

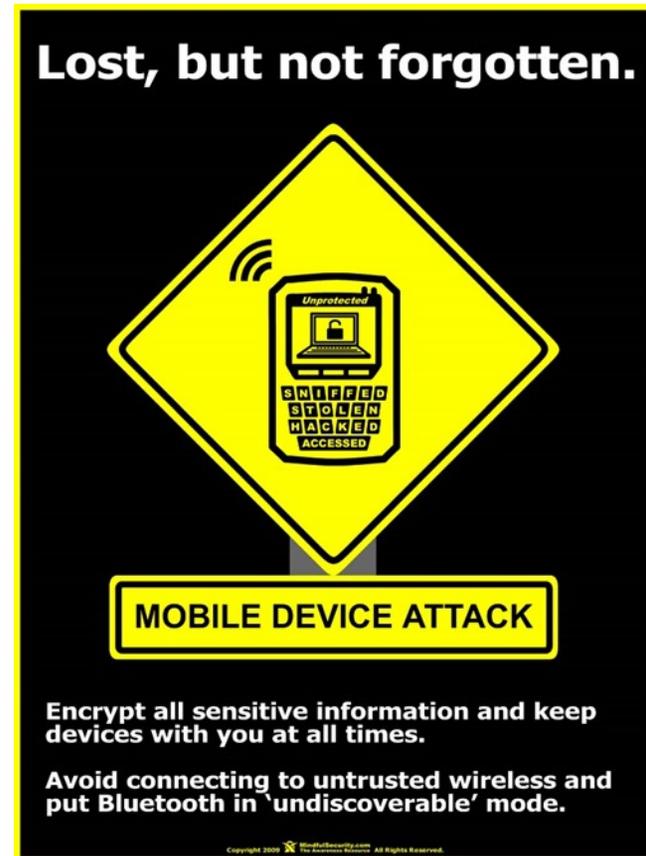
- **If you are installing an app, pay attention to the permissions requested by the app.** If the permissions seem excessive – like the ability to copy your contacts or access your photos and email – consider forgoing the app and trying to find another one with similar functionality that would be less intrusive.
- **Backup your mobile device on a regular basis.** You're doing that with your computer, right? So why aren't you doing it with the little computer in your pocket?
- **Never jailbreak or hack your own device.** Not only will this void most support, but it may cause built in security features to no longer work.
- **When using your device to surf the internet, remember that malicious sites may infect your mobile device just as they do your desktop.**
- **Turn off any functionality that automatically executes files or auto-plays videos.**
- **Watch out for phishing attempts in your email on your device and also in text messages.** If something looks suspicious or too good to be true, just delete it.
- **Be careful using Wi-Fi.** Consider disabling the function that automatically connects to available Wi-Fi networks or disable Wi-Fi except when you need to use it. If you're using public Wi-Fi, use a VPN to provide protection. NEVER conduct business, do your banking, or shop over public Wi-Fi.

- **Disable Bluetooth unless you need it.** Bluetooth capabilities are also an entry point for hackers.
- **Do not access or store work email or other information from your organization on your mobile device** unless you have been authorized and are using approved software.
- **Consider enabling remote wiping on your device.** If the device is ever lost or stolen you can erase all of your information to prevent it from being stolen.
- **Last, when you're replacing your device, make sure to wipe all data before disposing of it.** For mobile phones, remove the SIM and any memory cards from the device.

Mobile devices help us to stay in touch, be more productive, and share and communicate with co-workers, family, and friends. Protecting your device allows us to do all that more securely.



<http://sitsd.mt.gov/MontanaInformationSecurity>



Enterprise Security Program

Mobile Devices



Not so long ago – although it’s hard to remember those dark days – a phone was a how you called someone from across town or the country, a tablet was made of paper, and a mobile computing device weighed 10 pounds or more and was called a laptop. Phones, tablets, and laptops are all still part of our daily lives, but, boy, have they changed! And they’ve been joined by even more options for connecting and communicating. You can make phone calls, send text messages, watch television and movies, read books, do your banking, play games, shop for everything from clothes to groceries to a new car and even work from a device that fits in your pocket and weighs less than half a pound. There are apps for nearly everything you can imagine. These days most of us use a mobile device of one type or another and we’d feel a little lost without it (or them!). There’s even a word for the fear of being without one’s mobile phone: nomophobia.

All that functionality and power is incredibly useful, but it can also put you and your information at risk. Just like your computer at work and at home, you likely store, send, and receive emails, files, and pictures on your phone, tablet, and/or laptop. Without taking precautions, that information can often be stolen much easier than hacking into your home or business networks. You have a password or may even use two factor authentication

for your computers, but are you doing the same for your mobile devices? Surveys say that 70% or more people don’t password or may even use two factor authentication for your computers, but are you doing the same for your mobile devices? Surveys say that 70% or more people don’t password protect their phones.

Mobile devices are becoming attractive targets for malware and ransomware, too. While the thought of cleaning an infected phone might not sound too horrible – it’s “just” removal of the bad app and a factory reset – mobile phones have some of the same inherent risks as a USB drive. Plug an infected phone into your computer and you’ve just spread the malware. No longer does a cybercriminal need to access the network to infect it. He can infect the device of an employee and the employee will spread the infection.

Last, let’s not forget the low tech and all too common problem of losing devices. Small devices are great because we take them everywhere. But it’s also easy to leave them somewhere or have them drop out of our pockets and bags without us noticing. Losing an unlocked and unencrypted device is like dropping a file folder full of information on the street for a stranger to pick up and read.

Here are some steps you can take to protect yourself when using mobile devices:

- **Update and patch your device and the apps on it regularly.** If your phone is old and no longer supported, consider replacing it. When researching new devices take into consideration which manufacturers are more reliable about regular updates.

- **Protect your device with a strong password or passcode.** Use encryption when possible to protect the information stores on the device.
- **Use caution when installing apps on your device.** Download apps from trusted sources like the Apple Store, Google Play, Amazon, the manufacturer’s app store, or your wireless carrier’s store. If your phone is used for work, follow your organizations policy about installing apps, which may include only installing apps for the organization app store or getting approval prior to installing an app.
- **Install antivirus on your device and keep it updated with the latest version.**

SECURITY CAT

NOTICED THAT YOU ARE USING
A VPN TO CONNECT TO
PUBLIC WIFI AND THAT’S
PURRRRRRRFECT

