INFORMATION SECURITY

Brought to you by The Office of Information Security.
The estimated time to review this lesson is 25 minutes.
OVERVIEW AND OBJECTIVES

Information security is everyone’s business. As users of the university’s information resources (computers, data, network), we all must be careful in how we conduct business.

This information security training lesson will help you become an informed computer user.
If you cannot see the video, you may need to update your flash player or view it here.
You will be meeting four different employees. Each of these employees is facing a different kind of information security risk. Visit them one by one and see if you can keep them from making potentially devastating mistakes.

We’ll start with

LESSON I. SPAM, PHISHING, AND MALWARE
Amelia has begun to receive a lot of emails at work from her credit card company informing her that her account may have been hacked. The email explains that if she will use the attached link to logon using her username and password, they will work with her bank to verify if her account was compromised.

What would you advise Amelia to do?

- Since the email appears to be from her credit card company, Amelia should go ahead and open the link.
- Amelia should contact OITConnect for assistance in determining if the email is legitimate.
YOU’RE RIGHT.

Phishing is a type of spam email with appealing features that can put your computer, information, and identity at risk. **Think before you click.** Clicking a link can take you to an infected Web page that can harm your computer.
In the information security field, any unsolicited email is known as what?

Type your answer in the block below then press the Submit button.

Spam
YOU’RE RIGHT.

Spam is defined as any unsolicited email. Spam email messages are usually sent to thousands of recipients and usually try to persuade you to purchase something.
A type of spam email with appealing features that can put your computer, information and identity at risk is called what?

- Junk
- Clutter
- Phishing
YOU'RE RIGHT.

Phishing is a type of spam email with appealing features that can put your computer, information and identity at risk. Providing this information can cause you to become a **victim of identity theft**. Contact OITConnect for assistance in determining if the email is legitimate.
Some types of computer attacks involve 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.

Here’s a graphic that shows you how to handle email messages with file attachments. Click on the image to enlarge it.
You've unexpectedly received an email with an attachment...

Is the sender known and trusted?

Make the call

Ask the sender if it is legitimate.


NEVER open (double-click) a suspicious email attachment!
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.

How can you find out if an email is legitimate or not? Click [here](#) to find out.
When you get an email message with a link, place your cursor over that link. What you see is the actual destination address - where you will be sent if you click the link. Hover your mouse over the graphic below to follow along.

URL example
http://www.utsa.edu
LESSON II. DATA CLASSIFICATION
Paul is a UTSA researcher and has just been awarded a grant from the Department of Defense to work on personal health records of individuals in an ongoing study. The contract stipulates that these records must be protected at all times. Paul is unsure if his current computer has the right classification to store these records.

**What are Paul's options?**

- Learn about UTSA's data classification categories.
- Save the files on his iPhone since he always has his phone on him.
- Just be extra careful with the data.
YOU’RE RIGHT.

Paul needs to learn about the UTSA classification categories. Storing health-related research on a device without the proper protection can result in several negative risks for the University including:

- Long-term loss of reputation
- Long-term loss of critical campus services
- Long-term loss of research funding
- Research tampering
- Unauthorized exposure to litigation materials
- Identity or credit theft
At UTSA, data is classified by the degree of protection that is required and the risk that is faced if the data is compromised.

Click the button below to learn about the categories.

Data Classification Table
<table>
<thead>
<tr>
<th></th>
<th>Category I - Confidential</th>
<th>Category II - Controlled</th>
<th>Category III - Published Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>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.</td>
<td>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.</td>
<td>University data that are not identified as Confidential or Controlled data and 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.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>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.</td>
<td>Short-term loss of reputation, short-term loss of research funding, short-term loss of departmental services, unauthorized tampering with research.</td>
<td>Loss of data with no impact to the university, inaccurate general information.</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>Student records, litigation, law enforcement data, Social Security Numbers, Credit cards, health-related research, reports marked confidential, passwords</td>
<td>Business transactions that are not sensitive, project data, HR data that are not sensitive, research data or results that are not sensitive.</td>
<td>Institutionally published public data, directory data, academic course descriptions, faculty evaluation data, blogs and other social media</td>
</tr>
<tr>
<td>Category</td>
<td>Confidential</td>
<td>Controlled</td>
<td>Published Data</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>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.</td>
<td>Category I data is sensitive, which means it requires the highest level of protection. Category I data can only be saved on the department shared drive (I: Drive) or on a secured server.</td>
<td></td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Examples** | Student records, litigation, law enforcement data, Social Security Numbers, Credit cards, health-related research, reports marked confidential, passwords | Business transactions that are not sensitive, project data, HR data that are not sensitive, research data or results that are not sensitive. | Institutionally published public data, directory data, academic course descriptions, faculty evaluation data, blogs and other social media.
Now that Paul is aware of UTSA's data classification categories, which category does his research study fall in?

- [ ] Category I
- [ ] Category II
- [ ] Category III
YOU'RE RIGHT, CATEGORY I.

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. You will learn about InSight later in this lesson.

Remember – even if the data is stored on a non-UTSA computer or device, it still must be protected.
How should Category I data be protected?

- Save all Category I files to a floppy disk.
- Send Category I data as email attachments to your administrative staff.
- Save all Category I files ONLY to the I: Drive or to a secured server.
YOU'RE RIGHT.

Category I data can only be saved on the department 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. By not using the proper classification to protect the research data, Paul could put UTSA in serious risk.
Beverly often accesses sensitive information for her job at UTSA. She heard about a lot of recent security problems involving computer hacking and believes her desktop computer may be infected with a virus.

**How can she find out if her computer is at risk?**

- Download a virus protection program she found on Google.
- Give it a few more weeks to be absolutely sure.
- Contact OITConnect at 458-5555 as soon as possible.
YOU'RE RIGHT.

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.
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.

Because university computers often access sensitive information, they must be protected. 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.
Which of the items below are mandated by UT System to have encryption software installed?

Drag each picture to the appropriate box then press Submit.
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.
On May 7, 2014, PeopleSoft HCM/FMS replaced DEFINE. DEFINE’s unit code structure was replaced with PeopleSoft’s department ID structure, and some unit codes have been combined to form new department codes. Because of this change, some users may no longer be able to display their department’s assets. Please contact your department’s PeopleSoft support team for assistance. Also, please note that InSight contains some instructions for changing information within DEFINE. As soon as the steps for changing the information in PeopleSoft are developed, the documentation within InSight will be changed. During the DEFINE-to-PeopleSoft changeover period, some data will remain static until it is available from PeopleSoft.

To see the new DEFINE unit code to Peoplesoft department crosswalk, please go to the Peoplesoft website, [http://utsa.edu/utshare/Training/References/](http://utsa.edu/utshare/Training/References/), and click on the “DEFINE Unit Code to PS Department Crosswalk” link as shown below.
What functions does the InSight computer application provide?

- Keeps track of department information resources (computers, tablets, etc).
- Verifies if a computer is protected by antivirus software.
- Verifies the type of data that is accessed a computer (Category I, II, or III).
- All of the above
Insight at http://insight.utsa.edu is a tool that allows staff members to manage their information resources, 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.
At the end of each work day, Ray logs off of his computer without backing up or saving his data. Today, his computer crashed and he’s lost all of his files.

Will he be able to retrieve his data?

Yes  No
At the end of each work day, Ray logs off of his computer without backing up or saving his data. Today, his computer crashed and he’s lost all of his files.

Will he be able to retrieve his data?

Yes  No

You’re right! For the majority of UTSA-owned computers, no action is required from you to ensure your computer is protected from data loss. Click the next button to find out more.
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.
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 you have questions about domain membership or automatic updates, contact your department’s Information Technology Associate or OITConnect, 210-458-5555.

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.
What might be a good reason to have your department’s computers defined to the UTSARR domain?

- It is required by UT System
- It is required by the state of Texas
- The computers will receive automatic updates
YOU’RE RIGHT.

Computers will receive automatic updates if they are defined in the UTSARR domain.
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.

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"?

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

All of those are examples of information security incidents.
At UTSA, how does the Office of Information Security recommend you report an information security incident?

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

You should report suspected information security incidents by contacting OITConnect at 210-458-5555.
Example of how you can be involved in a security incident by surfing the web:

1. User clicks a picture on a suspicious website

2. Malware is automatically loaded onto the user’s computer

3. The files on the computer are encrypted (locked) by the hacker’s software

4. A “ransom note” pops up on the user’s computer, demanding money in exchange for the key

So what happens next?
In this scenario, everything eventually turns out fine. Remember, the key is the user who suspects an information security incident and 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.
STANDARD FOR ACCEPTABLE USE

All personnel seeking to access UTSA computing resources must be aware of the duties and responsibilities that are in place to protect the network infrastructure. All personnel must read the Standard for Acceptable Use policy in the link below.

Standard for acceptable use policy
You are finished! Remember, 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**.
Before You Continue

You have completed the Information Security lesson. What would you like to do next?

- **e-mail The Office of Information Security**
- **Review lesson**
- **Scroll up** and click the orange EXIT ACTIVITY button above this lesson to return to the course homepage and click on the **PUBLIC SAFETY** lesson