Cybersecurity Health Check

Catch of the Quarter
Mobile device attacks occur approximately every 39 seconds.
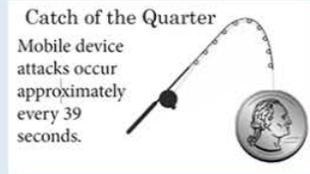
Mobile Security

It is not an understatement to say that cell phones have transformed nearly every aspect of our lives. The increased use and utility since the genesis of this technology have made this device less of a phone and more of a portal to the world around us. This connection, however, is a two way street. This means that bad actors are equally as able to reach and exploit us. With that in mind, it is of the utmost importance to arm ourselves with knowledge of the types of different threats our cell phones pose and how best to protect ourselves.

Be mindful of the following **threats:**

> **Mobile Malware**: Malicious programs such as spyware, trojans and ransomware are built to specifically target operating systems (Android, iOS, etc.). These can originate from compromised application downloads, infected links, and network based attacks.

> **Ransomware:** Yes! Ransomware is a type of malware, but often times when we hear about it, it is in regards to corporate attacks, however, we are all susceptible to this. Individuals can have files or directories encrypted to lock them out of their phones only to be blackmailed later for payment. Always be sure to update your smartphone to its latest firmware version to lessen the chance of becoming a victim.

> **The "ishings"**: As always, be on the lookout for phishing (email), vishing (phone) and smishing (SMS messaging). One device, three threats! Always be suspicious of unsolicited communications and verify senders. And never divulge any personal information without being 100% sure the recipient is authorized to have it!

> **Outdated OS and Apps:** Neglecting to update your operating system (OS) or applications may seem inconsequential, but it is not. Old OS versions and apps that have not been updated can be missing crucial security patches that protect from known vulnerabilities.

> **Unsecured Public WiFi**: One of the most common vulnerabilities we see. Many open and free public WiFi networks exist for public use and convenience. The problem is when bad actors simulate one of these networks for an individual to unwittingly connect. The end result more often than not is a man in the middle (MiTM) attack on the user.

> **SIM Hijacking**: SIM swapping or SIM porting are other names for SIM hijacking. Changing your SIM is actually a legitimate service required by telecom companies when customers need to swap their SIM and telephone number between operators or devices. The hijack comes in when bad actors pose as you to get a company to transfer your number to one of their SIM cards. In order to do so, they need personal information about you, often gleaned from social media. In this way, this is a targeted attack.

Checklist

THE UNSTOPPABLE FORCE   THE UNBREAKABLE OBJECT
IRRESISTIBLE FORCE PARADOX
A whole new dimension
Chuck Norris runs on 6G.

☑ As always, I exercise caution when clicking on links or opening email attachments and have reviewed SSA's resources on social engineering.

☑ I have reviewed SSA's Information Security Policy (ISP) section 3.1.6 on Wireless Technology and it's subsections.

☑ I have reviewed this NSA Infographic detailing Mobile Device Best Practices.

☑ When possible, I avoid using public WiFi networks.

☑ If I must use a public WiFi, I use a VPN.

Dad Joke(s) of the Quarter:

Q: "What happens when you cross an iron and a cell phone?"

A: "You get a smooth signal

Q: "How does a pirate communicate?"

A: "With his aye phone."
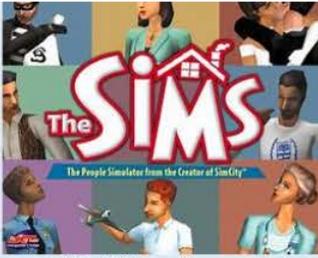
What SIM used to mean!

☑ I approach all unsolicited communication with extreme caution.

☑ I keep all of my apps and operating systems up-to-date.

☑ I use multifactor authentication (MFA) when accessing my accounts. Learn more about MFA and password security from our prior Cybersecurity Tip of the Month.

Q: "What happened when I connected my phone to the cloud?"

A: "I had a bunch of mist calls."

Want to know more about a topic? Have a topic suggestion for the next health check? Complete OIS' survey to let us know!

Thanks,
Office of Information Security

Like the information in this health check? Let us know by selecting the smile face or frown face link.

☺ ☹