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 21-127 **October 2021, Issue #62**

BusinesSafe Cybersecurity Awareness Month

October is Cybersecurity Awareness Month and this year's theme is "Do Your Part. #BeCyberSmart." Businesses and individuals can implement security measures to protect the network(s) and systems they use ranging from installing antivirus software to hiring information technology professionals. While instituting cyber protective measures can minimize the vulnerability and effects of cyberattacks, any network connected to the internet can still be vulnerable to external threats. These threats can gain access from something as simple as unintentionally clicking on a malicious link or forgetting to update or patch software. It is important to recognize the role individual users have when it comes to protecting any computer network, whether at work or at home, and include cyber security awareness training as a key component of your cyber safety plan.

Cyberthreats

1. **Ransomware –** Ransomware is one of the biggest cybersecurity issues that organizations, including small to midsized businesses, currently face. It is a form of malware that cybercriminals use to encrypt a victim's files or systems. After encrypting the files, cybercriminals will demand a ransom payment to restore access. Sometimes cybercriminals will also threaten to sell or leak stolen data or information if the ransom is not paid. Some of the most common ransomware attack methods are phishing emails, exploiting remote desktop protocol weaknesses, and taking advantage of software vulnerabilities. Ransomware can disrupt organizations' operations, cause financial losses, and may even impact other organizations connected to the network.
   Large Florida school district hit by ransomware attack
   Ransomware breach at Florida IT firm hits 200 businesses

2. **Phishing –** Phishing is one of the most common ways cybercriminals initiate their attacks. Cybercriminals will send emails or text messages that appear to come from a person or organization you know to trick you into giving up sensitive information or clicking on a malicious link. Protect yourself and your organization by carefully reviewing sender information and vetting any unexpected or unusual requests.
   Florida AG warns against scam that offers relief funds in exchange for personal info
   447,000 patients exposed after phishing attack on Florida practice

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us

Author: FL8642, Approval: FL8600, HSEC: 1, FSIN: 1.1.1, 1.1.2, 1.1.4, 1.2.1, 1.10, FFC: 1.1, 1.2, 1.3, 1.4

3. **Brute Force Attacks –** Brute force attacks are on the rise and are another common method that cybercriminals use gain access to computer networks. A brute force attack involves trying to crack the usernames and passwords of accounts through trial and error until a combination works. Cybercriminals can use automated software to conduct these attacks, and they can also use information from data breaches to supplement their efforts. Brute force attacks may lead to unauthorized access to computer networks, data theft, or paths to future cyberattacks.
   These systems are facing billions of attacks every month as hackers try to guess passwords
   30,000 Florida Blue Members Impacted by Brute Force Attack on Member Portal

Tips to Protect Yourself and Your Organization:

- Create strong passwords – Use passwords that have at least 15 characters with a combination of lowercase letters, uppercase letters, punctuation marks, and other symbols. Also, never share passwords - ensure that each user has their own log-in information.
- Do not click on unsolicited email links and attachments– The easiest way for someone to get unauthorized access to your network is for you to give it to them. Never click on email links and never download attached files unless they are from trusted sources. Reach out to verify their authenticity if you receive something unexpected.
- Know and follow your organization's information security policies - Your organization may have its own security rules on matters such as using USB drives, using personal devices on the network, or updating software. Follow these rules carefully.

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: FL8642, Approval: FL8600, HSEC: 1, FSIN: 1.1.1, 1.1.2, 1.1.4, 1.2.1, 1.10, FFC: 1.1, 1.2, 1.3, 1.4