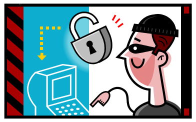
Information Security Tips



Passwords

DO NOT give your password to anyone! Put passwords on all user accounts on your computer-especially the **Administrator** account. Strong passwords should be between 8 and 20 characters long; include uppercase and lowercase letters, numbers, and special characters (*, &, ^). The longer and more complicated a password is, the less likely it is to be broken. You may use a sentence that is easy for you to remember, like "Excuse me, do you have 15 cents?" and make that into a strong password => "Em,dYH15C?". Never use personal information when creating passwords. UTEP's password policy requires you to use a strong password and change your password at least yearly. **DO NOT use the feature "Remember Password"** offered by various applications. Lastly, lock your computer, even if you step away for just a few minutes, or log-off.

Computer Viruses and Worms

Viruses and worms are programs that run on your computer without your knowledge. These programs can often be harmful, spread over an internet connection or email, may delete important system files, or gather sensitive information (SSN/Credit Cards) from your system. It is extremely important to enable the firewall, use an anti-virus program, download security patches, and keep them up-to-date. To better protect yourself never open unexpected email attachments, even if they are from someone you know. If unsure about an attachment, contact the person who sent it to you or call the HelpDesk for further instructions. For information and free/free trial anti-virus programs visit *security.utep.edu* under the "**Student or Faculty and Staff**" QUICK LINKS.

Spam

Spam is any unsolicited email that is sent in bulk—this usually refers to unwanted advertisements. It is important to know that spam is unavoidable. There are steps you can take to reduce the amount of spam you receive. Using a dedicated account from a free email service (like Hotmail or Gmail) to sign up for newsletters and post to newsgroups helps cut down spam in your main account. Also, if you have a personal website, don't post your email address on any of the pages, as addresses are often harvested and sold to spammers.

What Can I Do to Minimize Spam

- If your email address is not required, do not give it out or post publicly.
- If you receive a suspicious email or pop-up, do not reply or click on it.
- Do not open email attachments you are unsure of.
- **NEVER** reply to, or "unsubscribe" from, spam mailing lists; delete them instead.
- Create filters within your email application, such as Outlook or Eudora.
- Report campus spamming to *spam@utep.edu* (include email header information-call ISO for instructions).

NOTE: Reporting spam will not necessarily prevent it from happening again.

Confidential Information

SSNs should not be used as a form of identification; instead use the UTEP 800/880 number. Questions regarding this policy may be directed to the Information Security Office or email **security@utep.edu**. **NEVER** transmit SSNs in clear text in an email or unencrypted attachment. Visit the Security Awareness page for information on "**How to Protect Sensitive Information**"

Spyware

Spyware is any software that gathers information through a user's internet connection without the user's knowledge or permission. These programs are often bundled with shareware and freeware programs especially peer-to-peer (P2P) programs. To help avoid spyware, **NEVER** click on ads/pop-up banners when surfing the web, and don't download freeware or shareware programs from untrusted sources. Visit the Information Security website under "**Anti-Virus Information**" for links to various free anti-spyware programs.

Identity Theft

With identity theft on the rise, it is important that you verify who you're giving information to. **NEVER** give anyone your password or personal information. Look for a lock icon 🔒 on the browser's status bar, or the site address will contain "http**s**" in the URL. The "**s**" stands for SECURE. Please visit the Federal Trade Commission website on Deter-Detect-Defend tips for fighting back against identity theft. *www.ftc.gov/bcp/edu/microsites/idtheft*

Piracy/Copyright Infringements

Duplicating, sharing, or downloading copyrighted material for which you do not own the copyright is strictly forbidden. Anyone found using file sharing programs (P2P) like LimeWire, Ares, Azureus, Gnutella, BitTorrent, and Kazaa to illegally download/share movies, music, games, or software may be subject to loss of internet access (including email) at UTEP ***permanently***. Note that violation of these policies may also result in disciplinary action for employees and students, up to and including, termination of employment, suspension, and/or expulsion.