QUICK-GUIDE FOR PARENTS & TEENS

Safe Online Shopping

Don't be a sucker.

If it sounds too good to be true, it's too good to be true. If the price is MUCH lower than other advertised prices, it could be a scam or the item could be used, refurbished, or incomplete, which might be OK, but make sure you know what you're getting.

Happy returns.

Be sure you understand the return policy, including deadlines and whether you will have to pay return shipping, which can be expensive with large and heavy items. Also, check for "restocking" charges for returns. Make sure you know the full cost of the item including shipping and other charges. Consider shopping at an online store that has a physical location nearby that lets you return items for free.

> **You asked:**
> **How can I protect my personal info?**
> --------
>
> Never give out your social security number, Medicare number or any other identification unless you're sure it's necessary, such as applying for credit. Online merchants will need your name, email, billing address and a form of payment and only in rare cases (such as when purchasing alcohol, medical care or in compliance with child privacy laws) do they need your date of birth.

Know where you're shopping.

Only shop at reputable online merchants. When in doubt, ask around or research them online. Read reviews (not just those posted on their site) and look for any articles about the merchant with the word "scam." Almost all merchants will have a few bad reviews, so look at several to get an overall impression. Be especially careful before shopping at unknown merchants who solicit you via email.

Pay safely.

Never send cash or wire money. Use credit cards if possible, otherwise debit cards, or known payment services such as Paypal, Google Pay or Apple Pay. Credit and debit cards have fraud protection, which can vary depending on the type of card.

Shop securely.

When shopping or banking look for secure sites where the web address starts with HTTPS. The "s" stands for "secure." Also, make sure you're on the site of the merchant you meant to visit and not an imposter that may have shown up in a search. Also, use a unique password for each site so that thieves can't use the password elsewhere if the merchant you're visiting is compromised.

More Advice

Don't fall for phishing attacks.
Be very careful before clicking on a link (even if it appears to be from a legitimate site) asking you to log in, change your password or provide any other personal information. It might be legit or it might be a "phishing" scam where the information you enter goes to a hacker. When in doubt, log on manually by typing what you know to be the site's URL into your browser window.

Avoid shopping & banking on public Wi-Fi.
There are risks associated with shopping and banking when connected to public Wi-Fi such as at a coffee shop or airport because there is a chance that the network could be stealing your log-in and credit card information. If you do, make sure it's the official network and not a rogue network with a similar name (when in doubt ask an employee). The safest way to shop in public is to use your smartphone's cellular connection by either shopping from your phone or "tethering" your phone to your computer or tablet.

You can't win a contest you didn't enter.
Don't respond to messages claiming you've won money or goods unless it's a contest that you actually entered. There are many contest scams that typically require you to make a "small" payment or provide personal information. They're almost always scams. Never send money such as to "register" a car you've "won," or fees or taxes on "prize money."

Donate wisely.
Do some research before donating online to make sure the charity is legitimate and that the money is going to the right place. You can learn about most charities at CharityNavigator.org.

Don't respond to messages claiming you've won money or goods unless it's a contest that you actually entered.

For more info on secure passwords, visit ConnectSafely.org/passwords

GO

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.