66 Ways to Take Control

Do one, some, or all. Each one will make a big difference.

1 | Check Your Data Breach Status

Takes 14 seconds

Wondering whether your personal data is for sale on the web? At haveibeenpwned.com you can check your email addresses and usernames against lists from 120 known breaches at companies including Adobe, LinkedIn, and Snapchat. (You'll need to register to check the full database.) If your name pops up, change the password for the compromised account and any other site where—*tut, tut*—you were using the same password.

(Bonus tip: Pros pronounce "pwned" as "poned," not "pawned.")

2 | Stop WiFi Imposters

Laptops, smartphones, and other WiFi-enabled devices can automatically connect to familiar networks. That's convenient—no one wants to enter a password for their home or work WiFi every day—but it can also be risky. A hacker can set up a rogue WiFi network with the same name as a legitimate one such as "Google Starbucks" or attwifi and trick your gadgets into joining it.

Periodically get a fresh start by using your devices' network or WiFi settings to prune the networks you join automatically. Most devices let you delete networks one by one, but if you have an iPhone or iPad, you need to go to Reset Network settings under General settings and delete all of them at once.

3 | Use 10-Minute Mail

You're often asked for an email address to access a website or sign up for a loyalty card, even if you want to use the service just once. Comply, and you're in for years of marketing come-ons. "Everyone wants your email address these days," says Nathan White, senior legislative manager at Access Now, a digital-rights organization. But you don't have to provide a real one. White recommends 10minutemail.com, where you can get a functional email address for 10 minutes (or 20, if you need it), just long enough for you to log on to a site. When the time is up, the email address self-destructs—and 10minutemail.com doesn't retain any personal data.

4 | See Who Shared Your Private Data

Sometimes you need to register for a website with your real email address, say, if you plan to log in repeatedly to make purchases. Here's a neat hack for ferreting out which companies are sharing your data with email lists, if you have a Gmail account: Type "+" before the @ symbol and add the website's name. Email addressed to YourName+Websitename.com@gmail.com will go to the regular inbox for YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you've never heard of, you'll know whom to blame.

If it has a screen, it needs a password or PIN.

Lock Your Screens

Set a password or PIN for every laptop, smartphone, and tablet you own. Any lost device without a screen lock is an unprotected gateway for thieves, who may be able to access your email, banking, and social accounts, changing passwords and taking control of your digital life. Here's how to do a screen lock right:

5 | Go Long

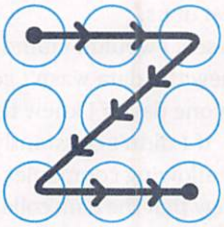
Use a screen-lock PIN made up of at least six digits, not four. (See page 30 for an explanation of the math behind that.)

6 | Try to Be Unique ...

Don't use any of the following PINs because they're far too common, accounting for almost 20 percent of those currently in use: 0000, 1111, 1212, and 1234.

7 | ... but Not Too Personal

Your birth date? The last four digits of your Social Security number? Your phone number? Those are all terrible, horrible, no-good, very bad PINs. Don't use them.



8 | Do Better Finger Art

Android users can unlock their phones by tracing a pattern on the screen. To be safe it needs to be unpredictable, but often it's not. For her master's thesis at the Norwegian University of Science and Technology, Marte Løge analyzed thousands of patterns. Seventy-seven percent began in a corner. One in 10 formed a letter—such as the Z above—often the first initial of the user's name.

abuse of its monopoly power. I set up Ida with a credit card (linked to my account), an email address, an Amazon account, a postal address, a cell phone, and even a few social media accounts.

Even though Ida was the thinnest of disguises—any decent investigator could link her to me—I found using her as an alias to be incredibly satisfying. I loved booking a restaurant reservation under her name and being greeted as Ida. I loved ordering books about the history of the National Security Agency from her account rather than mine. I loved using her name to sign up for stupid online games that I was embarrassed to be caught playing.

Ida is my homage to the fleeting pleasures of the past, a past anyone over the age of 40 can recall but younger people may find hard to grasp. Back when buying a video game or a frivolous magazine or a drink with an old boyfriend didn't create a data trail to be stored, scrutinized, and analyzed for generations to come. Using Ida's name empowers me by restoring anonymity to everyday life.

Ida Tarbell: Muckraker and the author's favorite alias.

Privacy as Mindfulness

Armed with my tracker-blocking software, my secure passwords—and, of course, Ida—I believe I've called the bluff of those who claim that privacy is dead. In fact, there's a lot you can do.

And yet.

The multibillion-dollar trade in personal data—what's often called the surveillance-industrial complex—continues to expand. I've had wins in my personal battles, and so have many others. But a larger win would be a shift in the balance of power between the data collectors and the rest of us.

You see, I wouldn't mind some of my behavior being tracked if I knew the data wasn't going to end up denying me a job or a loan one day. If I knew that I could successfully dispute it in court. If I didn't constantly have to sign unconscionable contracts allowing companies to use my data however they liked. If I knew that the data collectors would protect my information from being hacked. If I knew that my children's future wouldn't be forever marked by an idiotic video they posted when they were 8. If I knew that I could indulge in ephemeral, innocent joys without leaving a permanent record.

But I don't have any of those guarantees today. In Europe, companies that collect personal data are required to give people access to their data, the ability to dispute it, and in some cases, the right to remove it. But the United States has no such laws. And the companies themselves don't seem to be leading the way.

So until I can be assured how my data will be used in the future, I'm reluctant to employ it as a currency to buy services. Instead I choose to pay whenever possible with dollars, with my effort, and with my time. Three years after my experiment was supposed to end, I still do most of my privacy-protecting moves. I secure my computer. I block tracking. I reclaim my data when I can. I hoard my data at home. And I delight in using my fake identities. (Yes, I have a few others, too.)

Despite its hassles, I've grown to like the practice of privacy. To me, it's another form of mindfulness. Even though I know my victories are incomplete, they give me a sense of control over the technology that is encroaching on my life. Each new act of resistance gives me strength to imagine a better world, one where we have some assurances about how our data is used.

It's not that hard. And I hope that others find a few acts of resistance that work for them, too. ■

Julia Angwin is an award-winning senior reporter at ProPublica who covers technology and surveillance. She is also the author of "Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance" (Times Books, 2014).

Continued on next page ›

content of our emails scanned. We agree to have our friends identified and analyzed in "social graphs." We agree to have our images stored, shared, and tagged and our faces analyzed to help companies perfect their facial recognition tools. We agree to have our voices analyzed, our fingerprints scanned, and soon enough, the iris patterns of our eyes stored in vast, remote databases.

Theoretically, we could read all the fine print in the "terms and conditions" and "privacy policies" foisted on us and refuse to use products that track us egregiously. But who has time to do that? In a 2016 experiment by researchers at Toronto's York University and the University of Connecticut, 74 percent of people who joined a fictitious social network skipped reading the privacy policy altogether. And those who opened the terms and conditions must not have read them very carefully—because all of them agreed to give up their firstborn child to the social network.

In fact, failing to read privacy policies is perfectly rational. In 2008, Carnegie Mellon researchers estimated that it would take an average individual 154 hours to skim the privacy policies for the approximately 1,462 websites they encountered each year. In terms of wages and lost time, that would amount to $2,226 per person.

Even if we read all those policies, we still couldn't accurately weigh our privacy trade-offs. Our data is a currency that we trade for services, but we don't really know what the data will cost us in the future. Could it keep us from landing a job? Rob us of a good deal on insurance? Get us thrown in jail? It's impossible to say.

All we know for sure is that it seems like it would cost a lot of time and energy now to try to keep our data from costing us even more in the future. No wonder most people feel overwhelmed by the task.

Paging Ida Tarbell

One day in 2012, I was on a city bus talking to a friend about how hopeless privacy trade-offs can seem. She asked: "Is it hopeless because no one cares? Or is it truly hopeless?" In a flash, I realized that I didn't know the answer. I hadn't ever really tried to protect my privacy because I assumed it would be too difficult.

So I began a privacy experiment. For a year I sought to protect my data as much as possible while continuing to remain connected to the internet, my phone and my friends, and all the joys of the information age.

What I found was that protecting my privacy wasn't as difficult as I thought. There were plenty of steps I—or anyone—could take that were simple, cheap, and effective. And most important, my actions gave me a feeling of reclaiming control over the technology invading every corner of my life.

I started with the basics of computer security—essentially, locking the doors of my digital home. I updated all my software so I wasn't vulnerable to criminals who might exploit flaws in old versions. I deleted free applications that I was no longer using that could be stealing my data. I installed software and adjusted the privacy settings on my web browser to block the most common types of tracking used by advertisers. I purchased software to help me generate and manage strong passwords. I covered my laptop camera with tape so that hackers couldn't see anything if they took control of it remotely (which unfortunately is easy for them to do).

Once I had secured most of the entry points to my digital domain, I began trying to reclaim my data from as many places as possible. I took some big steps, and I realize not everyone will want to follow my lead.

"I've called the bluff of those who believe privacy is dead. In fact, there's a lot you can do."

First, I stopped using the social networks LinkedIn and Facebook. Surprisingly, I didn't miss them much—I discovered that I preferred staying in touch with friends through phone calls and visits. Next, I decided to break up with Google. The company had famously promised not to be "evil" in its corporate motto. But when I checked my account's privacy dashboard, I saw that Google had more intimate information about me than my closest friends and family. Google's search history revealed that I often browsed for shoes when I was stressed out on tight work deadlines. Google Maps recalled all the trips I had taken, foreign and domestic, along with my precise routes. And I already knew that Google's Gmail recorded the fact that I emailed my close girlfriends more than my husband.

I started by abandoning Google's admittedly excellent search engine. I began searching on the website DuckDuckGo.com, which doesn't track its users. It makes money the quaint old-fashioned way, by showing so-called "contextual" ads related to the search query rather than "behavioral" ads that track users across websites.

Replacing Gmail with a service that promised not to scan my personal correspondence was more expensive. I gave up both Gmail and Google Docs, and ended up paying about $200 per year for an encrypted cloud storage system—and then invested $100 for a hard drive to store my emails at home. I was starting to feel like a data survivalist, stockpiling terabytes of personal info.

Yet all these digital barriers didn't help me hide the details of my offline life—whom I had coffee with, where I saw movies, whom I emailed. So I pulled a real Jason Bourne move: I created a fake identity. (Yes, it is legal to maintain an alias if it's not used for fraud.) I began using the name Ida Tarbell, after the turn-of-the-century muckraker who revealed Standard Oil's

But first, read what investigative reporter **Julia Angwin** learned in her own quest to boost her privacy.

▶ WHEN I WAS growing up in the 1980s, my parents would occasionally take my brother and me for a special treat: an evening spent browsing for software at a local computer store.

We would wander among the aisles of shiny, shrink-wrapped boxes, lobbying our parents to buy us games such as the geography spy mystery "Where in the World Is Carmen Sandiego?," which cost about $40 a pop.

Flash-forward nearly 30 years, and my own kids can't believe I ever paid so much for a computer game. Most software packages—from games to productivity apps to health-tracking apps—are free.

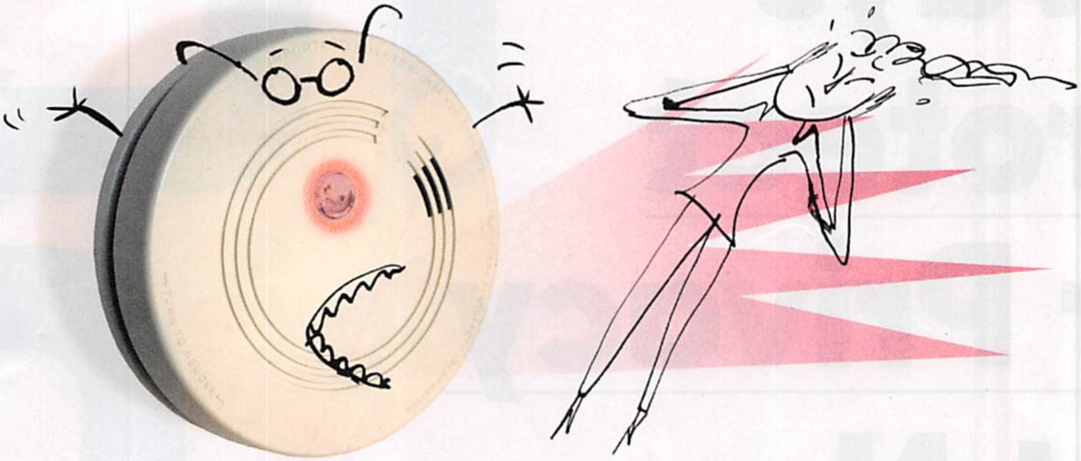
There's only one catch: We pay for all this software with a new currency, our personal data. Whenever we download an app, visit a website, watch a smart TV, use free WiFi, or partake of most of the joys of the information age, we agree to give up previously unimaginable amounts of personal data.

The shift toward data as currency began somewhat innocuously. At first, we simply accepted ads targeted to our search queries. But now, a decade later, the trade-offs have become more extreme. We implicitly agree to have our movements followed both virtually, as we browse the web, and physically, as our phones transmit our locations. We agree to have our interests cataloged and analyzed. We agree to have the

ILLUSTRATIONS BY MICHAEL BRANDON MYERS

66 Ways to Protect Your Privacy Right Now

Ah, the joys of the connected life: opportunities to engage with global communities, be educated and entertained, and shop with ease. But these go hand in glove with intrusions from marketers and threats from criminals. The tips on the following pages, compiled with input from dozens of security experts, will help you take control. Start on page 28.



My neighbors' smoke alarm went off at 3 a.m. Fortunately, it was a false alarm, but they didn't know how to turn it off. What do I do if mine does the same?

In 2014, 33 percent of false alarms that fire departments responded to were caused by malfunctioning smoke alarms, according to the National Fire Protection Association. Those noisy mistakes can be caused by dust, humidity, electrical malfunctions, and even spiders crawling inside, says Bernie Deitrick, a senior engineer in our testing department.

To know how to resolve a false alarm quickly, you need to understand your home's alarms and how they operate. There are three types of power sources: replaceable batteries, long-life lithium batteries, and 120-volt hardwiring (with batteries as backup power sources). Always assume a sounding alarm means there's a fire and get to safety if need be. But once you're sure it's an error, your approach should vary based on the type of power your alarm uses. Your first step is to find the device that's going off and reset it by pressing and holding the reset button. If that doesn't work, take the device down. If you can, remove the batteries; if the alarm has a lithium battery you can't take out, muffle it in a blanket, under a sofa cushion, or in your freezer until it stops.

As for hardwired detectors, "they're interconnected through the electrical wires, so if one alarm sounds, they'll all sound and it can be difficult to figure out what's going on," Deitrick says. First, try the reset button on each alarm. If that doesn't work, flipping the circuit breaker off and back on might stop the noise. If all of that fails, your ultimate solution may be to disconnect the units and remove their batteries one by one. A small connector at the back of each alarm can be unclipped to let you safely remove it from the network.

LEARN

We have more than 140 in-house experts who research, test, and compare—so you don't have to! Send your questions to: ConsumerReports.org/askourexperts ... and watch this space for the answers.

Then it may be time for new alarms. Our top recommended model is the First Alert 3120B, an interconnectable hardwired model with dual sensors and battery backup. CR.org subscribers can find full ratings at ConsumerReports.org/smokealarmratings.

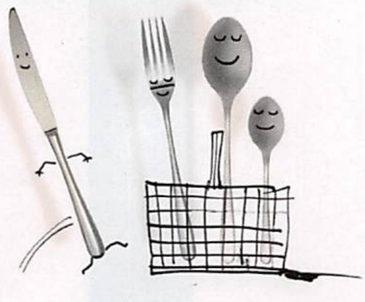
What's the best cash-back credit card for groceries?

Finding the best card for you involves taking into account not just how much cash you get back but also the card's fees and rebate rules. We recently ran the numbers for a family that spends $375 per month on groceries. The top choice we found among more than 50 widely used credit cards: the American Express Blue Cash Preferred. With a 6 percent rebate on charges up to $6,000 yearly at U.S. supermarkets, the card would return $810 over the first three years. The Amex Blue Cash Everyday came in next, offering $505 back during the first three years. And the Chase Freedom card could net that family $420 during the first three years. To help you navigate this tricky territory on your own, Consumer Reports created the Credit Card Adviser Comparison Tool, which guides you to good options by calculating the costs and benefits of major cash-back cards based on your buying patterns. Go to ConsumerReports.org/cardcompare to try the tool.

I put cutlery in the dishwasher handles down; my sister does handles up. Who's right?

You're both partly right, says Larry Ciufo, who leads dishwasher testing in our Home & Appliance testing labs. "Load forks with the tines up, so they get more exposure to the jets of water and detergent–same for the bowls of spoons," he advises. "Knives should go in with the sharp point down, so you can avoid cutting yourself as you remove them."

It's also important to rinse cutlery before loading because foods like coffee, mustard, and eggs can corrode the metal. "And avoid overcrowding," Ciufo warns. "If your dishwasher has an open basket, mix spoons, forks, and knives to prevent them from nesting." CR.org subscribers can find detergent ratings at ConsumerReports.org/dishdetergentratings.



ILLUSTRATIONS BY SERGE BLOCH

Snail-Mail Privacy

9 | Shred These 5 Document Types

Do you really need to destroy every piece of paper that has your name and address on it? "Probably not, but I shred a lot," says Kelley Long, a CPA and certified financial planner at Financial Finesse, a company hired by HR departments to coach employees on personal financial issues. In particular, Long recommends destroying any health-related documents. "Medical identity theft is a growing threat," she says. Your Long-approved list of paperwork to shred includes any documents containing the following:

- SOCIAL SECURITY NUMBER (even just the last four digits)
- BIRTH DATE
- CREDIT CARD NUMBERS
- ACCOUNT NUMBERS FROM FINANCIAL INSTITUTIONS
- MEDICAL INSURANCE NUMBERS

Does it show your birth date? Shred it.

10 | Shut Off the Flow of Credit Card Offers

These unsolicited mailings can be intercepted and filled out by identity thieves who have credit cards sent to their own addresses, then start piling up debt in your good name. You can put a stop to most of these offers by going to optoutprescreen.com or calling 888-567-8688. The service, run by the Consumer Credit Reporting Industry, will turn off the spigot permanently or for five years. You can always opt back in.

11 | Receive Less Mail

When you give a company your name and address, chances are good that the information will be added to direct-marketing lists and used by other companies to send you solicitations. Go to dmachoice.org to remove your info from many mailing lists if you don't want the offers.

12 | Return to Sender

Life as a direct-marketing target: You go to the mailbox, filter out the offers you don't want, put them in the recycling bin—and repeat. But if an unwanted envelope is printed with the phrase "Address Correction Requested" or "Return Postage Guaranteed," you have an alternative. You can write "Refused/Return to Sender" and mail it back—no postage required. You'll keep your recycling bin svelte while making the marketing company pay the return-trip postage. It's a tiny win, but still a win.

13 | Turn on Automatic Updates

Keeping your software up-to-date is the most critical step you can take to boost security, according to professionals surveyed last year by Google. "Software updates are like oil changes," says Mark Surman, executive director of the Mozilla Foundation. "They can be a hassle in the moment but a lifesaver in hindsight." Hackers are always exploiting more vulnerabilities, while security pros play nonstop malware whack-a-mole. If you've got old software, you're missing the latest protections. "Most modern software will update itself if you let it," Surman says. Make sure you have auto-updates turned on across the board.

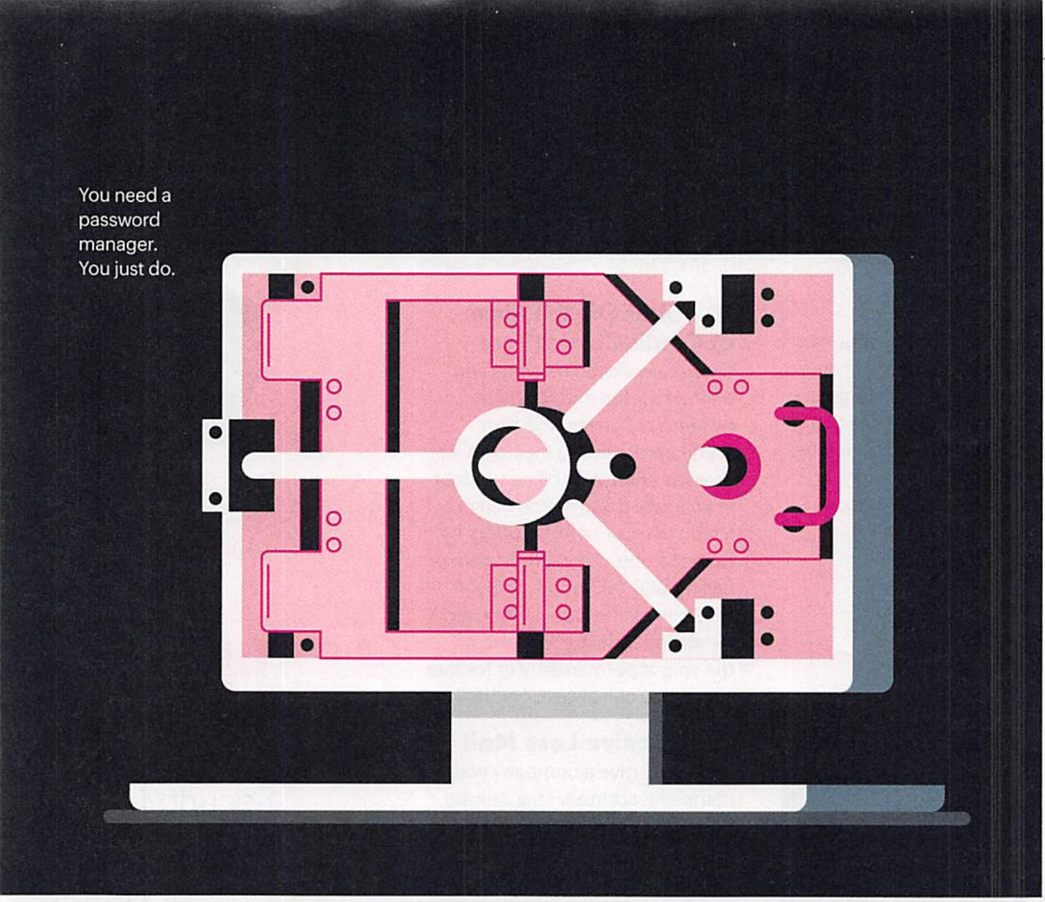
MY FAVORITE TIP

Dan Guido

CEO of Trail of Bits, a digital security firm

14 Make Sure There's Info-Security Staff

"It's hard to judge how well companies guard your data, but here are two smell tests for how seriously they take security. I like doing these before giving up personal data to a company or setting up its devices on my network. First, does the company have separate contact information for reporting security issues? You don't want that kind of problem to languish in a general customer service box. Another test: I check out the company on LinkedIn. Is there someone with 'security' in their title at the company? I wouldn't entrust my security to any company that doesn't have a software engineer dealing with these issues full time."



You need a password manager. You just do.

Make Unbreakable Passwords

It's easy to create passwords that are difficult for hackers to crack, but not enough people do it. Jeremi Gosney, the head of the password-security firm Sagitta HPC and co-founder of a hacker conference called PasswordsCon, recently cracked 173 million of them in just six days. That represented 98 percent of the passwords stolen from LinkedIn in a huge data breach in 2012.

A major problem, Gosney says, is that most passwords are just too predictable. "We know every trick people use: foreign words, movie or book titles, patterns on the keyboard, anything you can think of," he says. And it doesn't take long for experts armed with the latest computer technology to run through all of the familiar patterns.

Strong passwords have two things in common: They avoid patterns and they're just too darned long for a brute-force attack—in which a computer runs through every possible combination of characters—to succeed. But assuming that a password is a truly random collection of characters, how long is long enough? Security experts use some quick math to get the answer (see below). That's the theory, but you don't need to crunch numbers to boost your password potency. Just do the following:

15 | Stop Making Sense

🕘 Takes 75 seconds

One way to make a great password is to string together unrelated words. "It's the Diceware method, in effect," Gosney says. Diceware is a low-tech way to pick passwords that was developed in the 1990s. You roll dice to pick from a list of 7,776 words. But you don't have to actually roll dice. Just pick five long, random words and string them together into a nonsense sentence that you can remember.

16 | Use a Password Manager

Here's the rub: We all have a lot of passwords, and it's tough to remember long strings of random characters. Password managers can generate a complex, unique password for each account. "They used to be hard to navigate, or you had to copy and paste," Gosney says. "But now they actually eliminate steps from my workflow." He likes LastPass and 1Password. (LastPass was hacked last year, but users' passwords apparently remained safe.) You'll still need one well-crafted password for your password manager account—so review Tip 15.

17 | Got a Great One? Okay, Write It Down.

Everyone tells you not to commit your passwords to paper. Ignore that. "As long as you're not leaving Post-it notes under keyboards, it's totally cool to write passwords down," Gosney says. He keeps vital passwords—including the one for his password manager and his phone's lock screen—in a sealed envelope to be opened only if he's incapacitated. That way, his loved ones can access his online accounts to pay bills and take care of other business.

18 | Be Password Loyal

People also tell you to change passwords regularly. Don't, unless there's a good reason, such as responding to a data breach. Switch often and you'll probably end up using weak options.

PASSWORD MATH

$$\overset{1}{E}=\underbrace{LOG_2\underbrace{(\overset{2}{R}{}^{\overset{3}{L}})}_{4}}_{5}$$

1. E stands for "entropy," which is the opposite of an ordered pattern. Entropy is good: The bigger the E, the harder a password is to crack.

2. Let's say your keyboard has 95 unique characters. If you're randomly constructing a password from that whole set, R=95.

3. Let's say you have a 12-character password. If so, L=12.

4. The number R to the L power is 540,360,087,662,636,962,890,625—which is how many possible passwords you've got. Quite a mouthful, isn't it?

5. That's the same as $2^{78.9}$—and the $\log_2$ of that is 78.9. In info-security lingo, it's 78.9 bits of entropy. That approaches the "exponential wall," where a password could take ages to crack. And yes, 12 characters picked *at random from a keyboard* will do the job. Or just see Tip 15.

19 | Stop ID Theft After a Death

Identity theft affects 2.5 million estates every year, according to the IRS. If a loved one has died, send a copy of the death certificate to the IRS (the funeral home may help with that). Also, cancel any driver's license, and notify credit agencies, banks, insurance firms, and financial institutions.

20 | Go Belt and Suspenders with Two-Factor Authentication

Two-factor authentication (or 2FA) helps prevent unauthorized access to email, financial, and other accounts if someone steals your password. It's available for many businesses, from Google to Fidelity Investments to Snapchat. Once you enable 2FA, you'll have to enter an additional piece of information—usually a set of numbers sent by text to your phone—with your password when you log in to your account. So a criminal would need both your password and your phone to cause trouble. Go to twofactorauth.org for a partial list of sites that offer 2FA.

MY FAVORITE TIP

Nathan White

Senior legislative manager at Access Now, a digital and human-rights organization

23 Let Google Scan Your Files

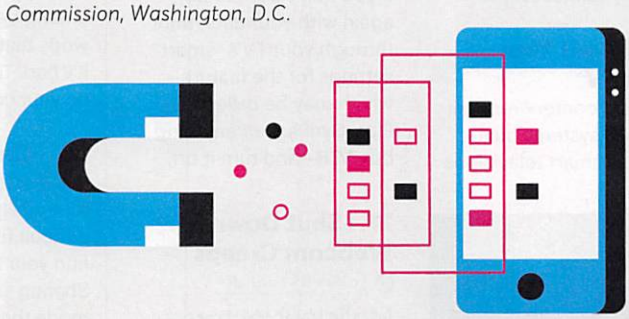
"If you're just a bit suspicious of a document you've received by email, save it to Google Drive and open it there. If there's any malware enclosed, it will be isolated in a virtual environment, away from your operating system. As a second benefit, Google Drive automatically scans files for known viruses. This doesn't take the place of your own antivirus software, but it's a simple way to add a layer of protection."

IT HAPPENED TO ME

My Mobile Account Was Hijacked

By Lorrie Cranor

Chief Technologist, Federal Trade Commission, Washington, D.C.



EARLY ONE EVENING last spring, my mobile phone stopped working. I wasn't too worried, but the next morning my husband's phone wasn't working, either. We went to one of the carrier's stores and learned that two iPhones had been purchased on our account.

When I called the carrier's fraud department, the rep confirmed that someone had "upgraded" our two phones and transferred our numbers.

I immediately logged in to my account and changed the password. I also placed a fraud alert with the credit-reporting agencies. And I had to spend many hours getting the carrier to finish cleaning up the mess.

But I still didn't know how the theft happened. Section 609(e) of the Fair Credit Reporting Act requires companies to provide victims of identity theft with all business records related to the incident. So I filled out a template at identitytheft.gov, a site run by the Federal Trade Commission where you can report thefts like this, and mailed it in to the carrier.

Two months later, I received the records. I learned that the thief had acquired the iPhones in Ohio, hundreds of miles from my home, at one of my mobile carrier's retail stores. She used a fake ID with my name and her photo. According to the records, the store clerk "followed proper authentication procedures."

The thief probably sold the phones quickly. And as far as I know, she hasn't been caught.

How to keep it from happening to you:

21 | Activate a PIN

Sprint requires customers to set a PIN and security questions for their accounts, and the other major mobile providers offer customers the option. Take it. Having a PIN can help keep strangers from making changes to your account.

22 | Watch Your Bills

Many wireless plans are based on a flat rate, so make sure your bill is consistent from month to month. If it's not, take a closer look at your account.

24 | Check on the Kids

Minors had their identity stolen 51 times more often than adults in a study by researchers at Carnegie Mellon University. Keep an eye out for letters from collection agencies, bills for unpaid balances, or a warning that pops up when you try to file your taxes electronically if you list your child as a dependent. But sometimes there's no hint that a minor is a victim of identity theft. To be safe, request reports from the three big credit-rating agencies by the time your children turn 15. That will give you time to clear up any problems before they apply for college loans, jobs, or credit cards.

Combat Snooping Gadgets

Web-connected devices promise convenience, but some can leak private data. Here's how to keep your information safe.

25 | Lock Down Your Baby Monitor

Hackers sometimes break into WiFi-connected babycams, even hijacking the speakers to talk to children and caretakers. That's often because users don't know to change the default settings. When you set up any internet-enabled camera, create a unique username and password. Also, turn off the babycam when it's not in use. That will make hackers less likely to discover it.

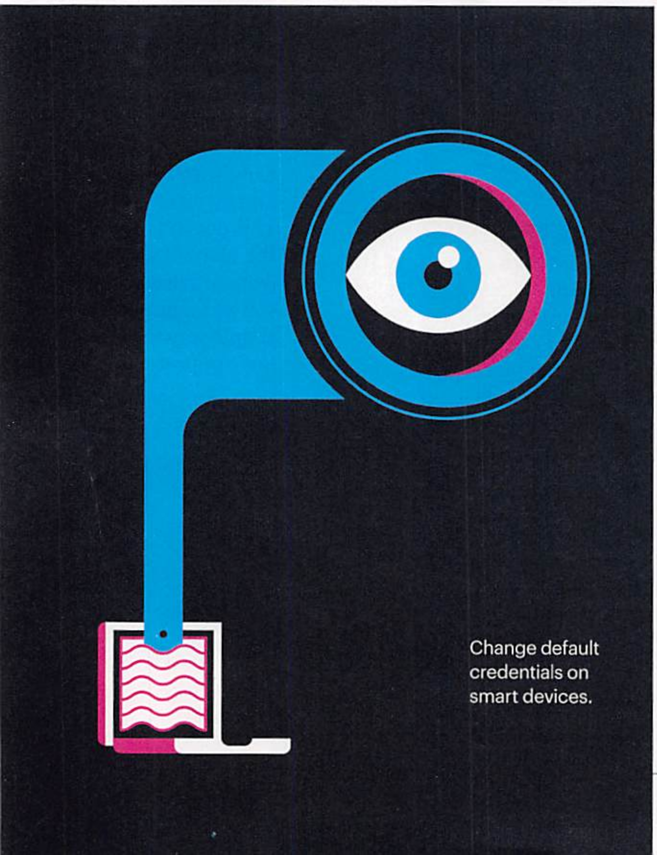
26 | Outwit Your Smart TV

Automatic content recognition (ACR) systems built into many smart televisions transmit data to analytics companies that may use it for marketing. You've already paid for your TV with money. If you don't want to pay again with your data, hunt through your TV's "smart" settings for the feature—which may be called Live Plus, SynPlus, or anything but ACR—and turn it off.

27 | Shut Down Webcam Creeps

Takes 8 seconds

Malicious actors have repeatedly proven that they can turn on a laptop's camera without the user's knowledge. The simplest solution? Do what Facebook CEO Mark Zuckerberg and FBI director James Comey do—put a piece of tape or a Post-it note over it. Hackers haven't yet cracked the adhesive code.



Change default credentials on smart devices.

Prepare Your Laptop for an Outing

Lots of stuff that's fine at home—hanging out in your PJs, using WiFi file sharing, eating peanut butter from the jar—is totally inappropriate at a coffee shop. Here's how to get your laptop ready to leave your home network.

28 | Deploy Your Firewall

Bad guys hang out at cafes and other public places, waiting for innocent laptops to wander by. To stop them, first turn on your firewall. This is software built into your laptop that restricts how outside computers can link to it. (At home, your WiFi network is probably protected by the firewall built into your router.) You'll find firewall controls under your laptop's Security settings.

29 | Restrict File Sharing

Takes 23 seconds

File sharing makes it easy to swap documents among devices. If you're on your home network, that's good. When you're on public WiFi, it's bad. Turn it off under the Sharing settings on your computer.

30 | Cloak Your Computer

You just turned off file sharing, right? Also turn off Network Discovery to make it more difficult for other devices on the network to find your laptop. On PCs, it's under Advanced Sharing settings. Mac users can enter Stealth mode through Firewall Options.

31 | Do All of This Automatically

Clicking away at laptop menus every time you leave home can be annoying. Windows makes it easy to automate the process using Advanced Sharing settings. Also, whenever you join a new WiFi network, Windows asks whether to add it to your "home" or "public" profile; the operating system forgets the public networks when you log off. To do something comparable on a Mac, use the free-to-download ControlPlane app.

32 | Use a VPN

Virtual public networks route your traffic through a single remote server that has tight security in place. Traveling with a work laptop? Turn on your company's VPN even for personal use, if that doesn't conflict with company policies. Or consider using a paid service such as IVPN or the free VPN that was recently introduced by the Opera web browser.

33 | You Know What? Just Fake It.

Toymakers are rolling out connected kids' products—including tablets and talking dolls—and asking families to divulge personal information to register them. But that essentially provides marketers and potential hackers with details about your children. So consider providing fake information. For an address, may we suggest Bart Simpson's—742 Evergreen Terrace?

Use Everyday Encryption

"Encryption is for everybody—activists, journalists, secretaries, grandmas," says Matt Mitchell, aka Geminiimatt, an info-security consultant and host of monthly cryptography-instruction gatherings in Harlem. "When you mail a letter, you seal the envelope so no one can read it. It's the same idea with your data and encryption." Basically, encryption scrambles your data so that it's unreadable by anyone who doesn't have permission to access it.

34 | Do Your Phone First

"Your smartphone knows everything about you," Mitchell points out. New iOS and many Android smartphones are encrypted by default; if you have an older mobile OS, you'll need to go into Settings.

35 | Next, Your Computer Files

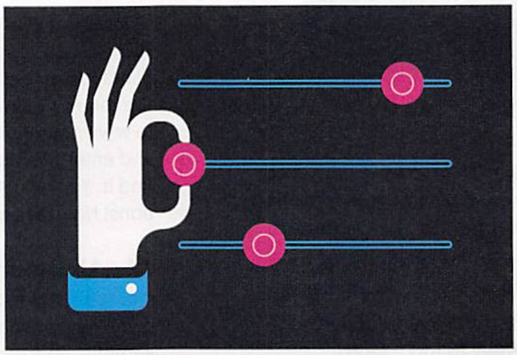
You can encrypt your whole machine or just sensitive files. To encrypt specific files on a Mac, use the Disk Utility. Windows 10 Home users can download a free app such as GPG4win (aka Gnu Privacy Guard).

36 | Finally, Your USB Drive

Flash drives can be misplaced—along with your files. Mitchell recommends Apricorn flash drives with built-in encryption. He says they're pricey but worth it, starting at $99 for 8GB.

Stop Oversharing on Facebook

It doesn't cost old-fashioned money to use Facebook, but you pay for access with your data, which is vacuumed up by the $350 billion behemoth in ways both obvious and hidden. Take these steps to boost privacy and limit how much Facebook—and its partners and users—can learn about you.



37 | Keep GPS Data Private

Facebook can extract your whereabouts from your mobile phone. But you can turn the function off using your phone settings. For an iPhone, you'll find the controls under Location Services. If you've got an Android device, look under Facebook Permissions in Applications Manager.

38 | Turn on Log-In Approvals

This is Facebook's name for two-factor authentication. (What's that? See Tip 20.) It keeps strangers from accessing your account—even if they steal your password.

39 | Become Elusive

Don't want people finding your Facebook page when they type your name into a search engine? You can change that and more under the "Who Can Look Me Up?" section of Facebook Settings.

40 | Leave a Group

Facebook lets users add friends to groups without their consent. But you can remove yourself from any group by going to your Activity Log.

41 | Reduce Ad Overload

You know those posts that read "So-and-so likes this" with a sponsored link? You can avoid being used in ads by tinkering with Facebook's Ad settings.

42 | Hide ID-Theft Clues

Your birthday. Your hometown. Your alma mater. Those are all things Facebook can reveal to the world—and they're answers to potential security questions. Hide such information by using the Privacy Checkup Tool found under the padlock on the upper right of any Facebook page.

MY FAVORITE TIP

Jeremiah Grossman

Chief of security strategy at SentinelOne, a digital-security company

43 Use separate browsers for low- and high-stakes websites

"Both my browsers are set up with anti-tracking and ad-blocking extensions, but I use one exclusively for all of my most important things, like banking and shopping. The other one I call my 'promiscuous' browser, and I do everything else on it, like reading the news or searching or whatever. If something bad happens within my promiscuous browser—a malicious software attack—it can't affect my bank account or credit card, because the promiscuous browser doesn't even know those accounts exist."

All your data goes through your router. Lock it tight.

Do an Engine Tuneup on Home WiFi Privacy

A couple of years ago, Craig Young, who works on the Vulnerability and Exposures Research Team at a security firm called Tripwire, found that 20 of the 25 most popular home routers sold on Amazon contained big security holes. (Some of those have since been patched.) And in 2014, it took Young just a few hours to find 10 flaws in wireless routers during a competition at Def Con, a hacking conference in Las Vegas.

This is bad, because the laptops, smartphones, and other devices you use at home all connect to the internet through your router. And so do web-connected devices such as smart TVs and some security cams and children's toys.

Here's how you can make your router more secure. The whole project shouldn't take more than 10 minutes.

44 | Find an Ethernet Cable

Then use it to temporarily connect the router to your computer. You'll be updating your router's firmware. And losing your connection during that process could turn your router into a doorstop. It's safer to rely on old-fashioned wires and plugs.

45 | Get the IP Number

Every router has two IP (internet protocol) addresses, an external one for communicating with the internet through a modem and an internal one for your laptop, smart TV, and other devices. To make changes to your router's settings, you need to access it through your browser using the local IP address. (Owners of Apple's Airport routers who have a Mac can make changes via Airport Utility.)

The local IP address is very likely to be 192.168.1.1, but you can double-check by looking in the router's manual. Lost it? Go to www.routeripaddress.com and enter the model name to find it. You're in. Congratulations! Now let's get to work.

46 | Update the Username and Password

If you never changed the default settings, do that now. (See Tips 15-18 for password advice.)

47 | Change the SSID ...

Your SSID—service set identifier—is your home network's name. Replace the default SSID with something more creative but not too personal. There's no need to identify this as your network, is there?

48 | ... Then Hide It

Router settings allow you to hide your WiFi network from prying outsiders. Note that once you do this, you'll stop seeing the network pop up in your own devices' WiFi lists, and you'll need to type the SSID into each device you want to connect.

49 | Embrace Encryption

Fasten your jargon seatbelts: You need to switch from WEP to WPA2-AES and disable the PIN method of using WPS. These acronyms represent ways to encrypt communications on your WiFi network. You want WPA2-AES because it's the newest and strongest. If you have really old devices, they may not be able to connect this way. And that means it's time to replace them.

50 | Update Firmware

Some routers today automatically update their firmware—they check for updates, install new software, and reboot in the middle of the night. But not all of them do—and many routers that say they have automatic updates require users to log on and hit "Okay." So do that.

51 | Make Sure Remote Management Is Off

Are you going to need to change your router settings when you're far away from home? Probably not. Do you want to allow anyone else to do it? No, so make sure that this feature is disabled. It's often referred to either as Remote Management, Remote Access, or Remote Administration.

52 | Shut It Down

Going out of town? Turn off the router unless you need it to access smart devices such as your thermostat or a security camera.

53 | And, Uh—Maybe Get a New Router

Signs it could be time for an upgrade: One, the router is too old to have WPA2-AES (see Tip 49); or two, it follows an old WiFi standard such as 802.11b or 802.11g. If you're getting a new router, skip 802.11n devices and choose one that follows the newer, faster 802.11ac standard. (We know—more jargon. Consult our routers buying guide at **ConsumerReports.org** for more details.)

54 | Check Links Before You Click

Suspicious of a link in an email or online ad? Check its safety with Sucuri SiteCheck (sitecheck.sucuri.net) or urlvoid.com. First, hover over the suspicious link and the full address will appear in the bottom corner of your browser; right-click to access the drop-down menu, and select Copy Link. Now paste the URL into your link checker to get a report. Foolproof? No. A good hint if there's a problem? Yes.

Up-Armor Your Browsers

Web browsers don't come with every protection you might want. Download extensions to improve security.

55 | Add HTTPS Everywhere

When you see "https" and a green padlock alongside a URL in your browser's address bar, it means that the data is encrypted as it travels back and forth between the website and your computer. (The "s" stands for "secure.") Some sites that support https use it inconsistently. Add the HTTPS Everywhere extension, which you can download from the Electronic Frontier Foundation, and your connections will be encrypted anytime you connect to a website that supports https. It works with the Chrome, Firefox, and Opera browsers.

56 | Block Snoops

Hate ads that steamroll over a web page? That's not the half of it. Many ads, along with webpage elements such as the Facebook "Like" button, send information about your online activity to their data-collecting masters.

"These ads aren't like billboards" that just sit by the side of a road, says Chris Jay Hoofnagle, who teaches privacy and internet law at the University of California, Berkeley. "They're live code being run by people you don't know and should not trust."

Extensions including Adblock Plus, Disconnect, Ghostery, Privacy Badger, and uBlock address this issue using varying approaches. Most let you add URLs to a "whitelist" of sites they won't check. You can do that if a favorite website stops working once you download the extension.

IT HAPPENED TO ME

My Files Were Locked Up by Ransomware

By Raul Glasgow

Owner, Shortcircuited Computer Repair Services, Brooklyn, New York

I DO INFO-TECH consulting and computer repair. I'm basically the computer guy for a number of dental and medical offices. One day last summer I got up and checked on the server where I keep my website–and the site was just gone. The files were encrypted, and I saw a message appearing in a pop-up window.

This wasn't the first time I'd encountered ransomware, so I knew what the message was going to say: To get the files back I'd have to pay the hackers in bitcoin, a digital currency.

I started seeing ransomware attacks targeting some of my clients two or three years ago, and since then it's become more common.

The first time it was a dental office, and they were being told to pay about $2,000 in bitcoin to get their files back. But we were worried they could lose the money if the hackers didn't actually restore the files–after all, we didn't know who these guys were. We ended up wiping everything and starting fresh with a new computer. We could do that because everything was backed up.

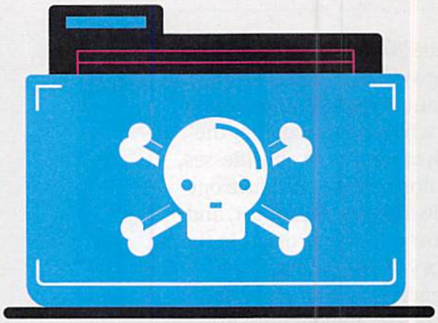
A few weeks before my own site was hacked, another dental office I work with had its patients' X-rays encrypted by ransomware, and they had no backups of those files. The ransom was lower this time, about $300 worth of bitcoin, and the client decided to pay up. There was no other good option.

With my own website, I really didn't want to pay a ransom so I said the hell with it–I'm just going to restore everything from a backup.

That would have been a big job.

But then I saw that one of the major anti-malware companies had a fix for at least some ransomware attacks–as long as you had a few of the files backed up and knew what ransomware software was involved. It wasn't something a lot of nontechnical people would be able to use, but it worked for me.

From what I've seen, antivirus companies are working on the problem, and they're starting to catch up. But the hackers are introducing even stronger encryption. And it's not always real hackers, people with skills. Anyone can just go online these days and buy the software they need to start a ransomware business. Instead of dealing drugs, a criminal can get into hacking.



How to keep it from happening to you:

57 | Back Up Your Data

Use a system that backs up your files automatically. If you're hit with ransomware, you'll have the option of restoring the data.

58 | Keep Software Updated

Ideally, set your computer and key programs to update automatically (see Tip 13).

59 | Try Haggling ...

Ransomware crooks are honing their "customer service," according to Philip Casesa, a strategist at the International Information System Security Certification Consortium. So it's worth asking for a ransom discount.

60 | ... But Not Right Away

Wait to click on the pop-up until you've obtained bitcoin, which can take time. The reason: The criminals will likely impose a time limit before deleting your data—and the clock starts ticking as soon as you click.

MY FAVORITE TIP

Cory Doctorow

Digital-privacy activist, co-editor of Boing Boing, and author of many books, most recently "In Real Life," a graphic novel

61 Use the Ubuntu OS

"Since 2006, I've used an operating system called Ubuntu, a variant of the GNU/Linux project, which binds together the work of volunteers, businesses, and nonprofits to produce one of the most stable, robust, and secure software projects in the history of computing.

It encrypts your hard drive, has an easy-to-configure firewall, and adds some esoteric under-the-hood protections. Because all its software is under free/open licenses, the Ubuntu project can distribute updates through one simple app, so my programs are always patched against all known attacks.

Ubuntu began as an OS that could run unsupported in poor sub-Saharan schoolhouses, and it relies on a community of users. It got its name from a Zulu word that means something like 'humanity towards each other.' This approach is our only hope for secure computing. Individually, we need good technology to protect our privacy—sure—but together we all need the rule of law when it comes to both corporate and government surveillance. That's why the best way to use technology to protect your privacy is to go online and tell your lawmakers how much this stuff matters to you."

Slip Through Phishing Nets

Pokémon Go is a mobile game—maybe you've heard of it. It was downloaded an estimated 75 million times in less than three weeks last summer, breaking records and attracting criminals armed with a phishing scam.

Phishing is when someone poses as a legitimate business to trick consumers into divulging information. In this case, fraudsters emailed Pokémon Go users saying that because of the popularity of the app, the game's servers were overwhelmed (that much was true) and that developers were starting to charge users $12.99 per account (a lie). The email prompted users to click on a link that went to a website that looked like the real Pokémon Go site and log in to their accounts. The goal? To get passwords.

One way to stay safe is to use two-factor authentication, which prevents a criminal armed just with a password from accessing your accounts (see Tip 20).

Here are two more:

62 | Scoff at Fake Email Notices

Surprised to find an email from a bank or social site asking you to log on? Don't click; open a new browser window and type in the address of the company website instead.

63 | Call Customer Service

Be leery if an institution asks for your log-on credentials through email or a text message. Instead of replying, call the company.

What Americans Say

Consumer Reports asked about privacy and security in a nationally representative survey of 1,012 adults. We wanted to explore two issues. Which marketing practices feel most intrusive? And how do people try to guard against tech-savvy criminals?

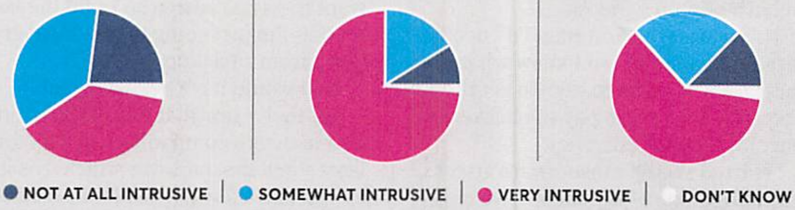
ARE MARKETING PRACTICES INTRUSIVE?

How do people feel about these real-world digital-marketing scenarios?

"You research an illness online, and then ads for remedies pop up in your browser."

"Without your knowledge, a data firm collects your web browsing and shopping history, then leases the information to advertising companies."

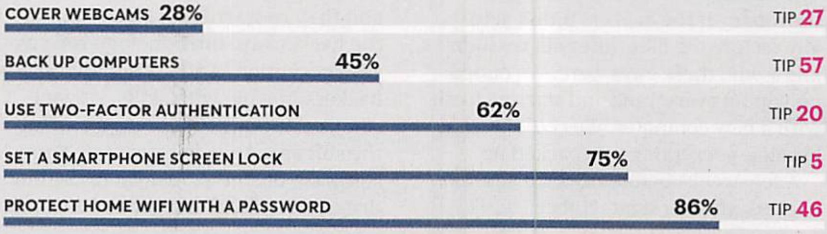
"The manufacturer of your smart TV tracks what shows you watch, then uses the information to sell ads targeting your family without your knowledge."



WHAT PEOPLE DO TO PROTECT THEMSELVES

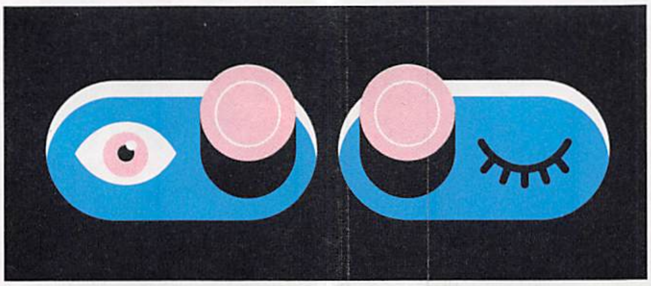
How many Americans take these simple steps to foil hackers?*

WANT TO DO IT YOURSELF? See these tips to learn how.



*Percentages don't include people who responded "not sure" or "not applicable."

PHOTO: JONATHAN WORTH



Tighten Google Privacy

For a seemingly all-knowing data machine, the search giant gives users a large amount of control.

64 | Tweak the Settings

Go to My Account to control what data about you is being collected and how it's being shared. In particular, go to the Personal Info & Privacy section to review Location, Search, and YouTube Search History. You can delete records one entry at a time or all at once, and if you'd like to, you can prevent Google from recording data going forward. Privacy Checkup lets you control what shows up on Google+, the social network.

65 | Make Google Forget You

Takes 35 seconds

Ready to push the big red Destruct button on Gmail, Google Drive, and the rest? You'll still be able to use tools such as Search but your account and—Google promises—the data used to target you with ads will disappear. Go to My Account and look for Delete Your Account or Services. Take a deep breath (you can't undo this) and follow the prompts.

66 | Keep Your Fitness Data to Yourself

Many wearables are paired with users' smartphones using Bluetooth technology—but those phones may not be the only hardware scooping up the signals. A 2014 study by the security firm Symantec and a June 2015 study by Germany's AV-Test.org found that many Bluetooth devices don't prevent data access by "sniffers" located nearby. Fitness trackers and running watches can broadcast sensitive information such as the user's name, address, password, and GPS data. Not all trackers let you shut off Bluetooth, but many do. If possible, keep your wireless settings turned off until you choose to upload the data to your phone at the end of a workout or at night. (As an added benefit, that will extend the battery life.)

Reporting by Andrew Chaikivsky. Additional reporting by Tercius Bufete and Catherine Roberts. Special thanks to Access Now, the Electronic Frontier Foundation, the Federal Trade Commission, Fight for the Future, the Ford Foundation, the Mozilla Foundation, the Privacy Rights Clearinghouse, and associate professor Lujo Bauer, who teaches computer security at Carnegie Mellon University.

WHERE CONSUMER REPORTS STANDS ON PRIVACY

Consumer Reports believes companies should tell you in simple language about the kinds of personal information they collect and how your information could be shared, sold, and used. You should be given clear options to control the collection and use of your data. And you should be confident that companies are handling your information securely.

Here at Consumer Reports, we strive to make our own privacy policies clear, concise, and actionable. We listen to our customers, and we take the safety of their data very seriously. In our business relationships with digital companies such as Google and other third parties, we follow best practices and strive to always act responsibly. Our ultimate goal is for our practices to reflect the ideal marketplace we want to achieve. While we are not there yet, we will continue to innovate and champion on behalf of consumers.

We believe that for too long, consumers have carried the entire burden of protecting their personal data online. Privacy policies are often drafted with an eye on the company's liability rather than the consumer's understanding.

That's why we have advocated for laws to better protect your privacy. We need clear rules of the road for companies to safeguard your data and ensure you have a say in how your information is used.

For starters, we need a strong law to help prevent harmful data breaches. According to the nonprofit Privacy Rights Clearinghouse, more than 900 million records have been compromised from more than 5,000 data breaches made public since 2005.

Members of Congress have introduced legislation endorsed by Consumer Reports that would set minimum standards for the security of your data, including requirements for companies to promptly notify you and the government when they discover a breach. But despite the long list of breaches we've seen in recent years–from Home Depot to Target to eBay–Congress still hasn't reached a consensus on how to put strong protections in place.

Meanwhile, the Federal Communications Commission has proposed privacy rules for broadband internet providers, in light of the vast amount of personal information available to these companies as well as how essential broadband has become to our daily lives. The details of the rules are still being hammered out, and we have urged the FCC to ensure that consumers have the safeguards they need so their private lives won't become an open book.

At the same time we're pressing for rules of the road, we encourage companies to highlight and compete on how they handle their customers' data.

Your personal information has tremendous value, and consumers should be able to exercise choice and control over the use of their data. When it comes to the sharing of your information, consumers and companies should have a fair and open exchange, where the benefits and obligations are clear and meaningful to the consumer.