JACKSON STATE UNIVERSITY CYBER AWARENESS TRAINING 2020 Part I

WHY IS CYBER AWARENESS TRAINING IMPORTANT?

- Promotes Awareness about scams and attacks
- Shows the importance of data protection
- Strengthens weakest link by educating employees on Cyber Attacks
- Violations and incidents can cost a company millions of dollars
- Technology alone is not enough to provide protection (hackers like to target employees who are unaware of their scams)

WHY IS CYBER AWARENESS TRAINING IMPORTANT

- Cybercriminals take advantage of your trust, fear, and plain old human error.
- Security awareness training teaches you to spot fakes emails and scams, avoid risks online, and use good cyber-hygiene practices at work and at home.

WHY IS CYBER AWARENESS TRAINING IMPORTANT

Cyber Security Provides Safety

Security: We must protect our data in the same way that we protect money and the way we protect our homes

Safety: We must learn to adopt behaviors that protect us against risks and threats that come with technology and internet activities.

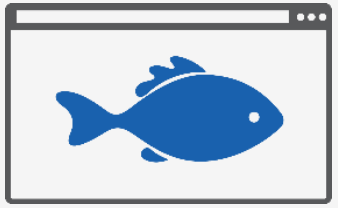
CONSEQUENCES OF NOT BEING CYBER AWARE

Failure to comply with the data protection security requirements of HIPAA, FERPA and GLBA due to the lack of cyber awareness can result in:

- Increases chances of being part of a data breach
- The employee or University paying fines and other legal costs due to a data breach involving sensitive data
- Loss in Federal Funding for the University and its students (ex. Financial Aid)

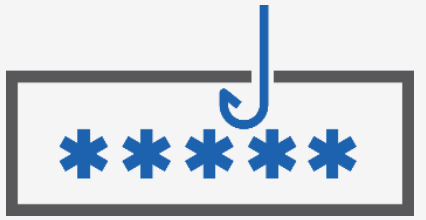
IT's NOT THAT DANGEROUS ONLINE RIGHT?

1 in 50 URLs is malicious[1]



Nearly 1 in 3 phishing sites uses HTTPS to appear legitimate[1]

90% of the malware businesses encounter is delivered via email[2]



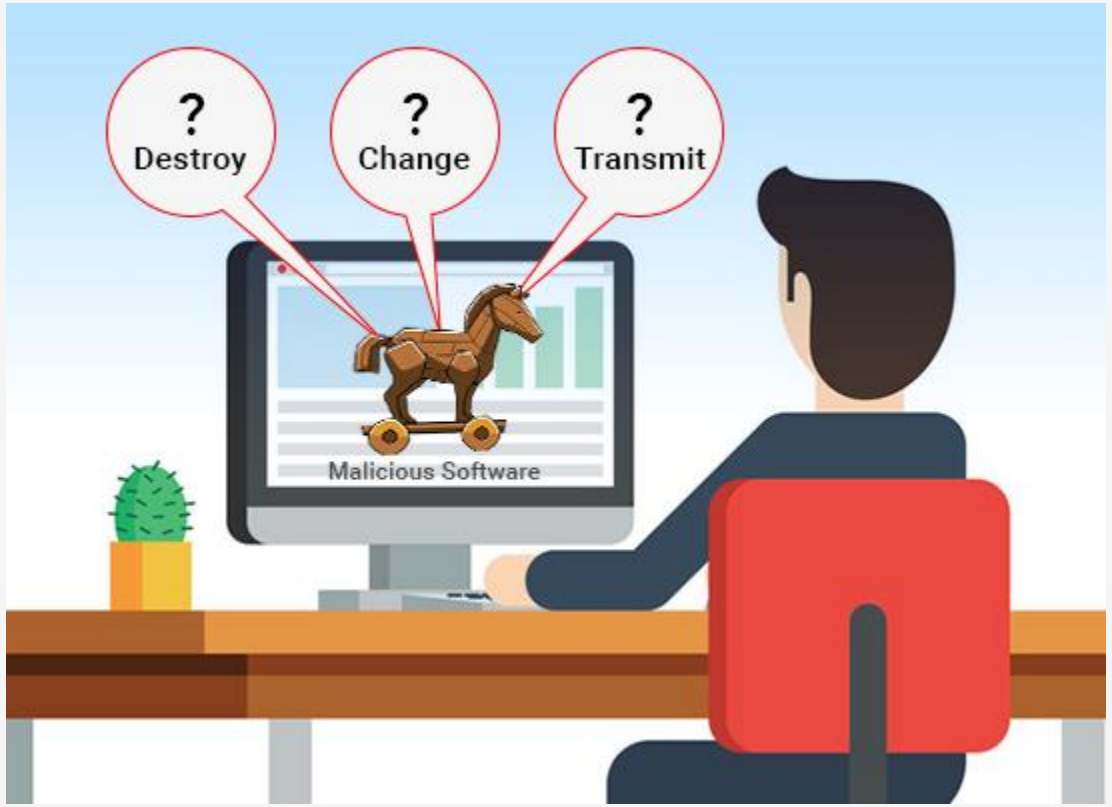
Most breaches involve phishing and using stolen credentials[2]

[1] Webroot Inc. "2019 Webroot Threat Report: Mid-Year Update." (September 2019). [2] Verizon. "2019 Data Breach Investigations Report." (May 2019)

Common Cyber Threats in Workplace

Some common cyber threats that employees face in today's workplace include:

- Viruses and Worms
- Ransomware
- Trojan Horses / Logic Bombs
- Social Engineering
- Phishing scams
- Botnets / Zombies



Common Cyber Threats in Workplace

Viruses

- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.

Worms

- Independent program that replicates itself and sends copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate.

Common Cyber Threats in Workplace

Phishing

- Phishing is a type of social engineering attack often used to steal user data, including login credentials

Trojan Horses

- Masquerades as a benign program while quietly destroying data or damaging your system.

Common Cyber Threats in Workplace

Ransomware

- A type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access

Social Engineering

- Use of deception to gain confidential information, commit fraud, or access computer systems from computer users through human interaction

Basic Tips to Avoid Cyber Attacks:

1 Keep A Clean Machine

- Keep Antivirus Software Current
- Turn On Automatic Software Updates
- Protect All Devices That Connect To The Internet

2 Lock Down Your Login

- Lock Down Your Login: Use 2FA OR MFA
- Create A Strong Password At Least 12 Characters Long (EX. IamLovingmy20s)
- Avoid leaving passwords stuck on monitors or lying on desks

3 Connect With Care

- When In Doubt Throw It Out By Deleting Suspicious Emails And Social Media Posts
- Avoid Using Sites That Require Personal Information When Using Public Wi-Fi
- Connect to A Virtual Private Network when dealing with sensitive data

Basic Tips to Avoid Cyber Attacks:

1 Keep A Clean Device

- Remove Apps That Are Not Being Used
- Keep Device Software Updated
- Avoid Using Apps That Collect Personal Data You Want To Protect

2 Lock Down Your Login

- Lock Down Your Login: Use 2FA OR MFA
- Create A Strong Password At Least 12 Characters Long
- (EX. IamLovingmy20s

3 Avoid Oversharing Data

- Avoid Oversharing personal information on Social Media
- Turn On Privacy Settings To Control Who Has Access to Your Page
- Stop and Think Before You post messages and Photos

Additional Training Material

- Please review Additional Training PDF Documents and Materials by clicking the cyber awareness training link on the https://www.jsums.edu/cyberawareness page of the JSU Website
- Part II of this training will be provided under your JSU Employee CANVAS Account and email containing login instructions will be provided.

Contact Information

JSU Department of Information Technology Incident Contacts:

Shayron Nichols, PhD
Cyber Security Awareness Training Coordinator

Josiah Dosunmu
Email Administrator

Report Cyber Incidents to:
cybersecurity@jsums.edu

*Feel free to contact us with questions or comments on information security or privacy at Jackson State University.