HOLIDAY SHOPPING—ONLINE SAFETY STILL IMPORTANT

While many people have protected themselves and others around them from COVID-19 by receiving a COVID vaccine, the effects of the pandemic still remain with us. Supplies of many products, including Christmas gifts, are spotty as we enter the holiday season. With ships backed up at ports, it may be hard to find the perfect gift, and if you do find it, you might pay a higher than normal price.

Unscrupulous people can take advantage of this situation with fake websites that look genuine and social media campaigns that try to get customers. Many will just take your money but not deliver what you ordered, or deliver a cheap knockoff. And when you call or email to complain, you find the website has been taken down and the phone number or email address no longer work.

Others will use your transaction to harvest your personal information such as credit card numbers. Or they may insert malware into your computer to harvest personal information from your hard drive.

Some warning signs to look out for when you are shopping online include,

- Huge discounts for hot gift items.
- Spelling errors or bad grammar on websites or emails.
- A shopping or travel site that does not list a street address or phone number.
- A site that does not have a privacy policy.
- An unsolicited email that asks you to click on a link or download an app to access a deal or arrange for delivery.
HOLIDAY SCAMS - STAYING SAFE ONLINE

With the holidays, scammers ramp up their efforts, not only to target online shoppers, but with other schemes to take your money and your personal information. Other scams can include,

- **Charity scams** – Americans do one-third of their charitable giving in December. Scammers will set up fake websites to look like legitimate charities or impersonate real charities with pushy telemarketing campaigns.

- **Compromised Account scams** – Scammers send out emails or texts, impersonating your bank claiming there is suspicious activity on your account. They will urge you to click a link. The email/text will have links that lead to phony sign-in pages to collect personal information or insert malware.

- **Travel scams** – Many more Americans will be traveling during this holiday. Scammers will have spoofed booking sites or email offers with travel deals that are too good to be true.

HOLIDAY SHOPPING – PROTECTING YOURSELF ONLINE

With the growth of online shopping, consumers have the convenience of ordering goods and having them delivered to their homes.

While shoppers can take advantage of the convenience of online shopping, there are pitfalls. Fraudsters can set up a fake web site, take your money, and your personal information, and not deliver what you ordered. Others can use phishing tactics to fool you into giving your personal information.

You can take practical actions to protect yourself.

**Be sure you are secure.** Make sure that you are updating your computer or mobile device for its antivirus software. Use good password discipline, long passwords, and no two accounts using the same password. A password manager can help. Also, where you can, use two-factor authentication.

**Checkout online vendors before doing business.** While not perfect, most larger vendors will have robust security measures to prevent hacking into their computer systems. An old rule of thumb is to look for the “https://” to be sure that you have a secure link. While still good advice, fraudsters are now making their websites secure.

Verify that you are ordering from a legitimate vendor. Do a search on the business name with the word “scam” and see what comes up. Be wary of brand new web sites, they are more likely to be scammer sites.

When paying, use a credit card. Don’t use a debit card! Also, dedicate a credit card to your online transactions. This would make it easier to regularly check out your statement for unusual transactions. Also, using a mobile payment service like Apple Pay or Google Pay, helps protect your credit card if the mobile payment information is stolen.

**Don’t take the phishing bait.** Scammers will send phishing emails to trick people into giving their personal information. And the Christmas shopping season is the perfect time to trick frazzled online shoppers.

Phishing scammers have used COVID-19 as a lure to convince victims to click on links to bad web sites or download files with malware. During the holidays, scammers will send out phishing emails claiming to be from the Postal Service, FEDEX, or UPS that says there is a problem with a package. Be wary of unsolicited emails, especially if they warn of dire consequences for not acting.

Do not click on any links from suspicious emails. If you need to, go directly to the service’s web site to conduct your business.
HOLIDAY SHOPPING— PROTECTING YOUR DELIVERIES

After you have made your online order, you need to receive your purchase. Package delivery remains fraught with thieves (porch pirates) trolling neighborhoods to find packages on front porches to take.

Some things you can do to reduce the chances of your package being stolen include,

Have the package delivered to another location. This can be to a UPS Store, FEDEX Store, your local Post Office, or an Amazon Locker. You can also have it delivered to a trusted neighbor who you know can retrieve the package promptly.

Going to be out of town? Have the package held until you return. The Postal Service has its “hold mail” service that will hold your mail for a minimum of 3 days and a maximum of 30 days. You can have a vacation hold with FEDEX for up to 14 days.

Use the delivery service’s tracking features. Tracking your package allows you to know when you can expect it on your porch. UPS, for example, has a service called UPS My Choice that allows you to track a package and re-route it if needed.

Request a signature. You can ask for a signature on delivery. If you are not at home to receive the package, it will not be left on the porch.

Give special instructions. If you are having the package delivered at home, you can give instructions to have it left somewhere out of sight of the street. This could be on the side of the house, on the back porch, or some other easy hiding place.

Consider installing a security camera. A security camera on your front porch can help you know who is at your front door. Some cameras will send you a text or email when they see motion in their field of view. Also, a camera that records images or video allows you to provide evidence to law enforcement in case your package is stolen.

Pick up promptly. If you are having the package delivered to your home, try to pick up from your porch as soon after it is delivered as you can. If you are away for the day, have a trusted neighbor pick it up for you.


USPS: https://uspsblog.com/postal-inspection-service-tips/
PRESENTS UNDER THE TREE—PROTECT THEM FROM BURGLARS

You have safely selected and purchased your gifts. Now they are in your home ready to wrap and sit under your tree. This is a time of year when burglars steal Christmas gifts from homes. You can improve the security of your gifts through the following steps:

- Always secure and lock your doors and windows, even if you are just popping out or when you are in the back garden - about one in four burglaries happen simply because the household left windows or doors unlocked.
- Make sure your security lights are in working order and put internal lamps on timer switches to come on when dark if you are away.
- If you have a security system, use it.
- Don’t hide your house keys near a door. Burglars know all of the secret hiding places.
- Don’t leave Christmas presents under the tree in full view of burglars who may be peering through windows - keep them in a secure place until the big day.
- Don’t put your empty boxes from Christmas presents (or any new purchases) out until your recycling collection day and make sure you break up the boxes and secure them together - the boxes and wrappings provide burglars with just the information they are looking for to see what new gadgets and items await them inside.
- Note down the serial numbers of all electronic goods such as TVs, videos, computers, and camera equipment and keep the list out of sight in a secure place. Also photograph valuable items such as jewelry.

AUTO THEFT PREVENTION CHECKLIST

- All vehicle doors locked
- All windows rolled up
- All personal belongings have been removed or stored in the trunk
- Vehicle is parked in a well-lighted area
- Vehicle is parked in a high-visibility location (avoid isolated areas)
- Anti-theft device on (Club, alarm system, kill-switch)