

Your Smartphone: A Gold Mine for Cybercriminals

A Pocket-Sized Disaster

Emma was enjoying a week-long vacation on a beautiful, sunny island. One afternoon, after spending several hours at the beach, she stopped at a small café for lunch before heading back to her hotel. Distracted by the ocean views and eager to get back outside, she accidentally left her smartphone on the table when she left. It wasn't until hours later that she realized her phone was missing.

At first, Emma wasn't overly concerned. She walked back to the cafe to find her smartphone, but it was gone. Whoever found the phone now had a potential gateway into her personal email, social media accounts, banking apps, and even the authentication app she used to verify her identity when logging into important sites.

In addition, because she was traveling, Emma relied on her phone for maps, hotel reservations, airline information, and communication with family. She could no longer access boarding passes, confirm travel plans, or receive security codes sent to her device.

Fortunately, Emma had enabled a screen lock and remote tracking before her trip. Using her laptop back at her hotel room, she logged into her account and discovered the device was no longer at the café. When it became clear she wasn't going to recover it, she remotely locked the phone and erased its contents to protect her information. Fortunately, she would also be able to recover quickly, as she had her information backed up.

Five Steps to Secure Your Mobile Device

1. Enable a strong screen lock

The first line of defense is preventing unauthorized access to your device. Use a PIN, passcode, fingerprint, or facial recognition to lock your phone or tablet. If your device is lost or stolen, a strong screen lock can prevent someone from immediately accessing your apps, accounts, and personal information. Think of your screen lock as the front door to your digital home. Set your device to lock automatically when it's idle for a time that's as brief as is comfortable for you. Make a habit of deliberately locking your phone when you set it aside.

2. Turn on device tracking and remote wipe

What happens if your device is lost or stolen? Most modern mobile devices include built-in services that help you locate them on a map, make them ring, lock them remotely, or erase all data if recovery is impossible.

© SANS Institute 2026

Apple users can enable "Find My." Android users can enable "Find My Device." These services are free and often already available on your device. Taking a few minutes to verify these features are enabled can save enormous stress later. If your device disappears, you can quickly locate it or remotely wipe your information before someone else gains access.

3. Enable automatic updates

Cyber criminals constantly search for weaknesses in mobile operating systems and apps. When these weaknesses are discovered, software companies release updates to fix them. The problem is that many people postpone updates for days, weeks, or even months. The easiest solution is to enable automatic updating, including for your mobile apps. This ensures your device receives security fixes as soon as they become available, often without requiring any effort from you.

4. Install apps only from trusted sources

One of the most common ways mobile devices become compromised is through malicious apps. Only download mobile apps from official app stores such as Apple's App Store or Google Play. Even then, review ratings, comments, and permissions before installing. Be particularly cautious of apps that request access to information or features they do not need. For example, a flashlight app should not require access to your contacts, microphone, or location. If an app seems suspicious or requests excessive permissions, choose an alternative app.

5. Enable automatic backups

Losing a device is stressful. If your phone disappears, gets damaged, or gets broken, a recent backup means you can restore everything to a new device in minutes, including not only all the apps you had installed but how they were configured. Make sure that automatic backups are enabled.

Guest Editor



Dr. Khushi Gupta is an Assistant Professor of Cybersecurity at the University of North Georgia. She holds a Ph.D. in Cyber Forensics, has authored 30+ publications, and brings law enforcement forensics experience to her work. She mentors through WiCyS, Women4Cyber, and BBWIC.

Resources

Download Danger: How to Outwit Malicious Mobile Apps: https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps
Text Messaging Attacks: A Smishing Saga: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga
How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

OUCH! Is published by SANS Security Awareness and distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch