JSU CYBER AWARENESS TRAINING 2022 EMPLOYEES

TRAINING OVERVIEW

JSU Cyber Awareness 2022

This JSU Employee Cyber Awareness training course covers the basics of security best practices for all JSU Employees. After completing this training employees will be aware of the following:

- Key Terms and Definitions
- What is Cyber Awareness?
- Why Is Cyber Awareness Important?
- The Benefits of Cyber Awareness
- Top Ten JSU Cyber Awareness Tips
- The Seven Signs of Phishing Scams
- Reporting Suspicious Cyber Activity

Key Terms And Definitions

- **Cyber Awareness** –an ongoing process of educating employees about the threats that lurk in cyberspace and how to act responsibly
- **Data Breach** - an incident where information (accounts & passwords) is stolen or taken from a system without the knowledge or authorization of the system's owner
- **Phishing Scams** - type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker
- **Business Email Compromise (BEC)** –a specific type of phishing attack, designed to trick employees into sending money to the attacker

What Is Cyber Awareness?

- Cyber awareness is knowing the dangers of browsing the web, checking email and interacting online
- It means knowing when and how to use best practices as a JSU employee when online or offline
- Also knowing how to do your part to help keep students' and employees' sensitive data safe on and off JSU's campus

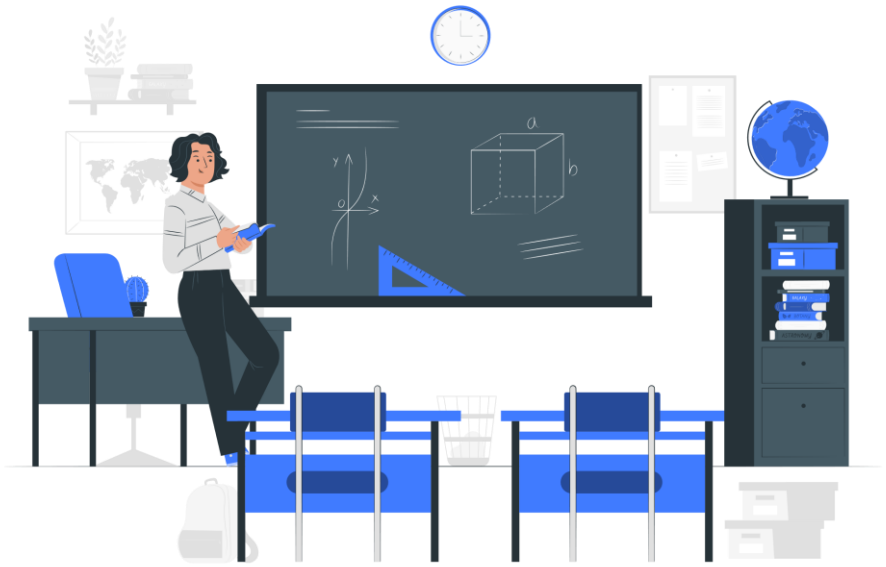
Why Is Cyber Awareness Important?

- Cybercrime is on the rise around the world due to increased use of digital resources
- Consumers' personal and financial data is collected everywhere, and hackers are getting smarter at stealing it
- Technology alone is not enough to provide protection (hackers like to target employees who are unaware of their scams)
- Training employees to become aware of threats and scams they face online and offline strengthens our defenses

Cyber Awareness Benefits?

- Become more aware of the threats and risks that come with using technology
- Learn how to use technology safely and responsibly at work and at home
- Learn steps you can make today to protect student, employee and your personal data and information from cyber criminals

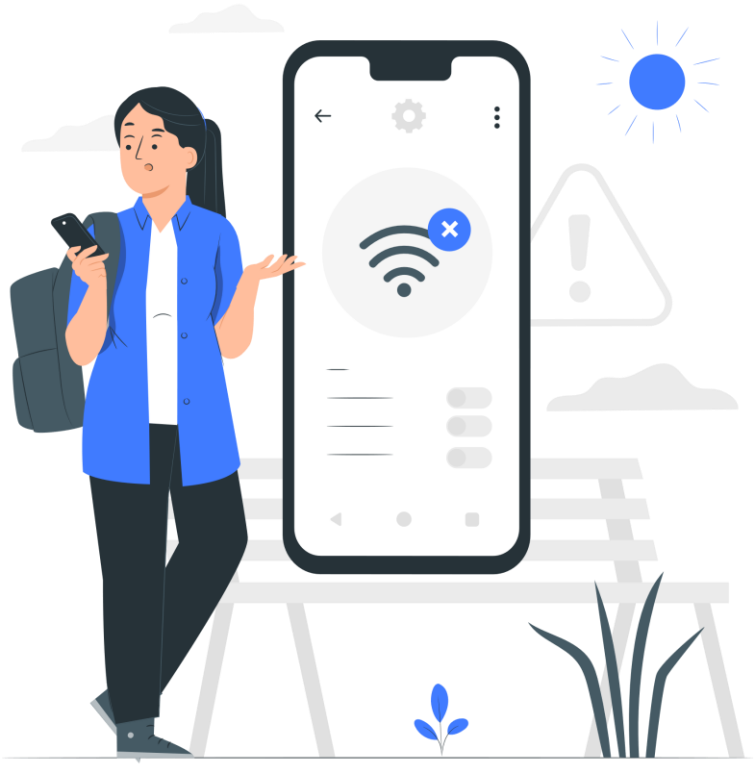
TIP 1: Avoid Random Removable Media



Removable media and devices are portable hardware that may be randomly left in/on office desks, classrooms, or parking lots:

- The most common is a USB flash drive but other forms could be an external hard drive, CD/DVD or SD card
- Removable media and devices may contain a virus that can infect your device or the JSU network
- As a best practice, avoid plugging or inserting removable media and devices into your computer if you do not trust or know the source

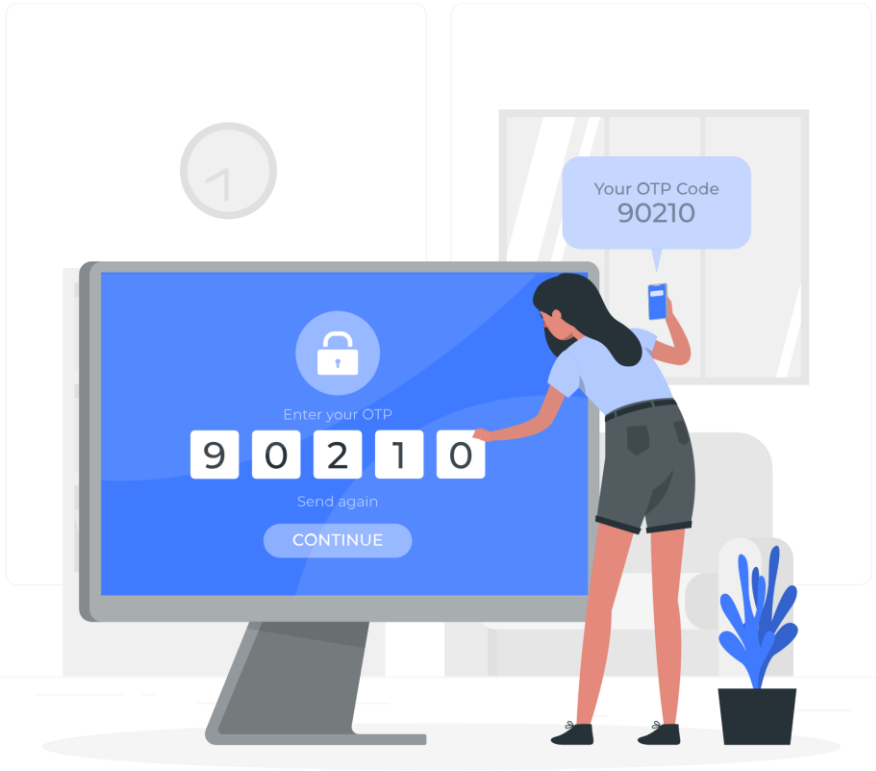
TIP 2: Connect To Secure Wi-Fi Signals



Always assume a public Wi-Fi network isn't secure especially in places like public parks, coffee shops, airports and hotels:

- Avoid accessing your work, personal or financial information on public Wi-Fi connections in public places
- When working on campus make sure that you are connecting to an official JSU Wi-Fi Signal or Access Point
- When working off campus and accessing sensitive data, always make sure to connect securely using a Virtual Private Network

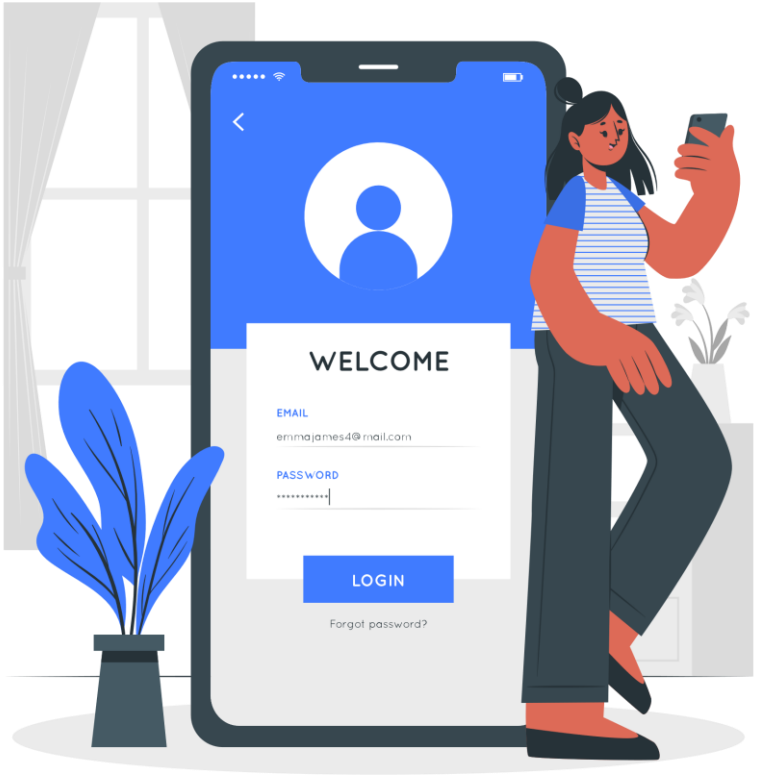
TIP 3: Use Password Best Practices



A strong password is your first line of defense for protecting your sensitive information: Use these best practices:

- Create passwords at least 15 or more characters long using a combination of letters, numbers, and symbols
- Use extra layer of security with a fingerprint, numerical token, or answer a security question when possible
- Use a different password for multiple accounts (ex. Social media accounts, JSU accounts, Banking accounts)
- Change your password immediately after a data breach

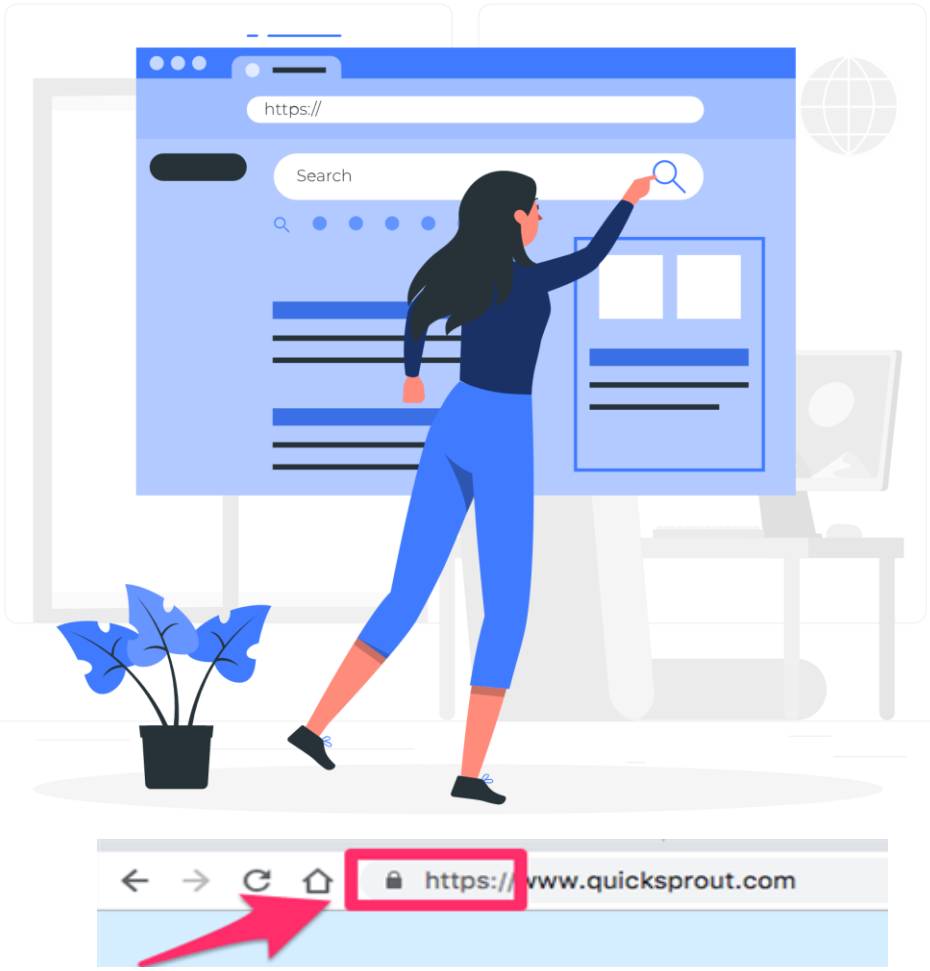
TIP 4: Avoid Bad Password Practices



Any password can be cracked if a user does not avoid the following bad password practices:

- DON'T share your password with others– not even your friends.
- DON'T use passwords that are easy for people you know to guess (ex. nickname or pet's name)
- DON'T use any private identity information in your password
- DON'T use a single word in the dictionary as a password
- DON'T post passwords where others can see them

TIP 5: Look For The Lock



*Always l*ook for the Padlock and the letters Https before entering sensitive data on any website:

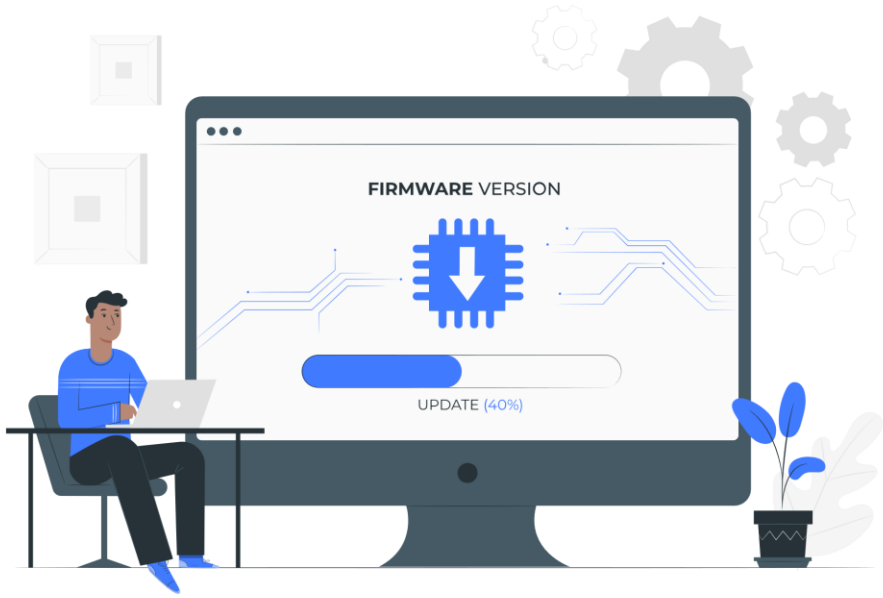
- Padlocks and Https means data you send to this website is encrypted and not visible to others
- A padlock does not mean safe from viruses or other online threats
- Make sure the website is not a look-alike or fake website set up by a cyber criminal before entering user names and passwords

TIP 6: Tailgaitng Only At Football Games

*Tailgaiting in cyber security- **is trailing someone else to get into restricted areas:***

- Someone can trail you in a car to get access into a gate on campus
- Someone can trail you into a door that requires badge access to enter
- Someone can trail behind you in computer lab and use your log in session instead of their own

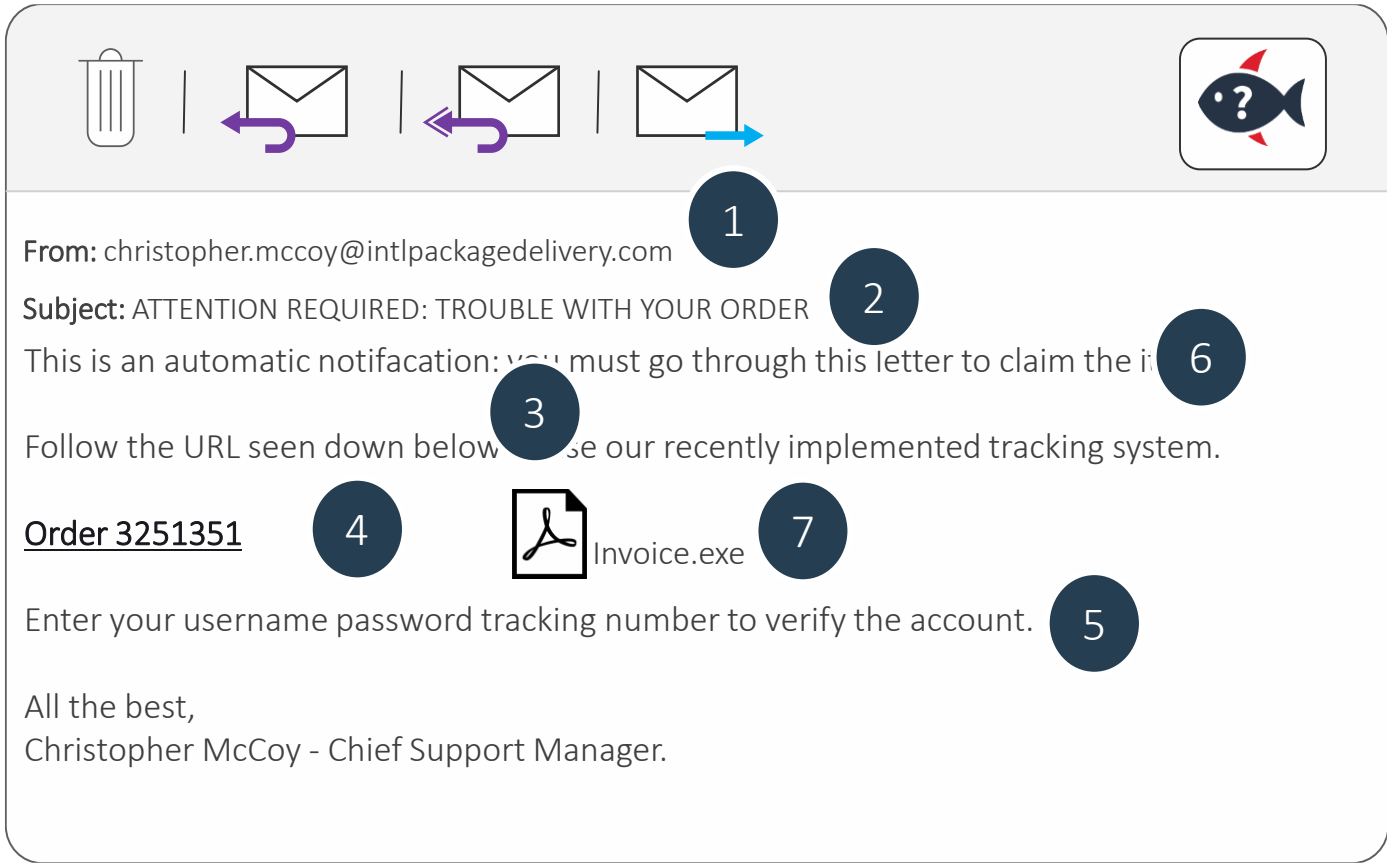
TIP 7: Keep Up With Updates



It is critical to install security updates to protect your systems from malicious attacks by cyber criminals:

- Updates help to patch security weaknesses that cyber criminals take advantage of
- Keep applications updated as soon as updates are released
- When possible keep web browsers updated and turn on automatic updates on devices, and applications

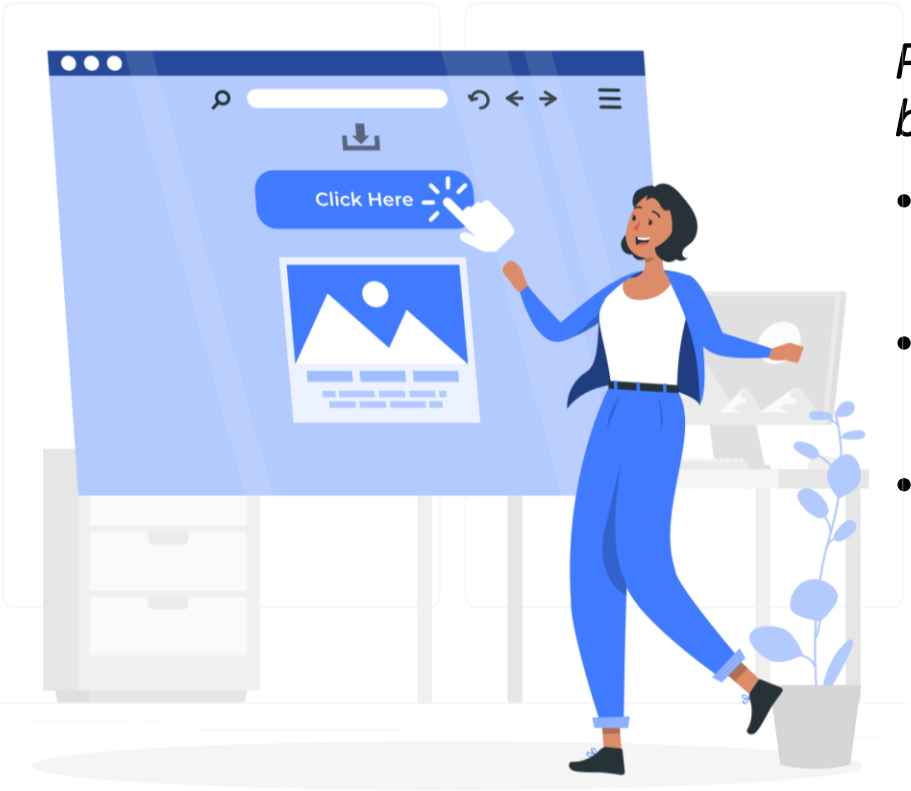
TIP 8: Recognize Signs Of Phishing



Look for the 7 signs of a Phishing Scam in every JSU email received from internal and external senders:

1. Unknown Sender
2. Emotional Appeal
3. Spelling/Grammatical Errors
4. Unknown URL Link, button, file
5. Asks for Sensitive Information
6. Generic greeting or no greeting
7. Suspicious downloadable attachment

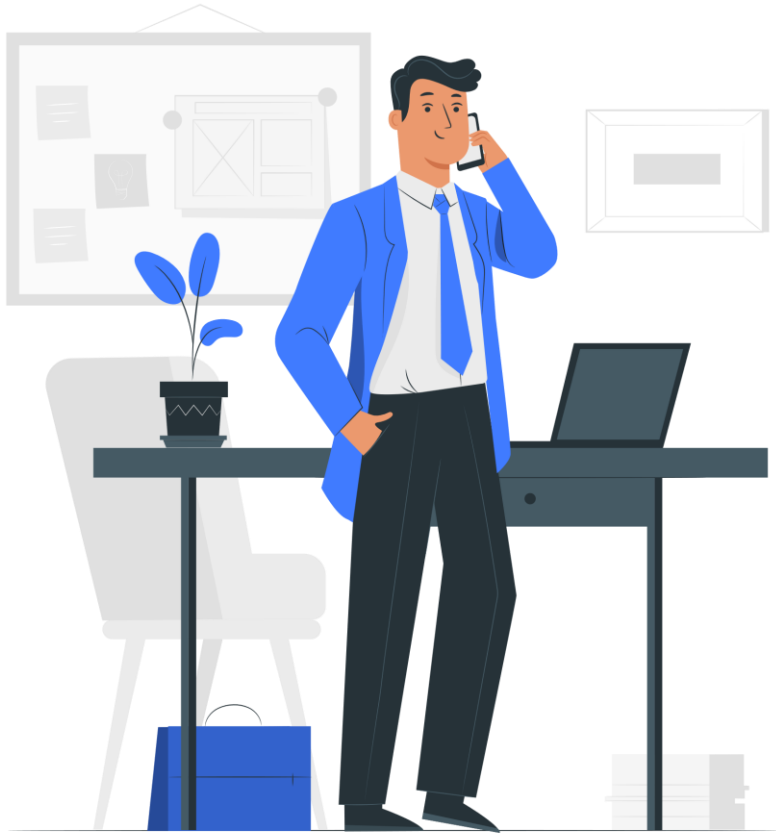
TIP 9: Think Before You Click



Phishing scams and attacks have evolved over the years and have become tougher to spot:

- Avoid clicking links or downloading attachments in a suspicious email from unknown sources
- First inspect the email using the seven signs of phishing scam tips
- If you are still unsure about an email and its content report it to **email.admin@jsums.edu** or cybersecurity@jsums.edu immediately

TIP 10: Got Hooked? Report It



If you get hooked or scammed by a Phishing or BEC attack make sure to report it and take action quickly :

- Step 1: Immediately contact the JSU IT Dept. to report it at cybersecurity@jsums.edu or call 601-979-2312
- Step 2: Forward the original phishing email to the JSU email administrator at email.admin@jsums.edu
- Step 3: Change the password to your email and other relevant accounts then delete the phishing email
- Step 4: Review training and phishing documentation on the JSU Cyber Awareness website to avoid getting hooked in the future

Types of Phishing Scams

Question/Report any text message or email that:

- Say they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- Say you must confirm some personal information using your username & password
- Want you to click on a link to make a payment
- Say you're eligible to register for a government refund
- Offer a coupon for free stuff
- Ask you to send money, your banking info, or purchase a gift card
- Sends you a fake invoice to confirm items you did not order

Types of Business Email Compromise

- False Invoice Scam: phisher pretends to be a vendor requesting payment for services performed for the company and requests a change in the bank account information to an account controlled by the attackers
- CEO Fraud: attacker sends an email – supposedly from the CEO – instructing the recipient to take some action(ex. a wire transfer to “close a business deal”, buy gift cards) or sending sensitive information to a partner
- Account Compromise: takes advantage of a compromised email account and request invoice payments from customers while changing the payment details to those of the attacker
- Data Theft: attack targets HR and Finance personnel and attempts to steal sensitive information about an organization’s employees

Beware of Google Drive Scams

Scammers are aware of the fact that Google Drive invitations may be likely to get through spam defenses because they emulate legitimate invitations:

- Delete any unsolicited invitations to share Google Documents
- Do not click on links you receive from people you don't know
- Avoid logging in to Google through emailed links; instead, go to the real Google.com and proceed from there
- Stop and think: If you use Gmail and are already logged on to your Google Account, you shouldn't need to log on again to access Drive

Beware of Payroll Scams

A Direct deposit phishing email scam will look something like this:

- A scammer contacts a payroll employee or JSU employee via a fake email address that appears to belong to someone within the university
- The email will state how the routing information for an employee's direct deposit paycheck needs to be updated; this is an attempt to get baking or other sensitive information
- Once bank account and routing number are changed, the deposits are transferred to an untraceable offshore account owned by the scammers

Beware of Gift Card Scams

If someone you do not know asks that you pay them with gift cards it's a scam and once they have the gift card number and the PIN, they have your money:

- Check /Gift Card Scam: You get a check from someone for way more than you expected. They tell you to deposit the check, then give them the difference on a gift card. Don't do it. That check will be fake, and you will lose all the money put on the gift card
- Boss Gift Card Scam: attacker sends an email, supposedly from boss, instructing the recipient to buy gift cards for them from Walmart, Amazon or Target because they are tied up in a meeting
- Never make purchases gift cards, if they have been requested via email or text by a unknown sender or unless you called and discussed it with a receiver (family member, friend, coworker) you know first

For more information on gift card scams and avoiding scams, visit the FTC website

Contact Information

JSU Division of Information Technology Incident Contacts:

*Feel free to contact us with questions or comments on cyber awareness at Jackson State University

Chief Information Security Officer : Dameion Brown

Cyber Security Awareness Training Coordinator: Shayron Nichols, PhD

Email Administrator :Josiah Dosunmu

Report Cyber Incidents to: cybersecurity@jsums.edu

References

- https://consumer.ftc.gov/articles/gift-card-scams
- https://cofense.com/
- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/business-email-compromise-bec/
- https://www.trendmicro.com/vinfo/us/security/definition/data-breach
- https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/