Attention, Online Shoppers! Don't be scammed!

Every year, thousands of people fall victim to holiday scams. The Allegheny County Police Department encourages shoppers to be aware of holiday scams and malicious cyber campaigns, particularly when browsing or shopping online.

The holiday season makes the public an attractive target for bad actors, as online purchases reach the highest levels of the year. The holidays are frequently used to push scams through online ads, misleading phone calls, phishing emails, and text messages. These messages are often carefully crafted to look legitimate. Phishing scams could easily blend in with regular holiday offer emails, orders or shipping notices, and bank account updates. Bad actors take advantage of the abundance of holiday emails, hoping users do not notice the phishing email.

Online shopping scams occur when bad actors offer too-good-to-be true deals via phishing emails or advertisements. They may offer brand name items at an extremely low price or offer gift card incentives. These items may not ship after payment or may not even be the true brand name item expected.

Social media shopping scams occur when bad actors post vouchers or gift cards on social media. These posts may appear as holiday promotions, quizzes or contests. Others may appear to be from known friends who have shared the link. Sometimes these scams lead victims to an online survey designed to steal personal information.

Gift card scams occur when bad actors ask victims to purchase gift cards for them. In this scam, victims receive either a spoofed email, phone call, or text from a person in authority requesting the victim to purchase multiple gift cards for either personal or business reasons.

Charity scams occur when bad actors set up false charities and profit from individuals who believe they are making donations to legitimate charitable organizations. Charity fraud rises during the holiday season, when individuals seek to make end-of-the year tax deductible gifts or are reminded of those less fortunate and wish to contribute to a good cause. Charity scam solicitations may come through phone calls, emails, crowdfunding platforms, or fake social media accounts and websites. They are designed to make it easy for victims to donate money.

Protect Yourself!

The best defense against holiday season scams is awareness. There are a few simple steps to take to be more secure while online. Pay attention to red flags in emails, phone calls, or text messages. Some red flags are asking for personal information, creating a sense of urgency, and utilizing attachments.

- Verify a charity's authenticity before making donations. Make sure the organization has a verified Taxpayer Identification Number. Review the Federal Trade Commission's page on Charity Scams for more information.
- Avoid clicking any suspicious links or unsolicited attachments in emails, on websites, or on social media.
- Be especially wary if a company asks you to update your password or account information through email, text messages, or phone calls. Look up the company's phone number on your own and call the company.
- Before making a purchase and providing any personal or financial information, make sure you're using a reputable, established vendor. Make sure the website uses "https" in the URL.
- Never use a debit card for purchases, use a credit card. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) recommends that shoppers choose a credit card over debit for their purchases. There are laws that limit an individual's liability for fraudulent credit card charges, but debit cards may not have the same level of protection. Additionally, because a debit card draws money directly from a bank account, unauthorized charges could leave the victim without funds to pay bills or other necessities. It's also a good idea to use a credit card for payment gateways, such as Apple Pay, PayPal, and Google Wallet. Never wire money to a seller. Never use pre-paid gift cards to send as a payment before receiving items.
- Check your online banking statements frequently for fraudulent charges to credit cards, debit cards, and checking accounts. **Keep** a record of your purchases and copies of confirmation pages and compare them to your bank statements. If there is a discrepancy, report it immediately.
- Install and update antivirus software on all your devices. Install firewall, anti-virus, and anti-spyware software on your computer, tablet, and smartphone. Check for and install the latest updates and run virus scans regularly.

If you become a victim of a scam ...

-Call your credit card company or your bank. Dispute any suspicious charges.

-Contact local law enforcement.

-Report the scam immediately at www.ic3.gov.

P.O. Joe Risher, Crime Prevention/Community Relations Officer
Allegheny County Police Department
875 Greentree Road, Ten Parkway Center, Pittsburgh, PA 15220