FSCJ Florida State College at Jacksonville

CYBER SECURITY TEAM

TOP 10 TIPS FOR SECURING YOUR COMPUTER & WORKSPACE

You are a target to hackers!

If you are like most of us, you've probably thought, "It won't happen to me." Unfortunately, we are all at risk for being the victim of a cyber security breach. The stakes are high to our standing and reputation and our financial well-being. The FSCJ IT Cyber Security Team works to keep attacks to a minimum, but we need your help as well! After all, keeping FSCJ computing resources secure is everyone's responsibility. By following the 10 tips outlined below, and remaining vigilant, you can do your part to protect yourself and others.

TIP #1 – KEEP YOUR DESK CLEAR OF SENSITIVE DATA

Every employee should follow a clean desk policy. Sensitive information on a desk, such as sticky notes, papers, and printouts, can easily be seen by prying eyes or taken by someone. The only papers that should be left out are ones relevant to the project you are working on currently. All sensitive and confidential information should be removed from the desk at the end of each working day. Any time you step away from your desk, all critical information should be placed in a locked desk drawer.

In general:

- Be aware of sensitive data that you come into contact with and any associated restrictions.
- Keep all sensitive data (e.g., SSN's, credit card information, student records, health information, etc.) off of your workstation, laptop, or mobile devices.
- Securely remove sensitive data files from your system when they are no longer needed.
- Always use encryption when storing or transmitting sensitive data.

TIP #2 – NEVER LEAVE YOUR DEVICES UNATTENDED

The physical security of your devices is just as important as their technical security. If you need to leave your laptop, phone, or tablet for any length of time, lock it up so no one else can use it. If you keep

sensitive information on a flash drive or external hard drive, make sure to keep these locked up as well. All external drives, including USB drives, should be encrypted.

For desktop computers, shut down the system when it's not in use, or at a minimum, lock your screen. Make sure your computer screen saver is set for no more than 20 minutes. Always lock your computer when you leave your office. When logging into your computer, make sure no one is behind you watching you type.

TIP #3 – AVOID SOCIAL ENGINEERING ATTACKS

The FSCJ Cyber Security team is taking steps toward educating employees on the common types of social engineering attacks, including baiting, phishing, pretexting, quid pro quo, spear phishing, and tailgating. While there are technological solutions that help mitigate social engineering (such as email filters, firewalls, and network or data monitoring tools), having an employee base that is able to recognize and avoid common social engineering tactics is ultimately the best defense against these schemes.

Social engineering is a serious and ongoing threat for many organizations and individual consumers who fall victim to these cons. Education is the first step in preventing our organization from falling victim to savvy attackers employing increasingly sophisticated social engineering methods to gain access to sensitive data.

Here is a breakdown of common social engineering techniques:

Baiting –

Attackers conduct baiting attacks when they leave a malware-infected device, such as a USB flash drive or CD, in a place where someone will likely find it. The success of a baiting attack hinges on the notion that the person who finds the device will load it into their computer and unknowingly install the malware. Once installed, the malware allows the attacker to advance into the victim's system. Be aware of public USB charging stations as they can be easily modified to create these attacks.

Phishing –

Phishing occurs when an attacker makes fraudulent communications with a victim that are disguised as legitimate, often claiming or seeming to be from a trusted source. In a phishing attack, the recipient is tricked into installing malware on their device or sharing personal, financial, or business information. Email is the most popular mode of communication for phishing attacks, but phishing may also utilize chat applications, social media, phone calls, or spoofed websites designed to look legitimate. Some of the worst phishing attacks make charity pleas after natural disasters or tragedies strike, exploiting people's goodwill and urging them to donate to a cause by entering personal or payment information. Also remember that the College's IT department will not email you to check your login and Microsoft support will not contact you to help with viruses. These should all be considered phishing attacks.

Phishing scams are a constant threat - using various social engineering ploys, cyber-criminals will attempt to trick you into divulging personal information such as your login ID and password, banking, or credit card information.

Pretexting –

Pretexting occurs when an attacker fabricates false circumstances to compel a victim into providing access to sensitive data or protected systems. Examples of pretexting attacks include a scammer pretending to need financial data in order to confirm the identity of the recipient or masquerading as a trusted entity such as a member of the company's IT department in order to trick the victim into divulging login credentials or granting computer access.

Quid Pro Quo –

A quid pro quo attack occurs when attackers request private information from someone in exchange for something desirable or some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift. Remember, if it sounds too good to be true, it probably is. There are no Nigerian Princes that need you to help transfer their wealth for a reward.

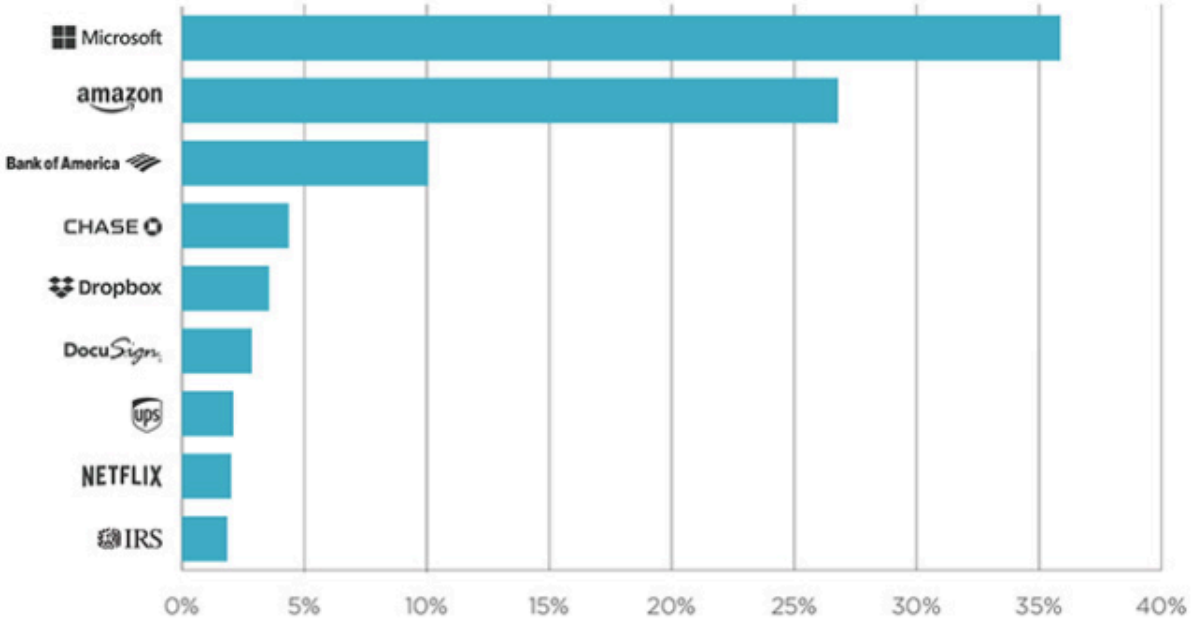
Spear Phishing –

Spear phishing is a highly targeted type of phishing attack that focuses on a specific individual or organization. Spear phishing attacks use personal information that is specific to the recipient in order gain trust and appear more legitimate. Often this information is taken from victims' social media accounts or other online activity. By personalizing their phishing tactics, spear phishers have higher success rates for tricking victims into granting access or divulging sensitive information such as financial data or trade secrets. These often come in the form of invoices from companies your family or office does business with regularly, but they are not from the real company you know.

Tailgating –

Tailgating is a physical social engineering technique that occurs when unauthorized individuals follow authorized individuals into an otherwise secure location. The goal of tailgating is to obtain valuable property or confidential information. Tailgating could occur when someone asks you to hold the door open because they forgot their access card or asks to borrow your phone or laptop to complete a simple task and instead installs malware or steals data.

Top Ten Brands Used for Impersonation Attacks



TIP #4 – PROTECT YOUR CREDENTIALS

Protecting your account username and password, or passphrase, is fundamental to proper security practices. This is especially true of your FSCJ credentials, which provide access to a wide array of online services for students, faculty, and staff. The theft of account information is one of the biggest threats facing the College. Here's what you need to know to protect yourself.

What is the Risk?

If your FSCJ account credentials are stolen, the following are more likely to occur:

- Your FSCJ payroll account and bank information are targeted for fraudulent actions.
- Restricted FSCJ data is compromised, resulting in a costly breach response and litigation.
- Thousands of emails could be posted using your fscj.edu account, advertising dubious or illegal activities. This would not only cause your account to be deactivated, but also lowers the email reputation score for FSCJ and can cause others to automatically stop accepting email from FSCJ altogether.
- All of your personal and work-related communication is read, including emails, chat, and private messages.

These things really do happen and they happen far too often!

Passphrase/Password Dos and Don'ts

- Don't give your passphrase to ANYONE. A legitimate system administrator can reset your passphrase if necessary and should NEVER request it by email or over the phone.
- Don't use a passphrase containing information about yourself that someone who knows you could guess, such as birthday or favorite movie.
- Don't type your passphrase while using someone else's computer. It is relatively easy to steal someone's passphrase by installing a keylogger on your computer and then letting someone use the computer.
- Look out for "shoulder surfers" when typing your passphrase, much as you would do when typing your PIN number at an ATM.
- If you are approached by a stranger and they ask you for permission to check your PC, ask them for their FSCJ ID badge and work order. FSCJ tech support will never ask you for your password in person, on the phone, or by email. Tech support staffers have their own login that allows them to handle most issues. If they need you to log in with your credentials, stay with them until they are done.
- FSCJ technical support will never send you an email asking you to check your ID or password - this is a phishing scam.
- Do not use your business email for personal use.

TIP #5 – BE CAREFUL WHAT YOU CLICK

Avoid visiting unknown websites or downloading software from untrusted sources. Pirate sites that provide free illegal downloads of movies, music and software, as well as many porn sites often host malware that will automatically, and often silently, compromise your computer. If attachments or links in the email are unexpected or suspicious for any reason, don't click on them. Remember nothing is free; you will always pay a price.

TIP #6 – TOO MUCH DATA ACCESS

Company data is one of the most valuable assets that any business controls, and it should be protected accordingly. To put it simply, data access should be controlled in a way that minimizes exposure and reduces the risk of accidental or malicious misuse. Make sure you understand the level of access you have been given. If you are unsure, contact your supervisor and ask them to review it with you. You may find that you have to much access for the duties you perform.

TIP #7 – BE CAUTIOUS WHEN YOU INSTALL OR DOWNLOAD

Don’t install or download any unknown or unsolicited programs/apps to your computer, phone, or other devices. These can harbor behind-the-scenes viruses or open a "back door" giving others access to your devices without your knowledge. Sites that offer free movies, music, software, and porn are usually providing infected content.

TIP #8 – USE MOBILE DEVICES SAFELY

Considering how much we rely on our mobile devices, and how susceptible they are to attack, you'll want to make sure you are protected. Here are a few things to keep in mind when using your mobile device.

- Lock your device with a PIN or password - and never leave it unprotected in public.
- Only install apps from trusted sources.
- Keep your device's operating system updated.
- Don't click on links or attachments from unsolicited emails or texts.
- Avoid transmitting or storing personal information on the device.
- Most handheld devices are capable of employing data encryption. Consult your device's documentation for available options.
- Use Apple's Find my iPhone (external link)or the Android Device Manager (external link) tools to help prevent loss or theft.
- Backup your data.
- Install antivirus and malware protection. (Yes, your smartphone can be attacked!)
- Most phone repair services will ask for your pin/password in order to work on your device, and often will not do the repairs in front of you. We recommend not giving anyone your password, even if access to the phone is needed to complete the repair.

TIP #9 – INSTALL ANTI-VIRUS PROTECTION

The computer issued to you by FSCJ already has the latest version of antivirus software installed and maintained by FSCJ tech support. For personally owned systems and unmanaged FSCJ-owned computers, please ensure that you are using a well-known antivirus software such as Norton, McAfee, Fortinet, Kaspersky, or Malwarebytes, to name a few.

NOTE: In the future, all BYODs (Bring Your Own Devices) will be scanned to ensure the device has proper antivirus and malware protection. All devices that do not meet basic requirements will be quarantined and only allowed minimum access.

TIP #10 – BACK UP YOUR DATA

Create a backup or copy of all files or data you are not willing to lose and store the copies very securely. Be sure to back up your files regularly. Microsoft OneDrive is provided free for all College employees for backup and storage purposes. If you are not sure how to use OneDrive, call the FSCJ helpdesk and open a ticket so that local tech support can show you on how to install and use.

If you are a victim of a security incident, the only guaranteed way to repair your computer is to erase and re-install the system and restore from backup (One Drive).