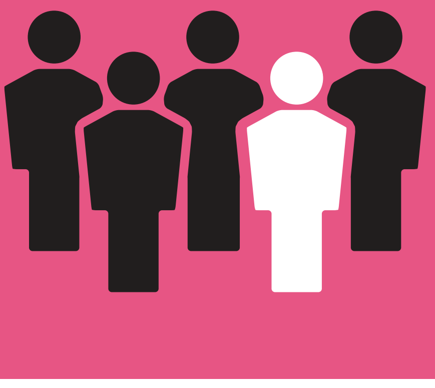
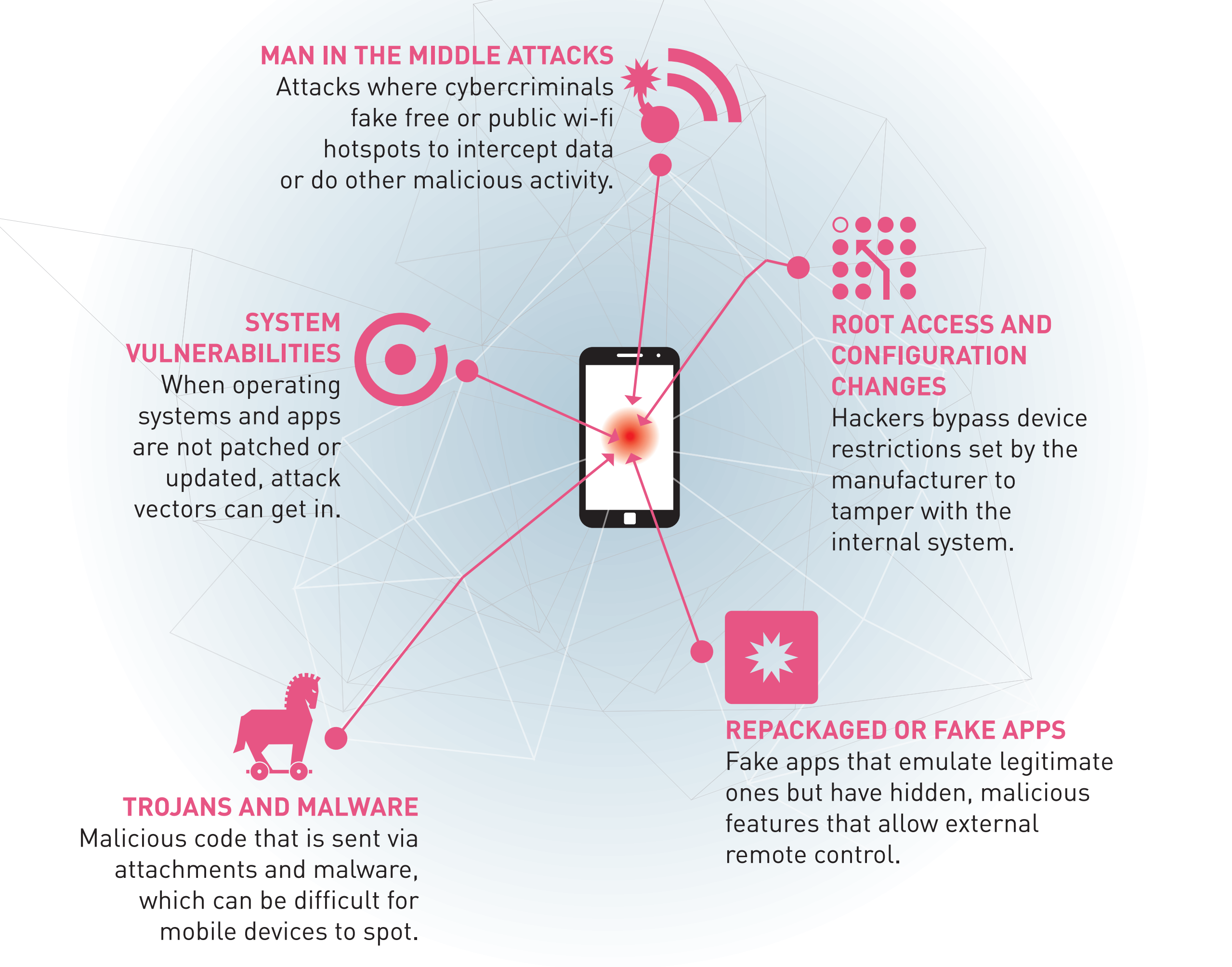
MOBILE SECURITY

THE RULE OF 5



1 IN 5 EMPLOYEES WILL BE THE CAUSE OF A MOBILE BREACH THROUGH MALWARE OR MALICIOUS WI-FI*

5 PATHWAYS TO MOBILE ATTACKS



MAN IN THE MIDDLE ATTACKS
Attacks where cybercriminals fake free or public wi-fi hotspots to intercept data or do other malicious activity.

SYSTEM VULNERABILITIES
When operating systems and apps are not patched or updated, attack vectors can get in.

ROOT ACCESS AND CONFIGURATION CHANGES
Hackers bypass device restrictions set by the manufacturer to tamper with the internal system.

REPACKAGED OR FAKE APPS
Fake apps that emulate legitimate ones but have hidden, malicious features that allow external remote control.

TROJANS AND MALWARE
Malicious code that is sent via attachments and malware, which can be difficult for mobile devices to spot.

5 BEST PRACTICES

1. **EDUCATE YOUR WORKFORCE**
Train your employees to understand the characteristics and consequences of phishing scams and unsecured wi-fi hotspots.

2. **DEFINE YOUR RISK TOLERANCE**
Set policies based on roles within the organization and on the sensitivity of data to which those roles need access.

3. **ENFORCE BASIC HYGIENE**
Insist on password or biometric locks on devices; ensure end users upgrade with each new operating system release; and activate remote location and wiping capabilities.

4. **SEPARATE WORK AND PERSONAL DATA**
Separate work-related messages and files from personal data with a secure barrier. This lets you take advantage of encryption and easier policy management.

5. **INVEST FOR AN UNCERTAIN FUTURE**
Look for prevention technologies that integrate with mobile security solutions you have in place.

Download our 2016 security report and learn more about the threat landscape
and best practices to secure your organization.

www.checkpoint.com/securityreport

Check Point®
SOFTWARE TECHNOLOGIES LTD

Source:

* Information Security. "2016 BYOD & Mobile Security Spotlight Report." Scribd. https://www.scribd.com/doc/309703246/BYOD-and-Mobile-Security-Report-2016