Cyber Tips for Safety

Ransomware Defense Recommendations:

- The best defense against ransomware is scheduling regular data backups on drives not connected to the network, which can be used to restore a system to the backup version without paying the ransom.
- Paying the ransom funds illicit activity and emboldens the adversary.
- Paying the ransom does not guarantee the victim will receive the encryption key.
- However, when faced with an inability to function, administrators and executives will evaluate all options to protect their shareholders, employees, customers, students, and reputation.
- Evaluate of how much data/services are worth and plan accordingly.

Business Email Compromise Recommendations:

- **Use a secure email solution:** Email apps like Office 365 automatically flag and delete suspicious emails or alert you that the sender isn't verified. Then you can block certain senders and report emails as spam. Defender for Office 365 adds even more BEC prevention features like advanced phishing protection and suspicious forwarding detection.
- **Set up multifactor authentication (MFA):** Make your email harder to compromise by turning on multifactor authentication, which requires a code, PIN, or fingerprint to log in as well as your password.
- **Teach employees to spot warning signs:** Make sure everyone knows how to spot **phishing links**, a domain and email address mismatch, and other red flags. **Simulate a BEC scam so people recognize one when it happens**.
- **Set security defaults:** Administrators can tighten security requirements across the entire organization by requiring everyone to use MFA, challenging new or risky access with authentication, and forcing password resets if info is leaked.
- **Use email authentication tools:** Make your email harder to spoof by authenticating senders using Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).
- **Adopt a secure payment platform:** Consider switching from emailed invoices to a system specifically designed to authenticate payments.

Password Recommendations:

- **Make your password eight characters or longer.** Create a password with eight characters or more and a combination of letters, numbers, and symbols.
- **Use a long passphrase.** Use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.
- **Don't make passwords easy to guess.** Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
- **Avoid using common words in your password.** Instead, substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L".

- **Get creative.** Use phonetic replacements, such as “PH” instead of “F”. Or make deliberate, but obvious misspellings, such as “enjin” instead of “engine”.
- **Never share your password.** Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls.
- **Unique account, unique password.** Use different passwords for different accounts and devices so that if attackers do guess one password, they will not have access to all your accounts.
- **Use stronger authentication.** Always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username.

Miscellaneous Tips:

- www.ic3.gov (Internet Crime Complaint Center) takes complaints, conducts trend analysis, and disseminates information for public awareness.
- cywatch@fbi.gov (CyWatch) is the FBI’s 24-hour command center for cyber intrusion prevention and response operations.
- Safe Online Surfing Program: A free, fun, and informative program that promotes cyber citizenship by educating students in **third to eighth grade** on the essentials of online security (https://sos.fbi.gov)
- FBI Child ID App: An easy way for parents to electronically store their children’s pictures and vital information to have on hand in case their kids go missing (Download in the App Store or Google Play Store)