CYBER SECURITY @ UBC

Threats to privacy include:

- **Phishing** - email or websites that spoof legitimate sites, tricking you into providing personal information
- **Social Engineering** - confidence tricks designed to manipulate someone by giving just enough information for you to give them what they need in order to commit fraud or gain system access
- **Mobile device/laptop/USB drive theft**
- **Viruses and spyware** - malware that could cause your computer to become accessible to unauthorized users, or could even corrupt or delete data without your knowledge
- **SPAM** - unrequested/unauthorized email or messages that can be used as a method of verifying a person's existence, leading to more malicious phishing or hacking attempts
- **Password compromises** and other hacking attempts

How to protect yourself:

- **Don't open suspicious emails** or follow links in suspicious messages. Always ask first if you're not sure if a message is valid
- **Don't download software without ensuring it is free of viruses or spyware.** Make sure you have strong virus/malware protection installed on your machine
- **Follow UBC policies and standards**
- **Use strong passwords** (minimum 8 characters with upper case, lower case, numbers and symbols) or a passphrase of at least 16 characters
- **IT staff will never ask for your password**; emails that ask for this should be reported to your IT support
- **Use encryption to protect files and drives**, or use encrypted devices to secure your data
- **Use common sense.** No one legitimate will ask for sensitive information via email or unsecure websites
- **Clear desk policy:** Don't leave passwords on sticky notes or in notebooks lying on your desk. Ensure you don't leave personal information out in the open

Take the Cyber Security Awareness Quiz for a chance to win great prizes: **it.ubc.ca/cybersecurity**