UNIVERSITY of HOUSTON | IT SECURITY

Safe. Simple. Secure.

www.uh.edu/infotech/security | security@uh.edu | 832.842.4695

Security Best Practices for Staff

Your Account…Your Responsibility

All University of Houston faculty, staff and students have their own individual user IDs and passwords for accounts and services offered and are responsible for any activity conducted with their user ID. Never share your user ID and password with anyone.

Don't get caught by the Spam Filter

Email messages with more than 100 recipients are likely to appear as Spam to the UH mail system and may not be delivered. To ensure your message is delivered correctly, the UIT E-communications team can send the message for you. They can also provide tracking statistics for the email message. Visit uh.edu/infotech/services/e-comm or email ecomm@uh.edu for more information.

Email: Don't Keep What You Don't Need

In the event your email account is ever compromised, you want to make sure minimal information is exposed to someone who gains access to your account. Take time on a regular basis to manage the messages in your email account. Refer to UH MAPP 10.03.07, Email Retention and Discovery, for assistance in determining how to manage and retain email messages.

Classify that Data

All data in use at the university must be classified. Depending on its classification, data may have required protections according to university policy. Knowing how to appropriately protect confidential, sensitive and mission-critical information is everyone's responsibility.

There's No Place Like Home

When working from home, or any other remote location, it is still possible to work securely. Use a VPN to establish a secure connection to the UH network and have access to all of your data. This eliminates the need for you to transport files from your office to your home on an unsecured removable media device, and ensures you always have the latest version of your data available to you.

Have a Safe Trip!

When travelling with a laptop or other mobile computing device, physical security must be a top priority. Make sure to keep the laptop properly secured (i.e. hotel room safe) when it is not in your possession. Confidential or sensitive information should not be stored on the laptop unless it is encrypted.

Mission: Device Security

While it's important to secure the data you have on your mobile device, it's also important to secure the actual device. Don't ever leave your device unattended and or in your car and make sure to password protect the device.

General Security Tips

You Maintain Your Car…Make Sure You Maintain Your Computer

- Keep your software current. Having the latest updates to your operating system and software applications are the best defenses against viruses, malware and other online threats.
- Automate software updates. Many programs will automatically connect and update to defend against known risks.
- Protect all devices that connect to the Internet. Smart phones, gaming systems and other web-enabled devices also need protection from viruses and malware.
- Plug & scan. Any external device, such as a flash drive, can be infected by viruses and malware. Use your security software to scan them.

Protect Yourself: Keep Your Personal Information Personal

- Use strong passwords. Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- Use separate user IDs and passwords for each type of account (e.g., banking, email). This will lessen the opportunity for identity theft if one of your user IDs and passwords is compromised.
- Keep your passwords safe. If you must write it down, store it in a safe, secure place away from your computer or device.
- Use Identity Finder. The University of Houston provides Identity Finder software to help prevent identity theft by locating sensitive and confidential data (such as social security numbers, credit card numbers and passwords) stored on your computer. You should never store your personal information on a UH computer.

Connect With Care

- When in doubt, throw it out. Links in email, tweets, wall posts and online advertising are often ways for cybercriminals to compromise your computer. If it looks suspicious, delete it.
- Don't get hooked by phishers. Do not reply to e-mail requests for personal account or financial information. Legitimate companies and organizations will not ask you to verify your personal information in this way.
- Protect your name and your $$. When providing information, banking or shopping online, look for web addresses with "https://" or look for the lock somewhere on the website. This will tell you the site is secure.
- UH has gone Green. Look for your address bar to turn green on "uh.edu" sites that ask you to enter your personal information. A green bar means the site has an EVSSL, which verifies the authenticity of the site.

Public Displays of Information

- Change your password. If you use a public computer (e.g., Internet café, library) to access any of your accounts, for instance your email account, change your password once you return to your own computer.
- Use open wireless carefully. When on an unsecured open network, avoid accessing sites that ask you to provide your personal information. Find a secure wireless network to do this.
- Don't check it! When using a public computer, or any computer that is not your own, never check the box that asks if you want the computer to remember your password.

Think Before You Click! | Once on the web, ALWAYS on the web | Stop. Think. Connect.