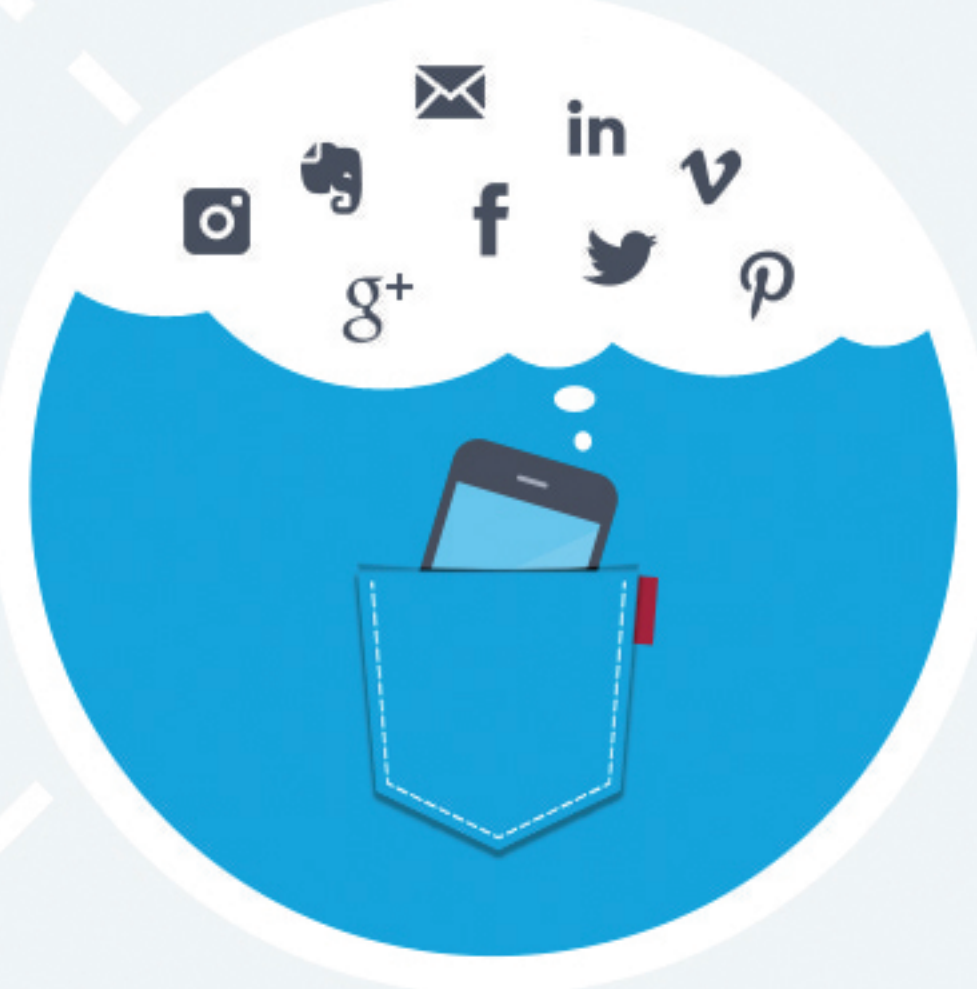
ENJOY SAFER TECHNOLOGY®

It doesn’t hurt to know...

(about Android malware)

Android is the most popular mobile platform

with nearly **2 MILLION** apps and games, more than **150 BILLION** app downloads and **1.4 BILLION** device activations.
(Source: Google™; AppAnnie)



Whole world in your pocket

Stored images, documents, passwords, synced applications, personal notes, locations, contacts, text messages, emails and social network data—you carry it all with you.

Users overlook security

Hundreds of millions of users overlook security despite having personal information stored on their Android devices.

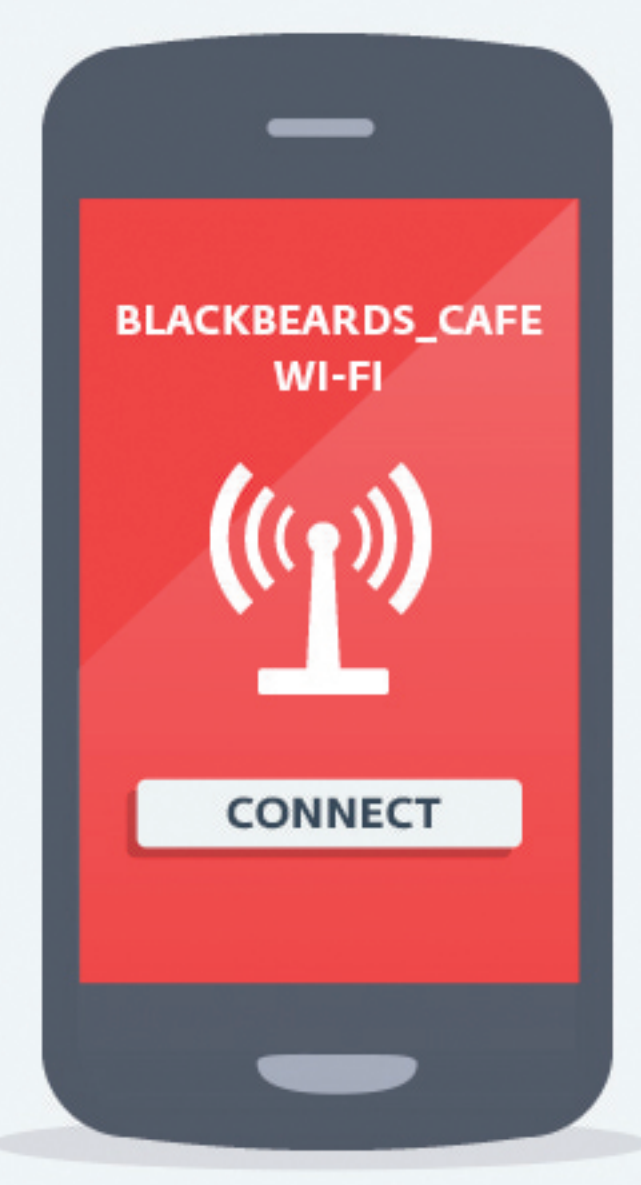
What is targeting your Android?

Ransomware is any type of malicious software that takes something valuable from its victim and demands money before it “releases” that resource. Depending on the type of malware, this might be access to a device or data stored on it.

SMS Trojans and dialers—dubbed jointly **GSM Trojans**—are known for calling or sending SMS text messages to paid numbers, without the victim knowing, thus inflating user’s phone bill.

Spyware looks for emails, text messages, contacts and locations on the user’s device and sends them to the attacker. It can also hijack the device’s camera or microphone and secretly live stream audio or video of everything the user does.

When to use extra caution?

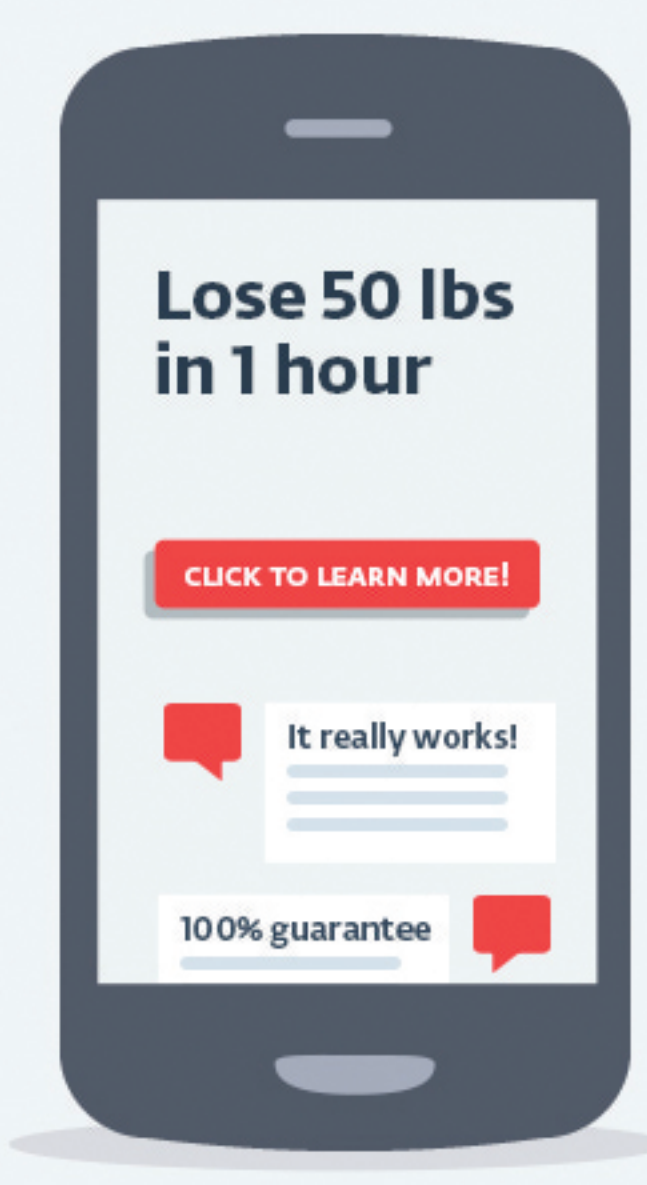


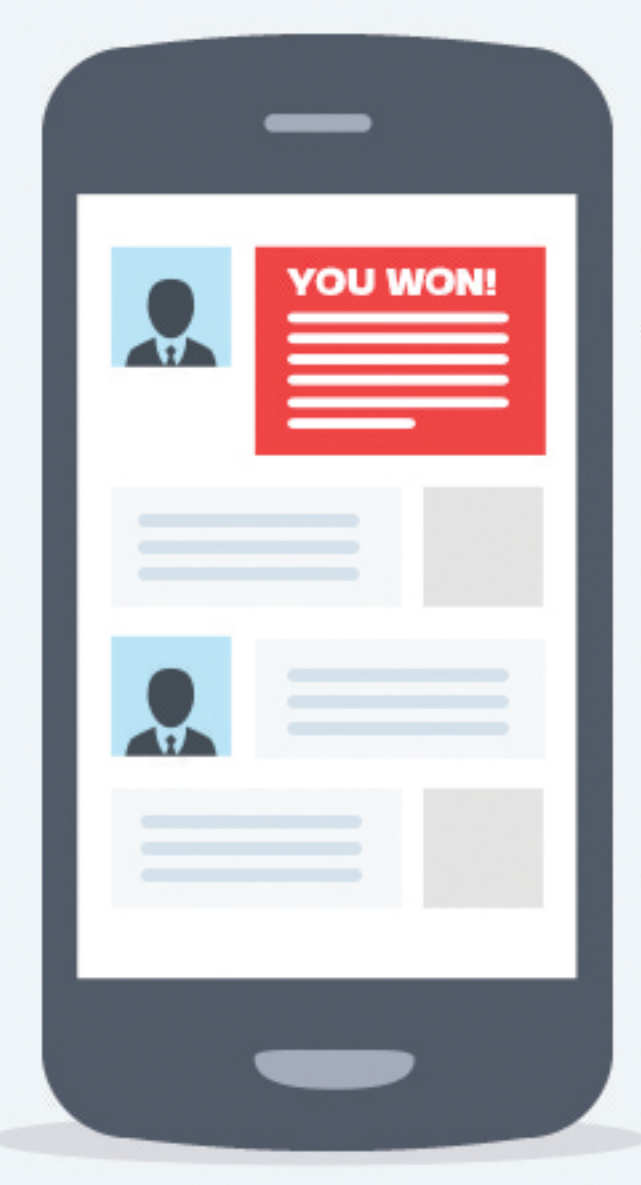
When you connect to unsecured Wi-Fi at your favorite coffee shop

Because it could be a way for attackers to get into your phone.

When you visit sketchy websites

Because you simply can't lose 50 lbs in one hour. And clicking the link could land you in a place that undermines your security.



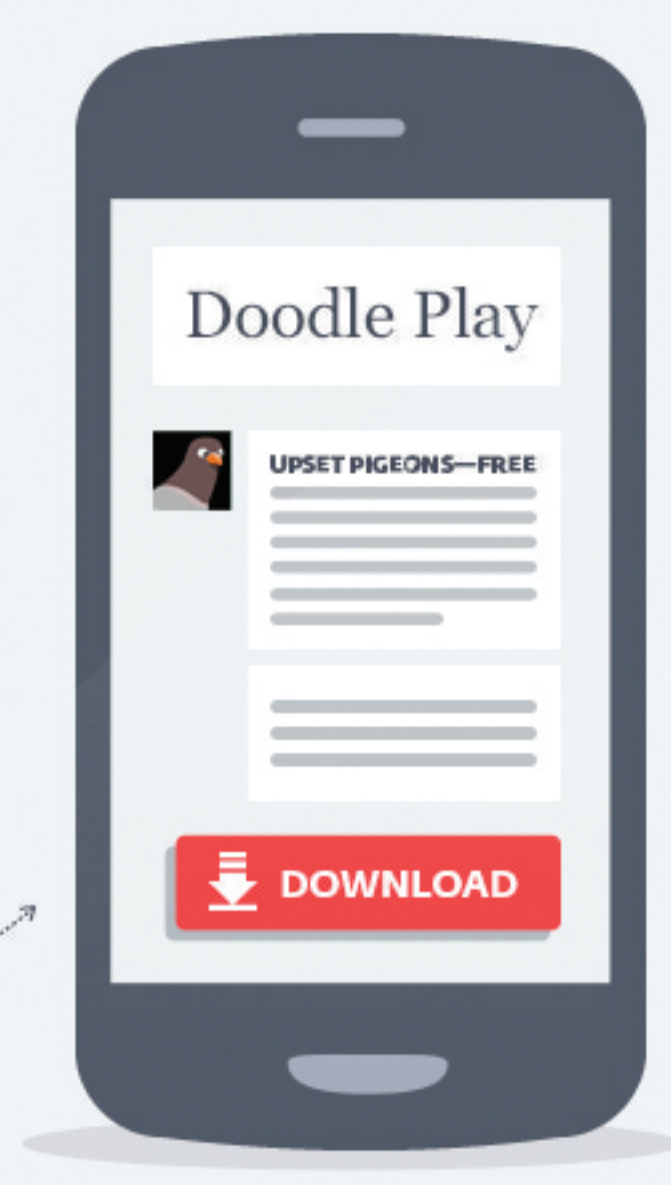


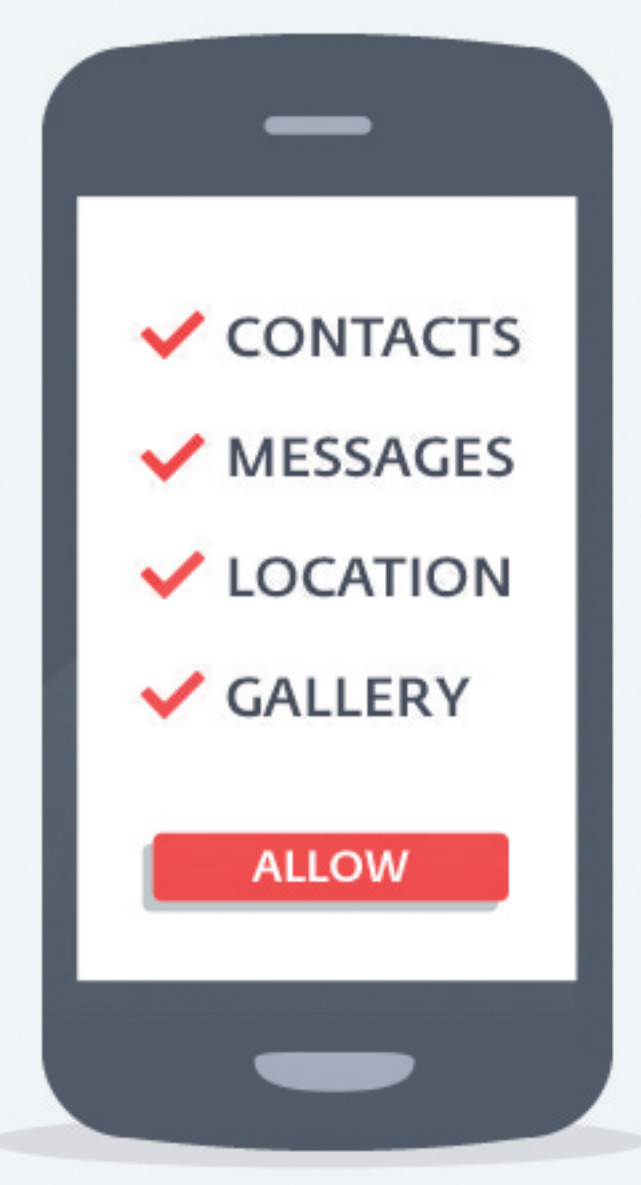
When you tap on email or chat messages

Because they can contain redirects to supposedly official sites like Internet banking. Double check the URL address before you log in.

When you download apps from unofficial app stores

Because when you download Google Play paid applications from an unofficial app store for free, you may save a few cents, but the original code of the app can be replaced by malicious content.





When you give permissions to apps before installing

Question why a simple app would need access to all your contacts, locations, data or SMS messages. Ask yourself if you are comfortable giving access to all this information and if something seems suspicious, do not accept it.

DOWNLOAD THE LATEST ESET MOBILE SECURITY APP.

ENJOY SAFER TECHNOLOGY®

GET IT ON Google play

TOP RATED SECURITY APP ON GOOGLE PLAY