ENJOY SAFER TECHNOLOGY®

5 TIPS FOR SAFE SUMMER TRAVELS

www.eset.com

5 tips for safe summer travels

1: KIDS AND MOBILE DEVICES

When you're on vacation with the family this summer, your kids are bringing along all of their friends. Not literally, of course, but more than likely they'll be using their smartphones to stay in touch with all their pals and telling them everything that's going on.

Posting geo-tagged photos, using check-in apps, and updating social pages with too much detail about their whereabouts are risky enough when you're in town because of the value the information can have to a potential stalker. It's an even bigger problem when they're telling everyone back home that you're away on a weeklong vacation. So unless you have 100 percent confidence in your home security system, ask them to tone down the social sharing while you're away. You don't want to ruin their fun, but you don't want your home ransacked, either.

Make your vacation even safer

If you'd like extra peace of mind, *ESET Parental Control* can help. This app lets you block inappropriate apps or websites on their smartphone, and set limits on time usage. But it also allows you to grant additional time or access if your child requests it, so you can keep them and your family protected while you build trust and educate them about responsibility.

And, if you trust your older kids to go exploring on their own during vacation, you can breathe a little easier there, too. *ESET Parental Control* lets you locate them if you need to know where other family members are, and stay in touch with a feature that requires they acknowledge your call or text in order to continue using their device.

By the way, a survey of 50 ex-burglars found that 80% of them used information on social sites to target homes. It's a real risk. You don't want to have a great vacation ruined by what you find when you return home.

2: BEING WI-FI WARY

When you're on vacation far from your handy home network, it's tempting to grab a quick connection through an unsecured Wi-Fi hotspot in a café, airport, library or the like. After all, it's right there, it's convenient (doesn't require that complicated security key) and best of all, it's free.

Before you make that connection, stop and think. No security key means that more than likely you'll be sending information in "clear text." That means "unencrypted." And anyone else who is connected to that hotspot, equipped with a few very simple hacking tools, can intercept and read everything you send.

Online banking? Don't risk it.

Above all, never, ever use unsecured Wi-Fi to access a banking site. Anyone else connected to that network with the right tools can read your log-in and password (sometimes even if the banking site itself is secure), grab control of your account and start moving your money out. If you need to do a bank transaction while traveling and can't find a secure connection, use the bank's toll-free number and call instead.

Never share with strangers.

When you connect to any public Wi-Fi network, whether it's secured or not, you're sharing that network with everyone else who's connected to it. Without some protections in place, anyone else could open a connection to your machine. First of all, make sure any file-sharing that might be turned on is disabled. Second, always use a software firewall—like the one in *ESET Smart Security*—whenever you use public Wi-Fi.

These concerns about public access points apply every bit as much when you're in your own hometown. But when you're traveling and looking for a way to connect, you're much more likely to be tempted by the convenience to use them in an unsecure way. And the bad guys know it.

3: PRACTICAL THEFT PREVENTION

Your personal electronic devices are valuable—not just the device itself, but the data it contains. If it's lost or stolen, it's sure to ruin your vacation. You might also lose your identity to a thief. Here are some steps to protect yourself:

- *Lock your phone down with a strong password or PIN, or use the fingerprint lock*
- *Preserve any photos, work data or important information on your phone by backing it up before you leave*
- *Print out and carry copies of travel documents, confirmations and important phone numbers you might need while traveling so you can continue your vacation—or get home—in case you lose your device*
- *Keep your devices close by and in sight at all times—thieves prey on inattentive travelers, and if you let yourself get distracted by your surroundings or the fun you're having, they'll swoop in*
- *Don't carry your phone around in your hand unless you're actually using it; a fanny pack around your waist keeps it snug and secure, and you can still get at it quickly for photo opportunities*
- *Don't put devices in your checked baggage or leave them unattended in your hotel room—and if your room has a safe, use it*

If you want to be extra safe, *ESET Mobile Security* lets you locate, track and lock your device if it's lost or stolen, lets you send a message to whoever found it, and improves your chance of recovery. You can even erase data on your device remotely to keep a thief who's stolen your device from prying open the contents. It's incredibly affordable for the protection it provides.

Take these few extra precautions and don't let a thief steal your fun.

4: SHARE WITH CARE

It's fun to share photos and files with relatives and others when you're visiting. It's a great way to share memories and catch up on what everybody's been doing. But just because you know the person doesn't mean that person knows whether the handy USB drive they handed you contains malware. Or whether that camera card contains something other than family reunion pictures.

Infected USB flash drives and other removable media are one of the more common ways that malware spreads. In fact, in some cases, you don't even have to open the portable drive — simply inserting it or connecting it to your computer will infect your machine. Here are a few reminders:

- *Always decline any request from anyone who wants to connect a USB or portable device to your laptop or phone—no matter how sincere the request seems*
- *Never use USB drives or software received as gifts or promotional items—even well-known, highly reputable companies have unknowingly distributed infected drives*
- *If you are going to share with friends or family, make sure that you have antimalware protection in place*

Want to be sure? ESET has two ways to protect removable drives and media. Install *ESET Smart Security* on your computer and you can protect it from being infected by malware carried on portable drives handed to you by others. Or install *ESET Drive Security* on any USB drives you share with others to make sure your own portable device remains malware-free.

Take these precautions and make sure the only things you're sharing are good times and great memories.

5: PACKING LIGHT

Some universities make stripped-down loaner laptops available to traveling faculty and researchers, and strongly recommend they take them instead of their personal, fully loaded machines. These folks and their institutions know the risks of carrying proprietary, sensitive, or personal information — especially when traveling to other countries. Take some tips from them:

- *Scrub your machine of sensitive or personal data before you take it on the road—and remember to empty the recycle bin*
- *Also, before you leave, clear your browser cache, remove saved passwords, password-protect all devices with strong passwords, and disable remote connectivity such as Bluetooth, Wi-Fi and file-sharing*
- *If you carry sensitive or personal information on your travels within the U.S., encrypt it*
- *Before you bring encrypted data (or encryption technologies) outside the U.S., check out this informational site*
- *Be aware that some foreign countries have different attitudes and standards for privacy, and officials may inspect the contents of your device*
- *When you return home, run a complete security scan and consider changing passwords on all the accounts you accessed while you were traveling*

If you feel you need to carry your sensitive, private information on your travels, the *Kingston Data Traveler Drive* is a great way to protect it. It lets you store the information separately from your computer's hard drive so you can encrypt just the files you're concerned about, and makes it handy and easy to access them if you need to.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®