Staying Safe At Work

- Lock your office when you leave; If you can't lock you area, lock your computer
- Lock filing cabinets; Shred documents with sensitive information
- Use a long and strong UU network password; Set it at **password.uu.edu ;** Never share it!
- Be careful when opening unsolicited email and suspicious-looking attachments
- Avoid logging into UU email/network services from wireless locations in foreign countries, airports, public wi-fi, etc.
- Never use public computers anywhere to check UU email or log into UU services
- Never forward suspicious emails, as this potentially may spread infection to other individuals or areas of the UU network
- Unless you are 100% sure of the source, do not click links within an email that direct you to a URL/address requiring log-in; instead, open a browser and type the URL of the site and then log in
- Never send email with personally identifiable information (PII) such as SSN, Date of Birth, etc. in the body or in an attachment, even to others at UU
- Be careful to recognize phishing attempts from sources that appear to be Netflix, Wells Fargo, Bank of America, Amazon, and others
- If you suspect you're the victim of an attack or you're suspicious about an email you've received, immediately contact IT Help at help@uu.edu or731-661-HELP

uu.edu/it/security

uu.edu/it/policies

uu.edu/it/security/TownHall-Feb2018.pdf