BUSINESSAFE

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 20-085 **April 2020, Issue #22**

BusinesSafe Threat Topic: Mobile Malware

Mobile malware is a form of malicious software developed specifically for mobile devices like cell phones and tablets. Although malware targeting traditional desktop or laptop devices is more prevalent, mobile devices can be attacked by malware as well. In fact, cybersecurity researchers reported that mobile malware attacks increased 50% in 2019 from the previous year.

As many adjust to working from home in response to the COVID-19 pandemic, more individuals are using mobile devices at an increased rate for telework, online education, entertainment, shopping, and communication. Cybercriminals have taken note of the increased dependence on and interaction with mobile devices and may seek to take advantage of this shift by deploying mobile malware in a variety of fashions.

- Banking trojans, for example, can be deployed as malware when illegitimate apps disguised as legitimate ones are installed on mobile devices and steal passwords and banking information. These trojans have become increasingly popular as individuals increasingly use mobile banking when managing finances.
  Ginp Banking Trojan Lures Android Users Amidst COVID-19 Outbreak
- Spyware is a form of malware that can be used to steal sensitive user information including log-in credentials, banking information, and internet usage data. Spyware may be downloaded unknowingly when users click a pop-up or download a malicious app.
  Coronavirus Scam Alert: COVID-19 Map Malware Can Spy On You Through Your Android Microphone And Camera
- Smishing attacks are phishing messages sent via SMS text message. These attacks continue to target users through social engineering tactics which trick users into providing sensitive information including log-in credentials and credit/debit card information.
  Watch Out! Scummy Scammers Target Home Deliveries

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1

Ways to Protect Yourself from Mobile Malware:

1. **Keep software updated.** Mobile device software is consistently being patched to address vulnerabilities. Ensuring that your device has the most recent update helps to protect it from malicious content.
2. **Download from official app stores.** Using official app stores, such as the Google Play Store or Apple Store, and downloading apps from trusted developers can help to ensure that the apps you download have been vetted and don’t contain malware.
3. **Install mobile antivirus software.** Mobile antivirus software works similarly to antivirus for your desktop. There are a number of free and paid antivirus apps available from trusted antivirus companies for mobile devices to scan your device for malicious content and prevent malware attacks.
4. **Check device settings.** If your mobile device is set to automatically join open Wi-Fi connections, you could connect to an unsecured network where your mobile device and data may be compromised. You can adjust Wi-Fi connection settings in your device’s settings menu.
5. **Consider using a VPN.** Virtual private networks (VPNs) allow private internet connection within a public or shared network. Using a VPN can give you secure access to your organization’s network while away from the office.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1