BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 22-094 **October 2022, Issue #87**

BusinesSafe Cybersecurity Awareness Month

October is Cybersecurity Awareness Month and this year's theme is "**See Yourself in Cyber**." Businesses can benefit from safety measures such as installing anti-virus software or hiring an IT professional to monitor and safeguard their network(s). While these measures are extremely helpful in thwarting attacks, any system connected to the internet may be vulnerable to external threats. Outside actors may gain access from actions as simple as a user clicking on a malicious link in a phishing email or by users forgetting to apply software security updates. Recognizing your role is a key component in protecting any computer network or device, whether it be personal or business. Additionally, including cybersecurity awareness training is an essential component of your cyber safety plan.

Cyberthreats

1. **Ransomware –** Ransomware is a type of cyberattack which can affect organizations, including small and midsized businesses. This type of cyberattack uses malware which allows cybercriminals to encrypt or lock a victim's files or systems. After encrypting the files, the cybercriminals will demand a ransom payment for the release of the files or affected systems. Cybercriminals will often threaten the release or sale of the information in an attempt to force the business or individual to pay the ransom. Ransomware can disrupt an organization's operations, cause financial losses and may even impact the organizations' customers and their business partners.
   Jackson Hospital IT thwarts ransomware attack
   Kronos hit with ransomware attack, could impact payroll for millions of employees globally

2. **Spear Phishing –** Spear phishing is a method which targets a specific individual or business through malicious emails. Unlike typical phishing which involves sending out mass emails to strangers in an attempt to scam as many as possible, spear phishing is methodical and the recipient has been researched by the cybercriminal. The email includes information specific to the target, which could include their name and position within the company and an attachment to be opened. Spear phishing is used to steal sensitive information, steal funds or to gain access to an individual's account, granting them access to the network and devices associated with that user.
   Scammer Stole $500 from Ocala, FL in Spear Phishing Attack
   Scammers trick City of Naples out of $700,000 in spear phishing cyber attack

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8563 Approval: FL8651, HSEC:1, 4, FSIN:1, 3.1, FFC:1, 4, 6.9

3. **Distributed-Denial-of-Service (DDoS)** – A DDoS attack is a cyberattack which attempts to disrupt the normal traffic of the targeted server, network or service by sending an overwhelming amount of internet traffic. This type of attack can render websites and systems inaccessible to external traffic, causing significant delays or disruptions to service.
   Teen arrested for 8 DDoS attacks that disrupted school's online classes
   DDoS and bot attacks in 2022: Business sectors at risk and how to defend

Mitigation strategies

- Organizations and individuals can enable Multi-Factor Authentication to create more secure logins.
- Simple and effective ways to protect yourself and your organization are to carefully review the email or phone number of the sender and vetting any unexpected or unusual requests.
- Organizations should require all employees to create strong and complex passwords.
- Employees should be trained to recognize and report phishing attempts.
- Organizations should ensure their software is routinely updated with the most current software and security patches.

Resources:

- The Cybersecurity and Infrastructure Security Agency (CISA) provides information and resources to assist organizations with participating in and learning more about Cybersecurity Awareness Month.
- Visit StopRansomware.gov for information and resources related to protecting your organization from ransomware attacks.
- The Federal Trade Commission offers information and reporting resources regarding How To Recognize and Avoid Phishing Scams and Cybersecurity for Small Businesses.
- For more cyber safety information or to schedule a free cybersecurity awareness training class, visit SecureFlorida.org.
- If you are the victim of a ransomware attack, contact your local Federal Bureau of Investigation field office, file a report with the FBI's Internet Crime Complaint Center and submit a report with CISA.
- You can also report computer-related crimes to your local law enforcement agency and the Florida Department of Law Enforcement.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8563 Approval: FL8651, HSEC:1, 4, FSIN:1, 3.1, FFC:1, 4, 6.9