5 Dangerous Mobile Security Breaches That Could Happen to Anyone

From malware to phishing and jailbreaking, there are several mobile security breaches that everyone should be aware of, as they can happen to anyone who owns a smartphone.

The experts at **SOAX** discuss five common mobile security threats with advice on how to stop them from happening.

Malicious Apps and Websites

Malicious apps and websites can achieve the same results as they would on a desktop computer.

These dangerous sites and apps can steal your data, encrypt your data, or activate spyware. The most common types of malicious apps and websites to look out for are trojans that perform ad and click scams.

In 2020, Uber lost over $100 million of its advertising spend to an ad and click scam, about a third of their advertising budget at the time.

There are various ad-blockers and click fraud detection tools available for mobile devices, such as ClickGUARD, TrafficGuard and AppsFlyer. You should only click ads that come from trusted websites and sources. If you are unsure, close the page.

Mobile Ransomware

Mobile ransomware is an extremely malicious security threat that can particularly target phones used for work and business.

Mobile ransomware encrypts important files on a mobile device and then requires a ransom payment to restore access to the encrypted data. This can infect your device from malicious websites, phishing attacks or compromised websites.

To avoid this, always download files from trusted sources, use security software if possible and regularly update your phone's operating system. These updates usually come with added security measures to prevent these attacks.

Phishing

Phishing is one of the most common cyberattacks in existence with over 323,000 peoplefalling victim to these attacks annually second only to malware. Phishing comes in the form of a malicious link or attachment containing malware.

This can be done through messaging services such as emails, SMS messaging or social media, which makes it so common to fall for if the message is convincingly written.

Whilst many associate phishing with malicious emails, they're not the most commonly used platform for phishing on mobiles. Emails account for just 15% of phishing attacks, whereas SMS and social media messaging is much higher.

To avoid falling victim to a phishing scam, never click on links or download attachments sent to you from unknown email addresses or phone numbers. Even if it comes from someone you know through social media, be vigilant and contact the person before doing anything, as their accounts could have been compromised.

Man-in-the-Middle Attacks

Man-in-the-middle (MitM) attacks involve a cyber attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. Mobiles are especially vulnerable to MitM attacks as SMS messages can be more easily intercepted.

This is especially prominent if you're connected to an untrusted or compromised network. This could be a public wi-fi service or a compromised cellular network.

If you are connected to a public wi-fi network, never send or share sensitive information and ensure that the network is safe and can be trusted. If you notice your phone's cellular network changes, contact your network provider immediately.

Advanced Jailbreaking and Rooting

Jailbreaking and rooting are terms for attackers gaining administrator access to IOS and Android devices. These attacks take advantage of the vulnerabilities in the mobile operating system to achieve root access to the device.

Rooting an Android device or jailbreaking an iOS device involves bypassing the built-in security mechanisms, enabling the installation of unauthorised apps and the modification of system files. While some users may be tempted to jailbreak or root their devices for customisation or app compatibility reasons, it poses risks to the security of the device.

Jailbreaking your device for whatever reason is not recommended, as it makes the device much easier to attack.