Internet Privacy

A guide to protecting yourself online

A publication of the Citizens Utility Board

December 12, 2017

309 W. Washington St., Suite 800, Chicago IL 60606 • CitizensUtilityBoard.org • 1-800-669-5556

Privacy is a pocketbook issue

As smartphones, tablets and home computers have become our favorite tools for connecting with the world, so too they have become a criminal's favorite tools for stealing our identity and our money. It used to be you could only get mugged on the street corner—now it can happen in your own home simply by logging in.

The Federal Bureau of Investigation's Internet Crime Complaint Center reports that victims of Internet-related crimes reported losing $1.3 billion in 2016—and Illinois is one of the hardest hit states. The Land of Lincoln ranked sixth, with $32.9 million in reported losses.[1]

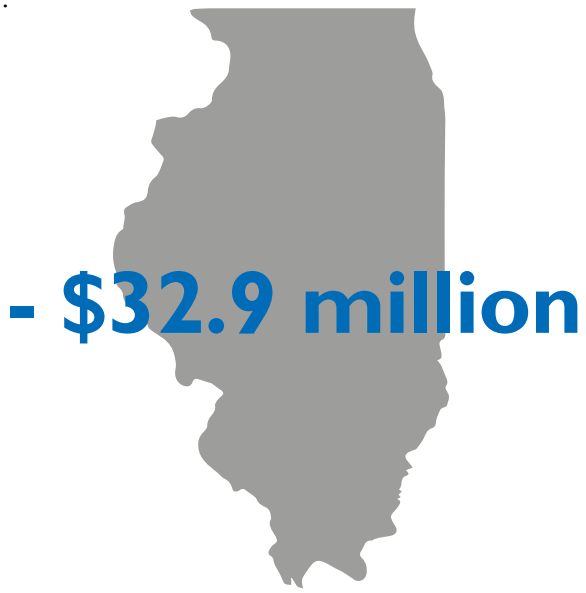
Overall, social media was the preferred medium for fraud, and people over 60 made up the largest group of victims.[1]

"With each passing day, cyber intrusions are becoming more sophisticated, dangerous, and common," Scott Smith, assistant director for the FBI's Cyber Division, wrote in the center's 2016 annual report.[1]

Your privacy is stolen by an email that looks like it's from a trusted friend, a pop-up that urges you to click on a link to get a required software update, or from a distant hacker monitoring your coffee shop's public Wi-Fi.

The Citizens Utility Board (CUB), one of Illinois' premier consumer watchdogs, focuses on utility-related issues, but it is always concerned with pocketbook issues—and digital privacy is a pocketbook issue.

This guide distills hours of research, showing consumers commonsense, every day tips they can employ to protect their privacy on the Internet, and, thus, protect their money.



The FBI reports that Illinois is one of the states hardest hit by Internet crimes, with $32.9 million in reported losses.

Table of Contents

Note from CUB

Amid major changes in the telecommunications industry, thanks to the explosion of the internet, CUB saw the need for a publication that would sift through technical jargon and present an easy-to-understand introduction to online privacy.

This is meant to be a starter guide used in conjunction with other resources. The online world changes often, so you should do more research to stay current.

CUB does not have the resources to perform tech support, so if you have questions and/or computer problems, we encourage you to consult with your:

- Computer manual/manufacturer;
- Smartphone manual/manufacturer;
- Mobile carrier;
- Internet Service Provider;
- Local computer repair service;
- Knowledgeable friends and family.

Thank you!

Strengthen your passwords

A survey by SecureAuth Corp. found that people were twice as concerned about somebody stealing their personal information than their wallet—and yet 81 percent also said they used identical passwords for multiple online accounts.[2]

Don't do it! Hackers use password-detection software that can quickly run millions of combinations of names and symbols, so having strong passwords is key. [3] The secret, wrote security expert Richard Barnes, "is a whole lot of randomness."[4]

Good "password hygiene"

Don't make it easy. Avoid common words and numbers connected to you—your name, birthday and phone number—as well as the easily hacked "1234" and "qwerty." [5] "Longer is stronger," says the Federal Trade Commission (FTC).[6] It recommends passwords at least 10 characters long. Include symbols, numbers and capital letters, but not in typical places, such as the beginning or end.[7]

One former hacker recommends using a passphrase. Don't use a famous saying ("To be or not to be), but something unique to you, such as "Uncle George is my #1 relative."[3]

Don't email or text passwords, or say them over the phone.[7]

Avoid storing passwords on a computer or device protected by those passwords. While it may seem counter to past advice, the Electronic Frontier Foundation says it's fine to write them down, because "you'll at least know if your written passwords go missing or get stolen."[8] Consider using the "Password Reminder" like the one below, kept in a secure place like your wallet. (Not under your keyboard.)[4,9,10]

Alternatively, use a password manager application. These apps generate strong passwords for all your accounts and "encrypt" them, making them unreadable to anyone else.

> See the "Helpful Resources" section for a great way to create a completely random password.

To access them, you just need to remember one master password. Examples of these apps include LastPass, Dashlane, RoboForm, and Password Boss. Search online for "password manager reviews" to find one you like.[3,9,11]

Consider two-factor authentication. Two-factor authentication (2FA) means if you want to login to your account you need to give a password and another piece of information. That second piece could be a code texted to your phone, or a random number generated by an app. It's an extra layer of protection in case your password gets hacked. Google, Apple and many bank accounts offer 2FA.[10] See a list of websites that support 2FA at twofactorauth.org. Read the Electronic Frontier Foundation's blog for set-up instructions in this guide's Helpful Resources section.[12]

Set a password or personal identification number (PIN) to lock every device—smartphone, laptop, and tablets. Similar to the rules for a good password, PINs should be long—four digits allow for 10,000 possible combinations, but six digits allow for a million possible combinations. Never use 0000, 1111, 1212, and 1234, and don't use your birthdate or any part of your Social Security Number.[10]

Be careful of security questions. Some websites may make you answer a security question to confirm your identity if, for example, you forget your password. Many times the typical answers — such as your mother's maiden name or a favorite pet—are easily harvested from social media or some other public platform. Experts advise making up fictional answers that you can remember for those questions.[4]

Password Reminder

Website:

_____

Password:

_____

Username:

_____

Additional information:

_____

_____

Keep your email safe

Our inboxes overflow with spam: emails you didn't ask for from people you don't know. "Nuisance emails" pitching a product are annoying, but "phishing" emails are dangerous.[13]

Scammers use phishing to trick you into disclosing personal information such as passwords and credit card details. Imagine checking your email inbox one morning and seeing one of the following messages:

- A request from your bank to "verify" your account number.
- An unexpected hello from a friend, who asks you to look at photos of his kids, or invites you to view a document.
- An urgent warning from "tech support" that your account has been hacked and you will lose vital information if you don't immediately respond with your password.
- A tempting offer of easy money, or donation requests in the wake of a disaster.[14, 15, 16, 17]

Crooks use emails like this to "phish" for your information. They direct you to click on a link to enter sensitive info at an imposter website. Or they may get you to open a document or click a link that installs malicious software, allowing a crook to remotely control your computer and steal information.

Use commonsense to fight this fraud:

Think before you click. If you're not expecting an email from a company or friend, and it requests an action—don't respond. Don't click on a link or download a file. The Privacy Rights Clearinghouse says clicking on a link or even opening spam could alert the sender that your email address works, inviting more spam.[13] If an email raises questions, call the company or friend, to verify that the message is legitimate.[15]

The same rules apply to "get-rich-quick" emails, donation requests, and "urgent" messages that threaten to suspend your account or warn you that your account has been "compromised.

Don't email personal information. Never reveal confidential account details in an email. An institution you do business with (Amazon, your bank, etc.) has that information already and won't ask you to submit it in an email or web form.[18, 19]

Rule Number One: If you're not expecting an email that wants you to act, do not click anything.

Consider a backup email account. Set up a second free email account to use any time you're unsure how a website will use your email address. That way any spam won't invade your primary account.[13]

Read the privacy policy. Before giving your email to a website, read its privacy policy. Not having a policy is a big red flag. Does the group sell your email address to other groups? Also look for any pre-checked boxes that would sign you up for spam.[13]

Join a "do not email" list. The Direct Marketing Association's Email Preference Service, at DMAChoice.org, allows you to reduce at least some commercial emails. The list is good for six years, after which you'll have to renew.[20]

Don't publicize your email address online. "Spammers use the web to harvest email addresses," the FTC says.[21]

Block spam. Email providers automatically send certain messages to a spam or junk folder, based on algorithms designed to detect unwelcome emails. See the "Helpful Resources" section to block spam that gets through filters.[22]

Report it. Forward a phishing email to the FTC at spam@uce.gov, to the business/organization that was impersonated in the email, and to the Anti-Phishing Working Group, which is battling the scam: reportphishing@apwg.org. Also, file a complaint with the FTC at FTC.gov/complaint.[19]

Spam's not just for email anymore

You could get text messages trying to steal your personal information and/or install harmful software. The FTC recommends:[18]

- Delete texts that ask you to confirm your personal information, such as account numbers and passwords.
- Don't reply or click on links in the text.
- Never text sensitive information, like your Social Security number.
- Copy an offending text message and text it to your carrier. For AT&T, T-Mobile, Verizon and Sprint text it for free to 7726 (which spells "SPAM").

Don't get hooked by PHISHING SCAMS

Email crooks want to trick you into providing your personal information. Watch for these signs that scammers are trying to reel you in.

Familiar sender, but unexpected content (1)

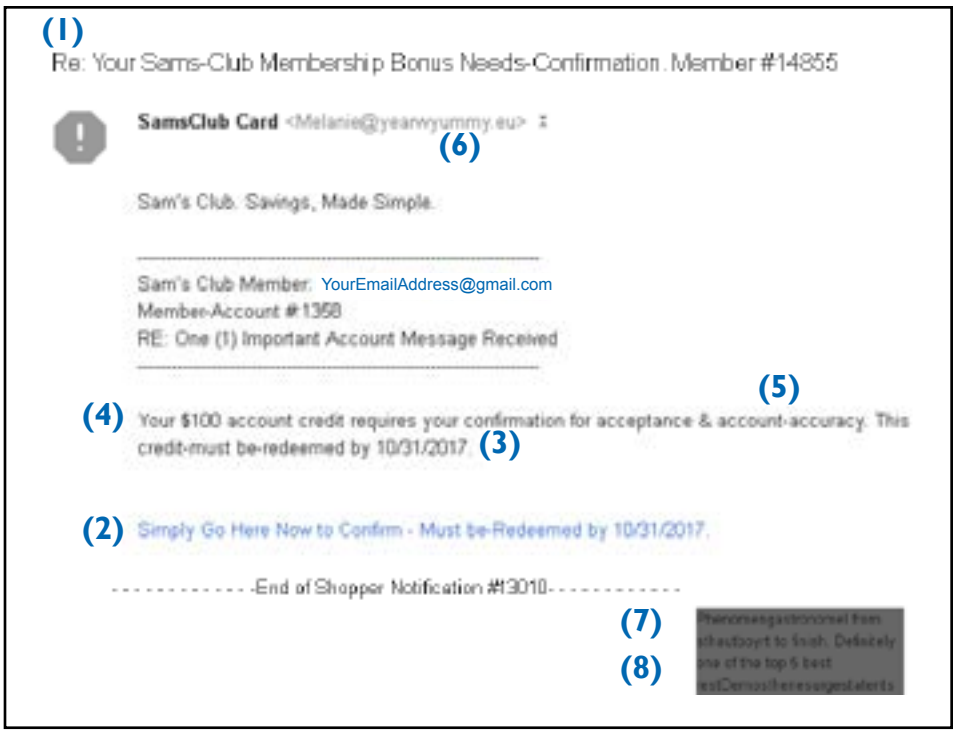
Scammers want you to think the phishing email is from a person or business you know, so you're more likely to trust what the email says. But in this example, were you expecting a Sam's Club credit? What is a Sam's Club "bonus"? Is that your Sam's Club account number? Are you even a Sam's Club member? Always err on the side of skepticism.

Links to strange URLs, or attachments (2)

Never open attachments unless you are sure they're legitimate, and don't click on links without checking them. Some attachments contain viruses, and some phishing scams take a previous, legitimate email and swap out the safe links for malicious ones. Hover your mouse over the link in the email to see the URL it would take you to. If it seems suspicious, don't click it. Close the email, open a new browser window, and type the address for the real website before logging into your account. The official site will tell you of any problems or offers .

Urgent or threatening tone (3)

Phishing scams will urge you to act right away. Common tricks include claiming there's a problem with your account, or too-good-to-be-true offer expires soon.



Asks for personal or account information (4)

This is the goal of the phishing scam: getting your credit card number, password, or other information. Emails that use generic greetings or only an email address should be viewed with suspicion - the real business will know your name!

Grammar, spelling, or punctuation mistakes (5)

Legitimate businesses take care to make sure their communications look professional. Scammers don't.

The sender's email is not the official domain (6)

An email from the real Sam's Club would end just like their official website: samsclub.com. So this strange or fake sender address is a huge red flag. Some fakes look like the real domain, such as paypal.au instead of the real paypal.com. Look carefully!

Strange signature or footer (7)

No contact information, only the link to log in (8)

IF IN DOUBT, DO NOT CLICK LINKS OR ATTACHMENTS

Protect yourself from harmful pop-ups, websites, and apps

Americans spend nearly six hours a day on their computers, laptops, tablets, or smartphones, according to research firm eMarketer.[23] As we browse the latest news, play games, conduct business, and catch up with friends on social media, criminals lay online traps designed to steal our personal information and money.

Malware —also called "scareware" because it employs scare tactics — is shorthand for "malicious software," and email is not the only way it can get into your devices.[1]

Say you're surfing the Internet, and a pop-up appears on your screen. Using official-sounding language, it urges you to update to new "antivirus" software. You take the message at face value and click the link. But instead of helping to protect your system, the malicious software deletes important computer files, captures your financial information, or even tracks your keystrokes to determine your passwords.

Types of malware

Ransomware. Hackers claim to lock down your computer, steal your information—maybe a social media password, financial details or key files—and demand payment before giving it back. The thieves may ask for gift cards or online currency like "bitcoin," which helps assure their anonymity.

Adware. Short for "advertising-supported software," adware delivers malicious software through online ads. Common examples are pop-up ads on websites.

Spyware. This software spies on a computer user's activity, even tracking keystrokes to harvest passwords.

Signs of a malware infection:

- Computer slows, freezes or crashes, won't shut down, or restart.
- Unusually large number of error messages.
- You see a lot of pop-ups or inappropriate ads.
- You can't eliminate unwanted software.
- Files are modified or deleted.
- Emails you didn't write are sent automatically.
- New toolbars or icons appear in your browser or on your desktop.
- Your laptop battery drains quickly, and it's not because of an old battery.
- Changes to your computer's internet home page.
- Inexplicable changes in your browser, such as using a new default search engine or displaying new tabs.[24,25]

Trojan Horse. This virus disguises itself as a normal program to trick users into downloading and installing it. Then a crook remotely accesses the computer, stealing data, installing more bad software, and tracking your computer activity.[25,26]

Identifying suspicious pop-ups

Fraudulent pop-ups are designed to look like they're coming from your own computer. The FTC says beware if you see these pop-ups: [27]

- Ads promising to delete viruses, protect privacy, remove harmful files, or "clean your registry."
- Alerts about malicious software or illegal pornography on your computer.
- Invitations to download "free" games.
- Alerts that your security software is out-of-date and your computer is in immediate danger.
- An unfamiliar website that claims it ran a security scan and prompts you to download new software.

What to do about pop-ups

Don't click anything in the pop-up (or banner ad). Don't click the link, don't click "No" or "Cancel" or even the "x" in the corner. Scam artists anticipate that move and hitting those buttons may activate the malware. It's better to shut down your Internet browser, the FTC says.

In Windows: Hold down the Control, Alt and Delete keys to open the Task Manager. Select the browser from the list of running programs and click End Task.

In a Mac: Press the Option, Command and Escape keys, select the browser in the list of programs and click the Force Quit button.[27]

Don't fall for "tech support." Just as you should hang up on these callers, the FTC recommends ignoring such pop-ups. If you think your software company has an alert, call it directly - but don't use the one listed in the pop-up.[28]

Be wary of downloading "free" software. Pop-ups that offer free software are more likely to have malware.[27]

Pay attention to warnings. Browsers often have security scanners that warn you BEFORE you visit an infected web-page or download a fraudulent file.[24]

Block pop-ups. Your web browser should block most pop-ups already, but if you want to check you can find instructions at the "help" webpages of each browser (do an online search for the name of your browser and "help").[29]

Identifying suspicious websites

A fraudulent pop-up or email may try to lure you to a website designed to damage your computer or steal your personal information. These phony web addresses are almost identical to legitimate sites, like Microsoft or Chase Bank. Always study a website for these red flags.

No "https." The Electronic Frontier Foundation calls this tip as "basic as putting on your seatbelt when you drive." Only give sensitive information to websites in which the URL begins with an "https"—the "s" stands for "secure"—along with the padlock icon and/or green lettering. When you input sensitive information, such as a credit card number, it will be "encrypted"—converted into code and protected.[30, 31]

A caution from the FTC: Some fraudulent sites forge these security icons, and others use encryption only on the sign-in page. "If any part of your session isn't encrypted, your entire account could be vulnerable," the FTC says.[32]

The URL's not quite right. The website's URL may begin with "https" and look like a business, but be different in key ways. For example, the URL for Chase Bank is chase.com—but an imposter could be chase-bank.com. If in doubt, open another screen and visit the business' website yourself.[33]

Sloppiness. A fake website may have a terrible design and be littered with misspellings and bad grammar.[33]

Too desperate. A fraudulent website is desperate for you to take action—download a program, take a survey, watch a can't-miss video or claim a free prize. But Komando.com says all of this could be a malware attack in disguise.[33]

Browse more securely with HTTPS

If a website doesn't support https, then don't give it any sensitive information.[39] The free HTTPS Everywhere browser extension from the Electronic Frontier Foundation assures your connections will be encrypted when you connect to a website that supports https. It works with Chrome, Firefox and Opera browsers.[10, 30, 31]

> "You know the old saying: If it's too good to be true, it probably is."

Scams: There's an app for that

An application, or "app," is software that helps your mobile phone complete a specific task. You can play games, track the weather, locate your lost keys, and find your car in a parking lot. But scam artists mimic real apps to trick you into downloading fraudulent ones to steal your information.

Go big. If you want to buy an app, the big stores run by Apple and Google are probably safest, because they do more vetting and security checks, Mark Jones of Komando.com writes.[34] Fakes can show up in the big stores too, so always follow the rest of these precautions.[34,35]

Beware of fake names. Overstock Inc. (fake) is NOT the same as Overstock.com (real), wrote Dan Graziano, of CNET News (cite). If you think an app might be a fake, do an online search for the brand name in question and "fake app" to see if the company has reported being spoofed.[36]

Beware of "free" apps. "Many free applications are actually malicious or virus software," says AARP writer Noemi Garcia. "They are intended to help steal credit card, bank or other vital information about you."[37]

Read the reviews. A real app could have thousands of reviews; an imposter may not have any. Be careful of sponsored reviews—where an app maker paid the writer—and remember reviewers can be wrong. Still, reading several will give you an idea.[36]

Look at the app's publish date. A real app will have an "updated on" date. Fake ones may have very recent dates.[36]

Spelling and grammar errors. Fake apps often come from scam artists who don't have the English or editing skills of a professional business.[36]

Beware unbelievable deals. "Apps that promise discounts are often fakes trying to steal your attention away from legitimate ones," wrote Jean Folger in Investopedia. "You know the old saying: If it sounds too good to be true, it probably is."[38]

If you're worried about fake apps, close whatever webpage is asking you to download the app, visit the website of the actual app maker, and click on the download link provided there. That will take you to the real app sold at the big stores.[39]

Your computer's infected. Now what?

It happens. Despite best intentions, you accidentally clicked on a link in an email or in a pop-up, or you downloaded a fake app. Your privacy and security are at risk.

Below are general guidelines on what to do, but CUB recommends consulting with several sources to determine the response that's right for your particular situation.

Stop using the computer. Immediately disconnect from the Internet. If you are using a wired connection, unplug the internet cable (or Ethernet cord) from your computer. If you're connected through Wi-Fi, locate the settings on your device and disconnect from your network, or go to your router and shut it off. This reduces the risk of malware spreading to other devices on your network and doing more damage.[40]

Change your passwords from a different, safe computer. Do this for all online accounts—email, online banking, social media, shopping accounts.[41]

Update your security software and run an antivirus scan. These scans don't use the internet. Delete malware they find. If you don't have an anti-virus program, download a free program, such as Malwarebytes. Even if you do have anti-virus software, run a second scan with a similar program. First, use a computer that hasn't been infected to download the program to a thumb drive. Then install it on the infected computer and run a complete system scan. After the scan is done, follow the on-screen steps to clean up suspicious files.[24, 40, 42, 43, 44]

Watch your credit report. Contact one of the three major credit bureaus and ask that a free 90-day fraud alert be placed on your credit report. Once you have notified one of the bureaus, they're required by law to notify the other two on your behalf. This will make it more difficult for criminals to open new accounts in your name. The bureaus are:

Equifax: (800) 525-6285
Experian: (888) 397-3742
TransUnion: (800) 680-7289

File a complaint with the Federal Trade Commission at FTC.gov/complaint.[45] Note: The FTC warns paying the ransom doesn't guarantee crooks will give your files back.

Getting Help

If, like many people, you don't consider yourself a technical expert, check if your computer is covered by a warranty with free tech support. Contact the manufacturer and have the model and serial number of your computer in hand, as well as any information about software you've installed and a clear description of the problem. Be specific, and write down your thoughts ahead of time.[24]

Ask friends and family for help—maybe you have a tech-savvy family member or neighbor, or somebody who can point you to a good professional.

If you do an online search for a local computer repair service, beware that scam artists may be lurking in the results. Search for the name of the repair service you're considering and "reviews" to see the experience other customers have had.[24]

Technology author Tim Fisher says a lot of fixes you can do yourself. But if you can't, there are simple tips you can follow to try to get a good repair service "Always, always, always get a specific referral," Fisher writes.[46, 47, 48]

What questions should I ask?

If you do seek professional help for an infected computer, ask these questions of a local computer repair service. If you don't like the answers, call other repair services.

- Can you save my important files?
- How long will it take to fix this problem?
- Do you charge an hourly or a flat rate? ("Don't wait until it's time to pay the bill to find out how much per hour you'll be paying," wrote Fisher. He said $50 to $75 an hour is average.[49])
- Do you have a minimum charge for quick repairs?
- Are there any other charges? (If the company charges extra fees, such as for travel time, get a list of them.)
- Do you charge extra for house calls?

Also, consider the age of your computer. Nobody wants to pay more for repairs than the price of a new computer.[49] "Systems five years or older are often worth replacing," wrote Angie's List contributor Nathanael Terra, owner of a computer repair service.[50]

How do I protect myself on the go?

Public places, such as your local coffee shop, library and the airport, set up wireless Internet connections called "hotspots" that allow you to visit websites with your phone or tablet.

If a Wi-Fi hotspot doesn't require a password, it's probably not secure. So while you can scan the Internet for news or visit your favorite webpages, it might be best to avoid doing banking business, credit card transactions or other activity that requires you to login to an account.[51, 52, 32]

Also, be careful of "honeypots," fake public Wi-Fi spots that crooks set up to steal your data. If you try to use a hotel's Wi-Fi connection, for example, you'll probably notice several possible Wi-Fi connections you could use. Some of these might be set up by scam artists. Always ask an employee about the correct hotspot. [53] Also, you might want to change the settings on your mobile device so it doesn't automatically connect to just any Wi-Fi.[32]

If you want to check email, you should set-up two-factor authentication, which gives you an extra level of protection when you're reading and sending messages via public Wi-Fi. (We referred to two-factor authentication earlier in this guide.) When you're done checking email, make sure you log out.[54]

If you have to access online accounts through Wi-Fi hotspots, make sure the website is fully encrypted, meaning every page starts with "https." Sometimes websites only encrypt the homepage. If you find other pages are not secure, logout immediately. [32]

The FTC and other experts recommend purchasing a virtual private network (VPN). It protects your data from crooks, the Internet Service Provider and the hotspot. Some examples are IPVanish, NordVPN and TunnelBear.[32, 55, 56]

Such connections encrypt the traffic to and from your computer and the internet. Eric Griffith of PC Magazine describes a VPN as a "private tunnel" your information uses to travel from your laptop or smartphone to a remote, anonymous server. [55]

"To the outside world, the anonymous server is doing the browsing, not you," writes Dustin Driver, for Mozilla. "The data is essentially gibberish to anyone who intercepts it."[57]

There are disreputable VPNs out there, so choose carefully. Read a PCWorld review of VPN providers. [56, 58]

Do you have a laptop? The FTC says treat it like cash. Never leave it unattended, and never keep your passwords with your laptop, or in its case.[59]

Shop smart online

A record 85 percent of U.S. consumers planned to holiday shop online this season, according to Nielsen.[60] For crooks, the holiday season is open season on unsuspecting online shoppers. Follow these tips to protect your information:

Shop online from your home computer. Going to your local coffee shop is risky, because crooks have ways of monitoring public Wi-Fi.

"Bottom line: It's never a good idea to shop online or log in to any website while you're connected to public Wi-Fi," writes Kim Porter in an article for Lifelock, the identity theft protection company.[61]

Use a credit card. Be wary of companies that want payment via Western Union or MoneyGram. Don't shop with a debit card. Credit card transactions are better protected by federal law. [62]

"In the event of a scam, with a credit card, the issuer must fight to get its money back. With a debit card, you must fight to get your money back," says PackageFromSanta.com.[63]

Make transactions only on "https" sites. Any website where you use your credit card should begin with "https" and have either a padlock or a green font. That means your credit card will be encrypted, and hidden from identity thieves. If you're being asked to make a purchase through a URL that begins only with "http," don't do it. [62]

Beware of fake websites. To make sure the website isn't just a sham to get your credit card number, study the site.

• Are the pitches too good to be true?

• Is the site asking for too much information? Why does it need a Social Security Number to close a sale?

"Don't answer any question you feel is not required to process the order," the Privacy Rights Clearinghouse advises.[62]

• Do the social media links work? Do customers comment on Facebook, and does the company respond?[63]

• Can you contact the company? The FTC says if there's no email address, phone number or address for a brick-and-mortar location, that's a red flag for a phony company. [64]

• Does it have a shipping and return policy? Any legitimate e-commerce company has one, and it shouldn't look like it was carelessly copied and pasted.[31]

• Does the website include strange pop-ups? "If you get an email or pop-up message that asks for your financial information while you're browsing," the FTC says, "don't reply or follow the link. Legitimate companies don't ask for information that way."[64]

Check customer reviews. Check the Better Business Bureau. Do an Internet search with the name of the company and the word "review" or "complaint."[7] AARP recommends checking for reviews at consumer-oriented sites, such as consumerreports.org and ripoffreport.com.[65]

Read the privacy policy. If the site is reputable, it should have a privacy policy. Find out if the company intends to share your information with anyone else. The Privacy Rights Clearinghouse says that could be a source of spam and mail and phone solicitations.[62]

Keep good records. Log all your online transactions, including the product's description, price, the online receipt, and emails you send and receive from the seller. Then read your credit card statements to check for suspicious charges.[64]

Protect yourself on social media

According to the Pew Research Center, 68 percent of adults in the United States use Facebook—more than double any other social media network.[66]

While Facebook brings families and friends together, it also can put your privacy at risk, exposing you to scams and, at times, unwanted acquaintances who want to "friend" you.

Facebook itself gathers a surprising amount of information about you. In 2016 it was reported that the site targets advertising based on 98 data points it collects about your Facebook activity.[67]

These tips will help you better control your accounts:

Don't be your own worst enemy. The Privacy Rights Clearinghouse says that in 2009 Carnegie Mellon University published a study showing it was possible to predict most and sometimes all of a person's Social Security Number based on information mined from social media and online databases.[68]

Don't post your phone number, email, date of birth, address or when you're going out of town on Facebook. "The more you reveal in profiles and posts, the more vulnerable you are to scams, spam, and identity theft," Microsoft warns.[69]

Log out when you're done. If you're using a computer you share with other people, logout when you're done. And when you login, don't choose "Keep me logged in."[70]

Use two-factor authentication. Go into Facebook's settings to stop crooks from accessing your account, even if they have your password.[10]

Turn on your privacy settings. In the upper-right corner of the page, there should be an arrow with a drop down list that includes "Settings." (On the Facebook app on your mobile phone, you can choose "Privacy Shortcuts.") Go through the sections for privacy, timeline, and tagging to see how you can enhance your privacy.

You can limit who sees your posts, who can see your friends list, who can send you friend requests, and who can search for you by using the email address or phone number you gave. You can prevent people from finding your Facebook page through a search engine. You also can require approval for any photos in which you are tagged.[71]

But remember to check the privacy policy and settings on a regular basis, because they change often.[71]

Block and report. People who are blocked can't see your posts, add you as a friend, tag you in photos, or message you. You can also report people who spam or harass you.[70]

Enable login alerts. Under the security settings, you can have Facebook alert you if someone logs into your account from a new location.[70]

Turn off location tracking. If you use Facebook from your mobile phone, don't let the site determine your location.[10]

iPhone: Tap "Settings," then "Privacy," then "Location Services."

Android: Tap "Settings," then "Privacy shortcuts," and then "More settings, and then "Location."

Pause before letting third-party apps use your account. Many websites, games and apps let you sign up using your Facebook account. This could give the makers access to your friends' details. Check what kind of information you will hand over if you use your Facebook account to sign up.

If you play games on the desktop version of Facebook, go to settings and then "Apps." Click the edit icon (it looks like a tiny pencil) next to each app to see what information you provide the app. Uncheck the details (email address, for example) you don't want the app to have.[70]

Limit ads. There is no way to completely eliminate ads, but you can limit them. You can turn off or say no to:

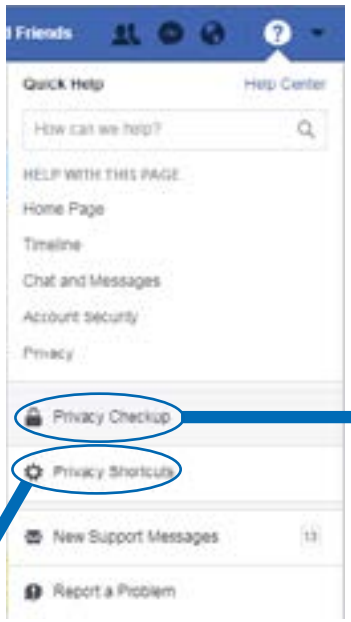
- Ads based on your use of websites and apps.
- Ads on apps and websites off of the Facebook Companies.
- Ads with your social actions.[71]

Watch for malware. Watch for pop-up windows or an apparent greeting from a friend who wants you to click a link on the site's Facebook Messenger feature. Click on that link and malware might spread to your computer and your Messenger contacts.[72]

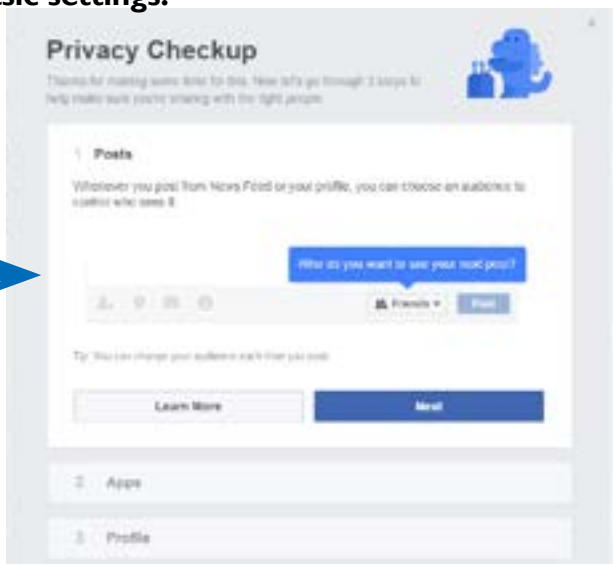
Improving your Facebook privacy

***Check the privacy policy and settings on a regular basis, because they change often.**

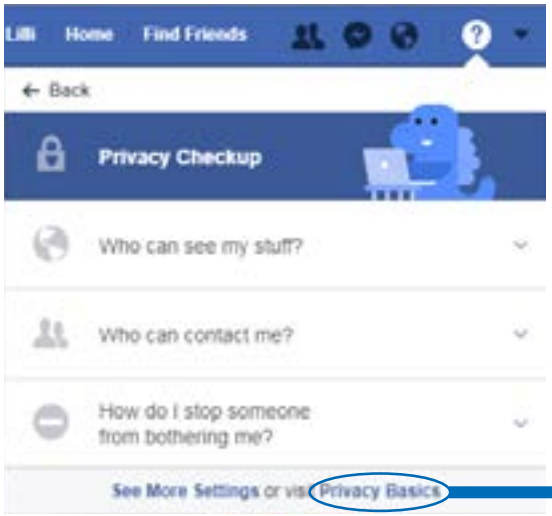
Start by clicking on the question mark in the upper right hand corner of the screen.



Click on Privacy Checkup to verify your basic settings.



Privacy Shortcuts gives you direct access to basic settings as well as managing who can contact you.



Clicking on Privacy Basics at the bottom of the Privacy Shortcuts box will take you to Facebook's separate web page where you can dive deep into all your privacy settings.

Secure your home network

You can lock your doors, lower the shades, and turn off the lights. But if your computer, cellphone or other devices are connected to a home network, you're still vulnerable to intruders who can snake through the virtual passageways of your data lines or Wi-Fi signals to swipe your valuables, such as bank account information, medical records, and other private details that can compromise your finances.

Just as with the front door to your house, you need to keep your home network secure from predators. First, we'll explain the concept of a home network, and then we'll review key tips for securing it.

What is a home network?

A home computer network consists of devices – such as a computer, smartphone, tablet – that link together through a central hub, called a router (examples to the right).[73] The router is the mechanism that connects all your networked devices through either cables or by transmitting a wireless (i.e. Wi-Fi) signal.

A home network's architecture is similar to your home itself. The router is akin to the main entrance, and each of the devices that it links can be thought of as individual rooms where prowlers can sift through your valuable information.

The most secure home networks include measures to block intruders both at the gateway to the network – the router – and within the premises. That means securing the router, as well as the information on each device within the network.

Examples of routers.

Key tips to lock down your home network

Your router is the central hub of your home network, linking all your devices together through physical cables or by transmitting a Wi-Fi signal. The router itself connects to the internet through a modem, which funnels a signal into the home.

Because the router ties the network together, it's arguably the biggest target for hackers. Keeping your router secure is and important step to bolstering the safety of the network.

Customize your router's default IP address and Password. An IP (short for internet protocol) address is a code – a series of numerals separated by dots (111.11.111.1) – that identifies the location of a device on your network. The password, of course, allows you to gain access to the device.

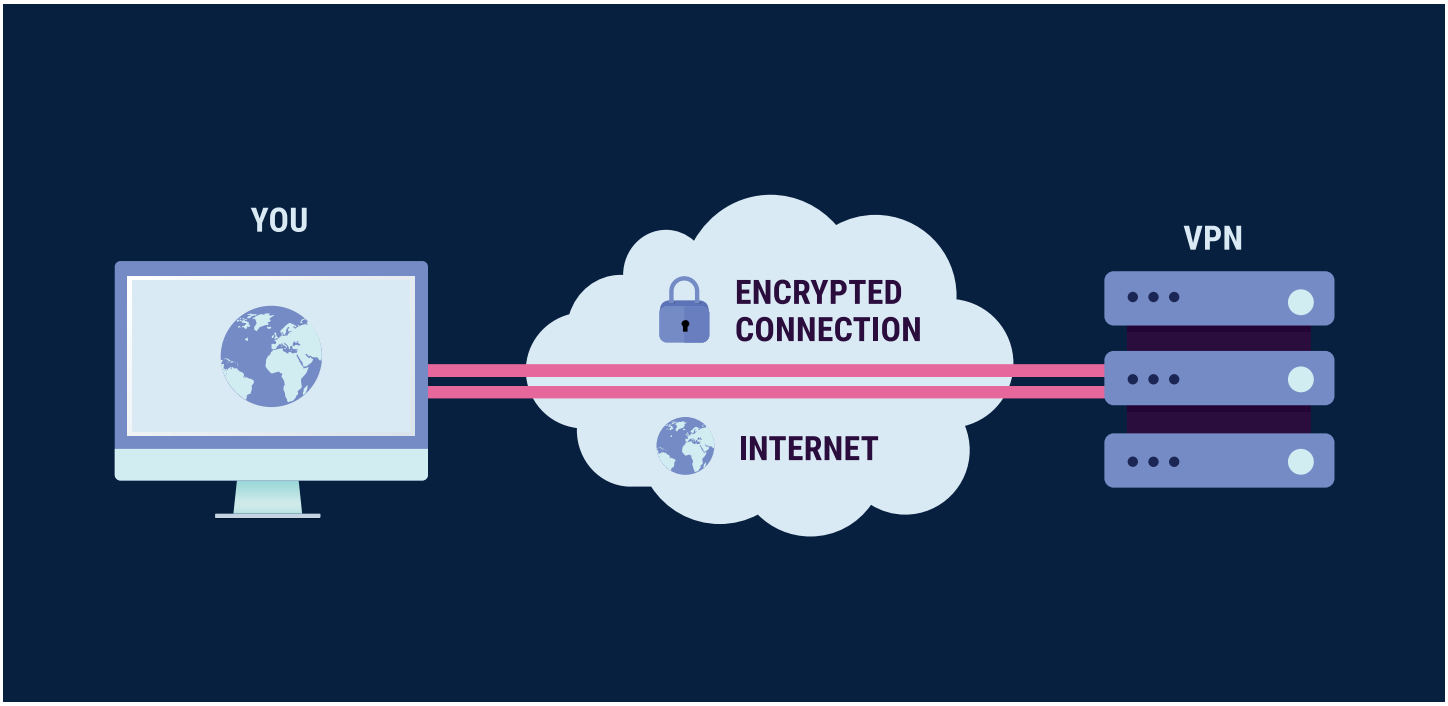
When you buy a router (or you receive one from the company that provides your internet connection, such as Comcast or AT&T), the device comes with a pre-assigned, or default, IP address and password.[74] Often these manufacturer-assigned defaults are generic and easily hacked. You can create an obstacle to online prowlers by changing the default IP address and password to something more unique and secure. (See instructions in "Helpful Resources.")

Prevent remote access to your router. Most routers include settings that would permit an outsider to manipulate the device through the internet. Turn those settings off.[75] You can always turn them on temporarily if you want to allow access to your router to a third-party – a technical support specialist, for instance, who might request remote access to troubleshoot a problem. (See instructions in "Helpful Resources.")

If your home network uses a Wi-Fi signal, encrypt it. Encryption converts information you transmit through your wireless signal into a code that hackers can't easily translate. Wireless routers often come equipped with encryption capability, but it may not be turned on. You can explore and manage the encryption options for your router online.

There are two main modes of encryption: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). WPA2 is widely considered to be the more stringent and safest means of encryption, but if your router is older it may not be compatible with this protocol. In that case, consider buying a new router that can accommodate WPA2.[76]

Install a firewall. A firewall is software or hardware that acts as a barrier around your home network, intercepting and



neutralizing suspicious data attempting to enter.[77] Many of the devices connected to your network are outfitted with firewalls. There are online tutorials (see "Helpful Resources") that will help you ascertain whether these firewalls exist and are activated. Also research additional third-party firewall protection.[78]

Install and update security software on your devices. Your computer and other networked devices are powered by software known as operating systems, which are continually updated by the manufacturers to repair any security defects that hackers may be able to exploit.

The same is true of the software that runs the applications, such as word processing programs and web browsers, that you may use on your computer. It's imperative to install the latest updates (sometimes called patches) to these software systems to ensure that your system is as protected as possible.

You can instruct your computer to receive and install these updates automatically. If you're not sure how to do that, try typing "automatic updates" in the search bar on your computer, which should give you a link to information that guides you through the key steps.[79]

Similarly, consider arming your computer with anti-virus and anti-spyware software. Some of this software is available for free, others for purchase. Do your research and be sure you install a reputable product.[79]

Back up your data. It's crucial to store a copy of all your files – known as a back up – at other locations.[80] There are two key rules to effective backups: redundancy and frequency. Redundancy means that you should back-up files and data at multiple locations outside your computer. The more back-ups you maintain, the more likely you'll be able to salvage your files and data if you're ever victimized by a hacker.

Is a creep spying through your webcam?

If your laptop has a camera, crooks may be able to turn it on and spy on you. Consumer Reports recommends doing what Facebook CEO Mark Zuckerberg does: Cover the web cam at the top of your computer with tape or a Post-it.[10]

Frequency means that back-ups must be conducted at regular and frequent intervals – weekly, at a minimum – so that your back-ups contain the latest content (new documents, e-mails, etc.) that you've added to your computer.

Files can be backed up through several means:

External Hard Drive. An external hard drive is just as it sounds: It's a compact, lightweight, portable storage device for your files and data. By plugging a hard drive into your computer, you can copy all of the material stored there onto the external hard drive – essentially isolating it from hackers.

One caution, however: external hard drives, like most electronic devices, can deteriorate over time. (Rough estimate: They last three to five years.)[81] For that reason, keep cognizant of the age of your hard drive, consider buying a new one occasionally, and, most importantly back-up your files at a second location.

Cloud Storage. You can also preserve a copy of your files and data at a cloud storage system.[82] Think of the cloud as storage capacity that you rent on a server residing outside your home. You can duplicate your files and data by streaming them over the internet to the storage company's site. But do your research - cloud storage can be hacked as well.

Control the information companies collect about you

We know online crooks and scam artists scheme to get our personal information, but big advertisers and corporations like Facebook and Google want it too.

You will never completely prevent companies from tracking your online activity, but you can do some things to limit it.

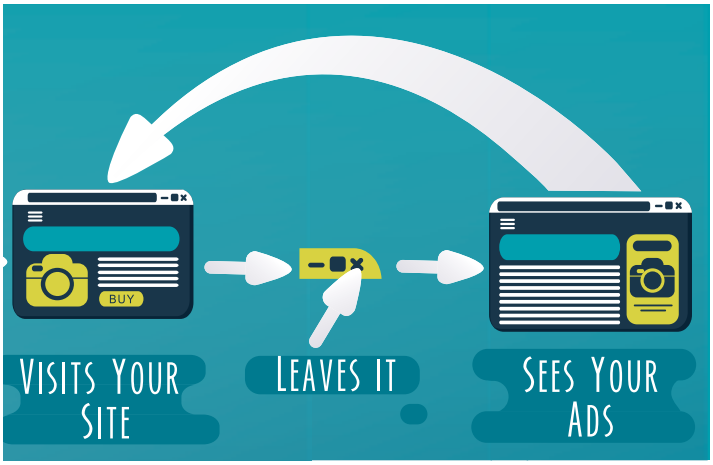
Whenever you visit a website, it gathers small files of information (also called first-party cookies) that can be helpful to our web browsing experience. For example, these cookies remember our logins and what's in our cart when we shop online.[83]

But third-party cookies, placed by advertising companies on websites and browsers, may be more of a concern to people. They track our online activity, develop a detailed history of the sites we visit, and help advertisers target their pitches. For example, if you read a lot of recipes online, you may see ads for cookware.[83]

Browsers have different ways to delete or limit cookies. If you do block cookies, you may limit your browsing experience and have to enter information repeatedly.[83]

You also can set most browsers to "do not track." Companies then know your preference not to be tracked from site to site. If companies have committed to respect "do not track" preferences, they are legally required to do that. However, the FTC says many companies haven't committed to that.[83]

You can get more information about protecting your privacy on the help pages of your favorite browser. See the Helpful Resources section.



Other tips

• See a tool for opting out of targeted advertising from the Network Advertising Initiative and the Digital Advertising Alliance (DAA) at OptOut.AboutAds.Info.[83]

• You can look into a plug-in that can help you reduce ads. An example of a free one is Privacy Badger, by the Electronic Frontier Foundation.[10]

• Advertisers also track our mobile app usage. The FTC says you can follow these steps to limit, but not eliminate, tracking.[83]

Phones based on the iPhone operating system (iOS): Settings-> Privacy-> Advertising-> Limit Ad Tracking

Phones based on the Android operating system: Settings-> "Google"-> Ads > Opt out of Ads Personalization

"Why would an application about the weather need to know your Social Security number?"

Even if an app isn't fake or malicious, it could compromise your privacy.

Any app will ask you for "permissions" to access certain data to do its job, and they could ask you for more permissions than they actually need.[84, 85, 86]

"For example, why would an application about the weather need to know your Social Security number?" wrote AARP writer Noemi Garcia. [37]

• Review the privacy policy, as well as the terms and conditions/license agreement for the app. Make sure the app has no plans to share your email address, phone number or mailing address.[85]

• Review the app permissions.[86]

On Android: Go to Settings, tap Apps, tap the app name, tap Permissions.

On the iPhone: Pick the name of the app from Settings.

• Apps can track your location, but your smartphone settings will allow you to disable these "location services" for each app. Aside from map and weather apps, there probably aren't many other apps that need to know where you are.

• Turn off app notifications. An app may send you notifications that pop up on your lock screen, and that could expose a private conversation and other info. You can turn off notifications for any app.[34]

iPhone operating system: Settings, scroll down to the app you want and select it, tap Notifications, slide the toggle to the left next to Allow Notifications.

Android: Settings, tap Notifications, select app, choose Block all.

Helpful resources

General

There are many excellent resources available if you want to learn more about protecting your privacy. CUB wishes to thank the following organizations and agencies for fighting to protect people on the internet.

- Consumers Union
- Electronic Frontier Foundation
- Federal Trade Commission
- Privacy Rights Clearinghouse

Also check the help pages of major internet browsers:

- Firefox
- Google
- Internet Explorer
- Safari

Strengthen your passwords

For instructions on setting up two-factor authentication, read this Electronic Frontier Foundation blog: "The 12 Days of 2FA: How to Enable Two-Factor Authentication For Your Online Accounts"

Check a list of websites that support two-factor authentication at twofactorauth.org.

Want a great password? Try the "Diceware" technique to create rock-solid, truly random passwords:
1) Roll a six-sided die five times. Each time write down the number.
2) Search online for "Diceware word list." You'll find a list of 7,776 words.
3) On the list, find the word that corresponds to your five-digit number.
4) Repeat this process five more times until you have a six-word passphrase that's nearly impossible to guess. (Put spaces in between the words, or not.)
5) Add a seventh word for another level of security.

Read more: Animated Overview: How to Make a Super-Secure Password Using Dice

Keep your email safe

- Block someone's email in Gmail
- Block someone's email in Yahoo Mail
- Block someone's email in Outlook

Sign up for free scam alerts at FTC.gov/scams.

If you are a victim of identify theft, report it at the FTC's special website: identitytheft.gov/

"5 ways to spot a phishing email," CSO

"How to recognize phishing email messages, links, or phone calls," Microsoft

"How to spot phishing," PhishMe

Protect yourself from harmful pop-ups, websites, and apps

- Block pop-ups in Chrome
- Block pop-ups in Safari
- Block pop-ups in Firefox
- Block pop-ups in Internet Explorer
- Block pop-ups on an iPhone/iPad

Helpful resources (continued)

Learn about more secure Internet browsing with the free tool HTTPS Everywhere.

Not sure a website is safe? Copy and paste the URL here: Google Safe Browsing Transparency Report. Click "Site status."

Your computer's infected. Now what?

"How do I protect myself against malware," Surveillance Self-Defense, Electronic Frontier Foundation

"Malware," Federal Trade Commission.

Tim Fisher, "How Do I Get My Computer Fixed?" Lifewire, Updated July 19, 2017

Tim Fisher, "Five Simple Fixes for Most Computer Problems," Lifewire, July 27, 2017.

Shop smart online

Better Business Bureau

Consumer Reports. (Also, check out Consumer Reports' article on privacy: "66 Ways to Protect Your Privacy Right Now")

Protect yourself on social media

Facebook Help Center

The Privacy Rights Clearinghouse

Brian Barrett, "How to Lock Down Your Facebook Privacy Settings," November 14, 2017.

Secure your home network

How to change your router's default IP address and password:

- CNET: "Home networking explained, part 6: Keep your network secure"
- Lifewire: "What is an IP Address?"

Keep your router from getting hijacked: CNET: "Home networking explained, part 6: Keep your network secure"

Manage the encryption options for your router online: Lifewire: "How to Encrypt Your Wireless Network"

How to determine if your firewall exists and is activated: Lifewire: "How to Test Your Firewall"

The information companies collect about you

Privacy Badger is a free tool from the Electronic Frontier Foundation that allows you to help limit online ads.

Get more information on cookies on the help pages of your favorite browser:

- Chrome
- Firefox
- Internet Explorer
- Safari

For general tips on enhancing your privacy, see this information on your browser's help pages:

- Google
- Internet Explorer
- Firefox
- Safari

Sources

CUB is grateful to the following sources in creating this guide.

[1]"2016 Internet Crime Report," Federal Bureau of Investigation Internet Crime Complaint Center, https://pdf.ic3.gov/2016_IC3Report.pdf.

[2]"Secure Auth Survey Majority Reuse Passwords," SecureAuth, July 19, 2017, https://www.secureauth.com/company/news-room/secureauth-survey-majority-reuse-passwords.

[3]Doug Shadel, "Build a Better Password," AARP, March 31, 2017, https://www.aarp.org/money/scams-fraud/info-2017/password-protection-tips.html?intcmp=AE-HF-TECH-EOA3-VID.

[4]Richard Barnes, "Don't Get Pwned: A Guide to Safer Logins," Mozilla (blog), January 25, 2017, https://blog.mozilla.org/internetcitizen/2017/01/25/better-password-security/.

[5]"Animated Overview: How to Make a Super-Secure Password Using Dice," Surveillance Self-Defense, Electronic Frontier Foundation, https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice

[6]Lisa Weintraub Schifferle, "Tech-savy seniors get online," Federal Trade Commission (blog), October 5, 2017, https://www.consumer.ftc.gov/blog/2017/10/tech-savvy-seniors-get-online.

[7]"Computer Security." Federal Trade Commission, https://www.consumer.ftc.gov/articles/0009-computer-security.

[8]"Protect your passwords," Microsoft Safety & Security Center, https://www.microsoft.com/en-us/safety/pc-security/protect-passwords.aspx.

[9] "Animated Overview: Using Password Managers to Stay Safe Online," Surveillance Self-Defense, Electronic Frontier Foundation, https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online.

[10] "66 Ways to Protect Your Privacy Right Now," ConsumerReports.org, last updated February 21, 2017, https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now/

[11] Rubenking, Neil J., "The Best Password Managers of 2018," PC Magazine, Dec. 7, 2017, https://www.pcmag.com/article2/0,2817,2407168,00.asp

[12]Gennie Gebhart, "The 12 Days of 2FA: How to Enable Two-Factor Authentication For Your Online Accounts." Electronic Frontier Foundation, December 8, 2016, https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts.

[13]"Anti-Spam Resources," Privacyrights.org, last modified October 16, 2017. https://www.privacyrights.org/consumer-guides/anti-spam-resources.

[14]"Avoid and report phishing emails," Gmail Help, https://support.google.com/mail/answer/8253?hl=en.

[15] "How to: Avoid Phishing Attacks," Surveillance Self-Defense, Electronic Frontier Foundation, https://ssd.eff.org/en/module/how-avoid-phishing-attacks.

[16] Adi Robertson, "Google Docs users hit with sophisticated phishing attack," The Verge, https://www.theverge.com/2017/5/3/15534768/google-docs-phishing-attack-share-this-document-with-you-spam

[17]"Email and web scams: How to help protect yourself," Microsoft Safety & Security Center, https://www.microsoft.com/en-us/safety/online-privacy/phishing-scams.aspx.

[18]"Text Message Spam," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0350-text-message-spam.

[19]"Phishing," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0003-phishing.

[20]"Stopping Unsolicited Mail, Phone Calls, and Email," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0262-stopping-unsolicited-mail-phone-calls-and-email.

[21]"Spam," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0038-spam.

Sources (continued)

[22]Amelia Griggs, "How to Set up Spam Settings in Yahoo Email," TurboFuture, March 9, 2017, https://turbofuture.com/internet/How-to-Setup-Spam-Settings-in-Yahoo-Email-Including-Marking-and-Unmarking-Email-Messages-Plus-Understanding-Spam.

[23]"EMarketer: Adults Spend Half Of Daily Media Usage On Digital," InsideRadio, Oct. 10, 2017, http://www.insideradio.com/free/emarketer-adults-spend-half-of-daily-media-usage-on-digital/article_24addc46-ad97-11e7-bbda-4f926ba26027.html

[24]"Malware," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0011-malware.

[25]Neil DuPaul, "Common Malware Types: Cybersecurity 101," Veracode (blog), October 12, 2012, https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101.

[26]"List of Types of Malware," MalwareFox, https://www.malwarefox.com/malware-types/

[27]"'Free' Security Scans," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0263-free-security-scans.

[28]"Tech Support Scams," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0346-tech-support-scams.

[29]Justin Ferris, "5 signs your computer or tablet might have a malware infection," Komando.com, https://www.komando.com/tips/12164/5-signs-you-have-a-computer-virus/all

[30]"Communicating with Others," Surveillance Self-Defense, Electronic Frontier Foundation, https://ssd.eff.org/en/module/communicating-others

[31]Patrick Nohe, "5 Ways to Determine if a Website is Fake, Fraudulent, or a Scam," Hashed Out (blog), https://www.thessl-store.com/blog/5-ways-to-determine-if-a-website-is-fake-fraudulent-or-a-scam/

[32]"Tips for Using Public Wi-Fi Networks," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks.

[33]"3 ways to spot a malicious website," Komando.com, April 10, 2017, https://www.komando.com/tips/294711/3-ways-to-spot-a-malicious-website/all

[34]Mark Jones, "7 ways to hack-proof your smartphone to keep your data safe." Komando.com, April 1, 2017, https://www.komando.com/tips/395055/7-ways-to-hack-proof-your-smartphone-to-keep-your-data-safe/all.

[35]Ivan, "How to Know if an App is Safe?" MacPaw, September 28, 2016 updated December 5, 2017, https://macpaw.com/how-to/how-to-tell-if-an-app-is-safe.

[36]Dan Graziano, "How to spot fake iOS and Android apps," CNET, November 9, 2016, https://www.cnet.com/how-to/how-to-spot-fake-ios-and-android-apps/.

[37]Noemi Garcia, "Just When You Thought Your Smartphone was Safe," AARP (blog), March 2, 2016, https://states.aarp.org/just-when-you-thought-your-smartphone-was-safe/.

[38]Jean Folger, "How to Know If an App Is Safe to Shop In," November 28, 2016. https://www.investopedia.com/articles/personal-finance/112816/how-know-if-app-safe-shop.asp

[39]Ari Lazarus, "There's an app for that (but it might be fake)," Federal Trade Commission (blog), December 22, 2016, https://www.consumer.ftc.gov/blog/2016/12/theres-app-it-might-be-fake

[40] Aaron Couch, "10 Steps To Take When You Discover Malware On Your Computer," Make Use Of, August 27, 2013, http://www.makeuseof.com/tag/10-steps-to-take-when-you-discover-malware-on-your-computer/.

[41]"How do I protect myself against Malware," Surveillance Self-Defense, Electronic Frontier Foundation https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

[42]David Nield, "How to remove malware from your computer," Popular Science, May 17, 2017, https://www.popsci.com/remove-malware-from-computer

[43]Eric Geier and Josh Norem, "How to remove malware from your Windows PC," PCWorld, Oct. 18, 2017, https://www.pcworld.com/article/243818/security/how-to-remove-malware-from-your-windows-pc.html

[44]Wendy Zamora, "10 easy steps to clean your infected computer," June 22,2015 (updated March 28, 2016), MalwarebytesLabs. https://blog.malwarebytes.com/101/2015/06/10-easy-steps-to-clean-your-infected-computer/

[45]"Place a Fraud Alert," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

[46]Tim Fisher, "How to Decide Where to Take Your Computer for Repair," Lifewire, March 13, 2017, https://www.lifewire.com/how-to-decide-where-to-take-your-computer-for-repair-2619039.

[47]Tim Fisher, "How Do I Get My Computer Fixed?" Lifewire, Updated July 19, 2017, https://www.lifewire.com/how-do-i-get-my-computer-fixed-2625167

[48]Tim Fisher, "Five Simple Fixes for Most Computer Problems," Lifewire, July 27, 2017, https://www.lifewire.com/simple-fixes-for-most-computer-problems-2618166.

[49]Tim Fisher, "Important Questions to Ask a Computer Repair Service," Lifewire, March 23, 2017, https://www.lifewire.com/important-questions-to-ask-a-computer-repair-service-2618168.

[50]Nathanael Terra, "How to Hire a Quality Computer Repair Tech," Angieslist.com, November 19, 2013, https://www.angieslist.com/articles/how-hire-quality-computer-repair-tech.htm.

[51]"Top 10 Emal Security Tips," https://www.theemaillaundry.com/email-security-tips/.

[52]"Top 10 Ways to Stay Safe On Public Wi-Fi Networks," The Lifehacker Staff, February 4, 2017, https://lifehacker.com/top-10-ways-to-stay-safe-on-public-wi-fi-networks-1791800347

[53]Elizabeth Harper, "How to Protect Your Privacy on Public Wi-Fi Networks," Techlicious, October 16, 2017. https://www.techlicious.com/tip/how-to-protect-your-privacy-on-public-wifi-networks/

[54]Anna Johansson, "Is Your Email Account Secure on Public WiFi?" The Blog, Huffington Post, February 3, 2017, https://www.huffingtonpost.com/anna-johansson/is-your-email-account-sec_b_14595516.html

[55]Eric Griffith, "14 Tips for Public Wi-Fi Hotspot Security," PC Magazine, August 16, 2017. https://www.pcmag.com/feature/254312/14-tips-for-public-wi-fi-hotspot-security

[56]Ian Paul, "Best VPN services of 2017: Reviews and buying advice," PCWorld, October 6, 2017, https://www.pcworld.com/article/3198369/privacy/best-vpn-services-apps-reviews-buying-advice.html.

[57]Dustin Driver, "Do you need a VPN?," Mozilla (blog), August 29, 2017, https://blog.mozilla.org/internetcitizen/2017/08/29/do-you-need-a-vpn/.

[58]"Choosing the VPN That's Right for You," Surveillance Self-Defense, Electronic Frontier Foundation, https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

[59]Laptop Security," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0009-computer-security. https://www.advertisemint.com/2-surveys-forecast-more-than-ever-purchases-made-online-this-holiday-season/

[60]Anna Hubbel, "Two Surveys Forecast More-Than-Ever Online Purchases This Holiday Season, Advertisemint, Nov. 2, 2017

[61]Kim Porter, "15 Tips for Safe Holiday Online Shopping," LifeLock (blog), November 06, 2017. https://www.lifelock.com/education/safe-holiday-online-shopping-tips/

[62]"Online shopping tips," Privacyrights.org, last modified October 23, 2017, https://www.privacyrights.org/consumer-guides/online-shopping-tips.

[63]Mrs. Claus, "Top 6 Tips to Avoid Getting Duped By Online Scams This Christmas," PackageFromSanta.com, November 22, 2017.

[64]"Shopping Online." Federal Trade Commission, https://www.consumer.ftc.gov/articles/0009-computer-security.

[65]Lorraine Mirabella, "Ways to Stay Safe While Shopping Online," November 7, 2016, https://www.aarp.org/money/scams-fraud/info-2016/protect-from-online-shopping-cyber-scams.html.

[66]Shannon Greenwood, Andrew Perrin and Maeve Duggan, Social Media Update 2016, Pew Research Center. November 11, 2016, http://www.pewinternet.org/2016/11/11/social-media-update-2016/

[67]Stacy Liberatore, "Tired of seeing annoying adverts on Facebook? Here's how to fix it," DailyMail.com, August 22, 2016 (updated August 29, 2016). http://www.dailymail.co.uk/sciencetech/article-3753526/What-Facebook-REALLY-knows-Firm-reveals-98-pieces-data-uses-target-ads-them.html.

[68]"Social Networking privacy: How to be safe, secure and social," Privacyrights.org, last modified February 1, 2016, https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and-social.

[69]"Help Protect Your Privacy in Online Communities," Microsoft Safety & Security Center, https://www.microsoft.com/en-us/safety/online-privacy/communities.aspx.

[70] Matt Hanson, Nate Drake, "Advanced Facebook privacy and security tips," Techradar, November 30, 2016. http://www.techradar.com/how-to/internet/facebook-privacy-and-security-tips-1307505.

[71]Brian Barrett, "How to Lock Down Your Facebook Privacy Settings," November 14, 2017. https://www.wired.com/story/how-to-lock-down-facebook-privacy-settings/.

[72]Sid Kirchheimer, "4 Surging Facebook Scams You Need to Avoid," AARP (blog), October 6, 2017, http://blog.aarp.org/2017/10/06/4-surging-facebook-scams-you-need-to-know/.

[73]Dong Ngo, "Home networking: Everything you need to know," CNET, February 15, 2017, https://www.cnet.com/how-to/home-networking-explained-part-1-heres-the-url-for-you/.

[74]Tim Fisher, "What is an IP Address?," Lifewire, November 7, 2017, https://www.lifewire.com/what-is-an-ip-address-2625920.

[75]Dong Ngo, "Home networking explained, part 6: Keep your network secure," CNET, December 22, 2015, https://www.cnet.com/how-to/home-networking-explained-part-6-keep-your-network-secure/.

[76]Melanie Pinola, "What are WEP, WPA, and WPA2? Which are Best?," Lifewire, November 3, 2017, https://www.lifewire.com/what-are-wep-wpa-and-wpa2-which-is-best-2377353.

[77]"What is a firewall?," Microsoft Safety & Security Center, https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx.

[78]Carrie Marshall, Cat Ellis, "The best free firewall 2017," Techradar, October 11, 2017, http://www.techradar.com/news/the-best-free-firewall.

[79]"OnGuard Online Tips to help you stay safe and secure online," Federal Trade Commission, https://www.consumer.ftc.gov/features/feature-0038-onguardonline.

[80]Sarah Mitroff, "Back to basics: The three easiest ways to back up your files," CNET, September 26, 2015, https://www.cnet.com/how-to/easiest-ways-to-backup-your-files/.

[81]Jeremy S., "How Long Do Hard Drives Last? Lifespan And Signs Of Failure," June 14, 2017, The Data Rescue Center, Prosoft Engineering, Inc., https://www.prosofteng.com/blog/how-long-do-hard-drives-last/

[82]"Hard Drives Types and Capacity Guide," Best Buy.com, https://www.bestbuy.com/site/clp/hard-drives-types-and-capacity-guide/pcmcat244100050004.c?id=pcmcat244100050004.

[83]"Online Tracking," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0042-online-tracking.

[84] "Understanding Mobile Apps," Federal Trade Commission, https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

[85]Kayla Matthews, "How to tell if an app is safe to download," Komando.com, https://www.komando.com/tips/412628/how-to-tell-if-an-app-is-safe-to-download

[86]Francis Navarro, "How to control your apps' permissions," Komando.com, October 25, 2017