

A Safer Naper

November – Shop Smart

### **Shopping Safety**

Whether you're out shopping for gifts for loved ones or groceries for a holiday meal, don't let your personal safety drop to the end of your to-do list! Here are a few tips to help keep you safe as you accomplish your seasonal shopping tasks:

1. Make sure your car is LOCKED and parked in a well-lit area while you're shopping.
2. Keep your purse closed and maintain a secure hold on it at all times. Never leave it open and/or unattended in a shopping cart!
3. Avoid carrying large amounts of cash or lots of packages.
4. Don't leave packages or other valuables in plain sight in the car while you're shopping. Similarly, don't drop packages off in your car and then head back into the store.
5. Report any suspicious subjects or behavior to store employees or 9-1-1.
6. Become a hard target! Minimize distractions, keep your head up and be aware of your surroundings at all times.

### **Online Shopping Safety**

During the 2018 holiday season, U.S. shoppers spent \$126 billion dollars online (Reuters). Online shopping is continuing to boom as more and more of us utilize this convenient way of shopping from the comfort of our homes or on our smart devices. It is important to remember, however, that while this method of shopping offers convenience, it could also bring with it trouble. In 2017, the FBI's Internet Crime Complaint Center received nearly 300,000 online-theft complaints with victims reporting losses totaling \$1.4 billion. With that in mind, here are some tips for a safer online shopping experience this holiday season:

1. **Use familiar websites.**  
Start at a trusted site rather than shopping with a search engine. Search results can be rigged to lead you astray, especially after the first few pages of links.
2. **Use credit cards and secure payment services instead of debit cards.**  
Credit cards, in comparison to debit cards, offer consumers additional protection when shopping online. There are laws that protect both when it comes to not being liable for any fraudulent charges, but credit cards are the safer option.
3. **Look for the lock.**  
Never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed. A SSL site can be identified because the URL for the site will start with HTTPS:// (instead of just HTTP://). Look for the locked padlock next to the URL.
4. **Don't share everything.**  
No online shopping store needs your social security number or your birthday to do business. However, if crooks get them, combined with your credit card number for purchases, they can do a lot of damage. The more they know, the easier it is to steal your identity. Scroll down for more information on identity theft.
5. **Opt for your mobile phone network over public Wi-Fi.**

Public Wi-Fi is convenient. However, when it comes to buying online, all the convenience that comes with public Wi-Fi can be overshadowed by the many risks. Don't log onto a public Wi-Fi to complete shopping transactions, banking or email.

6. **Check statements.**

Don't wait for your bill to come at the end of the month. Go online regularly during the holiday season and look at electronic statements to make sure you don't see any fraudulent charges.

7. **Protect your PC.**

Make sure your computer has the latest antivirus software. You need to protect against malware and other viruses with regular updates.

8. **Use strong passwords.**

We have all heard this before, but it is so important. Your password should be different on all your accounts (or at least different for business and personal accounts) and you should use a string of text that mixes numbers, special characters and both uppercase and lowercase letters.

9. **Think mobile.**

There's no real need to be any more nervous about shopping on an app than on the internet, but it is important to use apps provided directly by the retailers. Use the apps to find what you want and then make the purchase directly, without going to the store's website.

10. **Use a VPN.**

If you must shop online on public Wi-Fi, consider installing and using a VPN — short for “virtual private network” — on all mobile devices and computers before connecting to any Wi-Fi network. A VPN creates an encrypted connection between your smartphones and computers and the VPN server. VPNs use encryption to scramble data when it's sent over a Wi-Fi network. This makes the data unreadable. Data security is especially important when using a public Wi-Fi network because it prevents anyone else on the network from eavesdropping on your internet activity.

## **Internet Transaction Exchanges**

It is now commonplace for people to originate transactions to buy and sell property through the internet, which means the buyer and seller don't know each other when meeting to exchange items. That makes personal safety a critical factor in the transaction.

For years, the Naperville Police Department has encouraged the public to utilize our front lobby at 1350 Aurora Avenue as a safe location to meet and complete transactions that began online. It open and staffed from 7 a.m. until 8 p.m. on weekdays and from 10 a.m. to 6 p.m. on Saturdays, excluding holidays. As part of this month's A Safer Naper campaign, the Naperville Police Department is excited to expand our e-commerce safe transaction area to allow residents to safely complete these transactions even when our lobby is not open.

We now have dedicated “Internet Purchase Exchange Location” parking spaces directly in front of the department that have coverage by hi-definition cameras and safety features that we hope will deter criminals from taking advantage of people wanting to sell goods online. The area is well-lit, video recorded and has access to an emergency telephone. When the lobby is closed or if the item is too large, the public is encouraged to use these new dedicated parking spots.

Remember, if the other party doesn't agree to meet here, they're probably not someone you want to do business with.

Here are a few other safety precautions when conducting transactions:

1. Insist on a public meeting place; do not meet in a secluded location or a parking lot of a store. Meet in places that have lots of foot traffic and security cameras, preferably Naperville Police Department!
2. Avoid meeting at night, but, if you must, choose a location that is well lit and has a high volume of pedestrian or vehicular traffic.
3. Do not invite strangers to your home. Again, a public place is preferred, but if the item is too large to be transported, try to the garage or other area not accessible to the rest of the home. Have someone with you when the person comes over to look at the item.
4. Be especially careful when buying/selling high value items.
5. Tell a friend where you are going or have a friend accompany you.
6. Take your cell phone. Know your exact location if you need to call 9-1-1.
7. If a dispute arises during the buying or selling of goods or services, remember to exercise your right to terminate the transaction.
8. Trust your instincts. If someone is making you feel uncomfortable or the situation doesn't seem right, leave!!

### **Watch Out for Identity Theft**

To better prevent identity theft, know the warning signs that signal fraud is developing—or is happening already:

- 1. You no longer get your household bills in the mail.**  
An absence of bills in the mail could mean your personal data has been compromised, and the identity thief has changed your billing address.
- 2. You are turned down for a loan or credit.**  
If you're rejected for credit, but have a history of good credit health, you might have been targeted by an identity thief. If you're approved for a loan or credit, but at higher interest rates, that's also a sign you may have been victimized by identity theft.
- 3. You are being billed for purchases you didn't make.**  
Invoices for purchases you don't recognize, or if you're being billed for overdue payments for credit accounts you don't own, that's a sign you've been victimized by I.D. fraud.
- 4. Your financial accounts have transactions that appear fraudulent.**  
If your bank, credit card or other financial account show unauthorized transactions, those accounts may have been breached.
- 5. Your tax return is rejected.**  
If you filed your tax returns and received a rejection notice from the Internal Revenue Service, that could indicate a return has been fraudulently filed in your name
- 6. Test charges appear on your credit card statement.**  
It's common practice for identity thieves to "test" that a stolen card is still active by making low-cost purchases of under \$5.00. If the credit card is approved, the fraudster knows that the path is clear for larger transactions.

(Source: [www.experian.com](http://www.experian.com))

## Report Identity Theft

If you are a victim of identity theft, report it to your local police department. We will take a report and provide you with important information on reporting to the Federal Trade Commission (FTC). [IdentityTheft.gov](http://IdentityTheft.gov) is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

(Source: [www.usa.gov/identity-theft](http://www.usa.gov/identity-theft))

## Online Identity Theft Resources

- Sign up for [FTC Consumer Alerts](#)
- Check out the latest scam information from the [Better Business Bureau](#)
- Report identify theft and get help with a recovery plan at the Federal Trade Commission's [IdentityTheft.gov](http://IdentityTheft.gov) site.
- Learn more about identity theft from the [FTC](#) or [TransUnion](#), [Equifax](#) and [Experian](#).