Haverford Township
POLICE
DEPARTMENT

Online Safety Tips…..

These scammers can really suck the joy out of shopping. Check out our online shopping safety tips so you can avoid becoming their latest victim.

1. Shop with reputable retailers

It’s best to shop directly with online retailers you know and trust. Bookmark your favorite shopping sites to get there quickly and safely. Avoid typing the name of the retailer into your browser bar.
That’s because a tiny typo could land you on a fake site that looks just like the real one. Make a “purchase” on an illegitimate site and you may unwittingly hand the scammers your credit card number and other personal info.

2. Vet new-to-you businesses

Did you spot an amazing product from a new seller? Do your homework on any business you’ve never purchased from in the past. Look for online reviews and search the Better Business Bureau website for complaints. Check the “contact us” page on the website for a U.S. address and phone number. Then take it a step further: call the business to verify.
Why? The FBI reported that some scammers hijack the contact info of real U.S. businesses to make their shady site look legitimate.

3. Beware amazing deals

Did you spot an ad on Facebook or Instagram offering rock-bottom prices or an eye-popping offer of free stuff? Reports of lost money from social media scams have more than tripled in the past year, according to the U.S. Federal Trade Commission (FTC).
Remember, if an offer looks too good to be true, then it probably is. The FBI found that many sites at the center of its recent spate of complaints were advertised on social media platforms.

Compare prices before you buy. Unusually low prices could be a red flag that you've landed on a fake site that's been set up to snag your personal information or steal your money.

4. Don't browse on public Wi-Fi

Avoid shopping from public Wi-Fi next time you're sipping a latte at your favorite coffee shop. The guy staring at his phone at the next table could be a hacker spying on your online activity. And shopping online often requires giving out information that an ID thief would love to grab, including your name, address and credit card number.

5. Use a VPN

If you ever do use public Wi-Fi, protect yourself with a VPN (virtual private network). A VPN creates an encrypted tunnel between your computer and the server.
Cybercriminals lurking nearby won't be able to see what you're doing or intercept your personal information. A VPN is the only way to shop online safely from public Wi-Fi in airports, cafes and other public spaces.

6. Pick strong passwords

A strong password is like a secure lock that keeps cyberthieves out of the accounts where you store your private information. Here are some quick guidelines on how to choose a good password:

- Use a complex set of lower and uppercase numbers, letters, and symbols. Or consider a long passphrase that you can remember and others are unlikely to guess.
- Avoid dictionary words and personal information a thief could easily find or guess, like your kid's birthdate, your dog's name or your favorite sports team.
- Never reuse passwords across sites. If you do, a data breach at one company could give criminals access to your other accounts.

7. Check site security before you buy

Look for a lock icon in the browser bar of a site to verify that they use SSL (secure sockets layer) encryption. The URL also should start with "https" rather than just "http."
Secure websites are configured to mask the data you share, such as passwords or financial info. Shopping only on secure sites reduces the risk that your private information will be compromised while you shop.

8. Don't fall for email scams

You might get emails or texts offering amazing bargains or claiming there's been a problem with a package delivery. Delete suspicious messages from unfamiliar senders. And don't open attachments or click links in messages because they could infect your computer or phone with viruses and other malware.

9. Guard your personal information

Here’s a general rule: No shopping website should ever ask for your Social Security number. If a site does request this type of very personal information, run in the other direction.
Provide reputable sellers the minimum personal info necessary in order to complete a purchase.

10. Pay with credit, not debit

Always use a credit card to shop as securely as possible. First, a credit card doesn’t give a seller direct access to the money in your bank account. Second, most credit cards offer $0 liability for fraud.
That means you’re not out any money if a crook uses your account info to make a purchase. Your credit card company will ask questions, investigate the fraudulent activity and send you a new card.

11. Add extra security with a virtual credit card

A virtual credit card can offer even more online shopping security. Some credit card issuers will give you a temporary card number that’s linked to your credit card account.
You can use the temporary number to shop online without showing the seller your real credit card details. If a thief gets ahold of the virtual credit card number and later tries to use it, they’ll be out of luck.

12. Keep an eye out for fraud

Check your bank and credit card statements for fraudulent charges at least once a week. Or set up account alerts to notify you of any new activity on your card. When you receive a text or email notification, you can check your account to make sure you recognize the charge.

13. Mind the details

After you make the purchase, keep the details in a safe place. Hang onto the receipt, your order confirmation number and the tracking number the seller provides. If you have a problem with the order, this information will help you get the issue resolved quickly.

14. Track your stuff

After you make an online purchase, keep tabs on it to make sure it’s headed your way. If the merchant refuses to provide shipping info or respond to your requests for the status of your order, contact your credit card issuer for help. They may remove the charge from your bill and look into the matter.

15. Report scammers

Did you get scammed? If so, file a complaint with the U.S. Federal Trade Commission and the FBI’s Internet Crime Complaint Center. Tip: If you suspect you may be a victim of ID theft, the FTC offers an identity theft recovery plan.

But following these online shopping safety tips may help you foil scammers and avoid becoming a target in the first place.