Welcome to UTSA's Information Security Module!
Brought to you by UTSA's Office of Information Security

The estimated time to complete this acknowledgement module is 25 minutes.
You may exit this module at any time. However, be sure to note where you left off.

Click the button below to begin!
Dr. S. Introduction

Hello, I'm Dr. S. Thanks for volunteering to take the Information Security lesson of the Compliance Training module.

WHAT, you didn't volunteer? No matter, thanks for taking time out of your busy day.

As you know, an effective information security program begins with each of us doing our part to keep our computing environment safe.

Let's get started!
Let's get started

Information security is everyone’s business. What does that mean? It means, that as users of the university’s information resources (computers, data, network), we all must be careful in how we conduct business.

We hope this information security training module will help you become an informed computer user.
Section I. Spam, Phishing and Malware

One of the most popular ways for hackers and other criminals to attack is via email. Spam is defined as any unsolicited email. Spammers send thousands of email messages to try to get people to purchase a wide variety of products, from counterfeit watches to untested medicines and more.

Check out this quick GET IT video on Phishing Email. Pay attention - there’ll be a quiz after the video.

If you cannot see the video, click here.
In the information security field, what is "spam"?

- Any email from non-UTSA faculty or staff members
- Aloha! It’s that tasty processed meat product from Hormel
- Any unsolicited email
- That processed meat stuff from Hormel that is popular in Hawaii
According to the video, what does the term “phishing” mean?

- Phishing? I think that’s a made-up word. Nice try.
- An unsolicited phone call from someone trying to sell you a real product
- A type of spam email with appealing features that can put your computer, information and identity at risk
- A way that hackers trick people into purchasing overpriced rods and reels
What should you do if you receive an email that you suspect might be a phishing attempt?

- Click all links and quickly close the Web pages displayed if they look suspicious.
- Contact OITConnect for assistance in determining if the email is legitimate.
- Delete the email, no matter who it came from.
- If it includes a link to a Web page, click that link - what could possibly go wrong?
Email File Attachments

Another type of attack involves email attachments. You should always be suspicious of email messages from people you do not know, especially if the email contains a file attachment. If you click to open an attachment, you could infect your computer with a virus or other type of malware.

If you are not sure if an email message is legitimate, contact OITConnect, 210-458-5555, for assistance.

Here’s a graphic that shows you how to handle email messages with file attachments.

You’ve *unexpectedly* received an email with an attachment...

Is the sender known and trusted?  

Ask the sender if it is legitimate.  


NEVER open (double-click) a suspicious email attachment!
What should you do if you receive an email from an unknown sender with a file attachment?

- Click on that attachment to open it and to see what it is
- If you know the email does not pertain to you, don't delete it
- If you are not sure if the email is legitimate, contact OITConnect for assistance
- If you know the email does not pertain to you, delete it or if you are not sure if the email is legitimate, contact OITConnect for assistance
Links in Email Messages

Hackers can create email messages that look legitimate but are actually malicious. You should NEVER click a link that you find in an email message unless you are completely sure that the email is from a trusted sender and the link is legitimate.

When you get an email message with a link, place your cursor over a link. What you see is the actual destination address – where you will be sent if you click the link. As you can see in our example, if you hovered over the “utsa.edu” link, you can see that you will actually be sent to the Google site.

URL example

http://www.utsa.edu

A hacker won’t send you to Google’s site – they will send you to a fake page they created. Once you’re on that page, they can fool you into giving up your user ID and password or they can install a virus or other malware on your machine. Remember – a legitimate organization (like UTSA) or a legitimate business like your bank will NEVER ask you to provide your user ID and password through email.
What should you do if you receive an email asking you to provide your myUTSA ID and passphrase?

- Ignore and delete the email because UTSA will NEVER ask you for this information
- Assume it’s OK, so hit “reply” and provide the information
- Forward the email to your coworkers to make sure they also provide the information
- Hit “reply” but provide the information by including it in a file attachment
Dr. S

Wow! That section was a doozy. I promise, from now on, it will get easier.

Okay, Okay, I exaggerate, but it might get more interesting.

Anyway, let's get started with the next section.
Section II. Data Classification

At UTSA, data is classified by the degree of protection that is required and the risk that is faced if the data is compromised. Here is more information on the three data categories:

<table>
<thead>
<tr>
<th>Category I</th>
<th>Category II</th>
<th>Category III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential</td>
<td>Controlled</td>
<td>Published Data</td>
</tr>
</tbody>
</table>

**Definition**

- **Category I**: Data whose disclosure, destruction, display, or modification would violate state or federal laws or regulations, University of Texas System policies, or the Texas Open Records Act.
- **Category II**: University data that are not otherwise protected identified as Confidential data, but which are releasable with the Texas Public Information Act. These data will be protected to ensure a controlled release.
- **Category III**: University data that are not identified as Confidential or Controlled data. University data that have no requirement for confidentiality, integrity or availability. Public data, while subject to University disclosure rules, is available to all members of the University community and to all external individuals and entities.

**Risk**

- **Category I**: Long-term loss of reputation, long-term loss of critical campus services, long-term loss of research funding, tampering with research, unauthorized exposure of litigation materials, identity or credit theft.
- **Category II**: Short-term loss of reputation, short-term loss of research funding, short-term loss of departmental services, Unauthorized tampering with research.
- **Category III**: Loss of data with no impact to the university, inaccurate general information.

**Examples**

- **Category I**: Student records, litigation, law enforcement data, Social Security Numbers, Credit cards, health-related research, reports marked confidential, passwords.
- **Category II**: Business transactions that are not sensitive, project data, HR data that are not sensitive, research data or results that are not sensitive.
- **Category III**: Institutionally published public data, directory data, academic course descriptions, faculty evaluation data, blogs and other social media.

The table shows that Category I data is the most sensitive, which means that it requires the highest level of protection. Category I data can only be saved on the departmental shared drive (I: Drive) or on a secured server.

Every UTSA-owned computer must be classified by the highest level of data that is stored on that computer. The computer classification is set in the InSight computer application. Remember - even if the data is stored on a non-UTSA computer or device, it still must be protected.
What are the three data classification categories at UTSA?

- Category I, Category II, Category III
- Large, medium, small
- Top Secret, Secret, Unclassified
- High Risk, Medium Risk, Low Risk
Case Study - Research Data

In our next example, a UTSA researcher uses a computer that is currently classified as a Category II computer because the computer is not used to store Category I data.

- The user receives a grant from the Department of Defense
- The contract states the researcher will be working with personal health records of individuals involved in an ongoing study
- The contract stipulates the data must be protected

How should the user respond?

☐ The user should only save the research data on a personal (non-UTSA) computer.

☐ No change. The user should just be careful with the data.

☐ The user should reclassify the computer as Category III and should store the research data on the I: drive.

☐ The user should reclassify the computer as Category I and should store the research data on the I: drive or on a secured server.
Section III. Data Protection and Encryption

Data encryption is a process of securing computer files by instituting safeguards that make the files unreadable to everyone except for the holder of the encryption key. UT System has mandated that all university-owned laptops, all desktops that access Category I data and all newly-purchased desktops have encryption software installed. Because university computers often access sensitive information, they must be protected.

Any suspected information security incident – viruses or malware infections, unauthorized attempts to gain access to a computer application, lost or stolen computers or hard drives, etc. – must be reported as soon as possible by contacting the Office of Information Technology through OITConnect, 458-5555.
According to UT System, what UTSA information resources need to have their data encrypted?

- Desktops only
- None
- All laptops, all Category I desktops, all new desktops
- Laptops only
How should Category I data be protected?

- Save all Category I files ONLY to the I: Drive or to a secured server
- Save all Category I files to a floppy disk
- Save the files to your hard drive but rename them to disguise the file contents (for example, rename grades.doc to abc123.doc)
- Send Category I data as email attachments to your administrative staff
What should you do if you receive an email that contains an attachment with Social Security Numbers (SSNs)?

- Notify OITConnect
- Delete the email
- Forward the email with attachment to your supervisor
- Nothing. No one likes a tattletale.
Section IV. Tracking Information Resources

The Office of Information Technology created the InSight computer application to keep track of university-owned information resources (laptop/desktop computers, tablets, etc.). Within InSight, you can find out if a computer is protected by antivirus software, whether it has received important operating system patches/updates, the type of data that is accessed on the computer (Category I, II or III) and much more. Every faculty or staff member who has an information resource assigned to them has access to the InSight computer application.
Where can you go to review or set the classification of the data on your computer?

- Blackboard Learn
- John Peace Library (JPL) First Floor
- InSight computer application
- PeopleSoft
- WiseTrack inventory application
What is the required method to keep track of information resources (computers, tablets, etc.) in your department?

- Online, using DEFINE
- Tracking resources? Nobody has time for that
- Create a list on paper and update it as needed
- Online, using the InSight computer application
- Keep the purchase orders (P.O.s) in your department’s safe
You're almost done. And when I say "almost," I mean "halfway." More or less.

Onward!
Section V. Preventing Data Loss

There are some very important steps you should take to ensure your computer is protected from data loss. The good news is - for the majority of UTSA-owned computers – no action is required from you.

UTSA has a site license for CrashPlan Pro, which automatically backs up the data on your primary workstation (as defined in the InSight computer application) multiple times each day. If your computer ever crashes or you need a previous version of a backed-up file, you can restore these files from CrashPlan Pro.

If your computer is defined to the network component called the "domain," it can be managed by a central server. That allows your computer to automatically receive important patches and updates. Again, most UTSA-owned computers are members of the UTSARR domain, but some departments choose to manage and be responsible for their own computers.

If you have questions about domain membership or automatic updates, contact your department’s Information Technology Associate or OITConnect, 210-458-5555.
What might be a good reason to have your department’s computers defined to the UTSARR domain?

- The computers will receive automatic updates
- It is required by the state of Texas
- It is required by UT System
- All the cool kids are doing it
Can I just say that I admire your dedication?

Last section, coming up!
Section VI. Information Security Incident Reporting

The Office of Information Security is responsible for investigating all suspected information security incidents. One of the most common information security incidents is a computer that has been infected by a virus or other malware. A single infected machine can harm the university computer network or even be used to send spam messages or infect many more computers. Other information security incidents include attempts to gain unauthorized access to a computer system, cyber attacks that disrupt or cause a denial of service to a website or computer system and unauthorized use of a computer or computer system.

As with all other information technology requests, you should report suspected information security incidents by contacting OITConnect, 210-458-5555.
What types of events can be described as “information security incidents”?

- Changes to system hardware, firmware or software without the user’s knowledge
- Unauthorized use of a system for processing or storing data
- Unwanted disruption or denial of service to a system
- All of these are informational security incidents
- Attempts to gain unauthorized access to a system or its data
Security Incident Example

Here's an example of how you can be involved in a security incident just by surfing the Web.

Here's what can happen:

- User clicks a picture on a suspicious website
- Malware is automatically loaded onto the user’s computer
- The files on the computer are encrypted (locked) by the hacker’s software
- A “ransom note” pops up on the user’s computer, demanding money in exchange for the key

In this scenario, everything eventually turns out fine. Remember, the key is the user who suspects an information security incident notifies OITConnect in a timely manner. Also, if the user has CrashPlan Pro installed, the computer’s files can be restored from the last time the computer was backed up.
At UTSA, how does the Office of Information Security recommend you report an information security incident?

- No report is needed – UTSA is not required to report information security incidents
- Immediately contact the FBI (fbi.gov)
- Contact OITConnect
- Contact the UT System Office of Information Security

Submit
Dr. S Complete

Woo-Hoo!

You are finished! Remember, friends, an effective Information Security program starts with YOU.

Always be careful to protect your data and your information resources.

And, finally, take a minute before doing something risky - THINK before you click.