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

Seasonal Security
Protecting Yourself from Holiday Scams and Fraud

STAY ALERT

Recent Scams to Watch For:
Cybercriminals are targeting consumers through popular social media platforms like LinkedIn, TikTok, and Instagram, as well as via wrong number texts. Always approach unsolicited messages with caution.

Spot Dangerous Email Words:
ZeroBounce, an email validation platform, analyzed spam data and identified the most dangerous scam-related words that cybercriminals use to lure victims. The following words were found linked to the highest rates of click-through in scam emails:

Top 5 Dangerous Words:
1. Income | 2. Investment
3. Credit | 4. Billion | 5. Free

Why it matters: Scammers use these high-impact words to increase chances of you clicking a responsive link. If you receive unsolicited emails containing these words, approach them with caution. Scammers often use these terms to lure unsuspecting victims into sharing personal information or clicking on malicious links. Take time to research or ask for help. Don't feel pressured into making a transaction.

CYBERCRIMES CONTINUE TO RISE

In 2023, cybercrime contributed to losses exceeding $12.5 billion, marking a 22% increase from 2022. With the holiday season here, cybercriminals are using multiple platforms to conduct fraudulent activities, targeting consumers during holiday shopping events. Stay ahead of the criminals by familiarizing yourself with common scams and practicing safe online behaviors. If you'd like to learn more about scams and test your knowledge with a scams quiz, go to ***banksneveraskthat.com***.

1. **Beware of Urgent Account Notifications.** If you receive a call or message about a potential account problem or compromise, do not respond immediately. Hang up and call the organization directly using a number from the app, the bookmarked official website, or the number found on the back of your card.
2. **Secure Your Devices and Accounts.** Use strong passwords, enable two-factor authentication (2FA), and keep software updated. A VPN (Virtual Private Network) can also provide an extra layer of security when shopping or browsing online.
3. **Exercise Caution and Do Not Respond to Unsolicited Requests, Unsolicited Phone Calls, or Emails from your Financial Institutions or Anyone Requesting Personal or Financial Information**. Even if the message seems official, verify the source and confirm the legitimacy of requests by directly contacting the requesting entity through official channels.
4. **Verify Websites and Emails:** Always navigate to the official website directly—do not click on links from emails or messages.
5. **Initiate Contact Yourself**. Always take the initiative to contact businesses or institutions yourself. Never rely on unsolicited links or phone numbers.
6. **Avoid Clicking Links or Responding to Unsolicited Requests.** If someone contacts you urgently and asks you to click on a link or call a number, do not engage. Hang up and contact the organization directly using an official phone number or website.
7. **Don't Trust Caller ID.** Scammers can spoof phone numbers, impersonate legitimate institutions, fake identities and locations on calls. Always verify any call by hanging up and calling back using a number from the official website.
8. **Never Share Sensitive Information.** Do not share sensitive information like account log-ins, passwords, or social security numbers over the phone or online unless you initiated the call.
9. **Practice Safe Online Behavior.** Be cautious about the information you share online. Avoid oversharing personal details on social media platforms.
10. **Buy Only from Reputable Merchants.** Don't give out personal or account information to anyone who calls.

HOW TO AVOID COMMON HOLIDAY SCAMS

1. **Enable Two-Factor Authentication (2FA)**
   Strengthen your account security by using 2FA, making it harder for attackers to gain access to your accounts.
2. **Shop Smart – Buy Only From Trusted Sources**
   When shopping online, only buy from well-established and reputable merchants. Double-check the website URL to ensure it is legitimate and secure.
3. **Stay Skeptical of Urgent Requests**
   Scammers often create a sense of urgency (e.g., "limited-time offer" or "act now or miss out") to pressure you into making hasty decisions. Always take a moment to research before purchasing.
4. **Be Careful with Social Media and Online Ads**
   Scammers may promote fake products or services on social media or through paid ads. Avoid oversharing personal information, especially when interacting with unknown entities.
5. **Monitor Financial Transactions**
   Regularly check your bank and credit card statements for unauthorized transactions, especially after making online purchases. If you spot anything suspicious, report it immediately.
6. **Beware of Gift Card Scams**
   Never send gift cards to strangers or someone insisting you pay for goods or services with them. This is a classic sign of fraud.
7. **Use Credit Cards for Purchases**
   When shopping online, use a credit card for its fraud protection. Most credit card companies offer zero liability for unauthorized transactions.
8. **Don't Give Out Personal Information**
   Be cautious about sharing personal information, especially with unsolicited callers. Scammers use many tactics to steal your identity, including pretending to be from a trusted organization.

COMMON SCAMS TO WATCH FOR

1. **Gift Scams**
   Scammers target consumers with ads for popular or sold-out items at heavily discounted prices. If a deal looks too good to be true, it probably is.
2. **Vishing, Phishing, Quishing & Smishing**
   The above tactics involve fraudulent phone calls, texts, fake QR codes, and emails that impersonate trusted entities like banks or government agencies. Do not click on links, respond to unsolicited messages, or use your phone to scan unsolicited QR codes.
3. **Holiday Employment Scams**
   Fraudulent job offers may ask for sensitive personal information or payment for "background checks." Only apply to trusted employers.
4. **Social Media Scams**
   Scammers may advertise fake products through social media ads. Always research sellers and look for reviews before making a purchase.
5. **Charity Scams**
   Be extra cautious when donating during the holiday season. Scammers often create fake charities to take advantage of your generosity.

STEPS TO TAKE IF YOU'VE BEEN TARGETED BY A SCAM

Regardless of the type or severity of the crime, it's important to take action as soon as you realize you've been scammed. If you suspect that you've fallen victim to a scam:

1. **Contact the Merchant**
   Report the issue immediately to the merchant, who may help resolve the issue or freeze fraudulent accounts.
2. **Alert Your Credit Card Issuer**
   Contact your credit card company to report fraudulent transactions and request a chargeback.
3. **File a Complaint with the FBI's Internet Crime Complaint Center (IC3)**
   You may report an incident to IC3 www.ic3.gov for further investigation if you believe you or another person may have been the victim of an internet crime.
4. **Place a Fraud Alert on Your Credit Report**
   Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) to place a fraud alert and monitor for suspicious activity. Fraud alerts instruct lenders to contact you directly to verify your identity before extending new credit in your name.
5. **Consider Freezing Your Credit**
   If your personal data has been compromised, consider freezing your credit report to prevent further fraudulent activity. 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 making 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. 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/help/credit-freeze/**
   - TransUnion: 800-916-8800 or **https://www.transunion.com/credit-freeze**
6. **File a report with the Federal Trade Commission (FTC).**
   You may report scams at https://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.