

Protecting Your Computer



Every time we go online, open an e-mail message, click on a link, use instant messaging or download anything, we are running the risk of exposure to thousands of types of malicious software such as viruses, worms, spyware, bots and more. These programs can crash computers, hijack personal information and can be spread to the university's network.

When you connect to the university network from home, your home computer can become a threat to university resources. Therefore, it is important that you take steps to protect your work computer as well as your home computer from these types of threats.

Types of Malware



WORMS – A program that makes copies of itself. Worms can infect a computer through a Web page, an attachment, a download, over the network or a flash drive. Worms can overload a computer by tying up system resources and shutting the computer down. They can also overload a network by constantly attacking other computers.

VIRUS – A program that infects a computer, usually without the knowledge of the user. Much like a worm, a virus can also copy itself. However, this usually requires some user interaction such as opening an attachment, clicking a link or opening/downloading a file.

TROJAN – A method of delivery of malware. Trojans can be found in downloadable content – a free game, music, a video or software.

BOT – A collection of computers, remotely controlled by hackers, that can run independently and unknown by the users. These machines are often called “zombie” computers, and they run on networks known as botnets.

SPYWARE – Standalone programs that are downloaded when users visit a Web page, use instant messaging, open an e-mail attachment or download a file. Spyware can secretly monitor a user's activities by detecting and recording passwords, bank account information, social security numbers, credit card numbers and other sensitive information.

Results of Malware

Compromised computers are often used to send spam, launch attacks on other networks and probe other networks and systems for vulnerabilities. Collected information (such as Social Security numbers, Credit Card numbers, etc.) can be used by other hackers, spammers and identity thieves.

Icons courtesy of DryIcons at <http://dryicons.com>

What can you do to protect your computer?



Now that we know some of the bad things that can happen to your computer, let's look at what we can do to protect it.

- Enable automatic updates and make sure all patches/updates are installed
- Install anti-virus software and ensure that it is updating and working properly
Visit the OIT Web site to see if anti-virus software is available for home use
- Install and use spyware removal tools
*Spybot Search and Destroy (www.spybot.info)
Adaware (www.lavasoftusa.com)*
- Make sure all other software you have installed on your computer is up to date
Secunia Personal Software Inspector (www.secunia.com) can check many types of software
- Read e-mail as text only (instead of in HTML format)
- Use a non-administrator account
- Make sure that wireless access is protected
*Use strong encryption such as WPA or WPA2
Change default login passwords*

Web & Other Resources



UTSA Information Security Office:

<http://www.utsa.edu/oit/security>
e-mail: informationsecurity@utsa.edu
phone: (210) 458-5555

UTSA Office of Information Technology:

<http://www.utsa.edu/oit>
e-mail: oit@utsa.edu
phone: (210) 458-4555

OIT Support Services:

<http://www.utsa.edu/oit/helpdesk>
e-mail: oitssupportservices@utsa.edu
phone: (210) 458-5538

Information Security is
EVERYONE'S
Responsibility.



Information Security is
EVERYONE'S
Responsibility.

www.utsa.edu/oit/security
The Office of Information Technology

Information Security

With an ever-increasing volume of threats on the Internet, it is imperative that we understand that each of us is responsible for the protection of UTSA's information resources.

UTSA Information Resources - Policies

Remember that the use of information resources requires legal and ethical behavior from all users. We are governed by a wide variety of computer use policies including:

- FERPA and HIPAA
- Texas Administrative Code Information Security Standards
- UT System Administrative Policy (UTS 165)
- UTSA Handbook of Operating Procedures (the "HOP")
- UTSA Information Security Standards.

Links to these policies and regulations can be found in the Information Security Web site (<http://www.utsa.edu/oit/security>).

*If you violate university, state or federal policies dealing with information resources, UTSA can restrict or remove your access to the university's computers, networks or other information resources.

Incident Reporting

Use the online Incident Reporting form or call the Information Security Office at 458-5555 to report an information security incident. An incident is defined as "the act of violating an explicit or implied security policy."

Some common incidents:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- The unauthorized use of a system for processing or storing data
- Changes to system hardware, firmware or software characteristics without the owner's knowledge, instruction or consent

Note: Incident reports are confidential unless we receive your permission to release information.

Proper use of UTSA Information Resources

You should use information resources for university-related activities only. Incidental use of UTSA resources (limited personal use) is allowed. Incidental use does NOT include:

- Using UTSA information resources for commercial or financial gain (running a personal business)
- Allowing a friend/family member to use your computer
- Using the Internet such that it interferes with the normal performance of your duties or results in any direct costs to UTSA

Protecting UTSA Data

Many of us may have to deal with sensitive information at one point or another – from professors who enter and assign grades to admissions staff who must work with social security numbers in transcripts. Even Facilities staff members may find sensitive papers thrown thoughtlessly into the trash or in a hallway. It is important to understand what makes information sensitive and how to protect these types of data.

Data Classification & Encryption

Owners of confidential or sensitive information are responsible for classifying and protecting that data. Examples of confidential data include SSNs and student grades. Some financial data can be classified as sensitive as well. Thorough definitions of Confidential and Sensitive data are available in the Information Security Web site. The Web site also contains information on software solutions that can be used to encrypt and protect sensitive data.

E-mail & Phishing

E-mail should be treated with the same respect as printed communications. Remember that UTSA e-mail is considered to be public information and it may be disclosed to third parties under the Texas Public Information Act.

Phishing is the fraudulent practice of attempting to get sensitive information by masquerading as a trustworthy source. If you are uncertain of the legitimacy of any communication that you receive:

- Do not click on any links or open any attachments in the e-mail message
- Forward the e-mail to OIT Support Services or to Information Security to verify its authenticity
- Contact the company or person by phone
- Type the address into a browser instead of clicking any links

Social Networking

Being a part of a social networking site can be a great way to keep up with friends. However, revealing too much information can also allow you to become the victim of a crime. Some tips for making your online experience safer:

- Set your profile to private
- Don't post anything you wouldn't put in the public eye
- Watch out for malicious software (malware) – viruses can be disguised as pictures or software updates.
- Be suspicious of unusual instant messages – don't respond to them
- Cancel or Ignore suspicious "friend requests" – they might not be who they claim to be

Don't use/abuse copyrighted material

Copyrighted material includes software, audio recordings, video recordings, photographs and written materials. The following are examples of actions prohibited at UTSA:

- Unauthorized copying of UTSA-owned software
- Illegal distribution of software, recordings or data (i.e. P2P sharing software)
- Installation of unlicensed or unauthorized software on UTSA-owned PCs

Password - FAQs

Can I share my password with a coworker so they can help me with my work?
No. Sharing your password is strictly prohibited.

What do I do if I think my password has been compromised?
Contact OIT Support Services (458-5538) as soon as possible, and change your password if you are able.

Whom do I call if I forget my password?
The OIT Web site provides a link to a Web site (idm.utsa.edu) where you can reset your password. You may also call OIT Support Services, 458-5538, for assistance.

I received an e-mail that is asking me to reveal my User ID, password and other information. Is it legitimate?
No. This is a phishing attempt. UTSA, and other legitimate organizations/companies, will never ask you to reveal this type of information via e-mail or by visiting a Web site.