SecurityAwarenessNews

the security awareness newsletter for security aware people

The Computer in Your Pocket

Cybercriminals are opportunists. While they'd love to launch a single attack that results in a huge payday, their livelihood relies on pushing big numbers. The more scams they can distribute, the better their chances of finding success.

Enter mobile devices — the largest attack surface in existence. Cybercriminals have shifted their focus to smartphones and tablets thanks to a combination of three factors: quantity, access, and vulnerability.

Quantity

According to Statista.com, active smartphone subscriptions topped 6.7 billion in 2023. In 2016, that number was 3.5 billion, which showcases just how much this attack surface has grown in a short period of time.

Access

Mobile devices have access to an abundance of confidential information. Most people use dozens of apps for both work and personal reasons. It's not difficult to imagine the damage an attacker could cause if they successfully compromise someone's device.

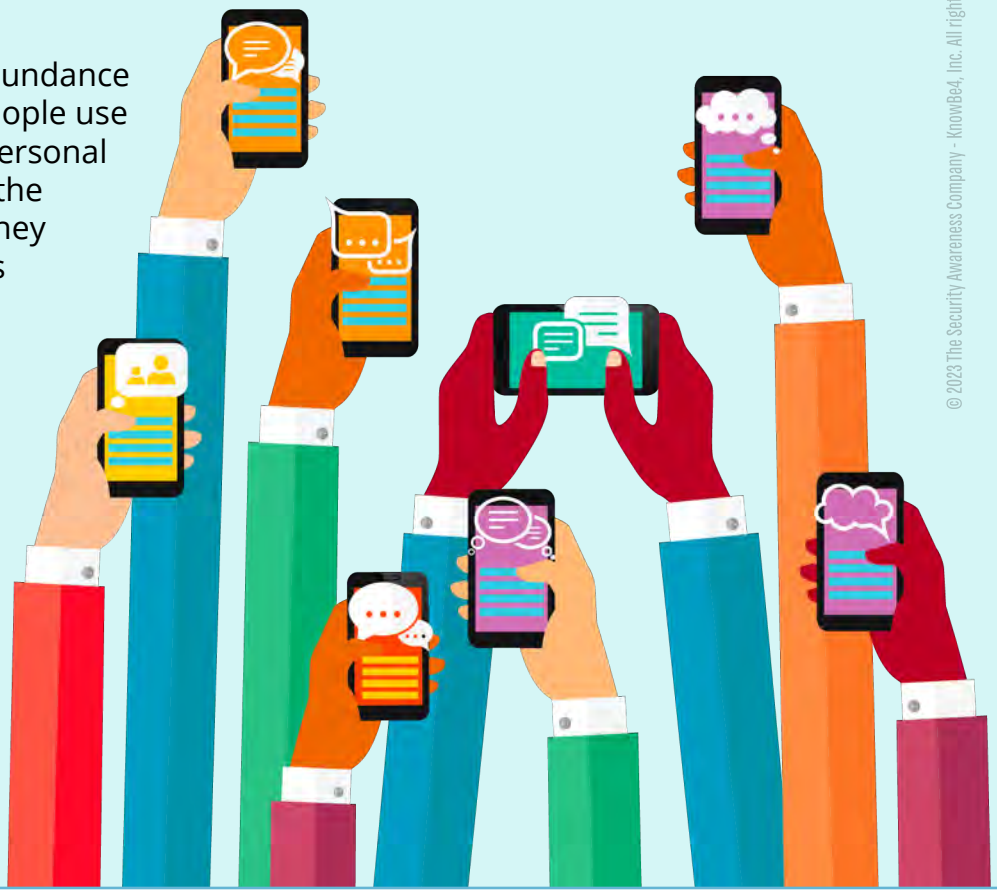
Vulnerability

Like desktop computers, mobile devices are just as susceptible to malware (malicious software) infections and other dangerous vulnerabilities. There's also the physical threat of losing a device or having it stolen, which is an additional security concern.

The combination of those three factors makes it easy to understand the mobilization of cybercrime over the years. To make matters worse, it's easy for scammers to discover people's phone numbers and use them to launch a variety of personalized attacks.

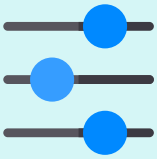
The fact is, modern smartphones come equipped with impressive amounts of power and accessibility. They also place a tremendous amount of confidential data in a dangerous location: everywhere you go.

Smartphones, after all, are the computer in your pocket (or clipped onto your belt, if that's your style). As such, they require the same level of security controls as any desktop or laptop computer. So, keep your mobile devices safe by staying alert, using situational awareness, and thinking before clicking.



Top 5 Smartphone Security Fundamentals

Protecting smartphones is a vital part of maintaining security, both at home and at work. To make that process simple, adhere to these five smartphone security fundamentals:



Manage App Permissions

Mobile applications need to be granted various permissions in order to function, but even legitimate apps sometimes request more permissions than necessary. For example, why would a music player app need to access your contacts or pictures? Always take note of those situations to prevent apps from accessing more data or personal information than needed.

Prioritize Physical Security

Not only should smartphones be protected with a unique PIN or code, it's also a good idea to have the screen automatically lock after a few seconds. Even better, lock it immediately when you're done with it or before putting it down. That way, if someone steals your phone, they won't get access to any information stored on it without knowing the passcode.

Beware of Malicious Apps

Malicious applications steal data and spread malware. You can avoid them by only installing apps from legitimate app stores and developers. A way to tell if an app is trustworthy is by checking out its reviews and total downloads. One with millions of downloads and thousands of reviews is most likely legitimate.

Enable Find My Device Services

Most modern phones offer "find my device" services. If you lose your phone, use a second device to locate your phone via an online map or prompt it to ring. If you determine that the phone has been stolen or is not recoverable, you can use the erase function to completely remove all personal information and reset the device to factory settings.

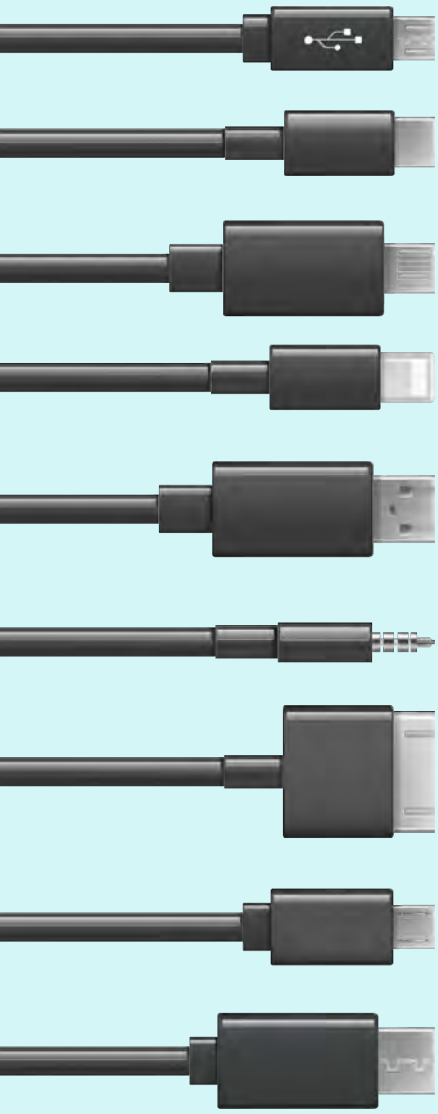
Keep it Updated

Updates are often issued to address crucial security concerns. By keeping your phone and all apps on the latest versions, you avoid potential threats associated with outdated software. Ideally, enable automatic updates so you never miss an important fix. It's also a good idea to occasionally review the apps you have installed and remove any you no longer need.

For work-issued devices, always follow policies for which apps you're allowed to install, when to run updates, and anything else required by your organization.

Mobile Attack Methods

While the methods cybercriminals use evolve with technology, there are a few common attacks worthy of everyone's attention. Let's quickly review what those are and how to avoid them.



Voice Phishing

Voice phishing is a scam where the attacker contacts someone over the phone and tries to con them into surrendering confidential information. They often impersonate someone the target is familiar with. For example, they might pretend to be a bank representative who needs you to confirm your account information.

Avoid assuming someone is who they claim to be, regardless of how they contact you.

Messaging

It's important to remember mobile devices are just as susceptible to malicious infections as desktop computers and laptops. That's why attackers use various services and apps to send messages containing links. Opening the link on a phone could infect it with data-stealing malware.

Never open suspicious links or respond to random messages.

QR Codes

QR codes (quick-response codes) are a type of barcode that can be easily read by smartphones and tablets. They're simple to create and distribute in both the physical and digital domains. Scanning a malicious QR code could yield similar results to opening a phishing link in an email or text message.

As a general rule, it's best to avoid scanning QR codes when possible.

Applications

The most popular app stores implement robust security processes to prevent cybercriminals from uploading malicious apps. Unfortunately, thousands still get through and end up on mobile devices. Banking trojans represent a common example. They steal login credentials and can give the attacker access to financial information.

Remain cautious and selective regarding which apps you install.

Charging Cables

Cybercriminals have a history of leaving infected USB flash drives in public places, which provides a simple way to spread malicious software to computers. They can also use USB charging cables to remotely attack mobile devices, install malware, or steal confidential information.

Only use the USB cables you own; never plug in a random cable.