U.S. DEPARTMENT OF TREASURY
The Office of Cybersecurity and Critical Infrastructure Protection

Securing the Season:
Preventing Holiday Cybercrime and Fraud

STAY ALERT

This holiday season keep yourself safe from scams and fraud.

Be Educated and Skeptical: Awareness is a key defense against scammers.

Cyber-crime is a multi-billion dollar industry industry that doesn't take time off.

If you are uncomfortable or feel pressured to send or spend money, STOP!

Take time to research or ask for help. Don't feel pressured into making a transaction.

HOW TO AVOID COMMON HOLIDAY SCAMS

1. Buy only from reputable merchants.
2. Stay informed of common scamming tactics, share your knowledge with others, and remain skeptical of unsolicited calls, emails, and texts, especially those creating a sense of urgency.
3. Exercise caution when receiving unexpected phone calls and emails from your financial institutions, unsolicited texts, and embedded links. Confirm the legitimacy of requests by directly contacting the requesting entity through official channels.
4. Practice safe online behavior. Be cautious about the information you share online. Avoid oversharing personal details on social media platforms.
5. Don't be pressured to purchase an item or pay for a service quickly. Take time to think, research, and talk to someone trusted. Fraud and phishing scams often capitalize on creating a sense of scarcity or fear of missing out. Legitimate businesses will give you time to decide.
6. Regularly monitor your financial and card credit statements for unauthorized or suspicious transactions. Report any discrepancies to the credit card or financial institution immediately.
7. If an online deal looks too good to be true, it likely is. Be suspicious. Scammers often offer products at significantly reduced prices. If a luxury item or an electronic device is offered at an extreme discount, it's likely counterfeit or will never be delivered.
8. Don't give out personal or account information to anyone who calls.
9. Don't rely on caller ID. Criminals can fake their identities and locations on phone calls.
10. Never pay someone who insists you pay via a gift card or using a money transfer service. Also, never deposit a check and then send money back to someone.
11. Use a credit card to pay for online purchases. As required by law, credit card companies provide a fraud liability guarantee which limits liability for unauthorized charges to $50 ($0 if the card was stolen and the card company is notified prior to purchases being made).
12. Enable Two-Factor Authentication (2FA). Strengthen the security of your accounts with 2FA, making it harder for attackers to gain access.
13. Never allow permissions to an unknown app and use different passwords for each downloaded app.
14. When using money transfer services, be certain to validate who you're sending money to and their contact details.

CRIMINALS MAY TARGET YOU IN MULTIPLE WAYS:

Gift Scams – Popular, sold-out items (for example, a toy unavailable in local stores and online) suddenly appear in ads. If an item is sold-out in box stores and reputable online stores you frequent, then the websites with availability are likely scams meant to steal your money, your personal information, or your credit card.

Vishing, Phishing, and Smishing Campaigns – Scammers use fraudulent phone calls, emails, websites, or texts to trick you into revealing private information, clicking links, or opening attachments. A trusted entity is often impersonated, like a bank or government agency. Watch out for unexpected phone calls and emails from your financial institutions, unsolicited texts, and embedded links. Don't click on any links in email, text, or advertisements!

Purchase Fraud – Online shopping provides criminals an opportunity to trick you into paying for goods or services that either don't exist or whose quality is sub-standard to what was advertised.

Holiday Employment Scams – In online ads, scammers may pretend to be employers from recognized companies. In the posted help-wanted ad, you're instructed to follow links to submit an application. The personal information you provide can be used for identity theft.

Credit Card Scams – Unrecognized charges appear on your monthly statement. In a quest to steal with credit cards, thieves may employ:

- Application Fraud – Thieves steal mail, dig through trash or skim cards to gather personal details so they can apply for a credit card in your name.
- Counterfeit Cards – Your data is stolen from fake card readers at a gas station or ATM. With the stolen data, thieves can create a duplicate card for illegal use.
- Card Not Present (CNP) Fraud – Credit card numbers are stolen through hacking or phishing and thieves then buy items online, by phone or through the mail.
- Account Takeover – Pretending to be you, a fraudster can get a new credit card issued to them and sent to their address.

Social Media Scams – While on social media, beautifully crafted items repeatedly appear in your feed. After seeing the item appear for days or possibly weeks, you order the item. When the item arrives it doesn't resemble what you ordered, or it doesn't arrive at all.

Charity Scams – The holiday season is when many people give to their favorite charities and scammers are targeting the season's generosity by creating fraudulent charities. Only donate to reputable and trusted charities with a history of charitable distribution.

Fake Mobile Apps – Downloaded apps have been found to record your screen when banking or deposit malicious trojan software. Once installed, these apps ask for extensive permissions – just say no.

Phishing Campaigns – Scammers use fraudulent websites, emails, and texts to trick you into clicking links and opening attachments to load malicious software. Don't click on any links in email, text or advertisements!

Romance Scams – The holidays are when many look for a partner and are also a time when romance scammers heighten their activity. According to the Federal Trade Commission, as many as 25 to 30 percent of dating site members registering each day are doing so to perpetrate scams. Don't feel pressure to send money to someone on a dating website.

WHAT TO DO IF YOU GET SCAMMED

Regardless of the type or severity of the crime, it's important to take action as soon as you realize you've been scammed.

- Contact the merchant. The merchant may have a money-back guarantee in the event of a scam or fraud. The merchant may also be able to take action to freeze the scammer's account to prevent further fraud. Do not attempt to contact the scammer directly.
- Alert your credit card company. The first thing to do if you detect illegal activity is contact your credit card issuer. Contact them via the toll-free number on the card. For a lost or stolen card, visit the company's website for the phone number. Immediately change any login information and PINs connected to the card.
- Notify the credit bureaus. Place a fraud alert on your credit record with one of the three main credit bureaus (Equifax, Experian, or TransUnion). Fraud alerts instruct lenders to contact you directly to verify your identity before extending new credit in your name.
- Consider freezing your credit report. If you have reason to believe your personal information has been compromised, you can elect to "freeze" your credit report. When your credit report is frozen, financial institutions and other lenders won't issue loans or extend lines of credit because they can't review your credit history. This makes it more difficult for identity thieves to make purchases or open new accounts in your name. You can "unfreeze" your credit report at your discretion, such as when you need to acquire a loan. To freeze your credit report, call the main credit bureaus directly or online at:
  - Equifax: 888-298-0045 or **https://www.equifax.com/personal/credit-report-services/credit-freeze/**
  - Experian: 888-397-3742 or **https://www.experian.com/freeze/center.html**
  - TransUnion: 888-909-8872 or **https://www.transunion.com/credit-freeze**
- File a complaint the FBI's Internet Crime Complaint Center (IC3) Internet Crime Complaint Center (IC3) | Home Page. You may file a complaint with IC3 if you believe you or another person may have been the victim of an internet crime.
- File a report with the Federal Trade Commission (FTC). You may report scams at **ReportFraud@ftc.gov**. Filing a report with the FTC won't resolve your individual case. However, the information you provide will be used to investigate and bring cases against those who engage in fraud, scams, and those who engage in disreputable business practices.