UW Medicine

OCTOBER: CYBERSECURITY AWARENESS MONTH

It is no secret that cyber-attacks are becoming more sophisticated and persistent. UW Medicine employees have accidentally compromised their logins over 300 times this year alone, by clicking on links or attachments in phishing emails. Phishing continues to be our biggest security challenge, even though it is a well-known threat.

During October, UW Medicine will observe Cyber Security Awareness Month, a national campaign designed to promote good cybersecurity practices. LEARN MORE: UW Medicine Information Security (https://depts.washington.edu/uwmedsec)

Cybersecurity habits that keep employees and patients safe

By forming good security habits, every faculty and staff member can help prevent cyber-attacks. Here are some simple and effective practices to adopt.

WHEN IN DOUBT, DELETE IT

Links in email and online posts are often the way cyber criminals compromise your computer. If an email is unexpected and looks suspicious, here is what you can do:

- **DO NOT** click on any links or follow them to any websites asking for login credentials
- **DO NOT** enter your NET ID login in any forms or websites
- **DO NOT** open any attachments
- **DO** contact the "sender" if known to you, but use a different, trusted way to confirm legitimacy
- **DO** delete the email (if reporting it, send it as an attachment before you delete it)
  REPORT PHISHING EMAILS - Send an attachment of the email to help@uw.edu
  REPORT SPAM EMAILS - Send an attachment of the email to reportedspam@cac.washington.edu

LOCK DOWN YOUR LOGIN

To reduce account theft at work or home, develop good habits that protect your login and identity.

- **DO** enable multi-factor authentication (MFA) on your bank, social media and work accounts. This simply means you agree to verify your identity multiple ways before getting access. Many applications offer MFA security. To get started, here are some factors you can combine:
  - *Something you know* like your username/password
  - *Something you have* like a text to your smart phone
  - *Something you are* like your fingerprints
- **DO** create strong passwords (try using longer sentences or phrases that are easy to remember)
- **DO NOT** use the same password for different accounts

IF YOU CONNECT IT, PROTECT IT.

Whether it is your work or home devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems.

- **DO** sign up for automatic updates
- **DO NOT** delay updating devices. Install security updates when your programs tell you they are available.
- **DO NOT** store confidential information on unapproved systems or devices.

RESOURCES:
Protecting Patients: Security & Compliance Guidance for Teleworking
UW Medicine Information Security (https://depts.washington.edu/uwmedsec)
To report a cyber security event, email UW Medicine Help Desk at mcsos@uw.edu.