Cyber Security Best Practices

Network

- Regularly back up data and verify its integrity. Ensure backups are not connected to the computers and networks they are backing up. For example, physically store them offline.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Employ best practices for use of RDP, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.
- Implement the least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write-access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Implement software restriction policies or other controls to prevent the execution of programs in common malware locations, such as temporary folders supporting popular internet browsers, and compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Categorize data based on organizational value, and implement physical and logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and network segment as an organization’s email environment.

Email Security

- Do not simply trust the name on an email: question the intent of the email content.
- If you receive a suspicious email with a link from a known contact, confirm the email is legitimate by calling or emailing the contact; do not reply directly to a suspicious email.
- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat how it is delivered, and trained on information security principles and techniques.
- Disable macro scripts from Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.

Web Activity Tips for Employees

- Check for misspellings or wrong domains within a link (e.g., if an address that should end in “.gov” ends in “.com” instead).
- Do not trust a website just because it has a lock icon or “https” in the browser address bar.
- Use virtualized environments to execute operating system environments or specific programs.
- Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall. For example, require users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.