WORLDLINE

Top mobile threats and how to prevent them?

What are the main type of attacks?

Man in the middle attacks
- Communications (VPN, public, WIFI, ...)
- Phishing, smishing, vishing, scams, ...

=

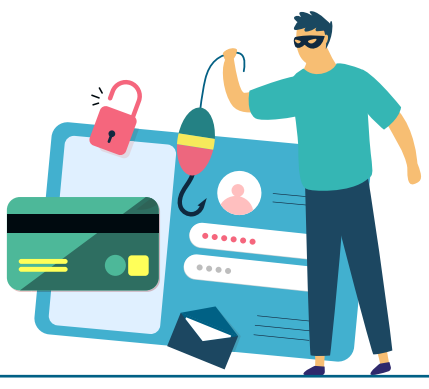
Attacks of the data exchange, account takeover, social engineering

Man in the device attacks
- Man in the disk
- Malwares

=

Attacks of the application / data stored or displayed

Phishing attacks



Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. *Smishing is based on SMS, vishing on voice.*

+45%

Increase of phishing attacks on the financial sector in 2020

Source: Akamai Technologies Inc. "State of the Internet / Security report: Phishing in Finance

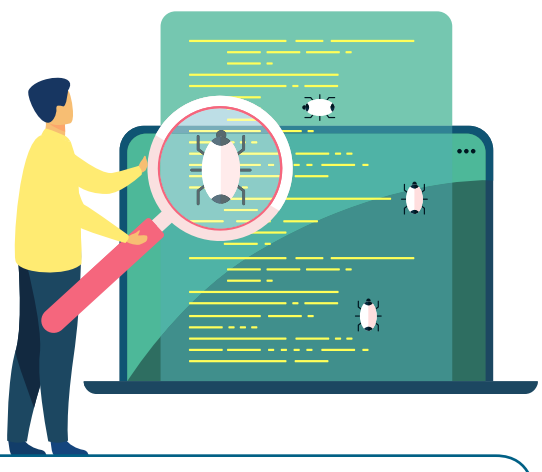
Malware: Advanced Jailbreaking and Rooting Techniques

75%

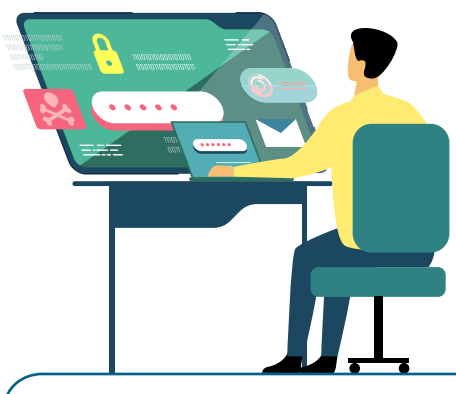
of popular free apps have been hacked at some point, exposing the user's data to malicious operators.

Source: https://teskalabs.com/blog/hacker-fun-time-android-apps

Users who have Jailbroken or Rooted devices are exposing themselves to potentially harmful malware from a wide range of untrusted or unverified publishers.



Brute force attacks



A brute force attack is the cyberattack equivalent of trying every key on your key ring, and eventually finding the right one.

+80%

of breaches within Hacking involve Brute force or the Use of lost or stolen credentials

Source: Verizon's 2020 Data Breach Investigation Report

Malware: Keylogger attacks

80%

of all keyloggers are not detectable by antivirus software or firewalls

Source: https://techjury.net/blog/what-is-a-keylogger/#gref

Keyloggers record every keystroke a device user types into a mobile, laptop, or desktop computer. The server records user ids, passwords, account details, and SMS messages.

Protect your devices

Based on GARTNER's Adaptative Security Architecture

Predict
- Threat intelligence
- Reputation / behavioral trends
- Machine learning models and continuous improvement

Prevent
- Data stored (safe, secure elements, whiteboxing, TEE)
- Data displayed (secure Display)
- Data entry (DVK)
- Code Hardening (obfuscation)
- Communication (secure Channel)
- Resource encryption

React
- Remote Policy to update local detection faster
- Fraud simulation impact simulator
- Fraud detection with device scoring based on IDS
- Dynamic permission modification and adaptive authentication

Detect
- Local Intrusion Detection System Monitoring for device eligibility and malware detection (anti-tampering, anti-hooking, anti-debugging, anti-emulator, root detection...)
- Device fingerprinting / binding
- Multi-factor authentication on the smartphone (MFA)

For further information please contact

claire.pipon@worldline.com

worldline.com

Digital Payments
for a Trusted World