JSU CYBER AWARENESS TRAINING 2022 FOR STUDENTS

Device Security

Computer Security

Global Security

Fingerprint

Secure Payment

CCTV

CYBER AWARENESS TRAINING OVERVIEW

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

WHAT IS CYBER AWARENESS?

- Cyber awareness is knowing the dangers of browsing the web, checking email and interacting online
- It means knowing and using best practices when online or offline
- Also knowing how to do your part to help keep your sensitive data safe

WHY CYBER AWARENESS?

- Cybercrime is on the rise around the world due to increased use of digital resources
- Examples include: social media, cloud storage, digital downloads, and mobile and online payments
- Consumers' personal and financial data is collected everywhere, and hackers are getting smarter at stealing it

BENEFITS OF CYBER AWARENESS?

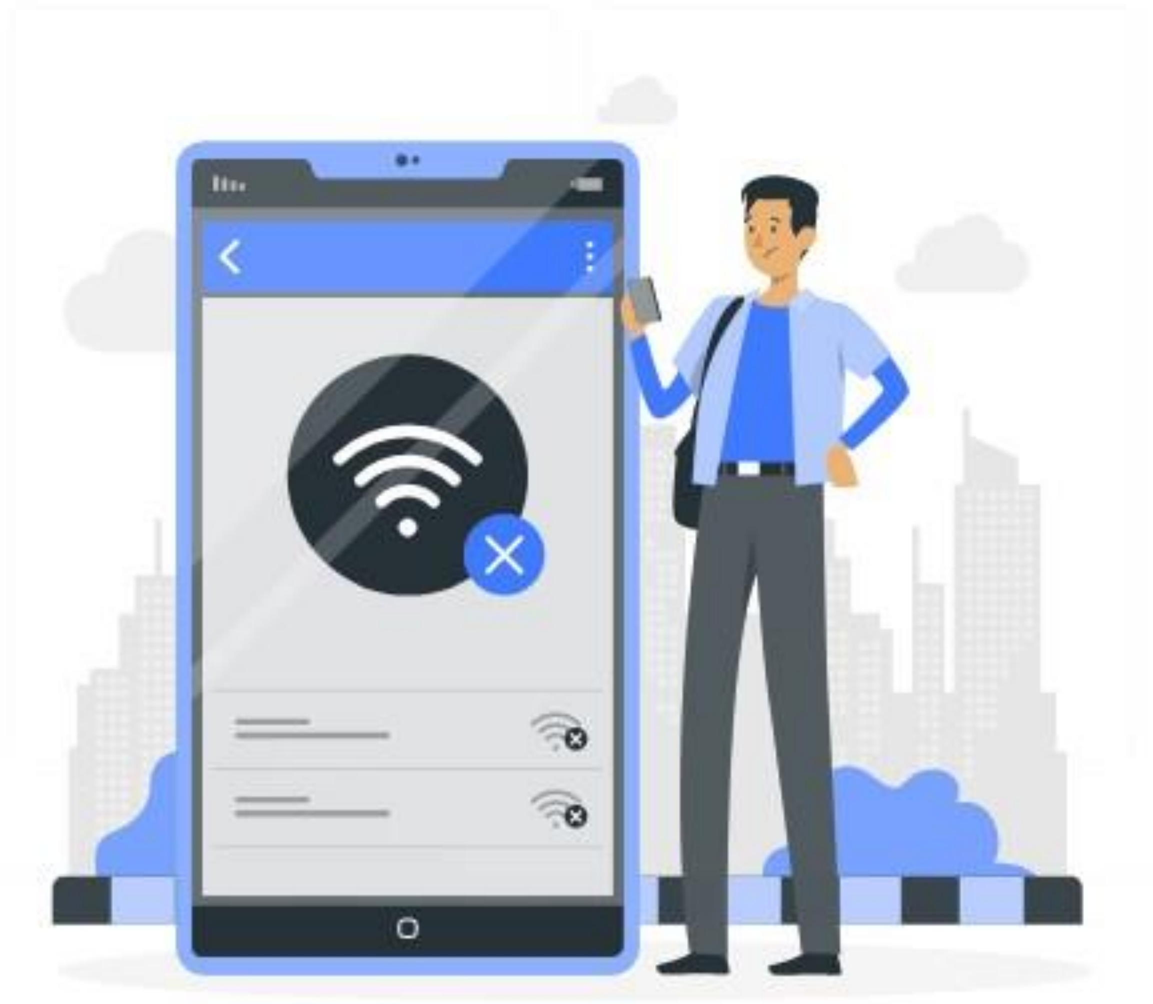
- Become aware of the threats and risks that come with using technology
- Learn how to use technology safely and responsibly on and off campus
- Learn to protect your personal data and information from cyber criminals

Tip 1: AVOID USING RANDOM USB DRIVES

- As a student you may randomly find USB drives in hallways, parking lots or computer labs
- Do not insert these random USB drives into your computer
- These drives may contain a virus that can infect your device or the JSU network

Tip 2: AVOID USING PUBLIC WiFi

- Most public WiFi used at coffee shops, airports, and hotels is not secure
- Hackers and cyber criminals can see sensitive information you enter on websites in plain text
- Protect your information by not using Public WiFi to do online shopping, banking, or bill paying

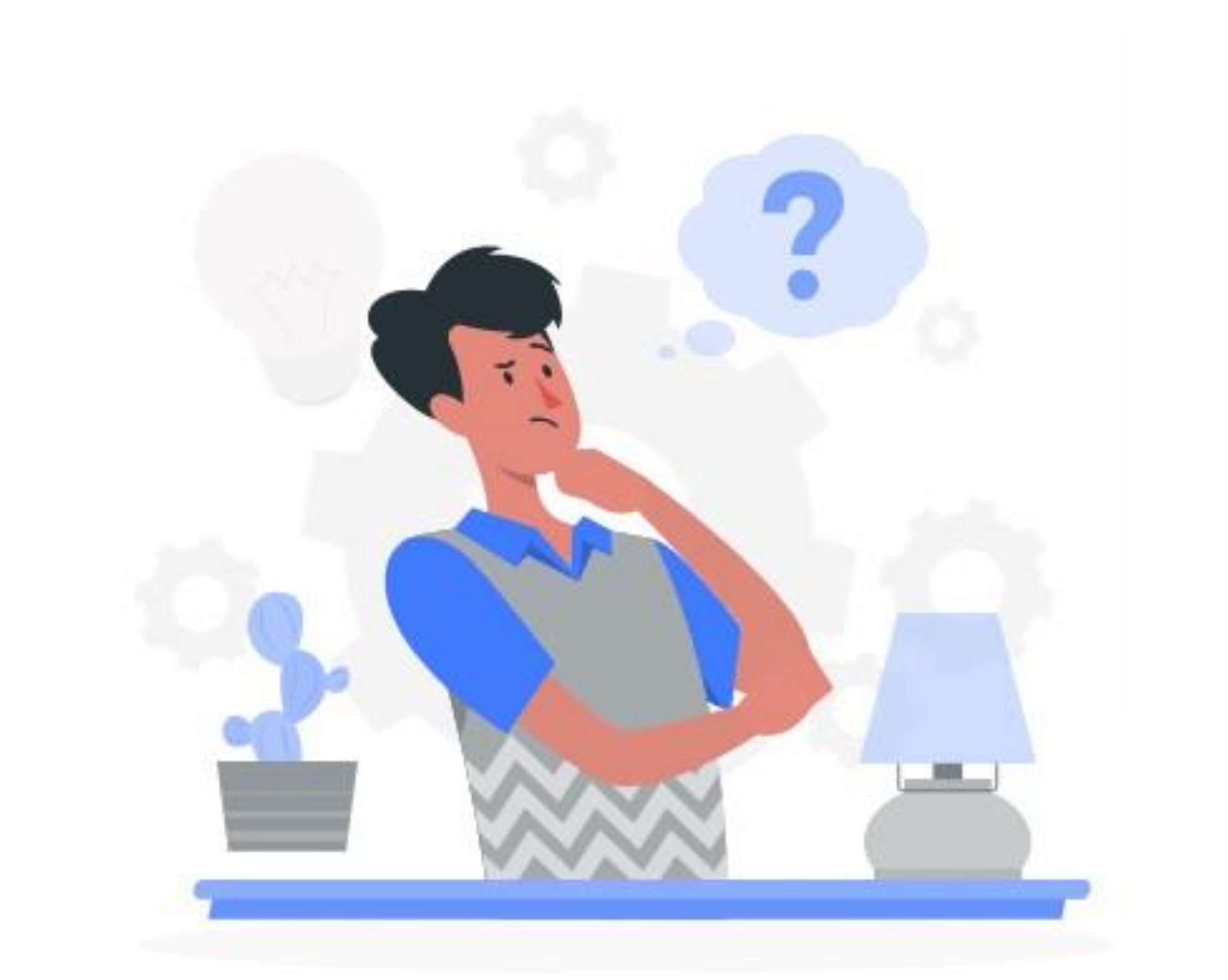


Tip 3: CONNECT TO SECURE WIFI SIGNALS

- Make sure that you are connecting to an official JSU WiFi Signal or Access Point
- Avoid connecting devices to signals that don’t require a password to gain access
- It could be a signal a cyber criminal created to steal your sensitive data

Tip 4: USE STRONG PASSWORDS

- JSU students have many accounts that require passwords (ex. JSU student email, PAWS, CANVAS etc..)
- A strong password is your first line of defense for protecting your sensitive information
- Use an extra layer of security like a fingerprint, numerical token, or answer a security question when possible



Tip 5: PRACTICE PASSWORD DO’s

- DO create passwords at least 15 or more characters long
- DO use combinations of letters, numbers, and symbols
- DO change your password regularly(every six months)
- DO use a different password for multiple accounts (ex. Social media accounts, JSU accounts, Banking accounts)

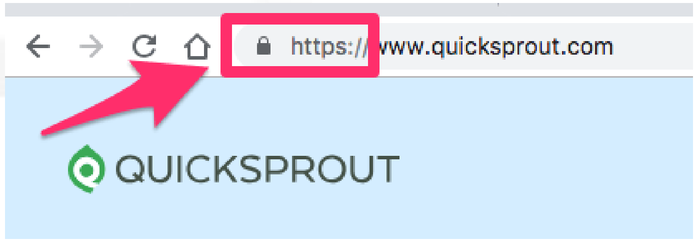
Tip 6: REMEMBER PASSWORD DON’Ts

- 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 7: ONLY TAILGATE AT FOOTBALL GAMES

Tailgating 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


https://www.quicksprout.com

Tip 8: LOOK FOR THE LOCK

Look for the padlock and the letters Https before entering sensitive data on any website

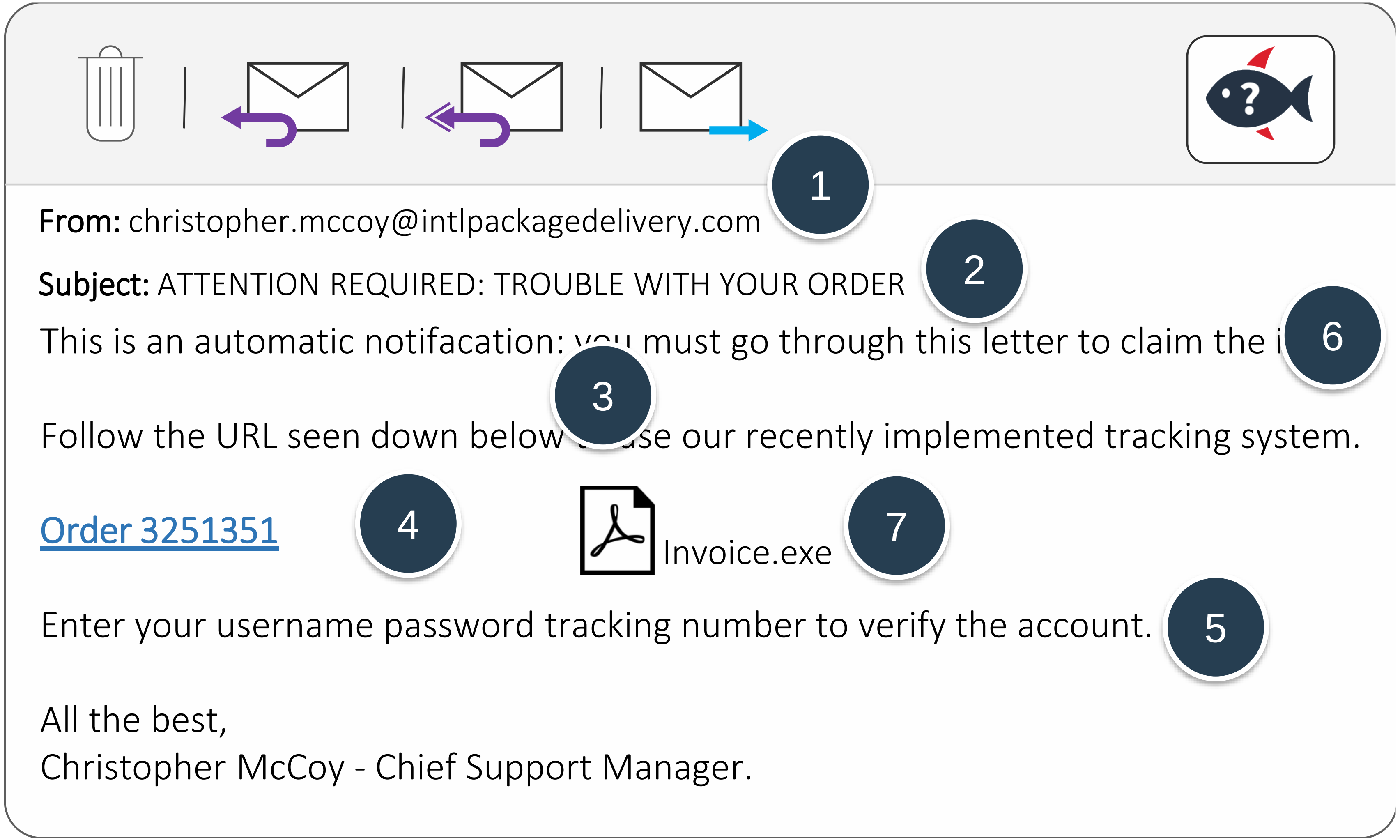
- Padlocks and Https means secure (data is not visible to others)
- Padlock does not mean safe from viruses or other online threats

Tip 9: BEWARE OF PHISHING SCAMS

Phishing emails and text messages may look like they're from a company you know or trust

- Scammers use this trust to trick you into giving them your personal information
- They may try to steal your passwords, account numbers, or Social Security numbers credit card numbers, etc..

Tip 9: SEVEN SIGNS OF PHISHING EMAILS



From: christopher.mccoy@intlpackagedelivery.com

Subject: ATTENTION REQUIRED: TROUBLE WITH YOUR ORDER

This is an automatic notifacation: you must go through this letter to claim the i

Follow the URL seen down below to use our recently implemented tracking system.

Order 3251351

Invoice.exe

Enter your username password tracking number to verify the account.

All the best,
Christopher McCoy - Chief Support Manager.

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

Tip 9: MORE SIGNS OF PHISHING EMAILS

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

Tip 10: REPORT ANYTHING STRANGE

- Think before you click a link, connect a device or download a file
- If you detect that something is suspicious or spot an email phishing scam, report it
- Contact the JSU IT department at cybersecurity@jsums.edu

CONTACT US

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

href="https://storyset.com/people">People illustrations by Storyset