Like Tweet Share

CANYON STATE CREDIT UNION™
Committed to You.

From coffee shops to planes, trains, and cruise ships, we've become accustomed to having ready access to the Internet just about anywhere. The problem is, it's easy to forget how vulnerable that makes us to security threats.

Think it can't happen to you? Think again. Fortunately, a combination of plain old common sense and some technology can protect your devices--quickly and fairly easily.

How Your Gadgets May Be Vulnerable
Whether you're traveling with a laptop, netbook, smartphone, iPad, or all of the above, the risks and defenses against them are basically the same, according to Joe Nocera, an information security expert and a principal with PricewaterhouseCoopers. "Many of the security concerns that people think about when they think about their personal computers are applicable in the mobile world." As mobile devices become more sophisticated, they lend themselves to the same types of access to e-mail, passwords, and other secure information that PCs have done in the past.

Because today's devices are so much more powerful and can hold so much more information than ever before, the risks are increasing, says Martin Hack, information security expert and executive vice president of NCP Engineering, a software company that helps businesses with their secure remote access systems. Add to that our tendency to carry both personal and business information around with us on the same device, and our mobile devices have never looked so appealing to hackers, he says.

As specific mobile devices become more popular, they become more of a target for hackers. More and more often we're seeing either Android- or iPhone-based vulnerabilities being targeted. The good news is it's not difficult or even expensive to protect your devices and the information on them. The fixes are simple.

9 Tips for Keeping Your Mobile Devices Secure

1. Make sure your software is up-to-date. The first line of defense, says Nocera, is making sure that all your software is up-to-date. "Almost every release of software patches a number of security vulnerabilities that are out there," he says. Before every trip, or at least every few weeks, it's a good idea to check the manufacturer's Web site (or search Google) to see if a software or firmware update is available. If there's a new one, download it, unless there's a massive firestorm of negative reviews from early adopters.

2. Employ strong passwords. "Be sure to use some combination of letters, numbers and/or special characters of 8 characters or more," says Jeremy Miller, director of operations for Kroll Fraud Solutions. "Avoid using dictionary words. Instead, [use] acronyms for things like favorite songs, restaurants or other items known only to you. And change the password frequently--at least once every six months."

3. Don't mess with the security settings. Nocera notes that most of the default browser settings in Android, iPhone, and Blackberry phones are fairly secure out of the box. "I recommend not going in to change browser security settings--they're pretty good already," he says.

4. Avoid unencrypted public wireless networks. Such Wi-Fi networks require no authentication or password to log into, so anyone can access them--including the bad guys. In some cases, bad guys set up an open network to snare unsuspecting people. Encrypted networks, on the other hand, are those that require an ID or password for access--you'll find such networks at many hotels and coffee shops that offer Wi-Fi services. These networks have two different types of security--WEP (wired equivalent privacy) and WPA (Wi-Fi protected access); the second is most secure. Even encrypted networks, though, have risks--it's possible for bad guys to gain access to encrypted networks at a hotel or café, for instance, so be cautious about the sorts of things you do on such networks.
Besides avoiding connecting to unencrypted networks, turn off Wi-Fi when you're not using it. This will prevent you from automatically connecting to networks (and it will extend your device's battery life).

5. Paying to access a Wi-Fi network doesn't mean it's secure. Access fees do not equal security. Just because you pay a fee to access a Wi-Fi network doesn't mean that the network is secure.

6. URLs beginning with 'https:' are safer (but not foolproof). Whenever you're accessing a site where you'll be sharing personal or confidential information--your bank's site, for example--you want to make sure that you're doing so securely.
The *s* in *https* means that you're connected to the site via the Secure Socket Layer

(SSL). In layman's terms, this means that all data transmitted to that particular Website over the Internet is encrypted.
SSL is not foolproof though: If you're on an unencrypted network connection, you may still be subject to man-in-the-middle (MITM) attacks, a form of eavesdropping where the bad guy makes a connection independently with two parties and then "gets in the middle," making both believe that they are talking directly to each other.

These types of attacks are rare, but to guard against them, make sure you're both connected to a secured network and that Websites use *https* when you're entering sensitive information.

In addition, says Nocera, most e-mail service providers have both a clear text option (that sends unencrypted data) and an encryption (SSL) option. "Make sure you have the SSL option enabled," he says.

7. Use VPN. If you have access to a VPN (virtual private network), use it. A VPN provides secure access to an organization's network and allows you to get online behind a secure layer that protects your information.

8. Turn off cookies and autofill. If your mobile device automatically enters passwords and login information into Websites you visit frequently, turn that feature off. It's convenient, but it can also be a privacy threat. In the end, a little inconvenience can go a long way toward added security.

9. Watch your apps! Apps are great, and many are free, so it can be tempting to download with abandon. But, Nocera cautions, you should be selective about the apps you download, particularly in the Android market, because "the Android app market is a little bit more open," without the strict developer guidelines found in Apple's App Store. Do some due diligence before downloading apps. Make sure that you trust the developer and have taken the time to review some of comments.

If You Still Get Hacked...
If you do everything right and still have your information stolen, what should you do? The damage can often be repaired simply by changing your password (to one much stronger) and sending a message via the network that was affected, explaining what happened. What if one of your devices gets stolen? Be sure that all of your mobile devices have a remote wipe or autowipe feature.

Article by Logan Kugler, PCWorld