Protecting Your Online Presence

UMRA

Jenny Blaine
University Information Security
security@umn.edu

September 15, 2020 Slide deck: https://z.umn.edu/20200915UMRA
Acceptable Use of Information Technology Resources

The acceptable use policy that applies to all users on the University Network. One important call-out from this policy:

- Do not share your Internet ID and password
  - We often get reports from a spouse that both spouses are using one spouse's UMN email account. This becomes problematic when the account owner passes away.

z.umn.edu/use
Your **accounts and identity** are valuable

You have valuable **access, assets, and trust relationships**

You are a **gateway** to the University’s and your own personal network; you hold the keys to the kingdom

Threats - What cyber attackers are doing

- **Fraudulent email and other scams** << Number 1 threat!
  - Try to trick you into spending your own money for something
  - Can be highly targeted or a random spamming event
  - Can also trick you into installing malware

- **Malware / Ransomware**
  - Infect your computer and steal your information; attachments or infected websites can be vectors
  - **Ransomware** is a type of malware that encrypts your files and the files of any shared drives mapped on your computer and holds them until you pay the ransom

- **Malicious websites or ads on websites**
  - Distribute malware or compromise your credentials
  - Use uBlock Origin or McAfee SiteAdvisor
  - Use UMN VPN to access U resources from off campus > safecomputing.umn.edu
Why?

The short answer: **Money**

- Cybercrime is a world-wide billion-dollar business.
- Cybercrime is how many people make a living.
- There are specialized tools out on the Internet so hackers/cyber attackers don't even need to have programming skills any more.
- Hacktivism is a very small percentage of cybercrime.
How does it work?

Scammers take advantage of current events and human greed/curiosity/needs to:

- Trick people into giving them **money**!
- Take over and hide in accounts.
- Steal identities.
- Steal money:
  - Redirect direct deposit (e.g. pay or student loans)
  - Request funds be wired to offshore locations

Email is most common but scams appear in texts and telephone calls too!
1. Know your data and where it is
2. Be wary of email and web site scams
   Think before you click to open an attachment or login; check with the sender via phone or in person.

1. Use multi-factor authentication (MFA)
2. Use strong and unique passwords
   Use a unique password or passphrase for each account you create. Use pass phrases or sentences. Longer = better

1. Keep your computers and devices up-to-date
   Turn on auto-updates for operating systems and apps, even on your phone

1. Enable Security Features on your device (e.g. whole disc encryption, firewall)
2. Back up your data regularly, use storage solutions like Google Drive and Box
   In case your device is lost, stolen, or fails + the only real protection against Ransomware

If in doubt, reach out! Get a second opinion before you click!
Multi-factor Authentication (MFA)

- Duo - Required for all staff and students since November 2019; anyone can opt in via my-account.umn.edu
  - [https://it.umn.edu/services-technologies/duo-two-factor-authentication](https://it.umn.edu/services-technologies/duo-two-factor-authentication)

Many companies and services now support MFA

- Set up personal DUO or use an alternative MFA (Google Authenticator, etc.)
- Check for options for MFA when setting up new accounts or check account settings for existing
  - Especially for accounts tied to purchases or money (e.g. bank, Playstation or Xbox, etc.)
Passphrase Selection

Caption: “Through 20 years of effort we’ve successfully trained everyone to use passwords that are hard for humans to remember but easy for computers to guess.”

Solution:
Use a passphrase rather than a password.
Managing Many Unique Passwords

- **Password Managers** - Many options
- Paper not a terrible option
- Open Source options
  - PasswordSafe
  - GNOME keyring
  - Keepass
  - Keychain (Apple built-in)
- Premium Options
  - 1Password
  - LastPass (free/premium)
  - Dashlane
Protect yourself with backups

Having a **backup** of your data is the only way you can recover files:

- If your computer breaks, or is damaged
- If your computer gets infected with malware/Ransomware, or
- If you accidentally delete a file.

Store files on systems that are automatically backed up, like Google Drive.

If you store files directly on your computer (e.g., on your desktop or in your Documents folder), your data IS NOT backed up by default. We recommend doing one of the following:

- Use **Google backup & sync** to backup your computer (note limit of 15 GB)
- Use an automatic backup system, such as TimeMachine for Mac or Windows backup, with an external drive.
Stay safe on wifi

● On campus
  ○ Use eduroam

● On open, public wifi
  ○ Avoid visiting sites that require you to log in
  ○ Use UMN VPN to access UMN resources

● At home
  ○ Set a strong passphrase
  ○ Use a separate password-protected network for guests (available on most modern home routers)
  ○ Use UMN VPN to access UMN resources
Protect your Mobile Devices

- Use screen locks
- Only install trusted apps
- Understand what permissions you are granting to applications
  - Why does BrickBreakerz need access to my camera?
- Enable remote location and remote wipe
- Don’t “jailbreak” to install non-validated apps
- Back up your data!

The Top 10 ways to protect mobile devices
Things in the Internet of Things (IoT)

- Any device that connects to wireless but cannot use eduroam (WPA2-Enterprise, un/pw auth)
  - Chromecast/Amazon Firestick/Roku
  - Xbox/PS4/Switch
  - Google Home/Alexa
- Review [resources for securing IoT devices](#)
  - Change default passwords
  - Disabled unused services
  - Use trusted apps
- [Register IoT Devices](#) for use on the UMN network
I got a weird...

Email
Phone Call
Popup

... is this legitimate?
Think before you click!

Recognize automatic behavior and work against it

Read popups carefully

When in doubt, reach out!

- Technology Help can assist with questions or cleanup: help@umn.edu or it.umn.edu/help
- Forward suspicious emails to phishing@umn.edu
- Report security events to security@umn.edu
  - Suspected social engineering
  - Popups that won’t go away
  - Ransomware
Information Security Resources

● Phishing Blog
  ○ Lists recent phishing and other scams targeting the University community [https://it.umn.edu/phishing](https://it.umn.edu/phishing)

● Information Security Awareness Training (ISA101)
  ○ Required for all new employees
  ○ Delivered via [training.umn.edu](https://training.umn.edu)

● Practicing Safe Computing (SecureU)
  ○ News and resources for security practices [https://it.umn.edu/secure-u](https://it.umn.edu/secure-u)
Questions or Stories?
Thank You