**Mobile Banking App is HERE!**


UNION BANK

March 2023

# How To Shop Online Safely (Without Getting Scammed)

Member FDIC

EQUAL HOUSING LENDER

### *Can You Get Scammed While Shopping Online?*

Online shopping is convenient and easy. But is it safe?

According to the FBI, the second most common internet crime of 2021 was related to online shopping — non-delivery of goods purchased. Just last year, online shoppers lost $337 million to fraudulent online stores.

Fraudsters create fake online stores and then use social media ads to lure you in to become a customer. But the products either don't arrive, aren't what you expected, or come with huge hidden fees.

But it doesn't stop with fake products and unreasonable fees. Shopping from fake online stores can also lead to identity theft.

Criminals use the information you provided — like your name, address, and credit card details — to take over your identity, drain your bank account, and commit financial fraud.

But this doesn't mean you need to give up shopping online entirely. Here are some essential steps to take to ensure you're getting a great deal and not a scam while shopping online.

### *What Are the Most Common Online Shopping Scams?*

Unfortunately, there are more online shopping scams than ever.

According to the Better Business Bureau's (BBB) 2021 Online Purchase Scams Report, 79% of victims lost money — making online shopping the riskiest scam type of all.

So, how are fraudsters trying to scam you while you shop online?

- **Fake online stores**: The most common online shopping scam is when fraudsters create a fake shopping website or app. These sites may look legitimate, but they're designed to steal your sensitive information and credit card numbers.
- **Using Instagram and Facebook ads to fool you**: According to one study, 40% of all online shopping scams come from Facebook and Instagram ads. These flashy ads often use hacked accounts and stolen photos, but the products either don't arrive or are cheap knockoffs of what was advertised.

*Continued on Page 2*

**Middlebourne Office**
**103 Dodd Street Middlebourne, WV 26149**
**304-758-2191**

**Sistersville Office**
**700 Wells Street Sistersville, WV 26175**
**304-652-3511**

**St. Marys Office**
**401 Second Street St. Mary's, WV 26170**
**304-684-2427**

**Hundred Office**
**3924 Hornet Hwy, Hundred WV 26575**
**304-775-2265**

**Ellenboro Office**
**90 Main Street Ellenboro, WV 26346**
**304-869-3232**

**Harrisville Office**
**1500 E. Main Street Harrisville, WV 26362**
**304-643-2974**

**Pennsboro Office**
**214 Masonic Ave. Pennsboro, WV 26415**
**304-659-2964**

**Marietta-Loan Production**
**Kroger Plaza 19 Acme Street Marietta, OH 45750**
**740-374-0010**
**This is not a full service location. Deposits/withdrawals cannot be processed at this location.**

**New Martinsville Office**
**638 N SR 2 New Martinsville, WV 26155**
**304-455-2967**

- Selling discounted "luxury" goods: Many online shoppers are scammed by looking at deals that are too good to be true. Criminals create ads for steeply discounted luxury items like designer sunglasses or bags. But the items either don't arrive or are counterfeit. Be especially careful when shopping for popular or difficult-to-find items.
- Sending shipping notifications for products that never arrive: The COVID-19 pandemic has caused significant shipping delays for almost all online retailers. One common Covid Scam is when scammers use this to their advantage and send fake shipping "updates" to stop you from reporting their scam.
- Using fake reviews to make you think they're a legitimate site: Most of us believe an online store if they have reviews. But scammers use what's called a brushing scam to create fake reviews on sites like Amazon or eBay.

These online shopping scams can appear in legitimate search results, pop up while you're on social media, or get shared by friends.

### *14 Essential Tips for Shopping Online Safely*

1. **Buy from online retailers you recognize**
2. **Choose stores that use secure websites**
3. **Scrutinize the details of any online store**
4. **Insist on using safe payment services**
5. **Learn the warning signs of a scam email**
6. **Always check shipping costs and terms**
7. **Never store your credit card details with a store**
8. **Create strong, secure passwords**
9. **Monitor your credit and bank statements**
10. **Check to see if your account details were leaked**
11. **Secure your devices with antivirus software**
12. **Watch your back when shopping in public**
13. **Use official shopping apps**
14. **Sign up for identity theft protection**

### *Were You Scammed by an Online Store? Here's What To Do*

Even if you're careful, online shopping scammers are getting better at tricking you. If you've given your financial and personal information to a fake store, here's what to do next:

- **Check your insurance policy.** If you're signed up for identity theft protection, you should have access to a fraud resolution team that can handle many of the next steps for you. Some companies also offer identity theft protection as part of their benefits package.
- **Notify your bank and credit card company.** Contact your bank and any lenders to let them know that your identity has been stolen and to stop fraudulent transactions. They'll close your accounts and help you open new ones.
- **File an official identity theft report with the FTC.** Go to IdentityTheft.gov and file an official report with the FTC. This is an essential step if you need to dispute fraudulent charges.
- **File a police report.** You can also file a police report for identity theft with your local law enforcement agency. This is an optional step. But you should do it if you have any information about the scammer that could help lead to their arrest.
- **Regularly check your credit report and bank statements.** Scammers are almost always after your financial accounts. Check for the warning signs of identity theft — such as strange charges on your bank statement or accounts you don't recognize. An identity theft protection service can monitor your credit and statements for you and alert you to any signs of fraud.
- **Set up a fraud alert on your credit report.** Contact one of the three credit reporting bureaus — Experian, Equifax, or TransUnion — and alert them of the fraud. They'll set up a fraud alert to protect your credit score from the scammers.
- **Change your online passwords.** If one of your accounts has been compromised, you can assume others are too. Update all of your passwords (especially for sites where you've used your credit card).
- **Dispute fraudulent charges and new accounts.** Contact any company where fraud has occurred and let them know what happened. They'll request your FTC report and then cancel any outstanding fraudulent debts.
- **Let others know about the scam.** Online shopping scams only work if no one speaks up. Send a report to the BBB's Scam Tracker and post negative reviews and comments on shopping sites where you were scammed.
- **Consider signing up for identity theft protection.**

### *The Bottom Line: Shop Safely Online All Year Round*

Online shopping scams are rampant during the holiday season. But that's not the only time to be careful. Any time you provide your banking information online is an opportunity for a scammer to strike.

***Source: Aura***

# Be cyber secure: Do's and don'ts for your family

## Advice for helping protect yourself and your family from cyber threats

ODDS ARE YOU WOULDN'T DISCLOSE personal details, like when you're planning to go on vacation and leave your house empty, to a random stranger on the street. But many people happily post that sort of information on their social feeds for anyone to see — and if you aren't divulging your family's schedule (and secrets) online, your teens just might be. Review the following do's and don'ts to help you and your family stay safe in today's super-connected world.

**DO educate your family about cyber risks.**

Children may not understand the risks of the online world. It's up to parents to teach them the dangers of sharing photos and personal information, like vacation routines or daily schedules — information that could be used by others to harm them. Teach them, too, that it's a good practice to avoid downloading apps from obscure or untrustworthy developers and playing games or taking online surveys that ask for personal information.

**DO keep your personal info private.**

Be careful about sharing valuable personal information, such as Social Security numbers, credit card information and birth dates, in a text or email with people you don't know well or trust. If you are shopping online, ensure you are on a reputable site before entering any sensitive information. And use a strong password, passcode or biometric login to protect your accounts online.

**DO consider setting up a VPN.**

A virtual private network (VPN) is a tool that encrypts your communications, from banking to shopping to texting to emailing, when you're connecting to the internet via Wi-Fi. Best of all, it can be used anywhere in the world. Setting one up can be easy and affordable, but it's important to choose a VPN you can trust. Talk with a security expert to determine which is best for you. Be aware, though, that you may have difficulty accessing some financial firms' websites through a VPN because of the anti-fraud protections they've put in place. If you encounter that problem, turn off your VPN and move to a location where you can use a secure, trusted internet connection.

**DON'T leave your home network unprotected.**

Be sure to change the password on your router as soon as you install it. The router is the gateway to your home and touches all of your connected devices, from phones to smart home gadgets. Also, don't forget to configure security and privacy settings on your devices, and invest in reputable antivirus software for your computers. Download software updates on all the programs you use — automatically, if that's an option. Software companies often discover vulnerabilities before cyber criminals do and rush to fix them. The longer you wait to update your software (or operating system), the greater the chance you'll be targeted.

**DON'T drop your guard on public Wi-Fi.**

We're so used to using our devices everywhere (or so concerned about hitting the data cap from our cell phone provider) that most of us don't think twice about logging on to the free public Wi-Fi system at the airport, coffee shop or dentist's office. Some Wi-Fi connections can't be trusted; cyber criminals can infiltrate these systems and collect data that's sent through them. That's why it's always best to take the precaution of connecting to sites through secure connections or a VPN.

**DON'T use easily guessed passwords.**

Despite repeated advice from all corners, some people still use the most basic of passwords for their email, shopping and financial accounts. Or worse, they use the same password for all of their online accounts, making those accounts especially vulnerable to cyber criminals. Variety and randomness are your best bets, so if one password is discovered, your other accounts won't be at risk. Even better, consider using a password manager, which assigns a random password to accounts. That way you only have to remember a single master password — for the manager itself. (You can find password managers in your app store.) For tips on creating your own strong passwords, read "Be cyber secure: Hone your password-writing skills with this quiz."

If you suspect that you or a family member has been targeted by cyber criminals, read "Cyber security checklist: Consider taking these steps if your family's devices have been targeted."

***Source:*** ***Merrill***

***Children may not understand the risks of the online world. It's up to parents to teach them the dangers of sharing photos and personal information.***