// E-SAFETY FACT SHEET

Phone & Device Security Basics

Locks, permissions, updates, and what your apps are quietly collecting for Students, Teachers, and Parents

A phone is not really a phone. It is a camera, a microphone, a location tracker, a wallet, and a permanently signed-in key to every account its owner has. Losing control of it — to a thief, to a badly-behaved app, or to someone who picked it up unlocked for two minutes — gives away far more than a device.

Most device compromise is not sophisticated. It is an unlocked screen, an app granted permissions it never needed, or an update that was postponed for six months.

This sheet covers the settings that matter, the permissions worth checking, and what to do when a device is lost, stolen, or behaving strangely.

In this document:

1 Know the risks

A. The Unlocked Screen

The most common device compromise involves no technical skill at all: a phone left unlocked on a desk, a lunch table, or a changing-room bench. Every logged-in app is available — messages, social accounts, payment apps, photos — and messages arriving on the lock screen can include the two-factor codes needed to take over accounts from somewhere else entirely. A short auto-lock timer and hidden lock-screen previews close both gaps.

B. App Permissions Nobody Reads

Apps ask for access at install, when the user is focused on getting to the fun part. A photo-editing app that requested contacts, a game that requested the microphone, a torch app that requested location — each one is a permanent data feed unless it is revoked. Free apps in particular are usually monetised through data collection, and the permission screen is where that is agreed to.

C. Location and Photo Metadata

“Always allow” location builds a continuous record of where a young person lives, studies, trains, and socialises. Photos carry hidden metadata too: many cameras embed GPS coordinates and a timestamp into the file. A picture posted from home can carry the home address inside it, even when nothing identifiable is visible in the frame.

D. Postponed Updates

Software updates are not just new features. Most contain fixes for security flaws that are already public and already being exploited. A device running last year’s operating system is vulnerable to problems that were solved months ago. “Remind me tomorrow”, repeated, is one of the most common reasons a device gets compromised.

E. Sideloaded Apps, Cheats, and “Free” Versions

Apps installed from outside the official stores — cracked paid apps, game cheats, modified clients, unofficial streaming apps — skip the review that catches malicious code. These often work exactly as advertised while also harvesting passwords, messages, and banking details in the background. On managed school devices, attempts to bypass restrictions frequently open the same door.

F. Public Wi-Fi and Public Charging

Open networks in cafes, airports, hotels, and shopping centres can be run or impersonated by anyone. Traffic on a badly configured network can be observed, and fake hotspots named after a real venue are trivial to set up. Plugging into an unknown public USB port carries a smaller but real risk of data access — a plug socket with your own charger avoids it entirely.

G. Shared, Borrowed, and Hand-Me-Down Devices

Second-hand phones and tablets can arrive with the previous owner’s accounts still signed in, and go out the same way. Shared family tablets keep sessions alive for whoever picks them up next. Devices lent to friends “just for a minute” are a common route to prank posts, read messages, and installed tracking apps.

→

2 What can you do?

The five-minute device check — do this once, then twice a year

CHECK 01	**Lock it.** A PIN, passcode, or biometric, with auto-lock at 30–60 seconds and message previews hidden on the lock screen.
CHECK 02	**Update it.** Install pending updates now, then turn on automatic updates for the operating system and apps.
CHECK 03	**Audit permissions.** Review camera, microphone, location, contacts, and photos. Revoke anything an app doesn't clearly need, and delete apps you no longer use — they keep their permissions and stop getting security fixes.
CHECK 04	**Turn on Find My Device** (iOS or Android) so a lost phone can be located, locked, and erased remotely.

For students

- Set location to **"while using the app"** rather than "always", and turn off location tags on your camera so photos don't carry your GPS coordinates.
- Only install from the official app store. No cracked apps, no cheats, no "free premium" versions.
- Don't lend an unlocked phone, and back up regularly so losing a device is an inconvenience rather than a disaster.
- On public Wi-Fi, avoid banking and shopping, and treat any network asking you to install something as hostile. Carry your own charger.
- Before selling or handing on a device, **sign out of everything, then factory reset**. Deleting apps is not enough.

For parents & caregivers

- Do the five-minute check together on a new device, before it goes into daily use.
- Use the built-in family controls on iOS and Android for app installs, purchases, and content — and revisit the settings as the child gets older, rather than setting them once.
- Keep charging out of bedrooms overnight. It solves sleep, late-night contact, and unsupervised use in one move.
- Discuss **tracking apps honestly**. Location sharing a child knows about is a family agreement; location sharing they discover later damages trust badly.

For teachers & schools

- Make the permission audit a hands-on classroom activity — students are usually genuinely surprised by what they find.
- Teach why updates matter, using the idea of a publicly known flaw waiting for an unpatched device.
- Reinforce signing out of shared and library machines, and make it clear who a student should tell if a school device is lost or acting strangely.

Career link. Device hardening, patch management, and mobile security are daily work for security engineers. See the roles at getintocyberjobs.com.

→

3 Resources and where to get help

If a device is lost or stolen

STEP 01	Use **Find My iPhone** or **Find My Device** from another device to locate it, then put it into **lost mode** — this locks it and displays a contact message.
STEP 02	**Change your email password first**, then passwords for anything logged in on that device. Sign out all sessions where the option exists.
STEP 03	Contact the mobile carrier to suspend the SIM — this blocks calls, data, and SMS-based 2FA codes going to a stolen number.
STEP 04	Remove stored payment cards from the device's wallet through your account settings, and tell the bank if card details were saved.
STEP 05	If it's not coming back, **erase it remotely**. Report the theft to police, and to the school if it's a school device.

- **CISA Secure Our World** — plain-language federal guidance on device updates, passwords, and phishing: cisa.gov/secure-our-world
- **Apple Safety Check & privacy guides** — review who and what has access to your data: support.apple.com
- **Google Security Checkup** — devices, permissions, and sign-in review: myaccount.google.com/security-checkup
- **FTC consumer advice** — lost devices, malware, and unwanted tracking: consumer.ftc.gov
- **IdentityTheft.gov** — recovery plans if personal information was taken: identitytheft.gov
- **FBI IC3** — report online crime or financial loss: ic3.gov

If someone is monitoring a device without consent — that is stalkerware, and it is not a technical problem to solve alone. Contact the National Domestic Violence Hotline at 1-800-799-7233 or techsafety.org before removing anything.

// Warning signs a device may be compromised

- Battery draining much faster than usual, or the device running hot when idle
- Apps you don't recognise, or apps you can't remove
- Camera or microphone indicator lights turning on unexpectedly
- Sudden spikes in data usage
- Pop-ups, redirects, or a browser homepage that keeps changing
- Settings that revert after you change them, or 2FA prompts you didn't trigger

Any one of these can have an innocent cause — an old battery, a badly written app. Several together, or a sudden change with no explanation, is worth investigating.