JSU'S Cyber Security Awareness Training 2021

Training For Privileged Users

Training Agenda

- Identify a privileged user
- Identify common types of privileged accounts
- Identify risk associated with privileged accounts
- Identify Privileged user best practices

What is a Privileged User?

- **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).

Common Privileged Users

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

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

What Do Privileged Users Do ?

- A privileged user may be given elevated privileges to perform job duties such as:

Install system hardware/ software

Reset Passwords for others

Log into all machines on the network

Change IT infrastructure systems

Access sensitive datasets

Value of a Privileged User

- **Having 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

- Privileged user accounts; abused or unmonitored have led to at least **74% of data breaches** (securis.com)

Attacks on Privileged User Accounts

- Once a hacker gets their foot in the door via privileged user accounts, they can access:
  - ✓ System applications
  - ✓ Critical data sets containing confidential information
  - ✓ Perform key administrative functions

Attacks on Privileged User Accounts

- **Having Access also allows hackers to:**
  - ✓ Impersonate a JSU employee
  - ✓ Create ongoing access into the JSU network and its' confidential data
  - ✓ Steal confidential information
  - ✓ Cause short term and long term damage to a company's network and other assets

Privileged Users Responsibilities

- As a privileged user **always** make sure to do your part by taking cyber awareness training for privileged users and by:

  Following privileged user **best practices** and JSU workplace policies:

  Become familiar with JSU's policies

  - ✓ Passwords and Change Management
  - ✓ Systems Network Share and Storage
  - ✓ Cyber Incident Response

Privileged User Accounts 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

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

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
- 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 users 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

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

Contact Information

- ***Report an Incident, Suspicious Activities or Question to:*** the CIO, CTO, or JSU Cyber Security Personnel immediately.

JSU Department of Information Technology

Shayron Nichols, PhD Cyber Security Awareness Officer

Cyber Awareness Training Coordinator

cybersecurity@jsums.edu

Office: 601-979-7049

REFERENCES

The Following sources were used in this privileged user training

- https://thycotic.com/company/blog/2020/03/03/privileged-users/
- https://securis.com/news/74-of-data-breaches-start-with-privileged-credential-abuse/
- https://www.jsums.edu/jsu-cyber-awareness/jsu-information-technology-policies/