SecurityAwarenessNews

the security awareness newsletter for security aware people



Securing Smart Devices

© 2026 KnowBe4, Inc. All rights reserved. | www.KnowBe4.com



Smartphone Security Basics

Your smartphone is a small yet powerful computer that holds access to your bank accounts, social media profiles, personal photos, and much more. Because you carry it everywhere, it faces unique risks. Use these fundamental habits to lock down your mobile security:

Stay Alert for Phishing Scams

Phishing is a scam in which cybercriminals send fake messages to steal your data (such as passwords) or install malware (malicious software). On mobile devices, this often happens through text messages. These texts might claim your bank account is locked and demand that you open a link to fix it. Never open links in random or urgent messages without thoroughly inspecting them first.

Keep It Locked

Always secure your phone with a strong password, PIN, or biometric check, such as facial recognition. Set your screen to lock immediately when you stop using it. This prevents potential thieves from instantly accessing your information if your phone is lost or stolen.

Turn On Automatic Updates

Outdated software has security gaps that attackers love to exploit. You can easily fix this by enabling automatic updates for both your phone's operating system and your individual apps. Developers often issue updates to provide vital security patches that address dangerous vulnerabilities.

Enable "Find My Device"

Most modern smartphones have a "find my device" feature that lets you locate a missing phone from a different device. When enabled, this feature lets you ping your device to make it ring, locate it on a map, and remotely erase all files if needed.

Security Note:

Never let a stranger use your phone for any reason. It may seem obvious, but there are countless stories of scammers stealing money from people by borrowing a phone.

© 2026 KnowBe4, Inc. All rights reserved. | www.KnowBe4.com



Avoiding Malicious Apps

Smartphone apps offer amazing convenience, but they are also a top target for cybercriminals. Attackers routinely create malicious applications designed to steal your data, money, or both. Even though major app stores work hard to block them, dangerous apps still slip through the cracks.

Let's review how you can avoid malicious apps and the dangers they present.

Research Before You Download

Cybercriminals excel at making fake apps look legitimate. Before you hit download, look closely at the app's details. Check the number of total downloads and user reviews. Avoid apps with very few downloads or a flood of negative reviews about strange behavior.

Always Download from Legitimate Stores

The main app markets have systems in place to review developers and the apps they create. These systems exist to prevent dangerous apps from ending up on your devices. As a general rule, avoid downloading apps from sources other than official marketplaces.

Review App Permissions

When you install a new app, it will often ask for permission to access parts of your phone, like your camera, contacts, or location. While some apps need this data to work, others ask for far more than necessary. Always review these requests and only allow the minimum permissions necessary.

Clean Out Unused Apps

Many people download an app, use it a few times, then forget about it. These abandoned apps can still collect your personal data in the background or develop security flaws over time. Make it a habit to check your device regularly and delete any apps you no longer use.

Security Note:

For any work-issued device, always follow organizational policies regarding which apps you can download. Installing unapproved software creates unnecessary security risks.

© 2026 KnowBe4, Inc. All rights reserved. | www.KnowBe4.com

The Internet of Hackable Things

The Internet of Things (IoT) refers to the vast network of smart devices that communicate with each other over networks and the internet. It includes devices such as security cameras, smart TVs, appliances, and many more.

While this technology makes life easier, developers often prioritize convenience over safety. Some smart devices are designed with weak security controls, making them easy targets for attackers.



How To Protect Your IoT:

Change Default Passwords

Many smart devices come out of the box with standard, factory-set passwords that are publicly listed on the internet. Cybercriminals know these passwords and use them to remotely hijack devices. Always change the default password to a strong, unique one as soon as you set up a new device.

Protect Your Privacy

Smart tech often collects vast amounts of personal information. Imagine, for example, if an attacker hacks into a poorly secured smart camera, allowing them to eavesdrop on someone's private life. Don't let this happen to you. Protect your privacy by choosing reputable brands that value security.

Turn Off Extra Features

Take a simple approach to your smart tech: if you do not use a feature, turn it off. Disabling voice control, remote access, or location tracking when they are not needed reduces the amount of data the device collects about you.

Consider Using a Guest Network

A guest network is a secondary Wi-Fi option that provides separation between the main network and everything else. If possible, create this network and have your IoT devices connect to it instead of the main one. Consult your router's documentation or online setup guides to help you configure this.

Security Note:

Be sure to enable automatic updates wherever possible. Doing so will keep your IoT devices on the latest security versions.

© 2026 KnowBe4, Inc. All rights reserved. | www.KnowBe4.com