SECURITY Smart™ NEWSLETTER

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Mobile Phone Do's and Don'ts

Whether using your mobile device for business or pleasure, make security a priority.

Now that many organizations are allowing employees to use their own mobile devices for work, keeping those devices secure has become imperative for both personal and professional reasons. In addition to learning and adhering to your employer's policies when using your device for work purposes, take into account the following tips from security experts:

Richard Greenberg, information security officer, Los Angeles County Public Health

DO: Most obvious, or it should be obvious, is password protect the phone. This is too often forgotten, resulting in potential identity theft.

Set up the remote wipe capability built into many phones, which is great for peace of mind in case of a lost device. Some phones have this capability; with others it has to be downloaded.

Make sure you have access to data backup systems from the phone, and make sure to back up data regularly. If the only place you have the data is on the phone, it could be lost permanently.

DON'T: Rely on mobile banking. I would recommend people do their banking from a PC they trust.

Connect to the Internet using a phone via an untrusted wireless hotspot. You're not using your own, so you have no idea who's listening in on that. It's so easy for someone in a car to listen in with a very simple and cheap device.

Bill Thirsk, vice president of IT and CIO, Marist College

DO: Set the device to auto-lock. This works in combination with the passcode. If the device is inactive for a few minutes, setting the auto-lock will require the passcode to be entered to gain access to it again. The timeout should be short; a minute or two is best.

Set the device to auto-wipe after several invalid password attempts. This will remove all user data. Enabling this feature will effectively prevent unauthorized use, prevent access to your data and block repeated attempts to crack a passcode.

DON'T: Leave the phone unattended. It only takes a few seconds for a thief to pick up a phone. You should always have your phone with you, even if you're just stepping away for a few seconds in a public setting. Keeping your phone physically secure will go a long way toward protecting your data.

V. Jay LaRosa, senior director of converged security, architecture, Automatic Data Processing Inc.

DO: Set up your mobile device with a PIN and a remote wipe service. Most enterprises require this, but this can also be done for your personal device with apps like "find my iPhone." If your device is ever lost or stolen you want to make sure it is hard to get into.

DON'T: Respond to or click links in unsolicited text messages. If your provider will allow you to block text messages from certain numbers, use that feature to stop future unwanted messages from specific numbers. Once you respond [to text messages], the people on the other end may barrage you with more unwanted messages, or sell your live number.

Jailbreak your phone [modify it to avoid limitations placed on it by your carrier]. You are opening yourself up to a world of unknowns. If you venture outside of the protections that the provider affords, you are putting your device at additional risk from unknown vulnerabilities or opening additional access that could not normally be exploited by an attacker.

Take Out Cash Safely

Card skimming at ATMs is an increasingly popular method for stealing money. Know what to watch for when you withdraw funds.

Depositing or withdrawing money from an ATM is so routine that your mind might be tempted to wander while you wait for your bills to come shooting through the slot. But letting your guard down can let unwanted criminals into your bank account. So-called card skimmers work by modifying the ATM's hardware or software or adding a separate card reader that looks like the real thing. Their equipment records the data from the bank card's magnetic stripe and may also steal a customer's PIN. This information lets them create dummy cards that they use to drain the victim's account.

Card-skimming is surprisingly common and affects both consumers, who lose their money, and banks, who suffer a blow to their reputation if one of their machines is hijacked.

So how can you protect yourself from card skimmers?

➤ **Check for fake readers.** Criminals might install fake readers over the slot where the card is swiped that can capture the card information. Another ruse is placing a fake PIN pad over the real one that can record PIN information as you type it in.

If you know what to look for, you can often spot these devices. For starters, see if you can wiggle the reader. A legit one should be sturdy. Criminals also might put up signs that say "No Tampering" on machines they themselves have tampered with, to discourage anyone who senses a problem from trying to explore further.

Your best bet is to use an ATM you are familiar with so that you're more likely to notice if something is amiss. Also, keep in mind that ATMs inside banks tend to be safer, and stand-alone, non-bank-related ATMs are the most vulnerable, such as those at convenience stores.

➤ **Protect your PIN.** Skimmers can also try to grab PIN info by installing hidden cameras somewhere inside the machine, in the wall or even inside one of those racks of innocent-looking pamphlets that sit off to the side. Get into the habit of covering your PIN with your hand, even when you are alone. Doing so may prevent a camera from detecting your code and may also stop another type of nontechnical scam: shoulder surfing, which occurs when a person lurks nearby and simply watches as you punch in your PIN.

➤ **Avoid overly helpful people.** Beware the good Samaritan hanging out near the ATM who offers to help. In this scam, a doctored machine captures the card and the victim is perplexed as to why the machine is having problems. A helpful bystander will offer to help and ask for the person's PIN. Once he has it, the card is as good as his.

➤ **Monitor your accounts.** Stay on top of your own financial records. Each month, check your bank statement for any withdrawals that you didn't make, and notify your bank immediately if you find any errors. Reporting fraudulent activity quickly ensures the best possible chance that you can recover your funds.

Preserve and Protect

Keep company information out of the wrong hands.

You are your company's first line of defense against loss of intellectual property. Con artists are often very cunning, but you can arm yourself with techniques to spot them. First and foremost, you need to know what information you should never surrender to outsiders, says Lynn Mattice, managing director of Mattice and Associates, a consultancy specializing in enterprise risk assessment. Here's what he says you need to keep to yourself:

❶ Information affecting the company's future that has not been made public. This could be targets for mergers, acquisition or divestiture, as well as new product development or strategic new markets that the company is developing.

❷ Market or financial performance data that hasn't been officially released to the public.

❸ Personally identifiable information about a customer, employee (including you) or anyone else affiliated with the company.

❹ Trade secrets.

❺ Any information beyond what has been authorized by the company for public release. What should you do if people ask you for this type of information? Ask them some questions. "Obtain sufficient information from the individual making the request to validate that they have a right or a need to know the information," says Mattice.

DID YOU KNOW?

Thirty-five percent of **data breaches** in 2012 were the result of negligence or human error and 29 percent were attributable to system glitches, according to a recent study. However, **malicious attacks** remained the single highest cause of breaches, at 37 percent.

Source: The eighth annual Ponemon "Global Cost of a Data Breach" study

Online Stolen Credit-Card Ring Exposed

Vietnam-based conspirators allegedly had data on more than 1.1 million cards.

Law enforcement agencies in the United States, Vietnam and the United Kingdom recently disbanded a crime ring that had allegedly been selling online credit card details since 2007.

The ring, which sold the credit card information through two websites, is said to have caused more than $200 million in fraudulent charges on credit cards issued in the United States and Europe.

Charges have been brought in a federal court in New Jersey against Duy Hai Truong, 23, of Ho Chi Minh City, Vietnam, who is suspected to be one of the ringleaders. Additionally, three men were arrested in London and seven people were arrested in Vietnam in connection with the case.

The alleged conspirators, who were based in Vietnam, obtained personal identifying information that consumers provided to retailers when shopping online and paying via credit cards, according to the office of the U.S. attorney for the district of New Jersey.

Data relating to more than 1.1 million cards was obtained through hacking of commercial entities, the United Kingdom's Serious Organized Crime Agency said. The people charged are alleged to have illegally obtained personal information, including purchasers' names, addresses, credit card information and Social Security numbers, from victims in New Jersey, according to U.S. authorities.

People wanting to purchase victims' credit card information either accessed the hackers' fraudulent websites or sent them an email requesting data, according to the FBI complaint. If convicted, Truong, who is charged with conspiracy to commit bank fraud, faces a maximum of 30 years in prison and a fine of at least $1 million.

On the Road with Your Computer

These pointers will help you work productively and securely when you and your laptop travel together.

Internet Connections The trickiest bit of a business trip is often getting Internet connectivity. While Wi-Fi hotspot access is generally fine, it can sometimes be flaky due to congestion or misbehaving wireless access points in public locations, and there can be security concerns. If a Wi-Fi hotspot isn't working right, devote no more than 10 minutes and one system restart to resolving the problem. After that, change venues or switch to a mobile hotspot to make better use of your time.

DIY Hotel Wireless

Depending on the hotel, Internet may be delivered to rooms using a wired Ethernet port or Wi-Fi. Wireless offers convenience for laptop users, especially since many new laptops no longer have an Ethernet port. Whether wired or wireless, a software utility can create a separate Wi-Fi network to deliver Internet access to tablets and smartphones (ask your employer's IT staff for help with this). Setting up a personal wireless connection can save you money on roaming charges.

Bring Another Battery

Laptop batteries are not designed for longevity. To substantially increase running time, you need a spare battery or a rechargeable power pack. A spare battery is a simple fix, though it can be a hassle to keep both charged. Rechargeable power packs cost more than replacement batteries, but their use of interchangeable power tips means that they can be useful even if you switch to a new laptop.

Pack a Mouse and Keyboard Cover

Despite the popularity of the touch interface, many people still prefer an external mouse. Standard optical mice don't track well on glossy tabletops, however, and it's frustrating to pack a mouse and not be able to use it. Some higher-end mice can track on reflective or transparent surfaces, but budget-conscious travelers should bring a mouse pad.

A keyboard cover will protect against cookie crumbs and coffee spills.

A Lock Is Not Enough

Given the cost of a laptop and how easily one can be spirited away, it makes sense to physically secure yours whenever possible. Most have the Kensington lock—a small slot on the side that is specially designed to prevent laptops from being stolen. To secure a laptop, loop the lightweight reinforced cable portion of a Kensington lock around a fixture such as a table leg, then affix the lock. Most use keys, though some come with combination locks.

While the Kensington lock can deter some thieves, it's not much protection against one who has some time alone with your laptop. That's why all data on a laptop should be properly encrypted with robust full disk encryption (FDE) technology, a last line of defense against data leaks should a laptop end up in the wrong hands. Before you travel, check in with the IT staff to make sure you're protected.

Pick the Right Laptop Bag

A bag or case that's designed to hold a laptop offers built-in padding to protect against bumps. The most versatile option is a bag with a detachable shoulder sling. These aren't ideal for long treks, though, and they may attract attention in unsavory areas. Backpacks designed for laptops are more comfortable to carry, but they don't look as good with business attire.

Frequent air travelers will want a bag with a slip pocket for sliding a bag over a luggage trolley handle. Easy access is necessary, too, as airport security procedures often require fliers to place laptops in a separate tray.

Social Networks for Private People

For privacy-minded folks who want to communicate with friends and family but aren't interested in broadcasting their photos and thoughts, social networking options other than the ubiquitous Facebook and Twitter can be very appealing. To share photos, videos and status updates, check out these social networks that are designed for close-knit groups who want to connect with each other.

Couple. Formerly known as Pair, Couple is a smartphone-based network designed expressly for couples. In fact, you can only have one friend on Couple: your significant other. Couple features a timeline that's a bit like a souped-up text message exchange—you and your partner can add photos, reminders, important dates, drawings and videos, along with regular text messages.

Family Wall. If you're looking for a slightly larger social network, FamilyWall helps you keep track of your entire family. In this private, Facebook-like social network for families, you can add dates and events, photos, videos, contacts, messages and even Foursquare-style check-ins. You can also add "family landmarks" such as schools, doctors and fitness centers.

23snaps. Instead of posting photos on Facebook or Instagram, try posting them to 23snaps, a smartphone-based social network that lets you create a unique, private online photostream. 23snaps lets you add photos, videos, and status updates to a special photostream and then share those photos with your friends and family.

Path. Perhaps the best-known private social network is Path. This smartphone-based social network limits your friends list to 150, the maximum number of friends a human being can realistically keep track of, according to studies.

Nextdoor. If you want to restrict your social network communication to people you know in real life, the neighborhood social network Nextdoor might be right for you. Nextdoor requires all members to verify their address (the service sends a physical postcard with a code on it) before allowing them to join their neighborhood group. As a result of this structure, the only people you can talk to on Nextdoor are those who live within shouting distance of you.

Ten Tips to Reduce Your Risk of ID Theft

Skipping the mall in favor of the Internet is the norm for many shoppers, but online credit-card users could be setting themselves up for identity theft if they aren't careful. Here are 10 tips from the Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center:

1. Ensure websites are secure prior to submitting your credit card number. Look for the padlock icon in the URL.
2. Do your homework to ensure the website is legitimate.
3. Make sure the business you are dealing with has a physical address, not just a P.O. box.
4. Never throw away credit card or bank statements in usable form.
5. Be aware of missed bills that could indicate your account has been taken over.
6. Be cautious of scams requiring you to provide your personal information.
7. Never give your credit card number over the phone unless you are the one who made the call.
8. Monitor your credit statements monthly for any fraudulent activity.
9. Report unauthorized transactions to your bank or credit card company as soon as possible.
10. Review a copy of your credit report at least once a year.

BUSTED

A phishing gang that stole and spent a British woman's life savings of $1.6 million has been handed heavy sentences by a London judge.

The three gang members will spend four to eight years in prison, and the ringleader must pay back the stolen money.

The conspirators spent most of the money on a lavish three-day shopping trip. Photos showed the gang leader posing with a "cash sandwich"—bills inserted between slices of bread—and holding up champagne bottles.