U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Online Shopping

Online shopping is convenient, easy, and quick. But it's wise to make sure you're protected before you start adding items to your cart.

WHAT ARE SOME THINGS I CAN DO TO PROTECT MYSELF WHEN SHOPPING ONLINE?

- Make sure security software, web browsers, and operating system are up-to-date. Keeping a clean machine is the best defense against viruses, malware, and other online threats.
- Antivirus software is good, but it usually attacks malware after the fact. Better protection is provided by tools such as traffic scanners that filter incoming and outgoing data and scan sites and block any that contain embedded malware.
- Check out sellers. Conduct independent research before you buy from a seller you have never done business with. Some malicious sites appear legitimate, so you should verify the site before supplying any information. Search for merchant reviews.
- Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill.
- Before you enter personal and financial information, look for signs that a site is secure. These include a closed padlock or tune icon on your web browser's address bar or an address that begins with shttp or https. This indicates that the purchase is encrypted or secured. You can also use a browser extension such as HTTPS Everywhere that encrypt your info for added security.
- Watch for signs of fake sites: strange URLs, odd brand selections (like a site that sells toys and lumber), odd product descriptions and bad grammar, suspicious contact information, extremely low prices, and poor site design. But even legitimate sites can be victims of malicious code that scans your computer for vulnerabilities (often caused by outdated apps) and installs malware.
- Never use an unsecured wireless network to make purchases. Beware of wifi connections that are open and don't have a password, that use simple encryption languages such as WPE/WPA that can be easily broken (even the better WPA2 AES can be broken by a dedicated hacker), or in places where the router is in an exposed location where it can be tampered with.
- Protect your personal data: When making a purchase online, be alert to the kinds of information being collected for the transaction. Make sure you think it's necessary for the vendor to request that information. Things such as birth date, Social Security number, or other items may not be needed for an online purchase. You only need to fill out required fields on a checkout form.
- Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.
- Use safe payment options. Credit cards are generally safest because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Unlike debit cards, credit cards may have a limit on the amount you will be responsible for paying if your data is stolen and used by someone else. When possible, use payment methods that employ two-factor authentication. Keep confirmation numbers and emails for all online purchases.

- Never send cash through the mail or use a money-wiring service because you'll have no recourse if something goes wrong.
- Review the vendor's return policies. You want a no-hassle ability to return items.
- Print and save records of your online transactions, including product description, price, online receipt, terms of sale, and copies of any email exchanges with the seller.
- Read credit card statements as soon as you get them to make sure there aren't any unauthorized charges. If there is a discrepancy, call your bank and report it immediately.
- Turn your computer off when you're done shopping. Leaving your computer running and connected to the Internet can give scammers access to install malware and commit crimes.
- Be wary of emails requesting information. Attackers may attempt to gather data by sending emails asking you to confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Contact the merchant directly if you are alerted to a problem using contact information found on your account statement, not in the email.
- Mobile apps are generally more secure than websites. Many vendors have dedicated apps that require dedicated attacks to hack, while sites can be hacked by general browser attacks.