ONLY CONNECT TO WHAT YOU CONTROL

For more information on cybersecurity for your business visit CleverDucks.com

Flee from FREE Wi-Fi

You cannot trust the security on a network you do not control. Hotel, cafe and airport free Wi-Fi are happy hunting grounds for hackers. Use your smartphone hotspot or create a secure channel over free Wi-Fi with a VPN. The same goes for public wired networks.

Don't Share More Than Power

The cord you use to charge your phone could also be used to inject malware or steal data; free charging stations are risky. Use you own adaptor, a portable battery pack or use a special power-only USB cable.

Avoid Unknown USB Drives

Don't plug unknown flash drives into your computer. USB drives can have malware that is injected on your system just by plugging it in. Make sure your security software scans USB devices before allowing them on your system.

Think About Links

Don't open links or attachments in messages sent to you that you did not initiate, EVEN IF it is from someone you know. A sender can be easily spoofed. Pick up the phone or send a separate message if ever in doubt. Control the conversation. Emails can be made to look like they're from Amazon, eBay, FedEx, etc. Login to your account online directly, and don't use the link provided unless you're sure it is legit.

Make Password Management Easy

Use unique password for each site and a password manager to keep them straight. Assume that any password you use online will eventually get compromised. Keep the damage limited to just one site.

Take Another Step

Use two-step authentication to protect your account. It is free and easy to setup with many online services. If your password ever gets compromised, the second step will stop the hack in its tracks.