MOBILE DEVICE HACKING

Mobile device hacking is turning into the new target of scammers and identity thieves. Whether it's a smartphone, tablet or other mobile device, more and more people are using their mobile devices not just to store important personal information, but to do financial transactions such as shopping and banking. Smartphone users almost always have their phones with them and tend to answer calls and e-mails quickly. Unfortunately, this makes for a perfect storm when it comes to hacking into portable devices. They contain much information of value to scammers and identity thieves. They are easy to hack into and the owners of portable devices are not taking the steps to secure these devices as much as they would their computers.

TIPS

- Make the physical security of your mobile device a priority. Theft of the devices is an easy way to fall victim to identity theft.
- Protect your portable device with hard to guess passwords.
- Use encryption software and make sure that your device is kept up to date with the latest security software patches.
- Finally, one of the biggest threats to your security on your portable device comes from downloading malware through corrupted apps. Only download apps from legitimate sources and only download apps you are sure are safe. Also, whenever you download an app, pay attention to the permissions and services that are part of the app agreement. Do not give access to transmit data that is not necessary for the operation of the app.

PHONY POP-UP MESSAGES

Phishing is by far the easiest way to steal login credentials for accessing secure online accounts. Various types of phishing allow fraudsters to copy the login page of any bank and set up a fraudulent website. Then they create malicious email messages and send them to customers with links that lead to these fraudulent websites.

There is a new variation of phishing attacks called "*in-session phishing*," which targets online banking sessions through a pop-up window posing as a legitimate message from the Bank.

A typical scenario would be as follows:

A user logs into their online banking account.

They might leave the browser open and navigate in another window to other websites.

A short time later a pop-up appears, allegedly from the bank, asking the user to retype their username and password because the session has expired, or to complete a satisfaction survey.

Since the user had already logged into the website, they don't suspect this pop-up is fraudulent and provide the requested details.

In order for "in-session" attacks to work, the following is required:

1.) A base website must be compromised from which the attack can be launched.

2.) The malware, which injected the compromised website, must be able to identify which website the user is logged into.

The first requirement is easier to achieve, since so many websites are compromised by criminals. Once a website is compromised, code is injected into the website, showing no difference in appearance on the website making it very hard to detect.

The second is harder to achieve, but not impossible. Once the compromised website identifies a website to which the user is logged on, it can inject a pop-up message in the browser pretending to be from the legitimate website and ask for credentials and private information. If the user enters their credentials in the phony pop-up, the phisher then steals the login information.

Since this is a browser based attack, the best way to defend against this is to be aware and practice browser security.

Users should:

- Be suspicious of unprompted pop-up windows that appear without clicking on a hyperlink.
- Deploy browser security tools and set security settings to disallow pop-ups and certain scripts from running.
- Always log out of online banking and other sensitive online applications and accounts before going to other websites, so that the sessions do not remain active.

PHONY TEXT MESSAGES

Smishing is similar to phishing on your computer, but this time the scammers message comes as a text message on your cell phone. Often it comes purportedly from your bank telling you that your account has been frozen for security reasons. The text instructs you to call a hotline. The phone number connects you to an automated response system which asks you to provide personal information or your account will remain frozen. This is enough information for thieves to create counterfeit cards and commit fraud. Smishing is also used by scammers, particularly during the holidays to appear to provide free coupons.

TIPS

Never respond to an unsolicited message. By doing so you only succeed in telling the scammer that you are out there. Never provide personal information in response to a text message from anyone. If you believe the message may be legitimate, contact the entity at a telephone number or website that you know is accurate. Don't download coupons from emails or text messages. Again, if you think it may be legitimate, go to the website of the company that you know is legitimate and download the coupons there.