

Security Awareness



Presented by:
Krystyn Schroll
IT Security & Policy (ITSP)



CYBERSECURITY AWARENESS MONTH

- Use multi-factor authentication (MFA)
- Create unique, complex, long passwords
- Regularly update software
- Be familiar with phishing indicators
- Use AI products wisely

October is **CYBERSECURITY** Awareness Month.

Stay tuned during the month for weekly tips.
Learn more at lsu.edu/securityawareness.



LSU | Information
Technology Services

Multi-factor Authentication (MFA)

- Common factors include:
 - Passwords, security questions, PIN codes
 - Security tokens or smartphones
 - Biometrics such as fingerprints or facial scans
- MFA is currently the most effective way to protect your accounts
- Only approve MFA authentication requests if you are actively logging into your account(s)

GETTING HACKED
SUCKS

Enable Multi-Factor Authentication when available to secure your accounts.

Visit lsu.edu/securityawareness to learn more.



LSU | Information Technology Services

Password Management

- Your password is your first line of defense
- Use a unique password for every account
- Password managers make this easy and often seamless
- A passwordless future with passkeys?
- Check for password exposure at haveibeenpwned.com



would be **Wise**
to use a password manager
to easily create unique and
complex passwords.

Visit lsu.edu/securityawareness
to learn more.



LSU | Information
Technology Services

Software Updates

- Update often or make it automatic
- Get it from the source
- Watch for fakes



Phishing/Smishing/Vishing

General recommendations:

- Learn the common indicators of a phish:
 - Check the sender's address
 - Always consider the context
 - Be wary of URLs
- Don't trust caller ID as numbers can be spoofed
- If you mistakenly share your password, change it immediately
- Never email SSNs, bank info, etc
- Don't respond to suspicious or unexpected texts—stay skeptical!



Phishing Awareness Program



- Regular phishing simulation campaigns designed to educate and expose users to different types of phishing attacks.
- New phishing reporter button
- Report the phish for a chance to win stuff!
- See lsu.edu/phishing for more details.

Artificial Intelligence (AI) Best Practices

Risks:

- Exposure of private data
- Confidential information

Think Before Using AI:

- Treat interactions like public forums
- Use vague or generic inputs
- Understand data retention policies
- Fact-check answers
- Use strong passwords and MFA



Cybersecurity Awareness Month at LSU

- New content posted each Monday in October at lsu.edu/securityawareness
- Read the content, take the quiz, locate the poster, scan codes, and win stuff!



Additional Resources

- **Cybersecurity Awareness Training:**
 - <https://moodle.lsu.edu/course/view.php?id=51448>
- **Managing MFA Enrollment:**
 - <https://grok.lsu.edu/Article.aspx?articleid=19929>
- **Reporting a Phishing E-mail:**
 - <https://grok.lsu.edu/Article.aspx?articleid=19636>
- **Has your password been exposed:**
 - <https://haveibeenpwned.com/>
- **Password Managers:**
 - [Best Password Manager in 2025 – CNET](#)
- **Passkeys:**
 - [Are Passwords Going Away?](#)
- **MikeGPT:**
 - <https://www.lsu.edu/academicaffairs/mikegpt/index.php>

Questions ?

When in doubt contact your IT Administrator
or email: security@lsu.edu