Top 10 Ways To Stay Secure On The Go

Between our lives at work and home exists an attack surface known as mobile. Our phones, tablets, and laptops easily outnumber people in the world, and cybercriminals have taken note. These connected devices have provided the bad guys a way to target us no matter where we are or what we're doing. As a result, we need to take extra precautions when connected on the go!

1. **Install anti-virus and anti-malware software on all devices. Computers aren't the only ones at risk of infections.**
2. **Never connect to public networks without a VPN. VPNs (virtual private networks) encrypt your connection and protect your information.**
3. **Put a sticker on it! Theft of devices is a major concern at airports, coffee shops, etc. Deter thieves by personalizing your laptop/devices with stickers or unique cases.**
4. **Enable remote access. Both Android and iOS have built in features that allow you to connect remotely to your device, change the password, ping it to ring, and completely reset it in the event of loss or theft.** (Read more: secaware.co/2icj6Uu)
5. **Lock it up. All of your devices need to be protected with a strong, unique password of some sort (a pin or a pattern, for example). But be careful with biometrics, like fingerprint scanners, which not only have security concerns, but can be used against you.** (Read more: secaware.co/2n9Scet)
6. **Verify the source of apps to ensure authenticity. With so many in the marketplace, cybercriminals have improved at launching malicious imposter apps.**
7. **Download apps before hitting the road so you're not using data or public networks. And make sure your devices and apps are up to date.**
8. **Turn off Bluetooth and WiFi when not in use. Cybercriminals can sniff out the networks you've connected to before and spoof them (after which your device auto-connects). You might save some battery life in the process!**
9. **Beware of card skimmers. When you need to get cash, it's best to find a bank and use the ATM located inside the building. If that's not an option, carefully inspect the ATM before shoving your card into the slot.**
10. **Beware of smishing. Smishing is a phishing attack via text (SMS) and it's a common social engineering technique. Never click on unsolicited links, and be wary of links floating around on social media.**

Lost Phone? Stolen Phone?

If you're not already familiar, now would be a great time to get to know '*Android Device Manager*' and '*Find My iPhone*'. These remote services allow you to ping your device to ring, change the password or otherwise lock the device, and, in a worst-case scenario, completely wipe the device and restore it to factory default. Remember to always follow policy for work devices. Read more: ***secaware.co/2icj6Uu***.

SAC the security awareness™ COMPANY