UTHealth Information Security – Employee Guide

The purpose of UTHealth Information Security program is to provide a secure information infrastructure for schools and departments to utilize in the pursuit of the Institution's goals in research, teaching and healthcare. Some of the most common cybersecurity issues are listed below.

Phishing

Phishing is when someone tries, via email, text, or phone call, to get you to reveal your personal information by pretending to be a trustworthy company, brand, or university. If you think an email may be suspicious, don't click!

- **https://inside.uth.edu/itsecurity/sac/phishing-awareness/**

Passwords

Your security is only as good as your password. Never give out your User ID or system password. The help desk will never ask for your password!

- https://inside.uth.edu/itsecurity/securityresources/

Virus Protection

Millions of viruses circulate on the Internet via emails, malicious websites, and instant messages. Don't let important data get corrupted by a computer virus.

- **https://inside.uth.edu/itsecurity/sac/phishing-awareness/**

Remote Access to Resources (VPN)

UTHealth's VPN service allows faculty and staff to securely access networks and access services, just as if they were actually at work.

- **https://inside.uth.edu/itsecurity/secops/vpn/**

Want to learn more?

The IT Security team serve as a resource for information relating to current technologies by providing employees with computer skills, knowledge, and competencies to thrive in the UTHealth workplace. To get more information:

- **https://inside.uth.edu/it-training/links-other-resources.htm**

Contact information

IT Security

https://inside.uth.edu/itsecurity/contact-us/index.htm

UT Help Desk

https://inside.uth.edu/helpdesk/index.htm

(713) 486-4848