Five Ways to Increase Mobile Device Security
By Wombat Security Technologies

Smartphones and tablets are only becoming more sophisticated, and the data we generate “on the go” continues to multiply. This growth brings new security challenges — and new opportunities for scammers and hackers. Here are five best practices to follow to increase the security on your mobile devices:

1. Get serious about physical security
Consider for a moment the amount of data and the number of systems smartphones and tablets can access. And then consider that some of these devices are no larger than the palm of your hand and are highly targeted by thieves.

As a rule, never leave devices unattended in public spaces (including office areas), not even for a few moments. If you make a habit of physically securing your devices, you will reduce risks associated with loss and theft.

2. Go above and beyond a basic password
Many devices do not require you to add a password out of the box. For those that do, four-digit passcodes have often been the default. Though four digits are better than none, this simple standard is not secure enough.

At minimum, use a six-digit passcode on each of your mobile devices — but avoid “easy” combinations (e.g., 111111, 123456, or your birthday/anniversary). For more advanced protections, implement a complex alphanumeric password or swipe pattern, or choose a biometric option (like a fingerprint scanner) that has been proven to be reliable and trustworthy.

3. Stay alert to social engineering scams
Email and phone scams are not limited to laptops and landlines, so you need to be cautious about the emails and text messages you receive and the calls you take on your mobile devices. Phishing emails and smishing (SMS phishing) text messages often have malware and dangerous links designed to infect devices. With vishing (voice phishing) attacks, scammers misrepresent themselves over the phone or in video chats in an attempt to gain confidential information.

Treat any unsolicited message or call with care. If something doesn’t seem right, delete or disconnect immediately.

4. Be cautious of open-access WiFi networks
Many people set their phones to find and connect to accessible WiFi networks. While this approach can help lower your mobile data charges, it can also expose you to significant risks. Open WiFi — whether paid or free — must be approached with caution, even if the network is located in a trustworthy place (such as your local coffee shop or a high-end hotel). Why? Because any WiFi network not protected by a password is vulnerable to attack.

If you do use WiFi on your mobile devices, keep these safeguards in mind:

- **Confirm a network is legitimate before you connect.** Hackers can set up “rogue” and “evil twin” WiFi networks with names that sound trustworthy or are similar to legitimate nearby networks. Once connected, your data is in their hands. To be safe, ask an employee (e.g., a cafe’s barista or a hotel concierge) or another trusted source to confirm that a Wi-Fi network is legitimate before connecting.

- **Use https or a virtual private network (VPN) to protect your data.** A VPN adds a layer of encryption and security that is valuable when using any unknown connection. Use a VPN whenever it is made available to you. At minimum, ensure that https is present in a web address before signing into an account (e.g., webmail, social media, or any website that requires a login).

- **Limit what you do on open WiFi.** Basic browsing on open WiFi is safe, but it’s safest to save other activities for times when you’re connected to a known, trusted network. Whenever possible, hold off on doing any financial transactions, including checking your bank balance or making ecommerce purchases.

5. Be selective about apps and pairings
Nearly every “smart” feature on mobile devices carries some risk. GPS tracking can reveal schedules and habits. Ill-advised Bluetooth pairings can leave your devices vulnerable. And virtually every app has multiple potential pain points disguised as permissions.

Don’t be careless about your connectivity. Be cautious about Bluetooth pairings and the features you allow to run on your devices. And make it a point to research every app prior to downloading it. Reviews and web searches can help reveal questionable permissions and dubious developers.

These best practices can help you secure your mobile devices and data. If you are concerned you’ve compromised a device, contact your service provider for advice. If you’re worried about a business device, alert your IT department as soon as possible.