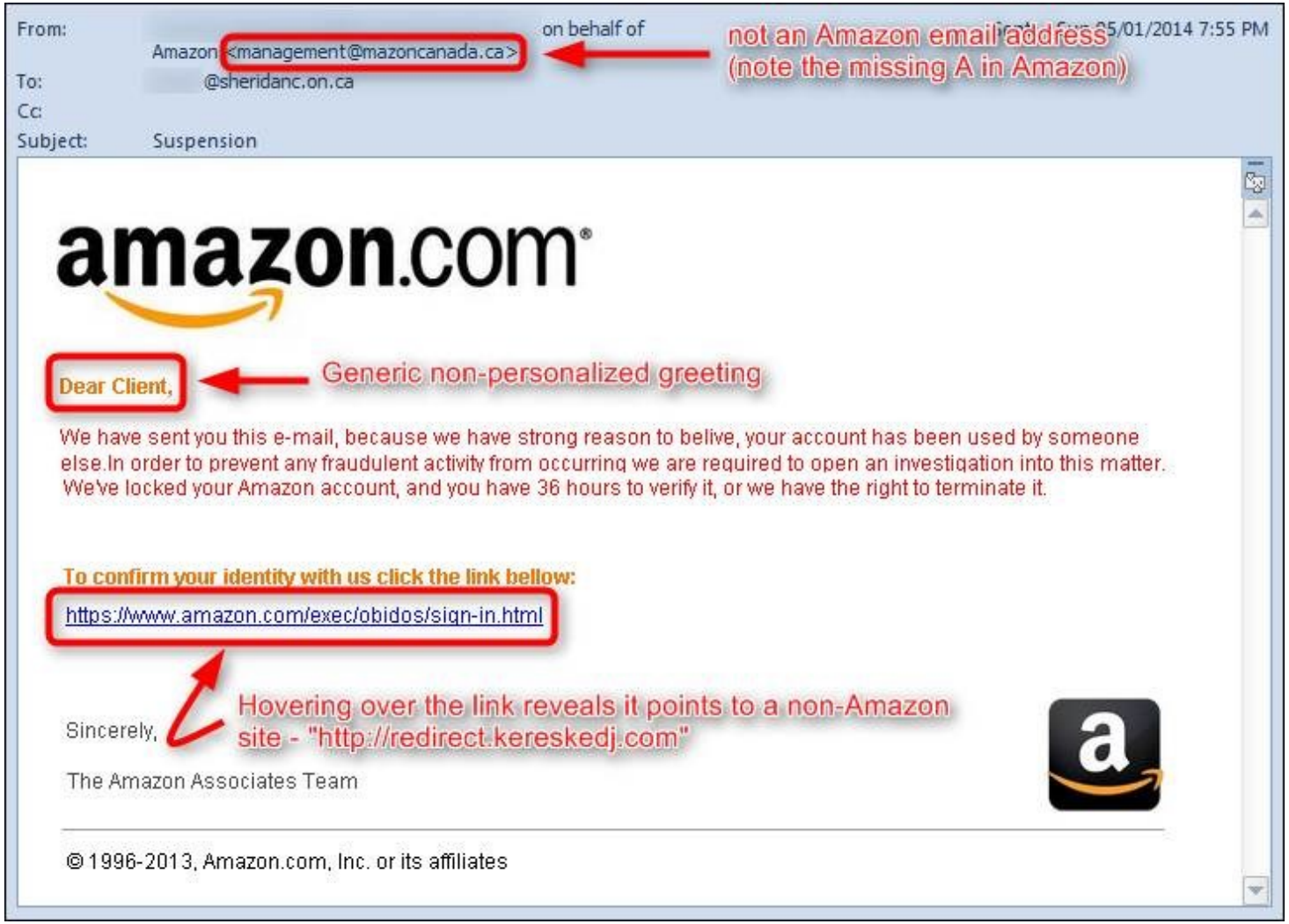
Phishing

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:

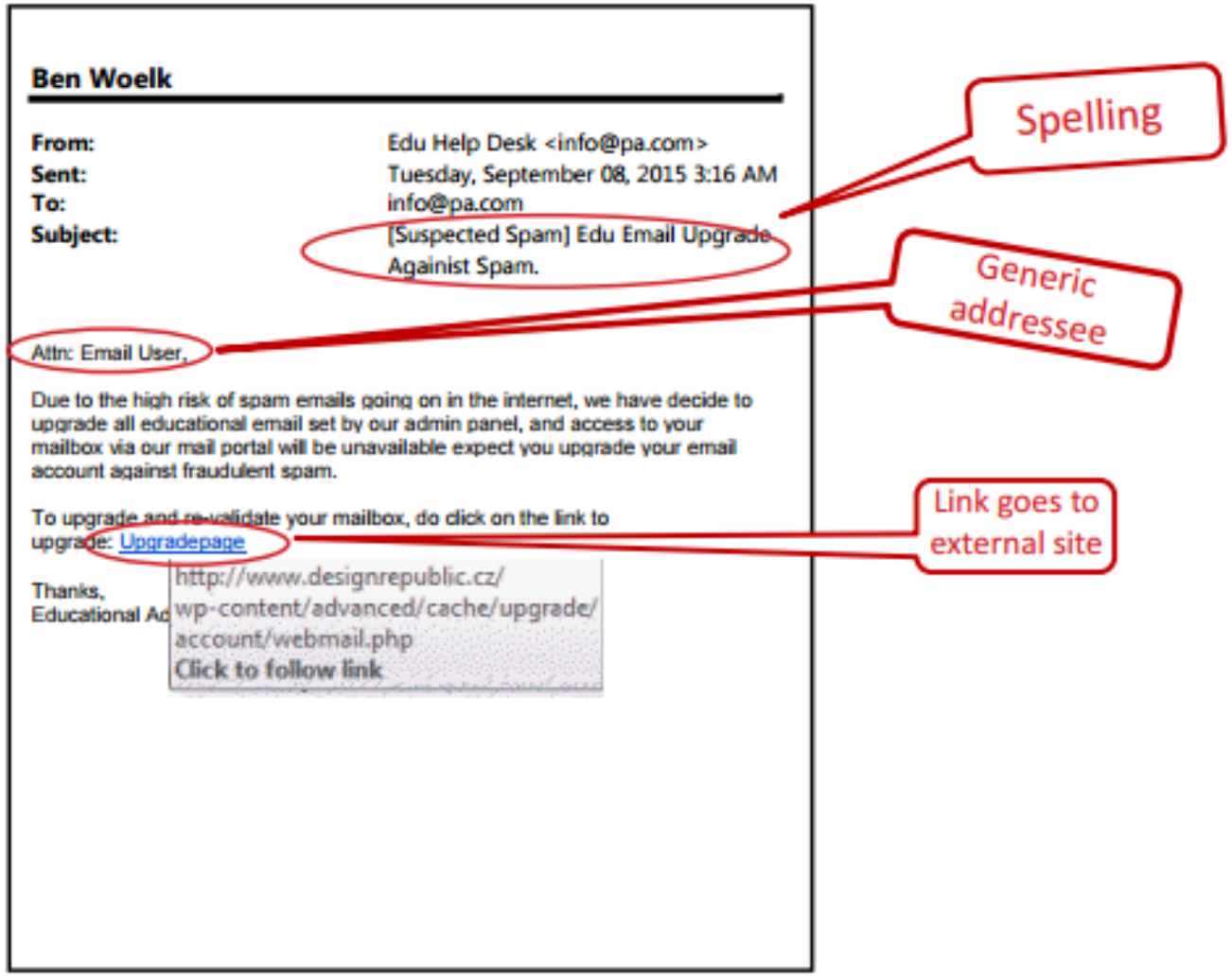
Mass phishing – a mass fake email sent out to many recipients.

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

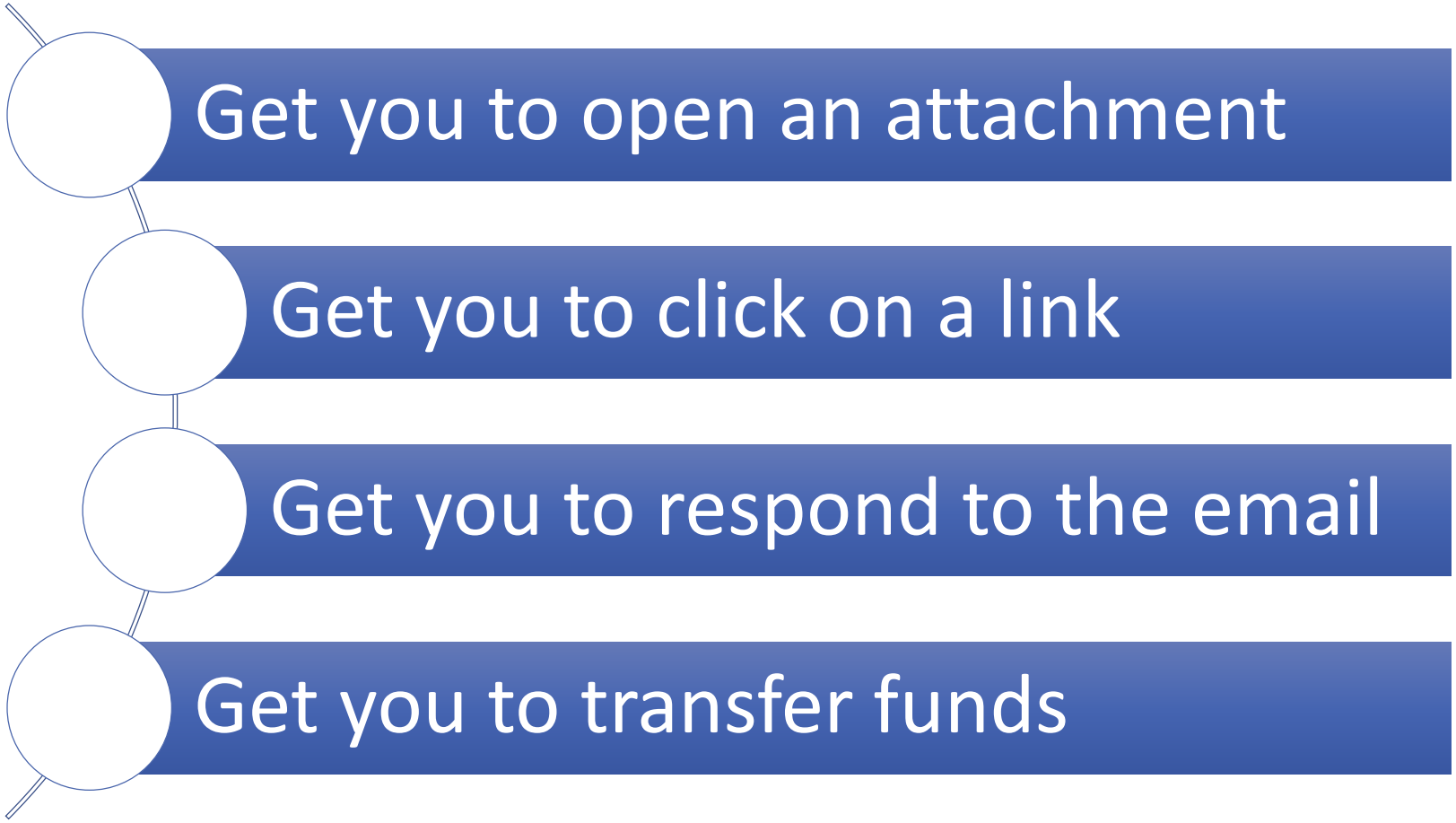
Mass Phishing Example



Spear Phishing Example



Phishing – How They Trick You



Bell Pensioners' Group
Together, Protecting our Pensions and Benefits

MARINER SECURITY SOLUTIONS

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 strickly 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