Black Friday online shopping: How to up your cybersecurity game and protect your identity

November 25 2022, by Katie Wedell

Credit: CC0 Public Domain

Online shopping is more popular than ever, with global e-commerce

sales expected to hit $5.5 trillion in 2022, according to eMarketer.

New research from marketing software firm Wunderkind found 71% of U.S. consumers planned to shop online this Black Friday and Cyber Monday.

With that surge has come more opportunities for identity thieves, hackers and scammers to get a hold of shoppers' financial information.

When the Association of International Certified Professional Accountants conducted a survey in December of 2020, nearly one in five respondents said they fell victim to identity theft or attempted identity theft in the past year.

Online safety expert Chris Bluvshtein at VPNOverview.com provided his top 10 tips for keeping yourself safe while shopping online during the holidays this year.

Stick to websites you know

You might be tempted by a Google link promising an amazing deal but before you click, look at the name. If it's not something you recognize, don't go there, Bluvshtein said.

"Hackers can use similar names to High Street brands to trick you into giving up your data so double check the site is the one you know. Google also tells you if you've visited the site before so it's worth taking your time and checking for those details," he said.

If you do end up shopping on an unfamiliar site, Brianne Cap, director of IT Security at DeVry University, said there are several warning signs to look for to decide whether a website is safe or not:

- The site looks unprofessional or poorly designed.
- Links are broken or disabled.
- No contact information is listed.
- Return or privacy policies are unclear or missing.
- Items are priced incredibly low.
- Credit card credentials are requested for additional reasons not related to your purchase.
- Shipping and extra charges seem unusual.
- The site has an excessive number of negative reviews, or no reviews at all.

Check the URL bar

"Make sure the website you're browsing is secure by looking for the 'lock' icon next to the web address," Cap said as part of Devry's published tips for online shopping.

"If a website doesn't have one of these then don't give your bank details or valuable information," Bluvshtein said.

Check your bank statements

By making it a habit to check your bank account and statements, you'll be able to catch any suspicious activity early on.

Your bank will have information on any time limits they have for reporting fraudulent purchases, so be sure to keep an eye on your statements.

Use a password manager

The safest thing you can do is use a unique, randomized password for all your accounts.

But instead of writing those down on post-it notes or in notebooks, use a password manager to keep them all in one place, Bluvshtein said.

"Password managers lock your information behind a master password and many of them autofill the website logins for you, keeping you safe from keylogger attacks," he said.

The National Cybersecurity Alliance echoed this tip and also recommends enabling multi-factor authentication whenever possible.

"(Multi-factor authentication) will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device," the alliance's tip sheet for online shopping says.

Don't shop on public Wi-Fi

You might be tempted to hop onto your favorite shopping site while having a coffee at your local cafe, but that public Wi-Fi connection is extremely dangerous to use, Bluvshtein said.

"Public Wi-Fi rarely has safety protocols such as passwords in place and hackers can piggyback and steal unsecured banking details and sensitive information without you knowing."

Use mobile payments

Apps like Apple Pay and Google Pay can protect your banking details so if a website accepts them, it's best to use them instead of your debit card.

Or use a credit card

If something is valuable, don't use your debit card to pay for it, experts advised.

That's because credit cards have more protections in place in case of fraud than debit cards.

Set up a temporary bank account

By opening an online-only bank account you can control the amount of money you can access with transfers from your usual account.

This way, even if your details are compromised, the hacker can't do anything to your real bank account, Bluvshtein said.

Use a VPN

A VPN protects your data from prying eyes. Everything you send is encrypted, so even if a hacker can see you on a network, they won't be able to access your sensitive information.

"VPNs connect you to a remote server and hide your IP, using one along with any of our other tips can make your online shopping super secure," Bluvshtein said.

If it seems too good to be true, it probably is

Be careful with any advertisements for amazing deals. You might never get the item or there could be hidden dangers. This old saying still rings true with online shopping.