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 23-071 **June 2023, Issue #107**

BusinesSafe: National Internet Safety Month

June is National Internet Safety Month, raising awareness of the risks of cyber threats and empowering Americans to be safe and secure online. Individuals can implement security measures to protect the network(s) and systems they use by installing antivirus software, and businesses can hire information technology professionals. While implementing protective measures can minimize the vulnerability and effects of cyberattacks, any network connected to the internet can still be vulnerable to external threats. Malicious actors can gain access to networks from something as simple as unintentionally clicking on a malicious link or forgetting to update software. It is important to recognize the role individual users play when it comes to protecting any computer network, whether at work or at home. Cybersecurity awareness training is a key component to your cyber safety plan.

Cyberthreats

There are many threats to an individual's or business's cyberspace. Some include:

1. **Ransomware:** Ransomware is one of the largest cybersecurity issues organizations currently face. It is a form of malware cybercriminals may use to encrypt a victims' files, systems, or networks. After encrypting, the cybercriminal will demand a ransom in exchange for a restoration of network access. 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 organizational operations, cause financial losses, and may impact other organizations connected to the network.
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 trusted person or organization. These messages are designed to deceive you into giving sensitive information or clicking on a malicious link. Businesses and individuals can protect themselves by carefully reviewing sender information and vetting any unexpected or unusual requests.
3. **Brute Force Attack:** A brute force attack is a method used by cybercriminals to gain access to computer networks. This type of attack involves trying to crack the usernames and passwords of accounts through trial and error until a combination grants access. To save time and effort, cybercriminals frequently use automated software to conduct these attacks. They can also use information from data breaches to supplement their efforts.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8888, Approval: FL8900 , HSEC: 1 FSIN: 1 FFC: 1

Brute force attacks may lead to unauthorized access to computer networks, data theft, or create paths for future cyberattacks.

How to Protect Yourself

1. **Turn on Multifactor Authentication.** A password is not enough to keep your online safety intact. By implementing a second layer of identification, you are giving yourself an extra layer of security. Multifactor authentication makes a user 99% less likely to get hacked online.
2. **Update Your Software.** Hackers will try to exploit software flaws and vulnerabilities. By regularly updating your software, cybercriminals will have more difficulty exploiting the security patches from the update. Automatic updates will make it easier to keep your online integrity strong.
3. **Think Before You Click.** More than 90% of successful cyberattacks begin by clicking on an unfamiliar link. If you do not recognize the link, do not click on the link.
4. **Use Strong Passwords.** A strong password has at least eight characters utilizing a combination of letters, numbers, and special characters. Avoid using the same password on various accounts. On top of this, the use of a password generator is encouraged.

Resources

- The Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS) offers additional information to keep you and your business safe online.
- Visit StopRansomware.gov for information and resources related to protecting your organization from ransomware attacks.
- Report computer crimes and cybersecurity incidents to the Florida Department of Law Enforcement (FDLE).
    - http://www.fdle.state.fl.us/FCCC/Report-a-Computer-Crime

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8888, Approval: FL8900 , HSEC: 1 FSIN: 1 FFC: 1