SECURITY & PRIVACY TIPS

01. REGISTER YOUR PROPERTY
UTPD offers a free online service to register personal property. If they ever go missing, serial numbers, makes, models and colors will be readily available for use by UTPD for property retrieval.

02. 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.

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

MAC

control + shift +

WINDOWS

+ L

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

05. RESTRICT YOUR INFO
Per the Family Educational Rights and Privacy Act, or FERPA, some info about you that UT Austin maintains may be disclosed to the public, without your consent, via the UT Directory. However, you are entitled to restrict this info.

06. SECURE YOUR UT ID
UT IDs not only contain information about you but may grant you access to certain buildings.

07. WATCH YOUR STUFF
Thieves are everywhere, even on our campus. Never leave your stuff unattended. But, if you need to, make sure to ask someone you know to watch your stuff.

08. 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 privates.

THE INFORMATION SECURITY OFFICE

WHO ARE WE?
The ISO assures the existence of a safe computing environment in which the university community can teach, learn, and conduct research.

To learn more about security, check out the Protect Your Privates section on our website:

SECURITY.UTEXAS.EDU/PYP

FOLLOW US!
Stay up to date with us and everything you need to know on cyber and information security at UT and in the world!

@utaustiniso
@utjiso
@utjiso
PASSPHRASES & PASSWORDS

WHAT’S 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, their only caveat is that 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 about an individual or organization by posing as a reputable entity, such as a bank, through email, IM, or other communication channels.

WHAT ARE SOME TIPS?

01. CONSIDER A PASSWORD MANAGER
Memorizing strong passwords can be a challenge. Thus, there are many programs, called password managers, which allow you to manage your passwords and sometimes offer integrated services such as password generators.

UT Austin has one available for all faculty, staff, and students to use named STACHE (created by the Information Security Office).

02. USE A STRONG PASSPHRASE/PASSWORD
Passphrases and passwords go hand in hand. When a passphrase is possible, make it memorable. 28 to 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 Texas at Austin in 2018!</td>
<td>910 septenvigintillion years to crack</td>
</tr>
<tr>
<td>IgfTUoTaAi2018!</td>
<td>16 billion years to crack</td>
</tr>
</tbody>
</table>

To test the strength of your password check out ‘How Secure Is My Password?’

HOWDOISEMYPASSWORD.NET

04. 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 only 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)

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.

HOW DO I ENABLE IT?

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 Pass Code 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

Android [Older Devices]
Before manually encrypting, a passcode must first be setup.

Go to Settings > Select Security > Tap on Encrypt Phone/Tablet

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

Windows