Common Scams

1. Phishing emails – Phishing, or emails with fake links designed to get your personal information, often ramps up at the end of the year. Fake delivery confirmations are an annual favorite.

   Popular ones include the personalized letter from Santa to your child, solicitations from unknown third parties that offer gift cards or discounts in exchange for taking a survey, and fake renewal requests for things like insurance coverage.

2. Fake Charities – Unfortunately, fake charities often pop up during the holidays to take advantage of people's generosity. Social media has become a popular method of attack for these scammers.

   Please support your favorite charities, but thoroughly vet any new charities that ask for your money. Legitimate charities will be happy to answer your questions.

3. Phone Scams – More people are home over the holidays, so phone scammers step up their efforts accordingly. In general, you should not give your personal information over the phone in any call that you did not initiate.

4. E-cards – Holiday e-cards are increasingly popular, but they can contain viruses. Verify them separately with the sender before opening.

5. Bogus Websites – Online-shopping bargains may be unusually good for a reason. Scammers may create slick websites offering merchandise at cut-rate prices without any intent of delivering – or worse, as a front to steal and misuse your account information. If you would like to monitor your credit to prevent identity theft and see your credit reports and scores for free, join MoneyTips.

   Before you order from a website, verify both that the company is legitimate and that you have not been directed to a spoof of their website. Do not use external links; enter the correct company URL in your browser. Look for "https" in the header – the "s" reflects a secure web page.

6. Take Care with Mobile Use – Ordering on your mobile device may be convenient, but if you are using a public, unsecured wireless connection, you are increasing the risk that your information may be intercepted and stolen.

   It is more difficult to verify on a smartphone that you are connecting to a legitimate site, and more tempting to use convenient links that could redirect you. Per the above suggestions, type in the correct URL in the browser. If you are connecting through retailer apps, verify that the app is valid.

7. Gift Cards – You can buy major retailers' gift cards almost anywhere now – even at gas stations – but check them carefully. If the activation codes are exposed, scammers may have already copied and used the information, leaving you with a worthless card.

8. Change Your Passwords – What could be more fun than sitting in front of a roaring fire with hot apple cider and changing all of your passwords? There are plenty of things that are more fun, but not many that are more useful.

9. Use Credit over Debit – Credit cards will not protect you from scams, but they can limit the damage. Your liability for defective/undelivered items or fraudulent use of your card is $50, and many credit companies will waive that. Debit cards are linked to your bank account, so it is easy for thieves to drain your account without your knowledge.

From CNBC:

10 ways to protect yourself against scams during Black Friday and Cyber Monday

Published Sun, Nov 24 20199:45 AM EST

Megan Leonhardt

@MEGAN_LEONHARDT

About 75% of Americans plan to do at least half of their holiday shopping online this year, according to TransUnion's 2019 Holiday Retail Fraud Survey.

But while online shopping helps you skip the crowds at the mall, it can be a cybersecurity minefield. "The holidays are a bonanza for cybercriminals," Dave Baggett, co-founder and CEO of anti-phishing start-up Inky tells CNBC Make It. "People are buying a lot of things over a short period of time, and they are hurried about it. This presents opportunities for crooks."

Here's a one-stop guide on how to best protect yourself while shopping this holiday season.

1. Don't click links in emails

Emails are a particularly common way for fraudsters to gain access to your credit card information or identity. Hackers send what's called a phishing email, in which they copy a store's sale or discount email and include a link to a false portal asking for your info.

"Email is the number-one way cybercrime of all forms happens. If a bad guy can get you to click on a link in an email, he can do all manner of bad things to your online life," Baggett says. If you do get a tempting promotion, go directly to the retailer's website by typing its name in your browser.

2. Don't open attachments from retailers

In the same way that you should avoid clicking on email links, you don't open up attachments from retailers. "Retailers won't hide deals in attachments – that's where attackers hide malware," says Michael Madon, senior vice president and general manager of security awareness for Mimecast and a former cybersecurity director for the U.S. Treasury.

Cyber criminals aren't only impersonating retailers, either. You could get a fake email that seems to be from a major shipping company like UPS, FedEx or DHL. Instead of clicking on a tracking number listed in an email or opening up an attachment, go directly to ups.com or fedex.com to check the tracking number.

3. Avoid pop-ups and ads

Malware and viruses aren't just spread via email. They can follow you around the Internet in the form of pop-ups and advertisements — these are actually referred to as malvertising, or malicious advertising.

These types of ads can send you to sites that ask for your information, but they can also infect your device with a wide variety of harmful programming such as adware, spyware and ransomware. This is a form of malware that locks up your computer or specific files and forces you to pay to get access back.

"If a deal is legitimate, it will be on the company's site. Pop-ups are an easy way for cybercriminals to lure you in," Madon says.

4. Beware of e-skimmers

Card skimming has been happening for years. It's a scam that typically happens at gas stations or ATMs, where a criminal installs a device that gathers credit card numbers and information when you swipe your card. That practice has gone digital, the FBI says. Cyber thieves can install malicious code on a retailer's website to gather credit card data when you check out.

To protect yourself from this practice, you can pay using a third party such as PayPal, Venmo or Amazon, if the retailer allows it, so the store never actually has your credit card number. Or you can create a virtual credit card through sites like Privacy.com, or on your card issuer's website, that provide temporary numbers so your information stays secure.

5. Use a credit card

Many experts recommend that you use credit cards instead of debit cards. That's because the Fair Credit Billing Act makes it so consumers are only liable for up to $50 in fraudulent charges. And major credit card companies, including American Express, Discover, Mastercard and Visa offer "zero liability" policies, so you don't have to pay for any fraud.

Save your debit card for taking out cash, Ally Bank recommends. Not just during the holidays, but year-round. And make sure to avoid suspicious ATMs. If the ATM looks broken, or anything on the front of the machine appears dislodged, or jerry-rigged, it could mean that someone has installed a card-skimming machine.

Looking for a new credit card this holiday season? Check out CNBC Select's roundup of the best cards for Black Friday and Cyber Monday shopping.

6. Use a secure network to shop

Almost half of Americans, 45%, have used public Wi-Fi to access sensitive information, according to a survey by payment compliance provider PCI Pal.

But with all the bad bots and cyber criminals lurking during the holiday season, it can be a particularly dangerous time of year.

When shopping online, make sure you're using a private Wi-Fi connection or your smartphone's cellular network to browse the internet. Public Wi-Fi networks are notoriously insecure and could open you up to malware or hacking.

"Without proper network precautions, the hacker sitting a few seats down at your local Starbucks could sneak into your device and watch you input your credit card information," Madon says.

If you absolutely need to use public Wi-Fi, use a Virtual Private Network, or VPN, that will encrypt your browsing history and activity. Hotspot Shield Free is a free VPN that will allow you to connect up to five devices from one account. If you're willing to pay, experts recommend ExpressVPN, which has packages starting at about $100 a year.

7. Be suspicious of free offers

During the holidays, Baggett says there's an "explosion" of survey and gift card scams. These are generally emails that supposedly offer you payments or gift cards in exchange for taking surveys.

Instead, when the user clicks through, they end up on websites that may look legitimate and ask you for your credit card information or Amazon account credentials "so they can pay you." Yet when you type your credentials in this site, you're giving them directly to the attacker.

These types of emails may also contain a common technique Baggett calls "hidden text." Normally invisible to you, this is text scammers put in to confuse the mail protections that Microsoft, Google, and others use to try to protect you.

8. Diversify your passwords

Almost half of Americans, 47%, use the same passwords over and over again, according to PCI Pal. But cyber thieves can use a stolen password and try to break into other accounts and sites that may expose your personal data.

This is especially common during the holiday shopping season. "Phishing attempts can often be disguised as signups for retail rewards programs," Madon says. "If you take up on the offer, use a password that you haven't used before," he recommends.

9. Monitor your accounts

Throughout the holiday season, keep a close eye on your bank and credit card accounts. “Often criminals will make small charges using bot technology to see if the charge will go through before making larger purchases,” Pavan Thatha, head of bot management at Radware, tells CNBC Make It.

To help protect your identity, set up alerts and monitoring — either with your bank or an outside app such as IdentityForce — that will let you know if any suspicious activity occurs. Also, keep a close eye on your annual credit report for any new accounts or queries you didn’t initiate.

10. Beware gift card scams

A gift card can be the perfect holiday gift for that hard-to-please person on your list, but scams tied to these cards are becoming increasingly popular. For example, one popular strategy used by criminals is to scan or write down the card number in the store, draining the funds before they are even gifted.

When buying physical gift cards off the shelf, carefully inspect it to make sure there’s no tampering and you cannot see the code or pin. Many experts recommend buying electronic gift cards online.

“At the end of the day, bad guys like to exploit our holiday spirit and use it against us,” Baggett says. “Sadly, we need to be more vigilant this time of year than at any other.”