HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #3 - Issue #98
March 10th, 2017

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Why You Should NEVER Charge Your Smartphone in a Public Port

A smartphone with a low battery is a real problem, especially when you are on the go. In such scenario, finding a USB port installed somewhere or charging facility at public outlets seems to be a blessing. Public charging ports are installed almost everywhere for the users and visitors convenience such as at airports, conference centers, cafes, parks and planes, etc. All you need to do is plug in your cell phone and feel relaxed and relieved. However, Drew Paik from IT security security firm Authentic8 told CNN that this is a very dangerous thing to do because the outlet might be hacked and all the data present in your phone could easily be transferred to a hacker.

Authentic8 is the developer of Silo web browser that facilitates anonymous web surfing. The revelation from Paik is surprising and concerning as he states that simply through plugging in your phone into a hacked charger or power strip would lead to getting your device infected at once and all your data will also be compromised. The reason is that the cord used to plug in your mobile phone is also used for sending data to and from the device.

For example, if you connect your iPhone to your Mac device using the same charging cord, you can easily transfer images and music from your mobile to your Mac. Hence, through compromising this particular cord, a hacker can extract all sorts of data from your mobile including pictures, emails, contact numbers, SMS messages, etc., without your knowledge obviously.

This kind of hacking is called “**Juice Jacking**“, which was a term created by security researchers in 2011 and this was followed by the creation of another term called “**Video Jacking**“, which was introduced in 2016. This referred to phone’s ability to record everything that you typed or looked at due to being compromised by a hacked port.

The findings of the research were demonstrated by Authentic8 at the RSA security conference held in San Francisco. The company installed a charging station at its stall and offered to charge cords to visitors so that

they could charge their devices. Then the security firm ran a social experiment to analyze the number of people who used this charging service, which turned out to be quite overwhelming with over 80% of the audience using the charging facility provided by Authentic8. Paik noted that none of these visitors seemed to care about the security aspect of charging mobiles from a public station despite the fact that they were attending a security conference.

The repercussions are various and diverse, and we recommend that instead of putting your data in danger, you should carry your own charger or invest in portable USB battery pack. The bottom line is that, if you are concerned about the security of your phone's data, it is better to stop using public ports at all.

This Week's Cyber Alerts:

Alert Issued 3/9/17: Secure' Messaging App Riddled with Security Flaws

Alert Issued 3/8/17: Firefox Kills Plugins – except Flash – and Runs up a Red Flag for HTTP

Alert Issued 3/8/17: Fake Facebook Lite App Infected with Trojan to Steal Users' Info

Alert Issued 3/7/17: Twitter Vulnerability Allowed Hackers to Access Locked Accounts

Alert Issued 3/3/17: Android Password Manager You Trust Could be Exposing Login Data

Alert Issued 3/3/17: 32 Million Yahoo Accounts Accessed via Cookie Forging Attack

Alert Issued 3/1/17: [Cloudpets Toys Leak Kid, Adult User Info, Voice Recordings]

Next Week's Newsletter Will Cover:
Pros and Cons of Using PayPal

Th[redacted]e have shared will make your online life a little easier.

Home Cyber Defense Weekly
is a service of
House of File Technologies