5 Safe Online Shopping Tips to Keep Your Holiday Merry This Year

Hackers love the holidays. With eyes focused on the retail sector, they ramp up phishing campaigns to catch harried, bargain-hungry shoppers unawares. Credit card and identity theft can put a damper on the holiday spirit. But safe online shopping habits can help.

Cyber criminals use a variety of tactics to con consumers, with great success. In fact, in 2021 they stole $337 million from online shoppers. For instance, that amazing online discount code might actually be a ruse to steal personal information or download a virus. And that slick retail website might not be the store it pretends to be.

Use these tips to keep your bank account, your identity, and your computer safe while shopping for the perfect holiday gifts.

1. Avoid Fake Websites

A favorite method that hackers use involves luring shoppers to a fake website and then stealing their personal or financial data. According to the Anti-Phishing Working Group, hackers created at least one million new fake websites in just the first quarter of this year.

Sometimes it can be difficult to spot fake sites but look for these warning signs.

- **Too good to be true** – By all means, look for bargains. But be careful and know what items should normally cost. If a site advertises a price more than 50 percent lower than normal, exercise extreme caution.
- **Unusual URL (web address)** – A URL that does not reference the actual store name, or one that includes random characters, might indicate a fake. Look closely. Hackers might change the name only slightly. For instance, a link could lead shoppers to a realistic looking Walmart website with a slightly altered URL such as walmrt.com.

- **HTTP instead of HTTPS, or no padlock** – A padlock icon should display to the left of the URL. Additionally, the URL should begin with HTTPS (not just HTTP), indicating an additional layer of security. Do not trust websites without these features. Keep in mind, however, that even the presence of these security protocols does not guarantee safety.
- **Marketplace sellers associated with a trusted site** – Retail giants like Amazon work hard to block fraudulent products in their official online stores. However, take extra care when purchasing products from marketplace sellers instead of the official site.

2. Use Safe Payment Options

Some payment options offer much greater security than others. For example, use a credit card instead of a debit card online. And when using payment services, remember that PayPal has a much better track record than Venmo, Zelle, Apple Pay or Google Pay at refunding money lost to scams.

Additionally, some credit card companies have begun to offer virtual card numbers as an extra layer of protection. With a virtual card number, online shoppers give merchants a temporary card number

unique to each purchase. The number links back to the shopper's credit card account, but hackers have no access to the real card number.

3. Share Only Minimal Personal Information

Online merchants prefer that shoppers create an account. This allows the merchant to market additional products. It also allows shoppers to track their purchases. However, if you must create an account, only enter the minimal information necessary. And avoid storing your credit card number with the merchant, no matter how convenient it makes future shopping.

4. Update Your Anti-virus and Anti-malware Before You Shop

No matter what precautions you take, you will occasionally stumble on fake or compromised websites. And those fraudulent or simply insecure websites can infect your device with nasty viruses and malware. To protect your device and the sensitive information on it, be sure to install anti-virus and anti-malware software and keep it up to date.

5. Always Use Strong Passwords

Shopping online typically involves creating a bunch of online accounts. It can prove tempting to use simple passwords or share the same password among multiple sites. But remember that these accounts include your personal and financial information.

Use a unique, complex password for every account you create, even if you never plan to access the website again. A good password should contain at least 12 characters, including a mix of uppercase and lowercase letters, as well as numbers and symbols. Password managers can help you store passwords securely.

Win Back the Holiday Season with Safe Online Shopping

The online retail environment can feel like the Wild West, with dangers lurking around every cyber corner. However, by slowing down and using cyber security best practices, you can shop safely without leaving the comfort of your sofa.