MOBILE MALWARE HAS INCREASED BY 500% - WHAT SHOULD YOU DO?

Cybersecurity researchers uncovered an alarming mobile statistic. During the first few months of 2022, mobile malware attacks surged by 500%.

For years, mobile phones have become more powerful. They now do many of the same functions as a computer. Yet, people tend to secure their computers better than they do their smartphones.

This is a behaviour that needs to change. Over 60% of digital fraud now occurs through mobile devices.

That makes them highly risky if proper safeguards aren't followed.

Use Mobile Anti-malware

Yes, your mobile phone needs antivirus/anti-malware too!
Malware can and does infect smartphones and tablets. Ensure that you have a reliable mobile anti-malware app installed.

Don't download Apps from unknown sources

Only download mobile apps from trusted sources. Do not download outside a main app store. Trusted app stores include places like:

- Apple App Store
- Google Play
- The Microsoft Store
- Amazon Appstore

Don't Assume Email is Safe

Many people prefer checking emails on their phone rather than on a PC because it's so handy. But they have a false sense of security about the safety of emails when viewed on a mobile device.

It's difficult to hover over a link without clicking when on a smartphone. If you see something questionable and want to check the link, open the email on your PC where you can do that.

Beware of SMS Phishing (aka"Smishing")

In March of 2022, text spam outpaced robocalls. Unwanted text messages rose by 30%, ten percent higher than robocalls. Many of those spam texts are smashing.

Be on the lookout for text messages that don't quite make sense.

For example, getting a shipping notification when you haven't ordered anything.

Remove Old Apps You No Longer User

Go through your device and remove old applications that you are no longer using.

There is no reason to keep them around, potentially leaving your the device at risk.

Keep Your Device Updated

Speaking of updates, you also need to keep your device's operating system updated. Are you using the current version of Android or iOS? Not installing updates can mean your phone has vulnerabilities. These vulnerabilities allow hackers to breach your data.

Use a VPN When on Public Wi-Fi

Public Wi-Fi is dangerous. Most people understand that, but many connect to it out of necessity.
Reduce your risk by using a VPN app.

Mobile Security Solutions to Prevent a Data Breach

Don't wait until your phone is infected with malware to secure it properly. It's only a matter of time before you are the next victim.

TRENDS IN DATA PRIVACY THAT MAY IMPACT YOUR COMPLIANCE

Data privacy has been a growing requirement ever since the internet age began. So much personal information is flying around through computer networks. Protecting it has become a mandate.

By the end of 2024, 75% of the world's population will have their personal data protected. It will fall under one or more privacy regulations. Privacy requirements hit all sized companies.

AI Governance

AI is running many of the algorithms responsible for keeping data protected. But what happens when there is a problem with the AI? This is the question that AI governance is working to address.

Consumer Privacy UX

A trend that we've seen over the last several months is putting more privacy power into the consumer's hands. Consumer privacy portals tell people what data is being collected, how it is collected, and what is done with it.

Increased Scrutiny of Remote Employee Monitoring

Monitoring remote employees opens a can of worms when it comes to data privacy.

Organizations need to ensure that they aren't encroaching on the rights of their staff.

Data Localization

Increasingly, organizations look at where their cloud data is being stored because the location governs the privacy rules and regulations that it may fall under.

Privacy-Enhancing Computation (PEC)

Data privacy by design is a fairly new term. Using privacy-enhancing computation is a way that AI is helping cybersecurity.

By using PEC as a built-in component of software and apps, developers provide value to clients. They address privacy concerns by making data protection more automated.

HAVE YOU HAD DATA EXPOSED IN A RECENT DATA BREACH

There's a reason that browsers like Edge have added breached password notifications. Data breaches are an unfortunate part of life. And can have costly consequences for individuals. Hackers can steal identities and compromise bank accounts, just to name a couple.

Cybercriminals breach about 4,800 websites every month with form jacking code. It has become all too common to hear of a large hotel chain or social media company exposing customer data.

Microsoft Customer Data Breach
5 Million Records Exposed in a Student Loan Breach
U-Haul Data Breach of 2.2 Million Individuals' Data
Neopets Breach May Have Compromised 69 Million Accounts
One Employee Computer Causes a Marriott Breach
Shield Health Care Group Exposes Up to 2 Million Records

01303 813700
www.iconology.co.uk
contact@iconology.co.uk
Iconology Ltd, The Oak, Ashford Road, Newingreen, Hythe, Kent,CT21 4JB