



8 TIPS

to Help

Protect Yourself

Against Holiday Identity Theft

The modern-day Scrooge can strike under many guises this holiday season, from a phishing link to full-blown identity theft.

Here are eight ways to help avoid holiday identity theft this year.

1. Use legitimate sites when shopping online

There are signs to help indicate that a website is secure, such as “https” in the Web address and an icon of a locked padlock on the left side of the URL.

You should also be sure that emails sent to you with promotional links don’t point back toward an altered link, often with one or two letters missing or changed. This could signal a phishing scam, designed to fool you into entering personal information, like your credit card number or your email and password, which may later be used in an attempt to compromise your identity.

2. Use a secure network

When shopping online, avoid using a public Wi-Fi connection. Digital personal information that is transmitted over the Internet or stored on your connected devices—such as your driver’s license number, Social Security number, credit card numbers and more—could be vulnerable if your network isn’t secure. Consider installing and using a Virtual Private Network, or VPN. When you connect with public Wi-Fi, a VPN will direct your online activity through a secure, private network.

Remember that your phones and computers can be gateways to your personal information, so make sure they are protected with strong passwords containing numbers, letters and symbols.

3. Be careful of what you share online

Over-sharing information such as your children’s names and dates of birth or holiday plans can lead thieves lurking on your “friend” list to gain access to valuable information that could help them hack into your online accounts or even know when you’re out of town to attempt to break into your property.

4. Choose cash or credit over debit

Credit cards provide more protection against fraudulent

activity, since credit card companies usually monitor suspicious activity and may be able to put a stop to fraudulent charges. Debit cards, on the other hand, immediately withdraw money from your account and don’t offer the same level of protection.

5. Use protection tools

Take advantage of protection tools, such as ID theft alerts, enrolling in an identity theft protection company plan, and new chip cards, which add an extra layer of protection for consumers. Check out Blackhawk Bank’s **Watchdog Checking** and **MyCardRules** for added layers of protection.

6. Be careful when opening new retail credit accounts

Many stores offer discounts and incentives to those who open a store credit card account, but it’s important that shoppers remain vigilant throughout the enrollment process. For example, you may be required to write down your Social Security number or other personal information when opening an account. Be sure no one is spying over your shoulder when you do so, and ask the sales associate how your information will be discarded after it is entered into the system.

If you receive promotional offers through email that seem too good to be true, be sure to do your due diligence. You’ll want to make sure these offers are legitimate and secure before submitting any personal information.

7. Be leery of skimmers

Remain on the lookout for devices attached to card readers or ATMs that could steal your financial data. Also, watch out for anyone behind you in a checkout line that could be snapping a photo of your credit card number or other personal information.

8. Check your statements and credit reports

Always check over your credit card statements and credit reports, especially during high-volume shopping periods like the holiday season. Remain vigilant and inquire about any suspicious activity to catch any attempt at identity theft before it escalates.

Source: By Renee Morad for Symantec