

NAPLES COMPUTERS HOW-TO • SECURITY & SAFETY

How to Shop Safely Online This Holiday Season

Holiday shopping online is easy, and scammers know it. This guide shows how to check a website's address (and what the lock really means), spot fake stores and too-good-to-be-true deals in social media ads, pay the safe way, protect your shopping accounts, ignore fake delivery-problem texts, skip public Wi-Fi when you shop, and check your statements.

Step by step

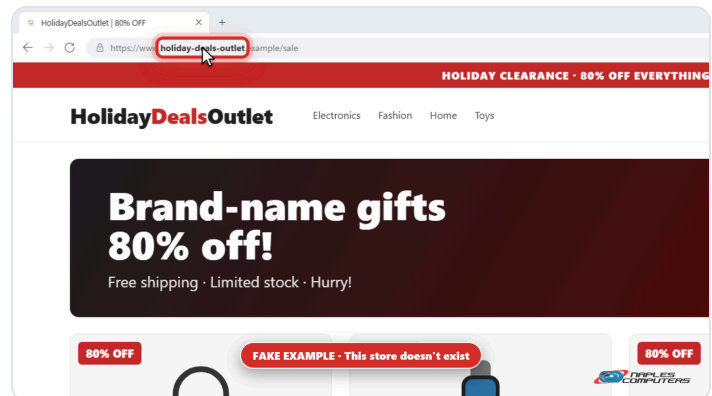
Step 1: Check the website

1 address, and know what the lock means

Fake stores use names and addresses that look almost right. Read the address bar: is this really the store you meant to visit?

WHAT TO DO

The lock only means the connection is private. It doesn't mean the store is honest. Type the store's address yourself, or use its app.



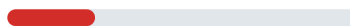
4 Strong passwords and two-factor sign-in

Give every shopping account its own strong password, and let a password manager remember them. Turn on two-factor sign-in, so a stolen password isn't enough.

WHAT TO DO

Use the store's app or a saved bookmark, instead of links in emails and texts.

patjones58



Weak

Pat . Jones . 1958



OK

Pelican-Sunset-Canoe-47



Strong

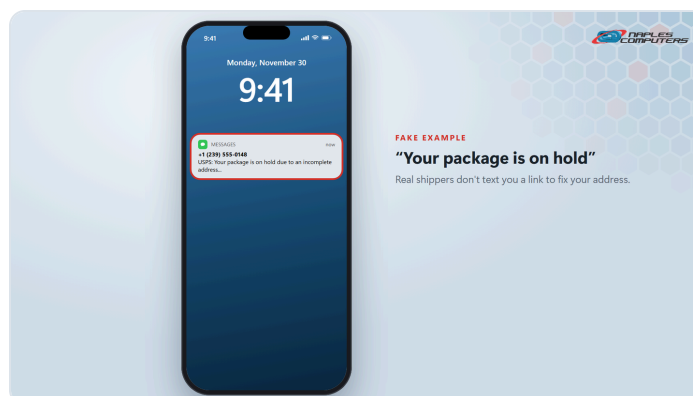
One **strong**, **unique** password per account

5 Step 5: Ignore "delivery problem" texts

Fake texts pretending to be USPS, UPS, FedEx or Amazon say your package is on hold and ask you to tap a link.

WHAT TO DO

Don't tap the link. On iPhone, tap Report Junk, then Delete and Report Junk. On any phone, you can forward it to 7726. Check a delivery in the shipper's own app or website.

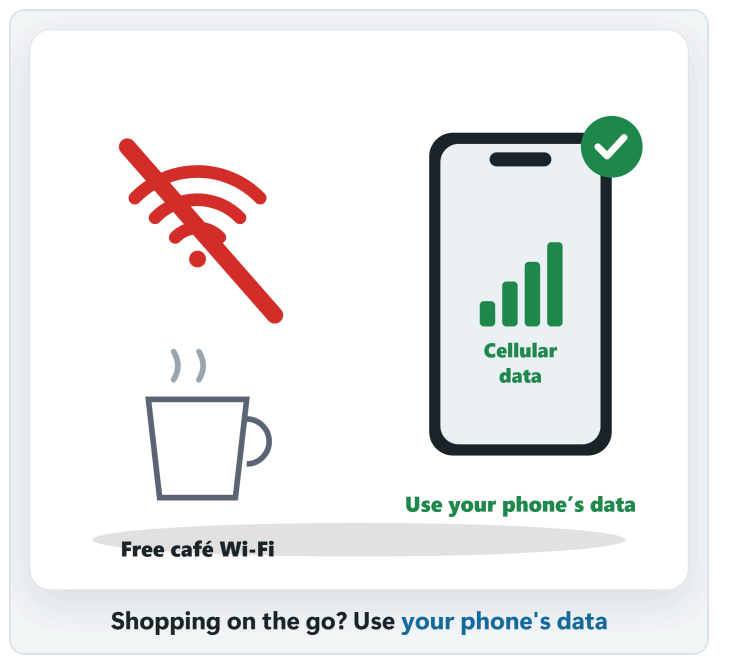


6 Skip public Wi-Fi when you shop

Free Wi-Fi at a café, airport or hotel is shared with strangers. Wait until you're home, or use your phone's cellular data.

WHAT TO DO

Never type card numbers or passwords on a network you don't control.



Step 2: spot fake stores and too-good deals

- ☐ Ads on social media
Fake stores buy ads that look just like real ones
- ☐ Discounts that are too good to be true
Brand names at a fraction of the usual cost
- ☐ Countdown timers and "only 2 left!"
Pressure to buy before you think
- ☐ Look them up first
Search the store's name with "scam", "complaint" or "reviews"

Step 3: pay the safe way

- ☐ A credit card
The FTC says it best protects you if something goes wrong
- ☐ PayPal or a trusted checkout
Linked to your credit card
- ☐ Gift cards
A store that only takes gift cards is a scam

- ☐ Wire transfers, Zelle or crypto
Once it's sent, it's very hard to get back

Step 7: check your statements

- ☐ Look at your card activity every week
Through the holidays, in your bank's app
- ☐ Turn on purchase alerts
A text or app alert for every charge
- ☐ Don't recognize a charge?
Call the number on the back of your card right away

Think you've been scammed?

- ☐ Call your card company or bank right away
Ask them to stop or dispute the payment
- ☐ Change your passwords
Start with the account you used, and your email
- ☐ Report it at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov)
It helps stop the scammers
- ☐ Clicked a link or installed something?
Have your computer checked: call us at 239-513-1960

Recap: shop safely online

- | | |
|---|--|
| ☐ Check the website address | ☐ Strong passwords + two-factor |
| ☐ Too good to be true? It is | ☐ Don't tap delivery-text links |
| ☐ Pay by credit card or PayPal | ☐ No shopping on public Wi-Fi |

Real shippers and stores don't text you a link to fix your address or pay a fee. Go to the store or shipper yourself, with its app or a bookmark. And remember: Naples Computers will never call you out of the blue asking to get on your computer.



Clicked a link or worried about a purchase? We can help.

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**