SECURITY GUIDE

The McAfee Safety Series

Black Friday and Cyber Monday Safe Shopping Guide

Table of Contents

Table of Contents (continued)

‘Tis season of giving. And unfortunately, taking.

Hackers, scammers, and thieves go where the money flows. And the money certainly flows online when Black Friday and Cyber Monday come around. With their roots in the U.S., these shopping holidays now account for a massive rush of holiday shopping that rakes in billions of dollars worldwide. It’s a time when the deals roll out—and so do some of the worst scams going.

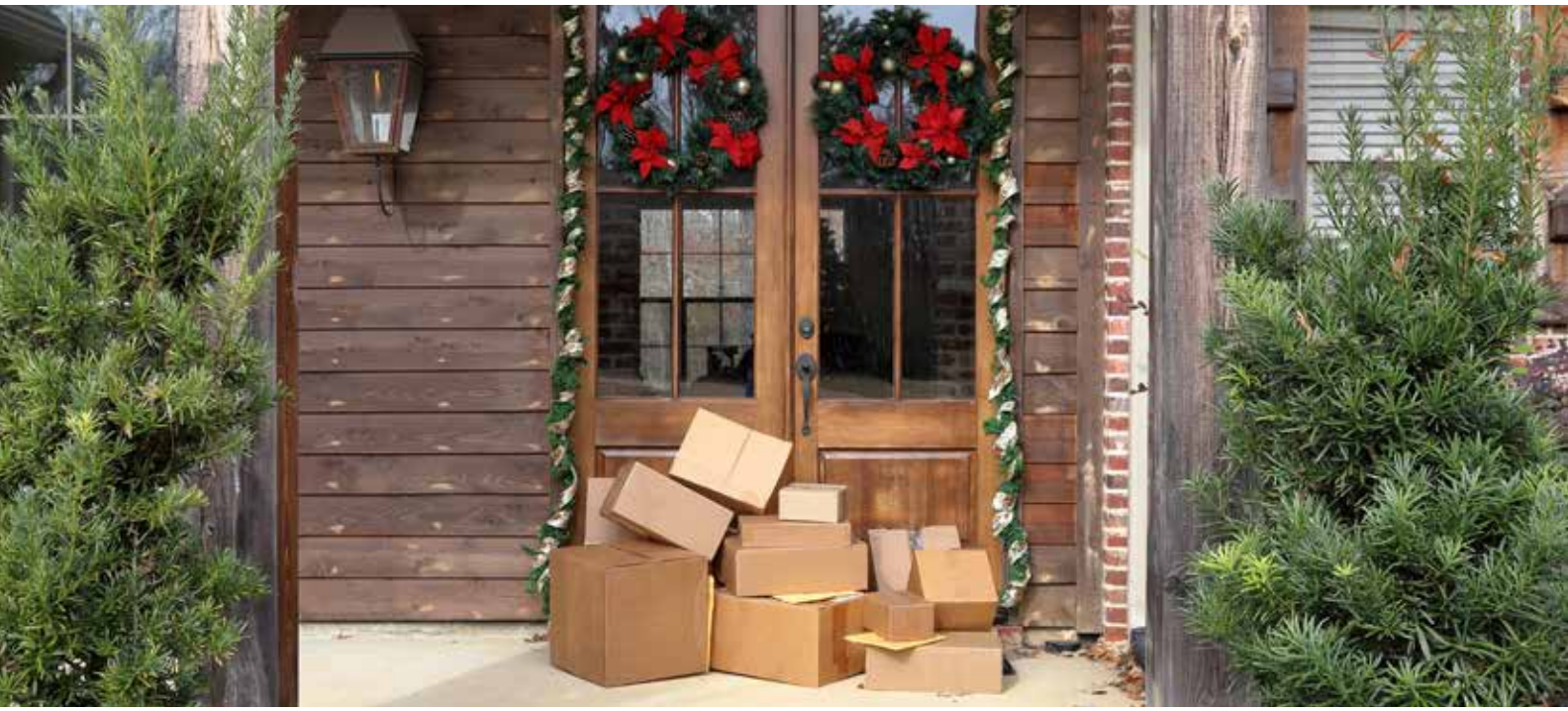
But you have plenty of ways you can protect yourself from it.

Cybercriminals of all kinds try to cash in this time of year by blending in with the holiday rush, as they spin up all manner of tricks to grift personal information from their victims or steal their money outright. They send out fake shipping notices packed with spyware, create copycat websites with phony deals, and even form bogus charities that look legitimate at first glance, yet are anything but. Taken together, they may lead to malware on your computer or phone, point you to phishing sites that steal your personal info, or simply may rip you off.

For hackers, scammers, and thieves, the holidays mark the season of taking. Not giving.

With this guide, we aim to get you wise to their tricks, what they look like and how they reel you in. Further, we’ll share ways you can avoid those scams—and how you can undo the damage if the unfortunate should happen to you.

Let’s start with a look at the top scams going during the holiday season.



"The Five Least Wanted"—Top holiday shopping scams to avoid

Classically, many online scams play on people's emotions. They create a sense of urgency or even fear with emails that say you need to "act now" or texts that say there's a security issue with one of your accounts. Now, during the holidays, scammers have another emotional lever they can pull. Stress. The stress of time, money, or finding that hard-to-get gift that looks like it's out of stock everywhere.

Cybercriminals will tailor their attacks around emotions, stress, and scarcity, hoping that they'll catch you with your guard down during this busy time of year. You'll see those themes run through holiday shopping scams like a red ribbon. And that makes them easier to spot.

Here's our list of the top five:

1. The fake order scam

Come this time of year, keeping tabs on all the packages you have in transit can get tricky. You may have an armload of them enroute at any given time, and scammers will look to slip into this mix with phony order confirmations sent to your inbox or your phone by text. Packed with either an email attachment or a link to a bogus website, they'll try to get you to download malware or visit a site that attempts to steal your identity.

These messages can look quite legit, so the best way to keep track of your orders is on the sites where you purchased them. Go directly to those sites rather than clicking on any links or attachments you get.

2. The phony tracking number scam

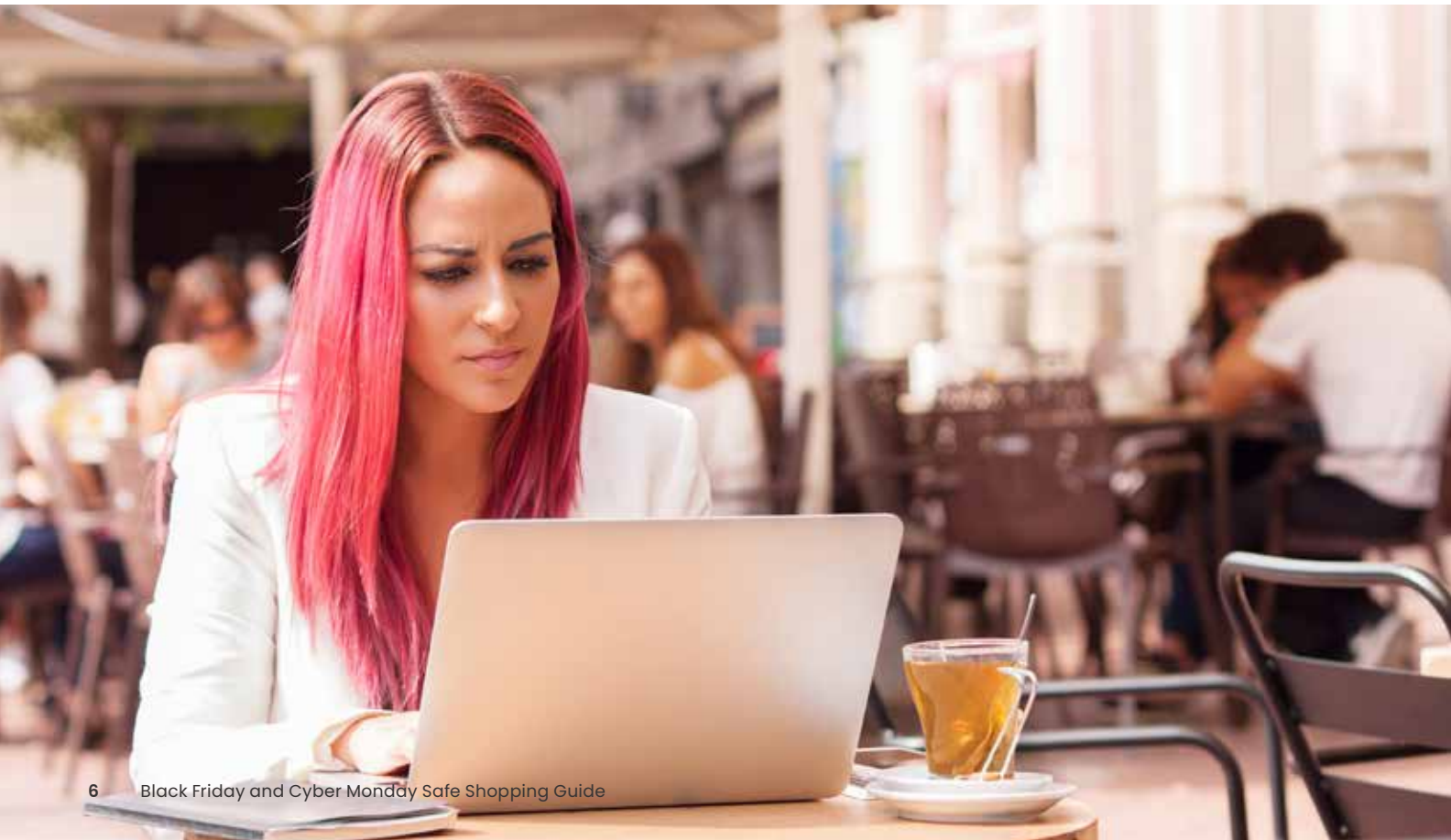
This scam plays out much like the fake order scam, yet in this case cybercriminals will send a phony package tracking notification, again either as a link or as an attachment. For starters, legitimate retailers generally won't send tracking numbers in an attached file. If you see anything like that, it's very likely a scam designed to inject malware onto your device. In the case of a link, the scammers aim to send you to a site that will steal your personal info, just like in the case mentioned above.

Once again, the best way to track your packages is to go to the source. Visit the online store where you made your purchase, open your current orders, and get your package tracking information from there.

3. The bogus website scam

A classic scammer move is to "typosquat" phony email addresses and URLs that look awfully close to legitimate addresses of legitimate companies and retailers. So close that you may overlook them. They often appear in phishing emails and instead of leading you to a great deal, they can send you to scam sites that can then lift your login credentials, payment info, or even funds should you try to place an order through them.

You can avoid these sites by going to the retailer's site directly. Be skeptical of any links you receive by email, text, or direct message—it's best to go to the site yourself by manually typing in the legitimate address yourself and look for the deal there.



4. The hot deal scam

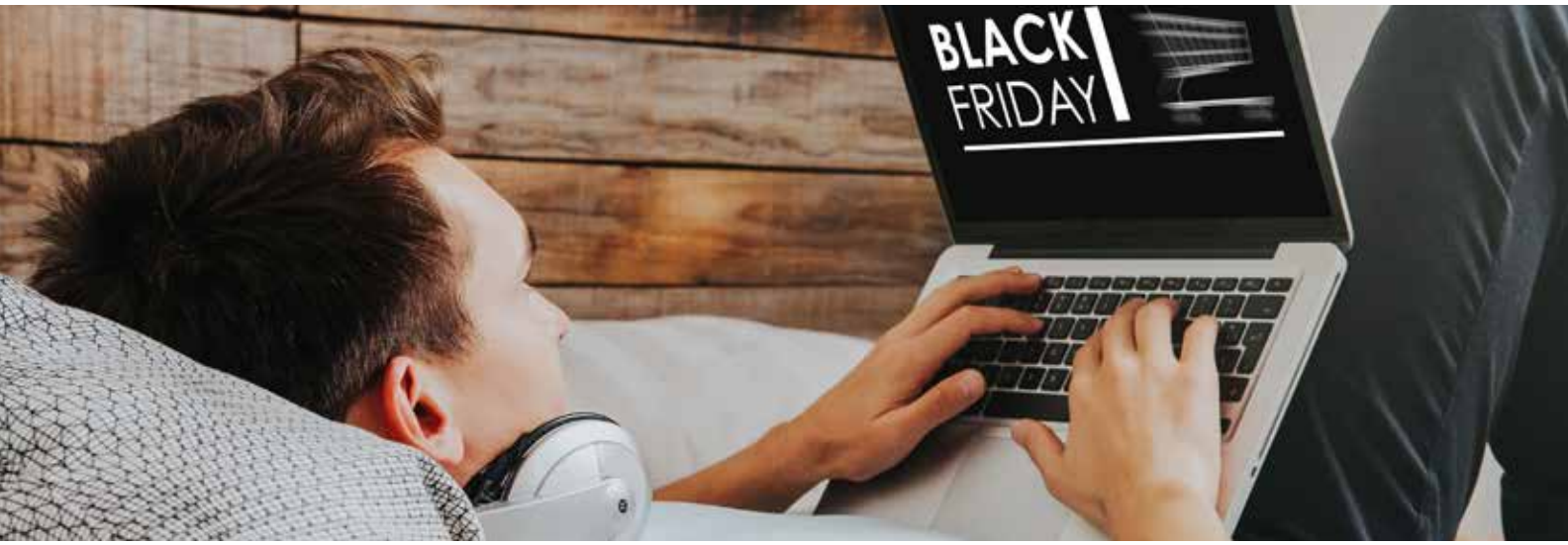
At the heart of holiday shopping is scarcity. And scarcity is something scammers love. There's always some super-popular holiday item that's tough to find, and scammers will spin up phony websites and offers around those items to lure you in. They may use the typosquatting technique mentioned above to pose as a legitimate retailer, or they may set up a site with their own branding to look legitimate on their own (or at least try). Either way, these scams can hurt you in a couple of ways—one, you'll pay for the goods and never receive them; and two, the scammers will now have your payment info and address, which they can use to commit further fraud.

If the pricing, availability, or delivery time all look too good to be true for the item in question, it may be a scam designed to harvest your personal info and accounts. Use caution here before you click. If you're unsure about a product or retailer, read reviews from trusted websites to help see if it's legitimate. (In the U.S., the Better Business Bureau is a great place to start—more on that in moment.)

5. The fake charity scam

During the season of giving, donating to charities in your name or in the name of others makes for a popular holiday gesture. Scammers know this too and will set up phony charities to cash in. Some indications that a phony charity has reached you include an urgent pitch that asks you to "act now." A proper charity will certainly make their case for a donation, yet they won't pressure you into it. Moreover, phony charities will outright ask for payment in the form of gift cards, wire transfers (like Western Union), money orders, or even cryptocurrency—because once those funds are sent, they're nearly impossible to reclaim when you find out you've been scammed.

There are plenty of ways to make donations to legitimate charities, and the U.S. Federal Trade Commission (FTC) has a site full of resources so that you can make your donation truly count.



How to protect yourself from scams on Black Friday and Cyber Monday

Some of it takes an eagle eye that can spot these scams as they pop up in your inbox, texts, social media feed, and so on. Yet you have further ways you can keep safe while shopping on Black Friday, Cyber Monday, and any time.

Stick with known, legitimate retailers online

This is a great one to start with. Directly typing in the correct address for online stores and retailers is a prime way to avoid scammers online. In the case of retailers that you don't know much about, the U.S. Better Business Bureau (BBB) asks shoppers to do their research and make sure that retailer has a good reputation. The BBB makes that easier with a listing of retailers you can search simply by typing in their name.

Look for the lock icon in your browser when you shop

Secure websites begin their address with "https," not just "http." That extra "s" in stands for "secure," which means that it uses a secure protocol for transmitting sensitive info like passwords, credit card numbers, and the like over the internet. It often appears as a little padlock icon in the address bar of your browser, so double-check for that. If you don't see that it's secure, it's best to avoid making purchases on that website.

Pay with a credit card instead of your debit card

In the U.S., the Fair Credit Billing Act offers the public protection against fraudulent charges on credit cards, where citizens can dispute charges over $50 for goods and services that were never delivered or otherwise billed incorrectly. Note that many credit card companies have their own policies that improve upon the Fair Credit Billing Act as well. However, debit cards aren't afforded the same protection under the Act. Avoid using a debit card while shopping online and use your credit card instead.

Likewise, if you're asked to pay with a gift card, wire transfer (like Western Union), money order, or cryptocurrency, that's an almost certain sign of a scam. With these payment methods, once the money is gone it's pretty much gone for good. The ways you can contest a payment or recover funds are extremely limited, if not nonexistent. Again, stick with a credit card where you have avenues of recourse available.

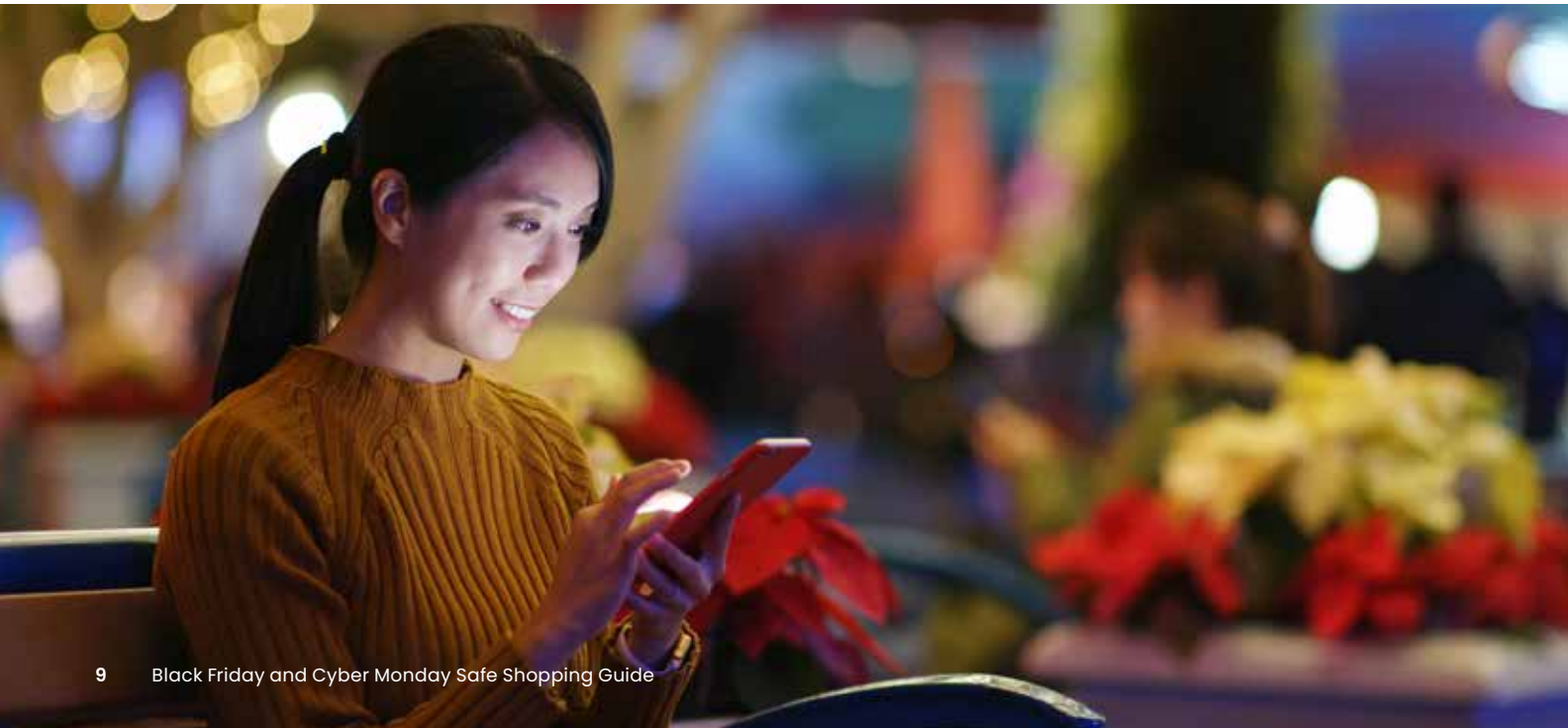
Use two-factor authentication on your accounts

Two-factor authentication is an extra layer of defense on top of your username and password. It adds in the use of a special one-time-use code to access your account, usually sent to you via email or to your phone by text or a phone call. In all, it combines something you know, like your password, with something you have, like your smartphone. Together, that makes it tougher for a crook to hack your account. If any of your accounts support two-factor authentication, the few extra seconds it takes to set up is more than worth the big boost in protection you'll get.

Use a VPN if you're shopping on public Wi-Fi

Public Wi-Fi in coffee shops and other public locations can expose your private surfing to prying eyes because those networks are open to all. Using a virtual private network (VPN) encrypts your browsing, shopping, and other internet traffic, thus making it secure from attempts at intercepting your data on public Wi-Fi, such as your passwords and credit card numbers.

What's more, a VPN masks your whereabouts and your IP address, plus uses encryption that helps keep your activities private. As a result, companies and data brokers can potentially learn far less about you, your shopping, your travels, your habits, and any other information that they could possibly collect and otherwise profit from.



Clean up your personal data online

Yes, it's true. Your information gets collected, bought, and solid online. In fact, personal information fuels a global data trading economy estimated at $200 billion U.S. dollars a year. Run by data brokers that keep hundreds and even thousands of data points on billions of people, these sites gather, analyze, buy, and sell this information to other companies as well as to advertisers. Likewise, these data brokers may sell this information to bad actors, such as hackers, spammers, and identity thieves who would twist this information for their own purposes.

Getting your info removed from these sites can seem like a daunting task. (Where do I start, and just how many of these sites are out there?) Our Personal Data Cleanup can help by regularly scanning these high-risk data broker sites for info like your home address, date of birth, and names of relatives. It identifies which sites are selling your data, and depending on your plan, help with removal. If you have one of our McAfee+ plans, data cleanup is included as part of the package.

Protect your identity from identity thieves

Another place where personal information is bought and sold, stored, and exchanged is the dark web. The problem is that it's particularly difficult for you to determine which, if any, of your info is on the dark web, stashed away in places where hackers and thieves can get their hands on it. Identity monitoring can help. McAfee's identity monitoring helps you keep your personal info safe by alerting you if your data is found on the dark web, an average of 10 months ahead of similar services.

Monitored info can range anywhere from bank account and credit card numbers to your email addresses and government ID number, depending on your location. If your information gets spotted, you'll get an alert, along with steps you can take to minimize or even prevent damage.

Take advantage of identity protection

Identity protection through McAfee takes identity monitoring a step further. Depending on your location and plan, it offers identity theft coverage for financial losses and expenses due to identity theft, in addition to hands-on help from a recovery professional to help restore your identity.

Monitor your credit

Keeping an eye on your bills and statements as they come in can help you spot unusual activity on your accounts. A credit monitoring service can do that one better by keeping daily tabs on your credit score and report. While you can do this manually, there are issues to consider. First, it involves logging into each bureau and doing some digging of your own. Second, there are limitations as to how many free credit reports you can pull each year. Our service does that for you and without impacting your credit score.

Depending on your location and plan, McAfee's credit monitoring allows you to look after your credit score and the accounts within it. There, you can spot fluctuations and help you identify unusual activity, all in one place, checking daily for signs of identity theft.

Protect your devices for shopping online

A complete suite of online protection software like McAfee+ can offer layers of extra security while you shop. In addition to the VPN, identity monitoring, and other features mentioned above, it includes web browser protection that can block malicious and suspicious links that could lead you down the road to malware or a phishing scam—along with a password manager that can create strong, unique passwords and store them securely as well. Taken together, McAfee+ offers all-in-one online protection for your identity, privacy, and security that can keep you far safer when you shop online—and as you spend your time online in general.

What should I do if I fall victim to a Black Friday or Cyber Monday scam?

Even if you take the proper precautions the unexpected can happen. Whether it's a scam, an identity crime, or flat-out theft, there are steps you can take right away to help minimize the damage.

Falling victim to a scam can be stressful. Yet take a deep breath and act as quickly as possible. Time is of the essence when your info gets compromised.

1. Notify the companies involved

Whether you spot a curious charge on your bank statement, discover a fraudulent account when you check credit report, or when you get an alert from your monitoring service, let the bank or organization involved know you suspect fraud or theft. With a visit to their website, you can track down the appropriate number to call and get the investigation process started.

2. File a police report

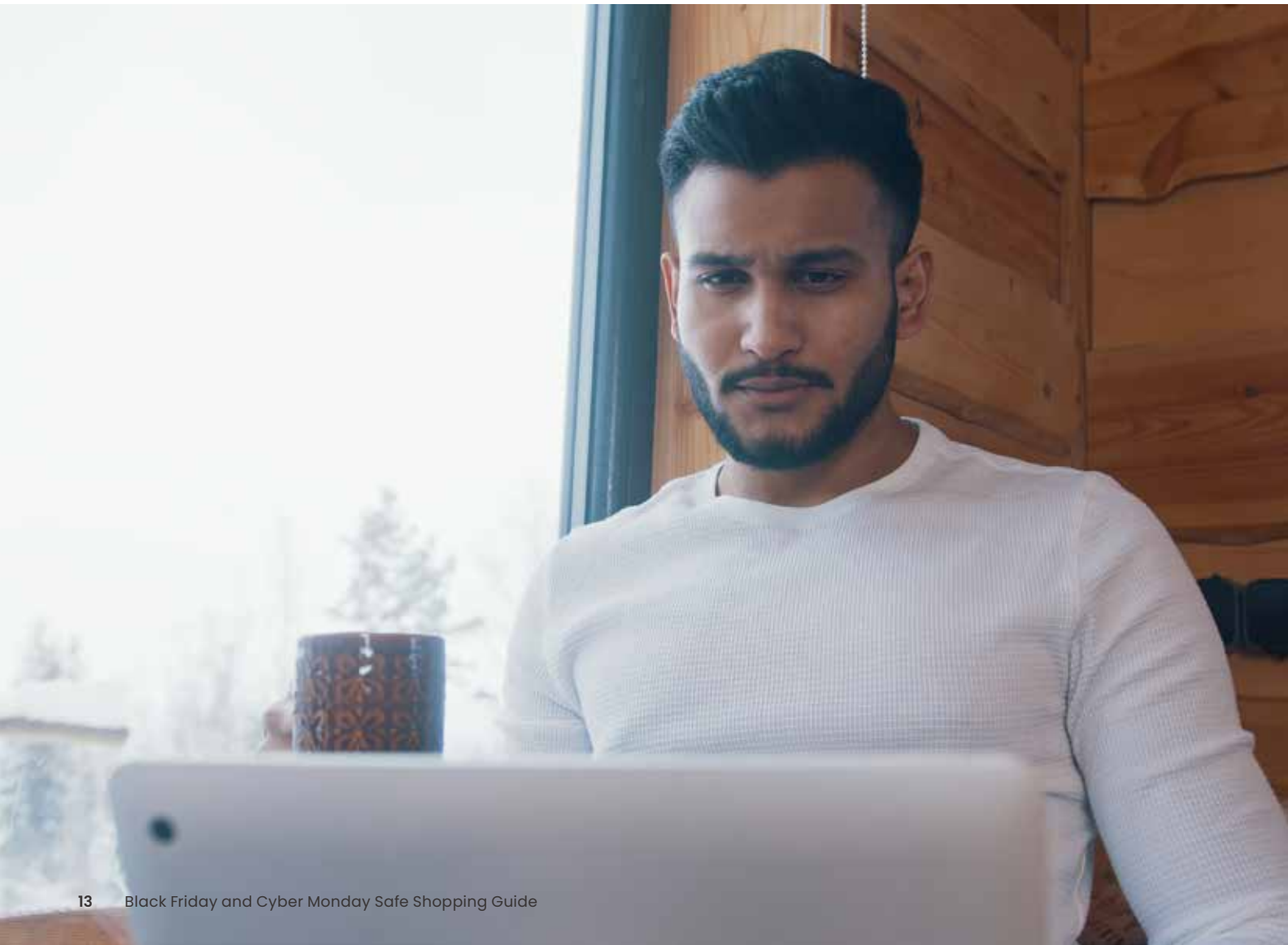
Some businesses will require you to file a local police report and acquire a case number to complete your claim. Beyond that, filing a report is a good idea in itself. Identity theft is still theft and reporting it provides an official record of the incident. Should your case of identity theft lead to someone impersonating you or committing a crime in your name, filing a police report right away can help clear your name down the road. Be sure to save any evidence you have, like statements or documents that are associated with the theft. They can help clean up your record as well.

3. Contact your governmental anti-fraud or trade organization

In the U.S., the identity theft website from the Federal Trade Commission (FTC) is a fantastic resource should you find yourself in need. In addition to keeping records of the theft, the FTC can provide you with a step-by-step recovery plan—and even walk you through the process if you create an account with them. Additionally, reporting theft to the FTC can prove helpful if debtors come knocking to collect on any bogus charges in your name. With a copy of your report, you can ask debtors to stop. If you're outside of the U.S., this article from our Knowledge Center provides steps you can take in your country.

4. Put on a credit freeze or lock

An instance of identity fraud or theft, suspected or otherwise, is a good time to review your options for a credit freeze or lock. As mentioned earlier, see what the credit bureaus in your region offer, along with the terms and conditions of each. With the right decision, a freeze or lock can help minimize and prevent further harm. Check out our blog article for more info as to which one could work best for you.



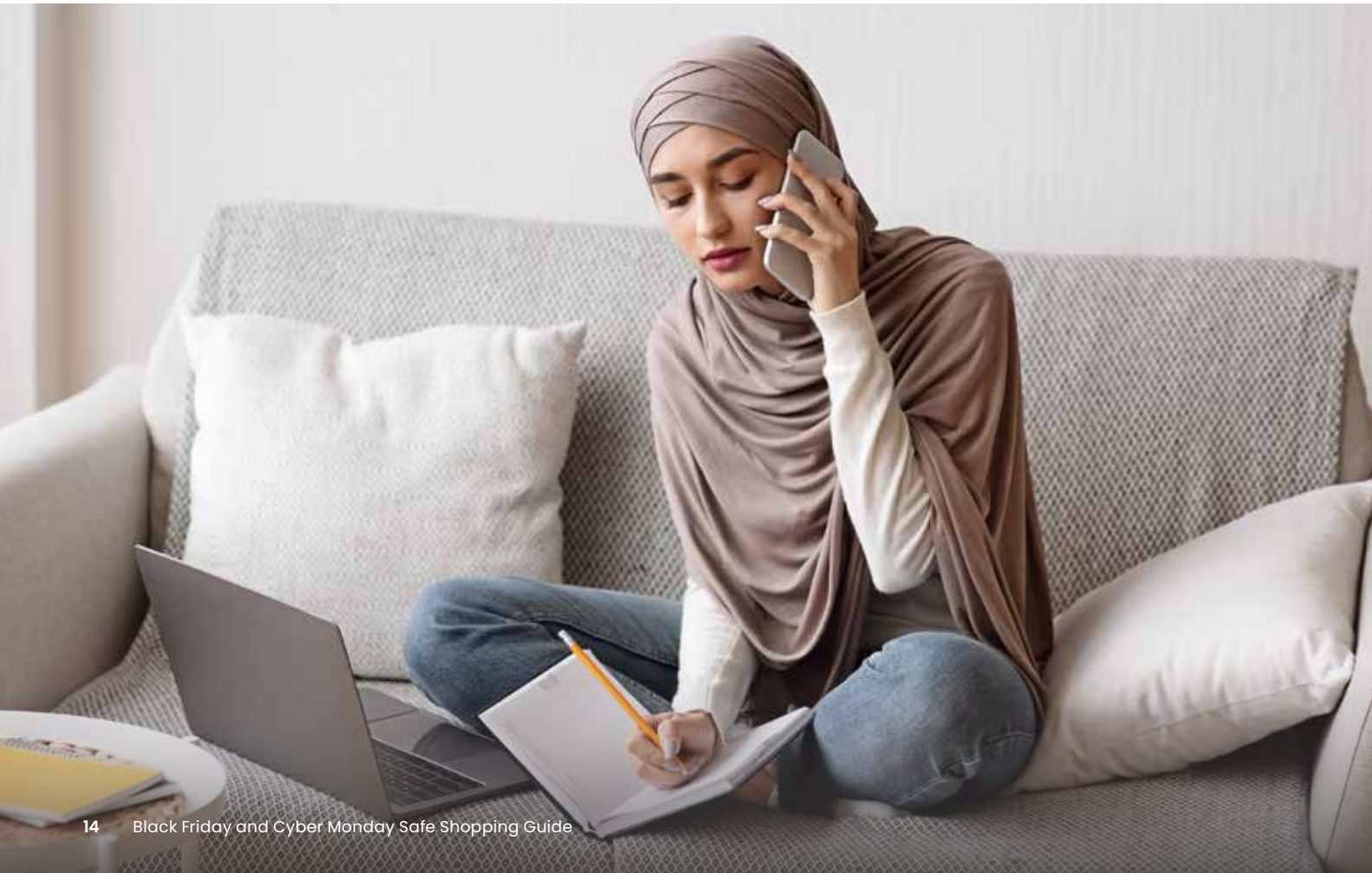
5. Continue to monitor

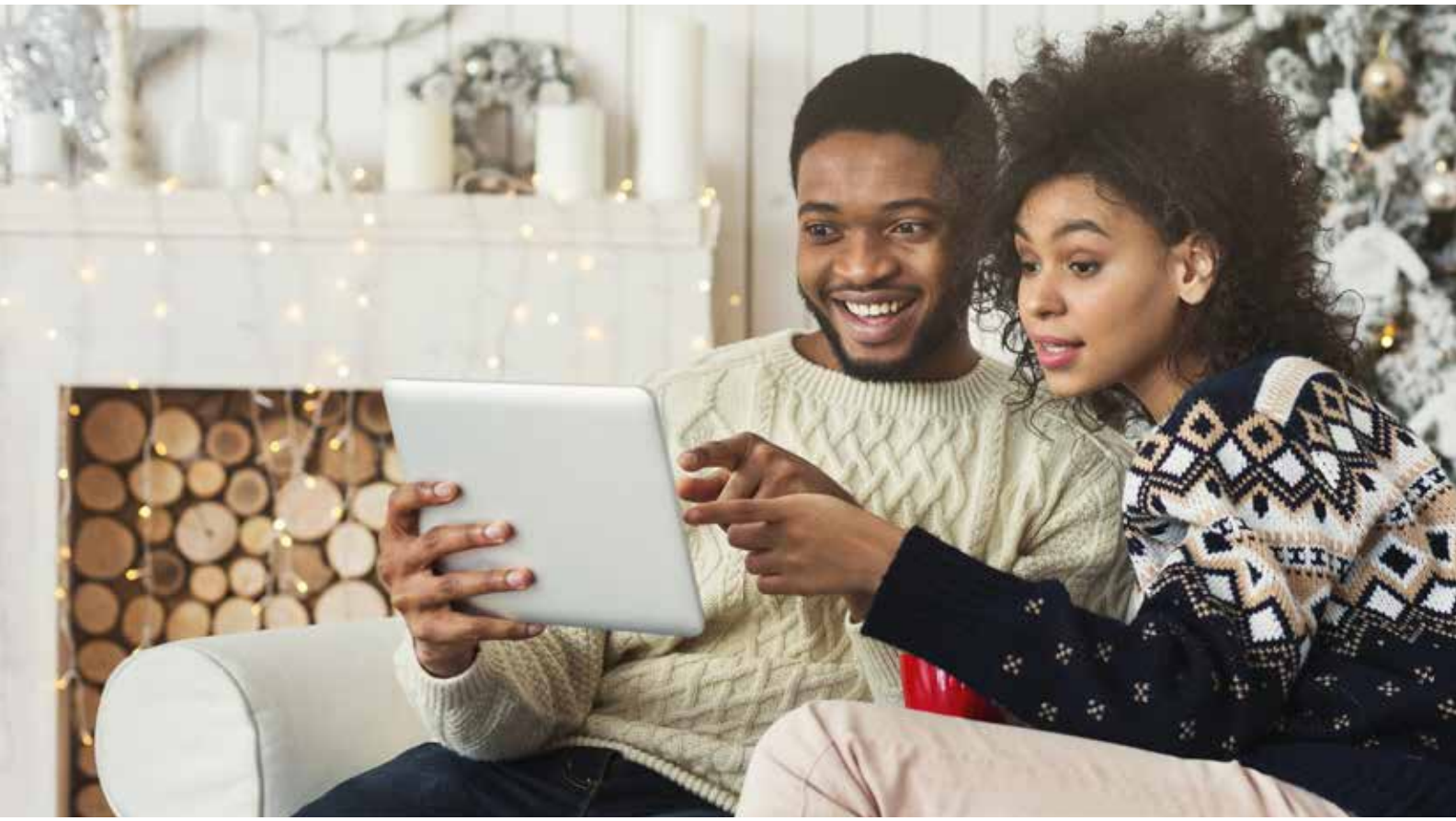
Strongly consider using a monitoring service like the one we described earlier to help you continue to keep tabs on your sensitive and personal info online and activity on your credit. The unfortunate fact of identity theft and fraud is that it can mark the start of a long, drawn-out affair. One instance of theft can possibly lead to another, so even what may appear to be an isolated bad charge on your credit card calls for keeping an eye on your identity all around. Many of the tools you would use up to this point still apply, such as checking up on your credit reports, maintaining fraud alerts as needed, and reviewing your accounts closely—along with utilizing an identity monitoring service.

6. Work with a recovery pro

A recovery service can help you clean up your credit in the wake of fraud or theft, all by working on your behalf. Given the time, money, and stress that can come along with setting your financial record straight, leaning on the expertise of a professional can provide you with much-needed relief on several counts.

If available, depending on your location and plan, McAfee+ offers identity theft coverage & restoration that includes up to $1 million toward legal fees, travel, and stolen funds reimbursement, $25k in ransomware coverage—along with the assistance of a licensed recovery pro who can help repair your credit and identity.





Take an extra moment to spot those Black Friday and Cyber Monday scams

Just as it's always been, hackers, scammers, and thieves want to ruin a good thing. In this case, it's your spirit of giving in the holiday season. Yet with this list of top scams and ways you can avoid them, you can keep bad actors like them at bay.

Remember, they're counting on you to be in a hurry this time of year, and maybe a bit stressed and a little disorganized to boot. Take your time while shopping out there and keep an eye out for their tricks. That extra moment can save you far more time and money than you may think.

For more about staying safe and getting the most out of life online, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-black-friday-cyber-monday-safe-shopping_1122 NOVEMBER 2022