SECURITY-MINDED

Practical security wisdom for daily life.

MOBILE DEVICE ADVICE

Lost, stolen, or compromised mobile devices create far-reaching risks

Imagine you're in a busy public place, such as a subway, airport, or restaurant. Now, imagine taking a wad of cash from your pocket—hundreds or thousands of dollars—and setting it down on a nearby table or seat. Next, you put on headphones, and maybe even close your eyes. Wouldn't having your cash in full view needlessly increase your risk of being robbed or attacked?

It's easy to forget that a criminal can easily grab an unprotected smartphone or laptop. They could sell it for quick cash—or use it to harm you or your organization.

With a basic smartphone, you can easily access information, connect with others, and multitask while on the move. But this convenience and connectivity also create opportunities for cyber criminals. A device that falls into the wrong hands or is compromised by a scammer carries serious risks. If your device is poorly secured, a criminal could quickly gain access to your contacts, bank accounts, personal and work email, social media accounts, and more.

Avoiding Theft and Loss

One of the best ways to protect your mobile devices—and yourself—is to stay alert to your surroundings, especially when you're around crowds or distractions. Ironically, mobile devices themselves can be major distractions, increasing the risk of theft or loss.

Here are some more tips for protecting your mobile devices:

- Only carry the devices you really need.
- Keep devices with you whenever possible, carried in a closed bag or an inside jacket pocket.
- Avoid putting devices down in places where you could forget them, such as a store's counter.
- Contact your security or IT team immediately if your device has been lost or stolen.

Protecting Your Data

Scammers don't necessarily need to steal your device in order to access your data and accounts. They can use malware, malicious apps, and other methods to compromise a device. They can also exploit vulnerabilities in out-of-date software.

- Use strong authentication to lock each device. Consider using a biometric lock, like a fingerprint, or PINs and passphrases that are long, complex, and difficult to guess.
- Be cautious about connecting to Wi-Fi networks and Bluetooth-enabled devices.

A criminal could use your mobile device to quickly gain access to your contacts, bank accounts, personal and work email, social media accounts, and more.

BLUETOOTH TIPS

Many people use Bluetooth to connect (or "pair") with nearby devices, such as headsets, fitness trackers, vehicles, and other computers. As with Wi-Fi, you should treat Bluetooth with caution.

Here's why: Each time you connect using Bluetooth, you're also providing access to your device. If a scammer connects to your device, they could send unsolicited messages, view your data, or even take control of the device.

These tips can help you stay safe:

- Turn off Bluetooth when not in use.
- Don't accept connection requests from unknown devices.
- Clear shared data from paired devices when no longer in use.
- Keep your software up to date to avoid known vulnerabilities.
- Install the latest security updates for your devices and software.
- Back up each device, in case it gets lost, stolen, or damaged.

What About Wi-Fi?

All public Wi-Fi networks are risky, whether you're trying to connect in a cafe, your gym, or an airport. When you're not on a trusted home or business network, you should use your mobile data whenever possible. But if you *must* use public Wi-Fi, there are ways to reduce the risk.

- **Avoid open Wi-Fi networks.** A password-protected Wi-Fi network is *safer*—since access is restricted—but still not *secure*. A coffee shop, for example, may offer a password-protected network for customers. But anyone else in the shop could also access the network.
- **Confirm the network.** When using a public network, confirm the legitimate network name with an employee. Scammers sometimes create fake open networks with names that *look* legitimate, but which give them direct access to your device and data.
- **Use a virtual private network (VPN).** Connecting over a VPN reduces the risk when using Wi-Fi to access work-related files, or applications like email or online messaging.

You can learn more about mobile device security in your organization's security awareness training.

Activity Corner // Mobile Device Security Word Search

L	O	S	T	N	I	A	N	S	L	C	I	O	P
E	C	O	M	P	R	O	M	I	S	E	D	E	A
I	T	H	T	O	O	T	E	U	L	B	L	P	I
V	U	L	N	E	R	A	B	I	L	I	T	Y	R
S	N	I	O	E	R	N	U	M	E	D	I	E	E
E	N	O	I	T	C	E	N	N	O	C	S	A	D
I	T	R	S	T	O	L	E	N	A	N	O	C	S
N	E	T	W	O	R	K	M	S	T	Y	L	C	Y
S	A	T	C	S	T	M	M	E	E	E	U	E	S
D	I	S	T	R	A	C	T	I	O	N	A	S	R
S	M	A	R	T	P	H	O	N	E	P	S	S	E
A	D	E	R	U	C	E	S	S	W	I	F	I	Y
B	R	L	S	T	A	B	L	E	T	M	S	O	T
C	Y	B	E	R	C	R	I	M	I	N	A	L	C

LOST
STOLEN
COMPROMISED
SMARTPHONE
TABLET
SECURED
CYBERCRIMINAL
DISTRACTION
BLUETOOTH
WIFI
CONNECTION
PAIRED
ACCESS
NETWORK
VULNERABILITY