Cybersecurity

This time, it’s personal.

University of Victoria

Why is this important?

- You are targets because of your individual value
- You are targets because of the access/authority associated with your position
- There is a financial motivation behind attacks
  - Your credit card information is worth $20-$30 USD
  - Average ransomware payout: $1400 USD

University of Victoria

Top Threats

- Phishing to steal your credentials
- Social engineering (phone/in-person)
- Mobile device theft
- Spyware and ransomware

University of Victoria

Agenda

1. The Internet of Things
2. Mobile
3. Banking and Finance
4. Shopping Online
5. Social Networking
6. Email

University of Victoria

The Internet of Things

- “Smart” devices that connect to each other via the Internet
  - Light bulbs, cameras, thermostats, appliances
- If you can access them, cybercriminals can too
- They can use them to spy on you, but can also take control of them to attack others: “bot-net”

University of Victoria

The Internet of Things

- Change the manufacturer's default user names and use strong passwords
- Update device software regularly
- Understand what personal information is being collected and why it's needed before you buy IoT devices or download apps
- Turn off geolocation when it isn't needed

Mobile

- It can get stolen! Make sure it has a secure passcode
- Be careful what software you install and where you install it from
  - Apple App Store does a better job than the Google App store, but neither is foolproof
- Beware of scams, like SMS messages from your bank
- Don’t connect to untrusted networks

University of Victoria

Banking and Finance

- Cyber criminals will go to extraordinary lengths to steal your bank account number, your password, your login information or your credit card information – directly from you via:
  - Phishing
  - Malware

University of Victoria

Banking and Finance

- Close/open your browser before you start
- Choose strong passwords and keep them private
- Look for the lock symbol on the website or "https://" at the beginning of the website address (the "s" means "secure") to be sure the site is encrypted
- Never allow "auto fill" or "auto-remember" of your password or personal information

University of Victoria

Banking and Finance

- When you're banking online, never use public Wi-Fi or public computers
- Remember that legitimate banks and businesses will never ask for your personal information in an email, so be suspicious if you get this request
- Always enter the website address in the browser yourself – never use a link
- As soon as you're done banking, log out and close the browser

University of Victoria

Shopping Online

- Online banking tips apply
- The biggest risks are being scammed or being defrauded by personal and credit card information you provide
- Pay by credit card if you can; do not send cash
- Be on the lookout for prices that are too good to be true; they're likely counterfeits
- Read your credit card statements and check for unauthorized charges; think about a dedicated card

University of Victoria

Social Networking

- Your personal information could be stolen, and the information you share could be used to target you for other types of attacks
- Use a strong password
- Change your privacy settings
- Think carefully about what you share online!

University of Victoria

Email

- Use a strong password
- If you think the email looks suspicious, DELETE IT
  - Do not forward suspicious emails
  - Do not click on suspicious links
  - Do not open suspicious attachments

University of Victoria

Campus Resources

- If in doubt about anything, before you take action ask for assistance
  - Desktop Support Services (DSS)
  - Computer Help Desk (CHD)
    - 250-721-7687
    - helpdesk@uvic.ca
- Take phishing awareness training: https://www.uvic.ca/phishing
- University Systems Service Catalogue:
  - http://www.uvic.ca/systems/
  - Section on Information Security

University of Victoria

QUESTIONS?

Thank you for attending!

Email: navbassi@uvic.ca

Twitter: @navbassi

University of Victoria