Cellphone Chaos

Recent headlines have been filled with mobile security concerns. This month's newsletter explores issues related to cell phones and provides information and advice from our our Cybersecurity professional, Simmer Principio.

Now that everyone is walking around with data in their pockets, mobile security is more important than ever! Follow good mobile security habits to keep your information protected.

Juice jacking

It's common to see USB phone charging stations at events, hotels and airports. This has led to an uptick in **juice jacking**. Juice jacking is when cybercriminals infect your device with malware or steal your data and track you.

This happens through a simple process. The power supply and data stream pass through the same cable, which cybercriminals can easily exploit during the charging process. The USB cord opens a pathway in your device, potentially allowing an attacker to install malware or track your keystrokes.This threat isn't widespread yet, but it's gaining traction.

Our Cybersecurity professional, Simmer Principio, has a few quick tips to protect yourself against this threat.

- **Avoid public charging stations.** Plan ahead by charging your phone in a secure spot like at home, your car or your own portable charging device.
- If it is necessary to charge your phone on the go, **be prepared.** Bring your own external battery and cords. Bring other necessary charging items such as a regular AC wall outlet plug. Data can not transfer through a typical wall outlet.
- **Lock your phone while charging.** If it is absolutely necessary to use a public charging station, lock down or power off your device. This will prevent any possible pairing with other devices in the area.
- If you receive a pop up to "share data" or "charge only" when plugging your phone into a USB charging station, **always choose "charge only."**

Public Wi-Fi

When using public Wi-Fi, you send data across a network controlled by someone else. Hackers use Wi-Fi hotspots to lure users onto their own networks and steal their information. Never do anything with sensitive data on an open wireless network!

Check your connection settings and turn off "auto-connect to Wi-Fi." This will ensure that you don't accidentally connect to an open, possibly dangerous Wi-Fi network.

Encryption

Encryption is the process of turning your information and data into a code that is unreadable to anyone else. This prevents unauthorized users from accessing your data.

Use your organization's approved VPN provider on work devices. A VPN creates a secure tunnel that encrypts all of your internet traffic, keeping you and your organization safe from hackers.

Recent Android vulnerability

A new malware named Goldoson has made its way into more than 60 legitimate apps on the Google Play Store and onto millions of phones.

Google has confirmed that most of the affected apps have been cleaned by developers. Additionally, they have removed others from their Google Play Store who have not complied with their policies.

It is critical to keep your apps up to date to stay on top of security patches. But in the unfortunate circumstance that your devices becomes infected with malware, here are some common warning signs:

- Device heating up
- Battery draining quickly
- Unusually high internet data usage even when the device is not in use

Cybersecurity roles — Cloud security

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

Cloud security engineer

A cloud security engineer is responsible for ensuring the security and protection of computer systems deployed in cloud environments. They focus on safeguarding data and applications that are stored in cloud-based applications, which are accessible from anywhere through the internet.

The role of a cloud security engineer is to implement measures that prevent unauthorized access, data breaches, and cyberattacks. As more organizations utilize cloud-based services, this role is becoming increasingly important.