



INFORMATION SECURITY SHORTS

Malicious Code

Malicious code describes software that is purposely designed to do damage to, or cause unwanted behaviors in, a computer system.

- Common types of malicious code are viruses, Trojan horses, and worms. Malicious code can also appear as a macro or script.
- The most common method for the spread of malicious code is through e-mail attachments, downloading files from the Internet, or by visiting an infected website that automatically downloads malicious code without the user's knowledge.
- Malicious code can corrupt files, erase your hard drive, or enable a hacker to gain access to your computer system.

Passwords

Using these guidelines at home keeps your home computer secure as well.


- When creating your password, use a combination of lower and upper case letters, numbers, and special characters, such as the number sign or percent sign.
- Avoid using personal information such as names of family members, friends, or pets. You should also avoid using birthdays, or the names of your favorite sports teams or bands.
- Don't use common phrases or words found in the dictionary, including foreign languages.
- Don't write down your password. Commit it to memory. Change your password according to policy and remember, creating a complex, strong password, and protecting its secrecy, is critical for protecting SFASU information and information systems, as well as for protecting your own personal information.
- Use different passwords for your work computer than you use for your home and general websites.
- Never share your password with anyone!



Phishing

Phishing is one type of social engineering that uses e-mail or websites to trick you into disclosing personal or sensitive information, such as credit card numbers, bank account information, your Social Security number, or passwords.

The intention is to steal your identity, run up bills or commit crimes in your name, or access your work computer systems. Phishing is a serious, high-tech scam.



Phishers try to deceive you by sending e-mails or pop-up messages that appear to be from the university, a legitimate business, or some other organization, such as your Internet service provider, or bank.

How to Identify Phishing Emails and avoid becoming a target

- The message might claim that you need to update or validate your account information. It might threaten some dire consequence if you don't respond. The message directs you to a website that looks just like a legitimate organization's site, but it is not affiliated with the real organization in any way. The bogus site tricks you into divulging your personal information. Just visiting the site may allow malicious code to download and install on your system.
- DON'T respond and provide your bank account information to any of these types of e-mails places your financial security at great risk.
 - Phishers can steal the money in your bank account, and can use your name and banking information to steal your identity. The thieves could then access your other bank accounts or obtain new credit cards or loans in your name.
- DON'T access the web by selecting links in e-mails or pop-up messages. If an e-mail appears suspicious, such as an unrecognized sender, mis-spellings, or foreign text, do not open it. Simply delete the e-mail. If you must view the e-mail, make sure to view it in plain text. This is especially important if the message contains an attachment.
 - Legitimate companies do not ask for personal information via e-mail. If you are concerned about your account, contact the organization in the e-mail using a telephone number you know to be genuine. If you want to check your account status online, type the web address directly into your browser, or use your personal bookmark.

Spear phishing

Spear phishing is a highly targeted phishing attack. Spear phishers send e-mails that appear to be from someone from inside . Spear phishers attempt to gain access to the entire network, putting the security of that organization's information at risk spear phishers may make you a victim of identity theft.

- For example, a message might appear as if it came from your supervisor, human resources, or the IT department. The message might include requests for user names or passwords.

Protect yourself from spear phishers by following these security tips:

- NEVER give out your password, to anyone!
 - IT, or any legitimate person from your organization, will never ask you for your password.
 - If someone from the IT department requires access to your computer, they will use their administrator user name and password.
- NEVER reveal any information system related information, or personal information, such as user name, address, or date of birth, in response to an unsolicited e-mail.

Internet hoaxes

- Internet hoaxes are e-mail messages, often designed to influence you to forward them to everyone you know. Hoaxes encourage you to forward e-mail messages by warning of new viruses, promoting moneymaking schemes, or citing fictitious causes.
- By encouraging mass distribution, hoaxes clog networks and slow down Internet and e-mail services for computer users. A forwarding request can also be a part of a distributed denial-of-service, or DDoS, attack, intended to bring down computer networks by flooding them with traffic. By forwarding an e-mail to large groups of other users, you are helping hackers execute their attack.
- You can limit the effect of e-mail hoaxes by following these security tips:
 - If you are suspicious about an e-mail, perform a quick online search to confirm or expose the message.
 - Many legitimate websites list the latest e-mail hoaxes.
 - If an e-mail requests that you forward the message to everyone in your address book, it is probably a hoax: do not forward it.

Protect your computer system from viruses, both at work and at home, by following these simple security tips.

Email Client Settings

- Set your e-mail to be read in plain text.
 - Many e-mail viruses rely on the language code used to design web pages to launch their payload. For this reason, do not view e-mail using a preview pane feature. You can stop them in their tracks by viewing your messages as plain text.
- Scan attachments.
 - Turn off the option for automatic downloading of attachments. This will enable you to scan each attachment before it can infect your system.
 - Don't assume an attachment is safe just because a friend or coworker sent it. Before opening an e-mail attachment, be sure the attachment has been scanned with up-to-date, anti-virus software.
- If you receive a suspicious message from someone you don't know, or from whom you were not expecting a message, delete it, without opening it.

Computer Settings

- Your system should be set up for your anti-virus software to scan your system daily.
- Enable the host-based firewall
- Lock your system

Spillage

Spillage includes the improper storage, transmission, or processing of sensitive information on a non-sensitive system.

To prevent spillage, follow these security tips:

- When storing or transmitting sensitive information, including PII, encrypt the information before storing it on mobile computing devices, including laptops; or transmitting it, such as by e-mail.
- E-mailing sensitive information is particularly dangerous, and should be done with caution. Store only on an information system that has been authorized to store this type of information.
- Remember, some systems are strictly non-sensitive.
- Never transmit, store, or process sensitive data on a non-sensitive system.

Use of E-mail

Although the university may permit some incidental e-mail use from your SFASU computer, e-mail is for official business.

Follow these guidelines for ethical use of e-mail:

- E-mail use must not adversely affect the performance of official duties. E-mail use must not reflect poorly on the university.
- Do not use the university e-mail to sell anything, or to send chain letters, or offensive e-mails, including pornographic, political, racist, or sexist e-mails.
- Do not send or forward mass e-mails. These overburden the system.
- Do not send or forward jokes, pictures, or inspirational stories. These also overburden the system.
- Avoid using Reply All unless it is absolutely necessary, especially for e-mails with large address lists.
- For any e-mail you send, select the addressee list carefully.

Personal E-mail

When you use web mail to check e-mail, you might bypass the security features built into your office e-mail system. The fact is, you may not even realize that the security has been compromised.

Here's an example of what can go wrong.

If you open a personal e-mail that has malicious code, without you even realizing it, malicious code is downloaded to your computer. In this instance, this code, called a bot, allows attackers to take command of and control your computer. In other words, it becomes a zombie, a member of a botnet, controlled by a bot herder. Bots can be used to steal data, host malicious content, launch other attacks, including worms and viruses, or to send spam. Advanced bots can be programmed to, among other things, look through a web cam, listen to a microphone, log key strokes, and capture screen shots.

To help protect SFASU information systems against ever-present cyber threats, be very cautious when accessing your personal web mail accounts using a SFASU-owned computer and network.

Social engineering

Social engineering is a collection of techniques intended to trick people into divulging private information. The social engineer attempts to use the information to gain unauthorized access to computer systems, or to commit fraud.

Social engineers use a variety of communication devices to contact their victims, including telephone surveys, e-mail messages, websites, text messaging, automated phone calls, and even, in-person interviews.

You may hear these scams referred to as phishing, spear phishing, vishing, or, when directed at senior executives, whaling. Regardless of the method of contact or type of request, what all of these scams have in common is that they are an attempt to get you to divulge personal information.

Avoid falling victim to these scams, and protect yourself, your fellow employees, and SFASU information systems, by following these security tips:

- Do not give out personal information about yourself or other SFASU employees, including names, positions, telephone numbers, and passwords.
- Do not give out computer system or network information.
- Do not follow any instructions from unverified personnel.
- When contacted, document the interaction:
 - Verify the identity of any individual who approach you.
 - Try to obtain as much information about the person as possible.
 - If Caller ID is available, write down the caller's telephone number.
 - Take detailed notes of the conversation.

Peer-to-Peer Filesharing

Unauthorized peer-to-peer software, or P2P, is frequently used to download music, pornography, movies, and other copyrighted material from the Internet, without purchase. Downloading files in this way is illegal if copyrighted and not purchased, can be unethical, and is prohibited on university-owned computers and networks. Your engaging in this activity may also result in criminal or civil liability charges for illegal duplication and sharing of copyrighted material.

Unauthorized personal software is not limited to peer to peer applications, but includes any software that is not authorized for use on your university system, such as personal software or applications for web cams, photo editing and sharing, video editing and sharing, cell phones, and digital music and ebook stores.

Many P2P and other unauthorized software applications are easily available, but using unauthorized P2P and other unauthorized software goes beyond a legal and ethical issue and becomes a security issue. It provides outsiders with a link into your computer, and into university-owned computer networks. This can result in significant vulnerabilities, including unauthorized access to data, a compromise of network configurations, and the spread of computer viruses and spyware.

Whether on a university-owned computer or your personal computer, using P2P software puts your personal information at risk. Using unauthorized P2P or any other unauthorized software on your university system not only puts SFASU at risk, but also puts you at risk of disciplinary or legal action.

The consequences could include fines, losing your job, or, even, jail. Remember, each time you log on to a SFASU computer system, you are logging into a state system and you consent to being monitored.

Avoid computer misuse.



Physical Security

By allowing someone to follow you into a secure area without his or her own badge or key code, you are evading and diminishing the physical security.

Physical security protects an entire facility. This includes the outside perimeter of the building to the offices inside the building, and all of the information systems and infrastructure.

You are responsible for knowing the physical security policies, and for following them. Know the procedures for gaining entry to a secure area, procedures for securing your work area at night, and emergency procedures. These may include the use of a badge or key code for entry as well as procedures for securing your work area.

Follow these general security tips:


- Always use your own badge or key code to enter a secure area.
- Never grant access for someone else using your badge or key code.
- Challenge people who do not display badges or passes.
- Report any suspicious activity that you see to the University Police.



Software Installation

Scan all external files before uploading to your university computer, or the computer network, if you are permitted.

Follow your department's policies with respect to loading outside files onto your workplace computer. This includes files brought in on external media, such as thumb drives, CDs, or floppy disks, as well as files e-mailed from your home computer to your work e-mail address.



If your system is acting erratically or running abnormally slow, it may contain a virus. The system may contain a virus, even if it appears to be virus free. If you discover or suspect that a virus has infected your system, do not e-mail the infected file to anyone. Immediately contact your technical support staff.

Internet Browsing - Cookies

A cookie is a text file that a web server puts on your hard drive. As you enter information at a website, the cookie saves the data, including which items you've placed into your shopping cart, your user preferences, and your user name.

Enabling cookies can pose a security threat, the most serious being when a cookie saves unencrypted personal information, such as your credit card numbers or Social Security number.

Cookies can also track your activities on the web, which poses a security risk, and may lead to a potential invasion of your privacy. Even when at home, shop online wisely. Follow these security tips. Use cookies with caution.

Configure your cookies setting, set your browser preferences to prompt you each time a website wants to store a cookie.

Only accept cookies from reputable, trusted websites.

Confirm that any e-commerce site conducts its business over an encrypted link before providing any personal information. An encrypted link is indicated by https the URL name or web address.

Make sure that an icon is visible that indicates the encryption is actually functioning. Note that not all https sites are legitimate, and you are still taking a risk by entering your information online.

Internet Browsing - ActiveX

ActiveX is a form of mobile code technology that allows Internet browsers to run small applications, or applets, online.

Many legitimate companies and government agencies require that ActiveX or other forms of mobile code technology be enabled to use mobile code on their websites.

These sites are then able to behave as applications, similar to an application installed on your computer. However, because mobile code works by providing access to your computer's operating system, you must use caution when enabling ActiveX. If the mobile code is from a non-SFASU web site, it may be malicious.

Protect your computer and University computer systems from malicious mobile code by requiring confirmation before enabling ActiveX or other types of mobile code technology.



It's your identity; protect it

Identity Theft


Identity theft occurs when someone uses your name, address, Social Security number, bank or credit card account number, or other identifying information without your knowledge to commit fraud or other crimes.

Identity thieves can use the information they obtain to open credit card accounts, take out loans, or drain a bank account without your knowledge. Identity theft is a serious problem with extreme consequences for its victims. You are the first line of defense against identity theft.


Minimize your risk

Never give out personal information, especially your Social Security number, without knowing how it will be used.

- Pay attention to credit card and bank statements for unauthorized activity.
- Avoid using common names or dates when creating passwords or personal identification numbers, or PINs.
- Pick up your mail promptly.
- Shred all personal documents and mail that contains sensitive information, especially pre-approved credit card offers.
- Do not carry your Social Security card or passport in your purse or wallet. Only carry your passport when it's required for travel.
- Order copies of your credit report every year.



What should you do if you discover you are a victim of identity theft?



Contact all three credit reporting companies and have your account marked for fraud. Contact your banks, credit card issuers, and other creditors to notify them of the identify theft and to cancel any affected accounts. Monitor your credit card statements for unauthorized purchases. Report the crime to the local police. If you do not make this report, you may not be able to recover your money, even if the perpetrators are identified.



Removable Media

Because removable media can store large amounts of information, and because they can be easily lost or stolen, you must take extra precaution when using removable media: Encrypt all data stored on removable media. Encryption must be in accordance with the data's classification or sensitivity level. When not in use, store all removable media in an approved location. Use only approved removable media. When no longer needed, purge sensitive media according to the university's policies. Contact your technical support staff for more information about the handling, storage, and labeling of removable media.

Please note, some departments may severely restrict or prohibit the use of removable media, especially flash memory devices, such as thumb drives.




Mobile Devices

Be extra vigilant when storing data on mobile computing devices, such as, PDAs, laptops, cell phones, and portable electronic devices, or PEDs. Note that portable media and storage devices also include wireless book readers such as Kindle, iPods or other music players, and multi-use devices like iPad and the iPhone. Because of their small size and portability, these devices are especially vulnerable to security risks.

All mobile computing devices connecting to SFA systems must be in compliance with University policy.

Laptop computers are considered as mobile computing devices. All laptops that store Personally Identifiable Information (PII) must be secured using a encryption solution to protect the sensitive information stored on them.



All sensitive data must be encrypted in accordance with the data's sensitivity level. This includes all PII, such as Social Security Numbers; dates and places of birth; mothers' maiden names; and biometric records. If a device is lost or stolen, immediately report the loss to your immediate supervisor and the University Police Department.

Personal Identifiable Information

Personally Identifiable Information, or PII, is information that can be used to distinguish or trace someone's identity. It can include information such as a Social Security Number, age, home and office phone numbers, birthdays, and spouse names. These are often found on office personnel lists, Rolodex cards, and electronic-based address books or contact records.

Other PII, such as marital status and educational history, may be included in personnel or medical records. Identity thieves can also exploit additional elements of PII, such as demographic, biometric, and financial information.

One or two pieces of information can be combined with other information to compromise someone's identity, even if the individual pieces of information seem harmless. While the Social Security card is a distinctive document linking a person's name and Social Security number, the number itself, when associated or combined with other PII, creates a high risk of identity theft.

It is your responsibility to protect any PII entrusted to you; including medical data and histories under the Health Insurance Portability and Accountability Act, or HIPAA. PII is a subset of sensitive information. If you handle PII, you are the first line of defense in preventing identity theft.

In addition, your department may have additional defined responsibilities for protecting PII and mitigating the damage when PII is lost or stolen.



Social Networking

Social networking can be risky business.

Cyber criminals make a living out of mining information such as birthdates, e-mail addresses, current and past jobs, and banking and financial information. Cyber criminals are experts at connecting the dots for malicious purposes.

Other examples of seemingly harmless information that could be used for malicious purposes include employer information, relationship status, networks or associations to which you belong, your whereabouts, people and facilities in backgrounds of photographs, which could also contain time and location in meta data; your schedule, especially time away from home, and hobbies and interests.

There are many other types of information found on social networking sites that can be mined and misused. Remember that it is practically impossible to delete information once you post it.

In addition to posting with caution, follow these best practices for social networking safety: Make sure you understand the privacy settings and defaults of the social networking site. There is no guarantee that a friend is who they say they are. Consider whether you know the friend, or verify who they are through another means.

Follow best practices recommended for creating strong passwords, user names, and answers to security questions. Also beware of links to applications, such as games and quizzes. These can lure you into providing additional information and or launching and installing malicious code on your computer.

Knowledge Check

If you ever receive an unsolicited telephone call from someone claiming to need your password, what would you do?

- a. Refuse and report it immediately
- b. Write the password on a piece of paper, put it in an envelope and send it by mail
- c. Tell him/her the password and change it the following day
- d. Send him/her the password via email

Of the following choices, which indicates when it is safe to open a file attached to an e-mail?

- a. When you know the sender, the attachment is expected, and it is not unusual in any way.
- b. When the e-mail is only sent to you
- c. When the attachment is not an .exe or .com
- d. When you know the sender

Knowledge Check

I have nothing of value on my computer. Why would someone break into my computer even though I have nothing of value on it?

- a. Because someone doesn't like me
- b. To use it to perform a crime
- c. Random vandalism
- d. For fun
- e. To use it to distribute pornography, music, videos, and software.
- f. All of the above

You can do whatever you want with your SFA computer as long as my permissions allows me to.

Yes. I am at my computer all day and it is not block then it is alright.

No. I have to be a responsible member of the networked community and am bound by the SFASU Acceptable Use Policy

Knowledge Check

Which of the following behaviors are considered inappropriate use?

- a. Sending email messages to harass or intimidate people
- b. Sharing passwords
- c. Sharing or using unlicensed, copyrighted software or multimedia outside their fair use provisions
- d. Trying to infect people with viruses or scanning computers you don't own
- e. Eavesdropping on others' activities by examining their computers or by using technology to access third-party communications
- f. Operating a computer with out of date operating software
- g. All of the above

SFA is authorized to monitor your computer use to identify improper activity.

True or False