

Svpeng malware targets Android devices

Cybercriminals have begun targeting Android™ mobile devices with malware known as Svpeng Trojan. Liberty Bank is aware of Svpeng and other mobile malware and continues to evolve its defenses.

Know what you're up against

Svpeng infects a mobile device when a user unintentionally opens an attachment and downloads a piece of software. The virus then scans for mobile banking apps. It will also freeze the device until a ransom is paid to the cybercriminals. Once your device is infected Svpeng is difficult to remove, so it's important to know what to avoid and take steps to help protect your mobile device.

Recognize and avoid phishing attacks

Avoid becoming a victim by following safe Web browsing habits. Online attackers can make a deceptive e-mail message (phishing) look like a genuine communication from your bank, friends or family, tricking people into downloading malware or revealing their personal information. Some scammers even take over legitimate websites and lure surfers into downloading their malware.

Additional Protection to Consider

- Beware of malicious applications. Download apps only from trusted sources like the Apple® App Store or Google® Play.
- Avoid links from unknown sources. This includes emails and social media posts. Malicious links could direct you to websites or install applications compromising your device.
- Use trusted networks. Connecting your device to unknown wireless networks can expose your data. Avoid accessing sensitive information, like banking, if using an unsecured or unknown network.
- Turn off unnecessary services. Wi-Fi, Bluetooth, location apps, NFC (near field communication) apps and other connection abilities can be disabled to help protect your device when you're not using it.
- Avoid using tools not meant for your device. This can expose you to greater security risks.
- Secure your data and photos. Back up all important documents and photos to an external storage device, such as a cloud-based server, external hard drive or flash drive.

- Install and use anti-virus software and browser protection tools. Some devices, especially those running Android, support the use of anti-virus software that helps prevent bad applications from attacking your device. Browser protection products provide an additional layer of security to warn you about malicious websites. You can learn more about capabilities offered by individual mobile anti-virus vendors by visiting their websites.

What should I do if I see suspicious charges on my account?

Monitor your account(s) and review your monthly statements carefully. Notify Liberty Bank immediately if you see any unauthorized activity. Also, you can sign up for text alerts in online banking.