UNIVERSITY OF ILLINOIS SYSTEM

CYBERSECURITY BEST PRACTICES

- Use a strong password. Longer, more random, and more varied phrases make the strongest passwords.

- Make each password unique. Don't reuse passwords across applications, websites, or systems. Consider using a reputable password manager.

- Use multifactor authentication for additional account security wherever possible.

- Be careful when clicking links or opening attachments in emails or on web pages.

- Set up password protection on all your devices, so no one can access the data on them without knowing the password.

- Set your operating system and other applications to do updates automatically. Set up reminders to manually update all your applications that don't update automatically.

- Back up important files frequently.

- Secure your mobile phone: use a passcode to lock it and store it in a safe place when you're not using it.

- Don't share passwords or other sensitive information. Lock your computer when you step away from it.

- Follow departmental and university policies on:
  - Financial transactions and other sensitive actions.
  - Data retention.
  - Communication.
  - Social media.

- If you work from home or work remotely while traveling, follow responsible remote connection practices like:
  - Avoiding public WiFi.
  - Using a VPN, especially if you must use an untrusted network.
  - Using a wireless hotspot, or connecting your computer to your cell phone, in order to avoid public WiFi altogether.
  - Changing settings or installing extra security software.

- Notify security@illinois.edu right away if any university device, or anything containing university data, has been compromised, lost, or stolen.