

THE GROWING THREAT OF SMARTPHONE HACKERS

MOBILE MALWARE

& WHAT YOU NEED TO KNOW



Do you think it's safe to access sensitive data on your **mobile phone**? Perhaps you should think again. With **malicious programs** designed to target cell phones skyrocketing, it's becoming increasingly **dangerous** to use your phone without the necessary **precautions**. Here's how to prevent malware from taking over your phone . . . and your life.

WHAT IS MOBILE MALWARE?



Malware is software with a malicious purpose. It may be designed to disable your phone, remotely control your device, or steal valuable information. Mobile malware uses the same techniques as PC malware to infect mobile devices.



The Real Dangers of Malware



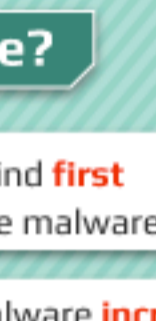
HOW MOBILE DEVICES ARE AFFECTED



Smartphones are mini computers that are being used for many of the same functions as traditional PCs – connecting to the Internet, banking, and more.

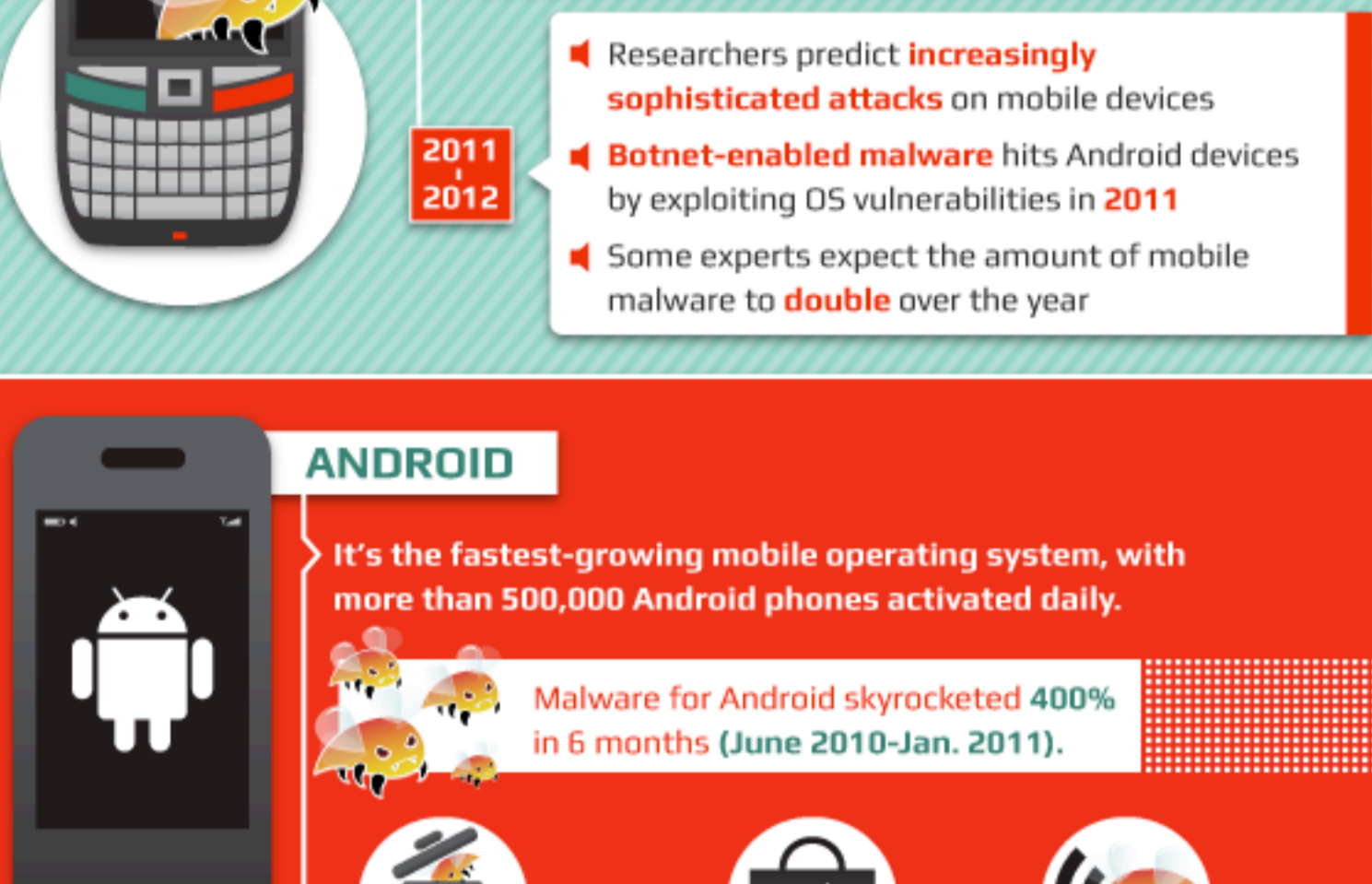


Like computers, smartphones are also vulnerable to hacking, malware, and viruses.



Considering that **35%** of American adults own smartphones, the devices are becoming a rich potential target for hackers and malware developers!

What's Lurking on Your Phone?



ANDROID

It's the fastest-growing mobile operating system, with more than 500,000 Android phones activated daily.

Malware for Android skyrocketed **400%** in 6 months (June 2010-Jan. 2011).

- More than **80** infected apps had been removed from the official Android Market by June 2011.
- Fake versions of popular games and apps were infected with malicious code.
- Several spoofed applications were botnet-enabled, allowing an attacker to remotely control the infected phone.

ANDROID MALWARE HAS AFFECTED UP TO 250,000 USERS

BLACKBERRY

Targeted in the 2010 **BY ZEUS BANK INFO ATTACKS**.

These suffer predominantly from spyware applications.

SYMBIAN & MICROSOFT WINDOWS MOBILE

Devices running these operating systems have been targets of the **MOST PROLIFIC AND EFFECTIVE** malware known to affect mobile devices.

WINDOWS MOBILE AND SYMBIAN ARE THE TWO OLDEST AND MOST RESEARCHED MOBILE PLATFORMS.

iOS (iPhone & iPad)

Many legit iPhone and iPad apps leak personal data to third parties.

10% of iPhone users use **0000** or **1234** as their password, making it easy to hack the device.

Jailbreaking puts iPhone users at risk for downloading infected or fake apps.

Jailbreaking techniques usually leave the device with a standard root password that may grant device admin-level access to an attacker.

In 2011, A HACKER PLEADS GUILTY TO STEALING DATA FROM MORE THAN 100,000 iPad USERS.

HOW THEY GET YOU

PHISHING

A fake version of a real site gathers your log-in and other private information.

APP STORES

Copies of legit apps are infected with malicious code and placed in official app stores.

THIRD-PARTY ONLINE APPLICATION REPOSITORIES

Unofficial websites where users can freely download applications. They are a general threat since there is **no control** on what applications are made available.

MAN-IN-THE-MIDDLE ATTACKS

Any mobile device that connects to a **Wi-Fi network** is open to this type of attack.



WI-FI SNOOPING

Can occur when you access a **public network** at any hot spot. An attacker can easily "watch" your online activities and access your private information.

90% of all mobile devices will be Wi-Fi enabled by 2014.

87% of smartphone owners access the Internet or email on their device, including 2/3 who do so on a typical day.

ALL OF THESE MOBILE DEVICES ARE IN DANGER OF CONTRACTING MALWARE.

SPYWARE

Silently collects information from users and sends it to eavesdroppers.

EXPLOITING

Some malware will exploit mobile platform vulnerabilities to gain control of the device.

WORM

A program that replicates itself, spreading throughout a network.

TROJAN

A program (or app) that seems to be legit, but is really **malicious**.

DIRECT ATTACK

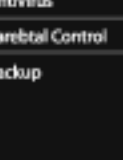
Comes from **files or viruses** sent right to your cell phone. **SMS text messages** can contain viruses. **Viruses** can send requests for **Bluetooth connections** in order to spread.

CAUTION! **DANGER!**

PROTECT YOUR MOBILE DEVICE



53% of users say that they are **unaware of security software** for smartphones.



24% of mobile users **bank from a phone**, yet most don't have security measures in place.

DO

- Make sure the **OS and software** are up to date at all times
- Download apps from **reputable sites** and closely review app permission requests
- Make sure to **check the feedback** from other users before installing the program from an app store
- Use a **strong, complex password**
- Use a **personal firewall**
- Turn off **Bluetooth** and other connections when not in use
- Install a **mobile security app**

DON'T

- Download apps from **third-party application repositories**
- Jailbreak your phone
- Leave your "Wi-Fi ad-hoc mode" on
- Access **banking or shopping sites** over a public Wi-Fi connection
- Leave your mobile device **unattended** in public places