Security Awareness & Policy Updates

Presented by:
IT Security & Policy (ITSP)
Agenda

- Cybersecurity Awareness Basics
- Phishing Awareness Program
- Cybersecurity Awareness Month at LSU
- IT Security Policy Updates
- Additional Resources
Cybersecurity Awareness Basics

- Use multi-factor authentication (MFA)
- Create unique, complex, long passwords
- Regularly update software
- Be familiar with phishing indicators
- Use social media wisely
Phishing Awareness Program

- Regular phishing simulation campaigns designed to educate and expose users to different types of phishing attacks.
- Report the phish for a chance to win a prize!
- See lsu.edu/phishing for more details.
Cybersecurity Awareness Month at LSU

• New content posted each Monday in October at lsu.edu/securityawareness
• Read the content, take the quiz, and play our geocache game!
Policy Updates

- 14 new IT Security Policies
  - Policies and standards support internal and external compliance requirements.
- Policy index available on GROK
- Policy FAQ coming soon
Policy Updates

- **Acceptable Use - PS 121**
  - Bring Your Own Device (BYOD): PS-121-ST-2
  - Software acquisitions: PS-121-ST-3
  - Data transmission: PS-121-ST-3

- **Data Management - PS 124**
  - PS-124-ST-2 Appendix A:

<table>
<thead>
<tr>
<th>Approved Storage Locations</th>
<th>Approved Secure Sharing Methods</th>
<th>Insecure storage/sharing Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSUAM Microsoft 365 environment</td>
<td>Encrypted Email</td>
<td>Regular email</td>
</tr>
<tr>
<td>ITS Datacenter</td>
<td>Filetoteaux</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>University provided Box* cloud storage solution</td>
<td>Box*</td>
<td>Social Networks</td>
</tr>
<tr>
<td>For physical material:</td>
<td>Office365 services</td>
<td>Personal Emails</td>
</tr>
<tr>
<td>- Locked filing cabinet, desk, or locked rooms with limited access</td>
<td>(OneDrive, Teams [Internal])</td>
<td></td>
</tr>
<tr>
<td>University owned encrypted end user computing devices or encrypted on-premises storage solutions supported by ITS and/or departments</td>
<td>Secure File Transfer Protocols, such as SFTP, HTTPS, FTPS, etc.</td>
<td>Unencrypted Computing devices – Personal or LSUAM owned (Laptops, Desktops, smartphones, tablets, etc.)</td>
</tr>
<tr>
<td>ITS offered integration services</td>
<td>Unencrypted removable media**</td>
<td>Personal Cloud storage services (Dropbox, Box, Google Drive, OneDrive)</td>
</tr>
</tbody>
</table>

*Box cannot be utilized to store health information, criminal justice information systems data, Payment Card Industry (PCI) data. **Removable media should only be utilized for data storage/sharing when other means are not available.
Additional Resources

- Cybersecurity Nuggets:
  - [https://moodle.lsu.edu/course/view.php?id=31855](https://moodle.lsu.edu/course/view.php?id=31855)
- LSU IT Policies and Index:
- Policy Exception Requests:
  - [https://itservice.lsu.edu/TDClient/30/Portal/Requests/ServiceDet?ID=875](https://itservice.lsu.edu/TDClient/30/Portal/Requests/ServiceDet?ID=875)
- Reporting a Phishing E-mail:
- Managing MFA Enrollment:
Questions?

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