What Hackers Don't Want You to Know

Michelle Crouch – Readers Digest

Computer hackers have lots of tools to threaten your internet security, but these tips from cybersecurity experts can help protect your privacy.

They send incredibly personal emails:

Spear phishing, the act of sending targeted emails to get you to share financial information or passwords, can be exceptionally sophisticated. "The old-style ones had spelling and punctuation errors, but today, it has really become an art," says Mark Pollitt, PhD, a former chief of the FBI's computer forensic unit. "They may call you by name, use your professional title and mention a project you're working on."

Outsmart them: Spot phishing emails by looking for incorrect or unusual URL's (hover over links to see the actual URL address), requests for personal information or money, suspicious attachments or a message body that's actually an image. Unless you are 100% confident that a message is from someone you know, don't open attachments or click links.

They've got all the time in the world:

Hackers have programs that systematically test millions of possible passwords. "They go to sleep and wake up in the morning, and the program is still going, testing one password combination after another," Says Peter Fellini, a security engineer with Zensar Technologies, an IT and software service firm. Look out for these signs your password could be hacked:

- Your password is "Password". Amazingly, 'password' always ends up in a top spot of most popular passwords according to hackers, along with '123456', '12345678', 'welcome', 'letmein' and 'jesus'.
- You didn't check its strength first. The Password Meter is a handy resource when setting up new accounts or changing your login information. It plugs your password into a formula and shows you exactly what its greatest strengths are (symbols) and weaknesses (sequential letters), thereby allowing you to tweak it to perfection.
- You use the same password for everything.
- Your security question is obvious. Sites often ask you to provide a security question and answer for use when you forget your password. Try for something complex or personal so nefarious types can't figure out the answer with a simple google search.
- You use a common phrase. Just like you don't want an obvious answer to a security question, you don't want your password to contain a word or phrase that's meaningful to you, like your sister's name and your hometown. These are too easy to guess (and can simply be found online). Try incorporating "opposite" words, like your least favorite color or the site of your least favorite vacation.
- You didn't use a mnemonic device. Lifehackers suggest using the 'Person-Action-Object (PAO) method to create an unbreakable password. Visualize a famous person doing a random act with a random object (say, Abraham Lincoln surfing with a gallon of milk). Now combine parts of the phrase to make a new word, like AbeLiSurfilk. Not only do you have a word that's too random for any hacker to crack, but you'll be the only person it makes sense to.

Outsmart them: Instead of a password, try a passphrase. Use letters and characters from a phrase and include special characters, numbers and upper and lower-case letters.

They love your Bluetooth headset:

If you leave the Bluetooth function enabled after using a hands-free headset, hackers can easily connect to your phone, manipulate it and steal your data.

Outsmart them: Always turn Bluetooth off after you use it. Set your visibility to “off” or “not discoverable,” and require a security code when you pair with another Bluetooth device.

They sneak while you surf:

A growing number of cyberattacks are arriving via “drive-by download,” says Giovanni Vigna, PhD, a computer science professor at the University of California at Santa Barbara and co-founder of anti-malware provider Lastline Inc. “You visit what looks like a perfectly harmless website,” he says, “but in the background, you are redirected to a series of other sites that send you an attack.” Often even the website’s owner doesn’t know the site has been compromised. Although search engines keep blacklists of known malicious sites, the bad sites are continuously changing.

Outsmart them: Make sure you install all available updates to your browser or use a browser that automatically updates, like Firefox. Vina’s research has found that Internet Explorer users are most vulnerable to these attacks.

They can infiltrate your baby monitor or smart TV:

Remember, your smart device is essentially a computer- and chances are, it’s not a particularly secure one. Anything in your house that’s connected to the Internet, from your smart fridge to your climate-control system, can be hacked. In several recent incidents, hackers were able to hijack a baby monitor and yell at a baby. Experts have also shown how hackers can turn on a smart TV’s camera and spy on you.

Outsmart them: When setting up smart devices, always change the default password. Most of these devices work from your wireless router, so password protecting your Wi-Fi can also help. Keep up with firmware updates; many devices will inform you when there’s an update available. Otherwise, look for an Update Firmware option in the main menu or settings.

They eavesdrop on free public Wi-Fi networks:

Even if you’re connected to a legitimate public network, a “man-in-the-middle” attack can allow hackers to snoop on the session between your computer and the hot spot.

Outsmart them: Avoid public Wi-Fi, if possible, especially unsecured networks without passwords, advise security experts at MetLife Defender, a personal data protection program. Instead, set up your smartphone as a secure hot spot or sign up for a VPN (virtual private network) service. If you must use public Wi-Fi, avoid financial transactions and consider using a browser extension like HTTPS Everywhere to encrypt your communications.

They lure you with “shocking” videos on Facebook:

A friend just posted a video of an “unbelievable animal found in Africa.” If you click to watch, you’re asked to download a media player or take a survey that will install malware on your computer, says Tyler Reguly, manager of security research at the cybersecurity firm Tripwire. It also shares the video with all your friends.

Outsmart them: Type the video’s title into Google and see if it’s on YouTube. If it’s a scam, someone has probably already reported it.

They take advantage of your typos:

Fake sites with slightly altered URLs like micrososft.com or chse.com look surprisingly similar to the real site you meant to visit, but they’re designed to steal your data or install malware on your computer.

Outsmart them: Double-check the site’s address before logging in with your name and password, especially if the home page looks different. Check *https* in the address before typing in your credit card information.

They crack your password on “easy” sites

A 2014 study found that about half of us use the same password for multiple websites, making a cybercrook’s job easy. “A hacker will break into a soft target like a hiking forum, get your email address and password, and then go to your email account and try to log in with the same password,” says Marc Maiffret, chief technology officer at BeyondTrust, a security and compliance management company. “If that works, they’ll go to your bank account and try the same password.”

Outsmart them: Use two-factor authentication, a simple feature that requires more than just your username and password for you to log on. In addition to your password, for example, a site may require you to enter a random generated code sent to your smartphone to log in. Many companies-including Facebook, Google, Microsoft, Apple and most major banks – now offer some form of the safeguard.

They can easily break into routers the use WEP encryption:

Many older routers still rely on a type of encryption called WEP (Wired Equivalent Privacy), which can easily be cracked with a widely available software program that anyone can download.

Outsmart them: Make sure your router uses WPA2 (Wi-Fi Protected Access 2) the most secure type of encryption, or at least WPA. Click your computer’s wireless network icon to check the security type. If your router doesn’t give you one of those choices, call your router manufacture to see if you need to do a firmware update – otherwise, plan to get a new router. Don’t forget to change your preset Wi-Fi password, since any good hacker knows the default passwords for all major routers.

They impersonate trustworthy companies:

You may get a fake financial warning from your bank or credit card company, order confirmation from a retailer or social networking invitation.

Outsmart them: Remember, most companies never ask you outright for your account information. You can sometimes spot this type of scam by hovering over the address in the 'From' field or by hitting 'Reply All' and looking for misspellings or strange addresses. Also, check to see that the email was sent to you and only you. If you're not sure it's legit, call the company instead.

They debit tiny amounts – at first:

Cyberthieves may test-drive a stolen card number by running a small charge under $10 to see if anyone notices.

Outsmart them: Check your transactions online regularly – even daily. If you spot a charge you don't recognize, report it immediately to your card issuer. To prevent hackers from getting your card information remember these 10 times you should never pay with a credit card.

- When a website does not begin with "HTTPS"
- When you're responding to an email
- When charity fundraisers approach you on the street
- When speaking to anyone over the phone
- When an online merchant has no reviews or previous listings
- When you are making a purchase you can't afford
- When a merchant needs to take your card out of view for payment
- When purchasing online while connected to public Wi-Fi
- When purchasing something on a public computer
- If you see bulky, plastic, exposed wires on devices you're about to swipe through

They hacked that ATM you just withdrew cash from

Crooks install cleverly disguised "skimmers' to steal your card information, while a hidden camera or a thin skin over the keypad captures your PIN. Now, scammers even have ways to target ATMs remotely.

Outsmart them: Try to use ATMs inside financial institutions, where it's tougher for criminals to install these devices, and inspect the machines carefully before you use it.

They count on your downloading our free, fake version of popular apps:

These apps steal confidential information or bypass your phone's security settings and subscribe you to premium services. "You choose the free version of a game, it asks for all sorts of access, and you say 'yes, yes, yes' to all the permissions," Vigna says. "The next thing you know, it's sending you premium SMS text messages and stealing your money."

Outsmart them: Before installing an app, check the ratings and number if people who have installed I – hackers can fake positive ratings, but they can't stop other posters from warning that the app is a trick. Most fake apps have to be downloaded straight from a website, so make sure you always download from an official market like Google Play or Apple's App Store.

They love that you always leave Wi-Fi on:

Though it's convenient to leave Wi-Fi turned on while traveling with your laptop, tablet or smartphone, your device will constantly try to connect to known networks. Connecting to open Wi-Fi can be risky since attackers can identify those networks and set up rogue networks that impersonate them.

Outsmart them: Get in the habit of turning off your Wi-Fi every time you leave your home.

They fool you with bogus software updates:

You know you're supposed to update your software to protect it, but hackers may send you fake updates that actually install malicious backdoor programs on your computer.

Outsmart them: If you get a pop-up message about an update, go to the software provider's actual website, and check to see if it's real. You can also try closing your browser to see if the pop-up disappears – if it does, it may be a fake.

They can crack supposedly safe retailers:

Experts say big brands will continue getting hacked until retailers can better protect their data. Hackers sell your information on the black market, and other criminals then use it to make counterfeit cards that can be used for shopping.

Outsmart them: Don't save your financial information when you shop online – check out as a "guest" when you can. If you fall prey to an attack, ask your bank to issue you a new card, take advantage of any credit monitoring that's offered, and scrutinize your statements.

Safety in real life:

Readers who recovered from or prevented a cybercrime share their advice:

Try not to apply for credit cards online – Credit card companies require your Social Security Number. Once you put that out there, it's out there forever.

Avoid debit cards – They allow hackers much easier access to bank accounts than credit cards do. Also, when logging in to an online account, never check the box that says, "Remember me." It takes only a couple of seconds to type in your username and password each time, and you don't want that information 'remembered.'

Consider freezing your credit – with the three credit bureaus and simply thawing your file when you need to open a new account. Keep passwords you need to thaw the account in a safe place. This is free or inexpensive in most states.