6. WATCH YOUR STUFF
Thieves are everywhere, even on our campus. Never leave your stuff unattended. Make sure you ask someone you know to watch your stuff.

7. BE INSANE ABOUT PRIVACY
Whether it’s a government organization or a low-key hacker, someone will always be interested in not only your personal data but the devices that hold it. Be insane and be aware of your privacy at all times and remember to protect your data.

THE IT SECURITY & COMPLIANCE OFFICE

WHO ARE WE?
The ITSC (Information Technology Security and Compliance) Office assures the existence of a safe computing environment in which the university community can teach, learn, and conduct research.

TO LEARN MORE ABOUT US:
If you’d like to learn more about ITSC Office please visit our webpage:
https://www.uhd.edu/infosec

1. TRACK YOUR DEVICES
Enabling Apple’s Find My iPhone, or the Android Device Manager will help track, lock and erase your devices in the event they are misplaced or stolen.

2. LOCK YOUR COMPUTER
Leaving devices unlocked for even a second, allows anyone to steal data physically later. Use the following keyboard shortcuts to lock a computer quickly.

MacOS
control + shift + power button

Windows

3. ENABLE ADBLOCKERS
Beyond blocking online ads, adblockers provide personal security by blocking offensive material and malicious software while you browse the web.

4. RESTRICT YOUR INFO
Per the Family Educational Rights and Privacy Act or (FERPA), some info about you that UHD maintains may be disclosed to the public, without your consent, via the UHD Directory. However, you are entitled to restrict this info.
uhd.edu/registrar/students/records-requests

5. SECURE YOUR UHD ID
UHD IDs not only contain information about you but may grant you access to certain buildings.
2. USE A STRONG PASSPHRASE/PASSWORD

Passphrases and passwords go hand in hand. When a passphrase is possible, make it memorable, 20-30 characters long, and use uppercase and lowercase letters, numbers, and symbols. For passwords, follow the same routine and simply translate it into an acronym.

<table>
<thead>
<tr>
<th>EXAMPLES</th>
<th>STRENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>I graduated from The Univ of Houston Downtown in 2018!</td>
<td>910 septenvigintillion years to crack</td>
</tr>
<tr>
<td>IgfUoHDI2018!</td>
<td>16 billion years to crack</td>
</tr>
</tbody>
</table>

Want to test the strength of your password?
Check out: HOWSECURISIMYPASSWORD.NET

3. USE TWO-FACTOR AUTHENTICATION [2FA]

(Also known as) 2FA, two-step verification or TFA, is an extra layer of security that not only requires the usual password and username but also something that user has on them; two of the following three:

- Something You Have (e.g. a phone)
- Something You Are (e.g. a fingerprint)
- Something You Know (e.g. a password)

WHAT ARE THE DIFFERENCE?

A passphrase, similar to a password, is simply a memorable phrase or arrangement of words separated by spaces. Because of their lengthy nature, they are much harder to crack and thus the logical alternative to passwords. However, the only caveat is they aren’t supported across the board yet.

HOW ARE THEY COMPROMISED?

- Relentless Frenemies:
  A “friend” may be able to guess passwords or security questions by using social engineering tactics.

- Brute-Force Attacks
  An attack that works by trying all possible password combinations until the right one is found.

- Data Breaches
  Usernames and passwords may be compromised if a site is hacked and its data breached.

- Phishing Attacks
  A type of fraud where an attacker attempts to learn sensitive information by posing as a reputable entity, such as a bank, through email, IM, or other communication channels.

WHAT’S THE DIFFERENCE?

- Relentless Frenemies:
  A “friend” may be able to guess passwords or security questions by using social engineering tactics.

- Brute-Force Attacks
  An attack that works by trying all possible password combinations until the right one is found.

- Data Breaches
  Usernames and passwords may be compromised if a site is hacked and its data breached.

- Phishing Attacks
  A type of fraud where an attacker attempts to learn sensitive information by posing as a reputable entity, such as a bank, through email, IM, or other communication channels.

WHAT ARE SOME TIPS?

1. CONSIDER A PASSWORD MANAGER

Memorizing strong passwords can be a challenge. Thus, there are many programs, called password manager, which allow you to manage your passwords and sometimes offer integrates services such as password generators. Try one of the following:

- KEEPASS.INFO
- LASTPASS.COM
- 1PASSWORD.COM

HOW DO I ENABLE ENCRYPTION?

MacOS
Although a lengthy process, it’ll run in the background.
Go to System Preferences > Click Security & Privacy > Click the FileVault Tab > Click the Lock Button to Unlock > Enter the Admin Password > Click Turn On FileVault

iOS
Setting up a passcode or password enables encryption automatically.
Go to Settings > Select Touch ID & Passcode > Tap on Turn Passcode On > Enter a Strong Passcode or Password

Android [Newer Devices]
Setting up a security code or fingerprint enables encryption automatically.
Go to Settings > Select Security > Select Screen Lock > Enter a Strong Security Code

Windows PC
Bitlocker may not be available on all Windows operating systems.
Go to Control Panel > Click System and Security > Click BitLocker Drive Encryption > Click Turn On BitLocker

Windows Mobile
Go to Settings > Tap on System > Tap on Device Encryption > Enable Device Encryption

PHISHING TIPS

- Don’t open email attachments or click on links from untrusted sources.
- Always use caution when opening any attachments or links.
- If you are not expecting an email or it just doesn’t look right, don’t open it. It could be a phishing attempt!

ENCRYPTION

WHAT IS IT?

Encryption is the translation of readable data into a secret code. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. In case your device is ever lost or stolen, your secret selfies and the rest of your data will be safe.