JSU PRIVILEGED USER TRAINING 2022

TRAINING OVERVIEW

This JSU Employee Privileged User Training course covers the basics of Privileged user best practices. After completing this training employees will be aware of the following:

- Key Terms and Definitions
- Types of Privileged Users
- What Privileged Users Do
- The Value of Privileged Users
- Attacks on Privileged User Accounts
- Privileged User Best Practices
- Privileged User Responsibilities

Key Terms And Definitions

- **A Privileged User-** is a trusted user who has been authorized to have administrative access to critical systems
- **A Privileged User Account**–provides a trusted user with administrative or specialized levels of access based on elevated levels of permissions (thycotic.com).
- **Multi Factor Authentication (MFA)-**authentication through verification of two or more of the following methods: (1) a password; (2) a token; or (3) fingerprint (4) security question
- **Encryption-** translating data from plaintext (unencrypted) to a format that is unreadable (encrypted) by a human or computer

Common Types of Privileged Users

Typically **privileged user** accounts are used by IT employees such as:

- Chief Information Officers
- Chief Technology Officers, Chief Information Security Officers
- System Administrators, Database Administrators
- Network Administrators
- Email Administrators
- Webmasters
- Application Developers, contractors, third party vendors

What Do Privileged Users Do ?

A **privileged user** at JSU may be **given elevated privileges** to manage, create, delete, disable, modify, or configure student, and employee accounts, and IT systems and infrastructure such as:

- Install system hardware and software
- Email accounts
- Firewall Configurations
- Provide Server access and setting configurations
- Managing and configuring databases
- Reset passwords
- Accessing sensitive datasets

Value Of A Privileged User

- Having **permissions** and **access** **to critical systems** makes privileged users a very important asset to Jackson State University
- It also **makes** privileged users and **their account** information a **big target** for hackers and cyber criminals
- It is important to **protect, monitor, and audit** this account at all times

Attacks on Privileged User Accounts

If a hacker gets their foot in the door **via privileged user accounts**, they can:

- Access an modify system applications
- Access critical data sets containing confidential information
- Perform key administrative functions

Attacks on Privileged User Accounts

Having access to **privilege user accounts** allows hackers to:

- Impersonate a JSU employee or student
- Create ongoing access into the JSU network and assets
- Steal confidential information
- Cause short term and long term damage to JSU's network and other assets

Privileged User Accounts Best Practices

As a privileged user **always** make sure to follow best practices:

- Use the concept **of least privileges** when creating accounts
- Only **give** the user **enough access** to perform their specific job duties
- Use strong complex passwords to protect privileged user accounts
- Change your privileged user passwords as often as JSU's policies require
- Change your privileged user passwords immediately after a data breach

Privileged User Accounts Best Practices

- **Avoid using** the **same passwords** for multiple privileged and non privileged user accounts
- **Conduct audits**, monitor, and/or disable default accounts, and inactive accounts
- **Do not use** privilege user accounts to perform standard non-privilege user routine tasks
- **Use MFA** as an extra layer of security for privileged user accounts ex. numerical token, security question(GLBA mandatory safeguard)

Privileged User Database Best Practices

- **Create** and perform proper **database backups** as often as possible
- **Ensure** that the **connection** to the database is **secure**
- Ensure that the database **credentials** are **not misused**
- **Encrypt** data being stored or in transit (GLBA mandatory safeguard)
- Remember to **remove third party accounts** or temporary accounts when access is no longer needed

Privileged User Server Best Practices

- **Always** remember to **sign out** of servers after each session
- Ensure **server patches and updates** are made in a timely fashion
- **Notify** appropriate JSU IT staff and other affected JSU employees **when performing** server **maintenance** and updates
- **Create** and perform **proper backups** as often as possible

Networks and Data Centers Best Practices

- **Avoid** allowing unauthorized individuals not on the data center checklist inside the data center
- Make sure to **secure all data center doors** and locks upon exiting data center
- **Ensure security** through access controls, backups and firewalls
- **Keep a proper log** of any person(s) entering and leaving the data center

Privilege User Data Security Best Practices

If you are a privileged user that handles or access confidential PII data
(ex. FERPA, GLBA, HIPAA, Class Schedules, Grades etc.)

- **Avoid allowing** unauthorized users access to PII data without a “legitimate educational interest”
- Make sure to secure or **encrypt** any locally **stored PII data**
- **Practice a clean desk policy** if you have paper documents or reports generated with confidential/PII data
- **Avoid transmitting** electronic confidential/PII **data** internally or externally if it is **not encrypted** or protected

Privileged Users Responsibilities

As a privileged user **always** make sure to do your part by:

- Taking Cyber Awareness training
- **Following** privileged user **best practices** and JSU workplace policies
- Becoming familiar with JSU's IT policies
- Following Passwords and Change Management policies
- Following Systems Network Share and Storage policies
- Knowing Cyber Incident Response

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://www.trendmicro.com/vinfo/us/security/definition/data-breach
- https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/
- https://thycotic.com/company/blog/2020/03/03/privileged-users/
- https://www.jsums.edu/jsu-cyber-awareness/jsu-information-technology-policies/