With the holidays coming up and seasonal shopping in full swing, criminals are also gearing up for a busy season. Criminals do not take the holidays off. Shoppers should be more vigilant than ever for scams designed to steal their money and personal information. Though criminals are often aggressive and creative in their efforts, there are certain red flags and common schemes holiday shoppers can guard against this holiday season. Share as you deem appropriate.

- Scams take many forms, but if a deal looks too good to be true, it probably is.
- Consumers should not open any unsolicited emails or click on any links if they do open the email.
- Consumers should secure banking and credit accounts with strong and different passwords, and secure all other accounts that contain anything of value, such as: rewards accounts, online accounts that save payment information, and accounts containing private and personal information.
- Consumers should steer clear of untrustworthy sites or ads offering items at unrealistic discounts or with special coupons.
- Consumers should be careful when downloading mobile applications.
- Consumers should be vigilant when receiving items purchased from online auctions and third-party marketplaces.
- Consumers who believe they are a victim of a scam should call their bank, report the crime to law enforcement, and file a complaint with www.IC3.gov.

➢ ***Online Shopping Scams***
  - Scammers often offer too-good-to-be-true deals via phishing emails or advertisements. Such schemes may offer brand-name merchandise at extremely low prices or offer gift cards as an incentive. Other sites may offer products at a great price, but the products being sold are not the same as the products advertised.
  - Consumers should steer clear of untrustworthy sites or ads offering items at unrealistic discounts or with special coupons. They may pay for an item and give away personal information and credit card details, and receive nothing in return except a compromised identity.
  - Secondary markets for airline miles, gift cards, rewards credits, and other similar products have inadvertently increased the demand for and the resale value of stolen information. Consumers should be vigilant when receiving items purchased from online auctions and third-party marketplaces. If an item arrives from another online merchant, it may have been purchased using a stolen credit card number or stolen rewards points, etc., and then shipped directly to the consumer. These cases should be reported to both the marketplace where purchased and to the merchant who sent it.

➢ ***Social Media Scams***
  - Consumers should beware of posts on social media sites that appear to offer vouchers or gift cards. Some may appear as holiday promotions or contests. Others may appear to be from known friends who have shared the link. Often, these scams lead consumers to participate in an online survey that is actually designed to steal personal information.

- Consumers should not post pictures of event tickets on social media sites. Fraudsters can create a ticket using the barcode obtained from the photo and resell the ticket. Consumers should protect ticket barcodes as they would credit card numbers.

➢ ***Smartphone App Scams***
- Some mobile apps, often disguised as games and offered for free, are designed to steal personal information. Before downloading an app from an unknown source, consumers should research the company selling it or giving it away, and look online for third-party reviews of the product.
- Consumers should also be mindful that alternative app marketplaces available to "jailbroken"* or "rooted"* devices can potentially include copyright-infringing, stolen content, and compromised versions of otherwise trustworthy applications.

➢ ***Work-From-Home Scams***
- Consumers should beware of sites and posts offering work they can do from home. These opportunities rely on convenience as a selling point, but may have fraudulent intentions. Consumers should carefully research the job posting and individuals or company offering employment.

➢ ***Gift Card Scams***
- During the holiday season, consumers should be careful if someone asks them to purchase gift cards for them. In these scams, the victims received either a spoofed email, a spoofed phone call, or a spoofed text from a person in authority requesting the victim purchase multiple gift cards for either personal or business reasons.
- As an example, a victim receives a request to purchase gift cards for a work-related function or as a present for a special personal occasion. The gift cards are then used to facilitate the purchase of goods and services which may or may not be legitimate. Some of these incidents are combined with additional requests for wire transfer payments, as described in classic Business Email Compromise (BEC) scenarios. The following link to IC3's BEC PSA provides additional information about business email compromise and gift card requests (https://www.ic3.gov/media/2018/181024.aspx).

➢ ***Charity Scams***
- Fraudulent charity scams, where perpetrators set up false charities and profit from individuals who believe they are making donations to legitimate charitable organizations, are common after natural disasters or man-made tragedies. Charity fraud also increases during the holiday season when individuals seek to make end-of-year tax deductible gifts or are reminded of those less fortunate and wish to contribute to a good cause. Seasonal charity scams can pose greater difficulties in monitoring because of their widespread reach, limited duration and, when done over the internet, minimal oversight.
- Charity scam solicitations may come through cold calls, email campaigns, crowdfunding platforms—soliciting money from many people usually over the internet—or fake social media accounts and websites. They are designed to make it easy for victims to give and feel like they're making a difference. Perpetrators may divert some or all of the funds for their personal use, and those most in need will never see the donation.

- ***Consumers can do the following to reduce their chances of being victimized:***
  - Check credit card statements routinely. If possible, set up credit card transaction auto alerts, or check balance after every online purchase. It is important to check statements after the holiday season, as many fraudulent charges can show up even several weeks later.
  - If purchasing merchandise, ensure it is from a reputable source.
  - Ensure a site is secure and reputable before providing credit card number online. Don't trust a site just because it claims to be secure.
  - Beware of purchases or services that require payment with a gift card.
  - Beware of providing credit card information when requested through unsolicited emails.
  - Do not respond to unsolicited emails.
  - Do not click on links contained within an unsolicited email.
  - Avoid filling out forms contained in email messages that ask for personal information.
  - Be cautious of emails claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders, and scan all attachments for viruses if possible.
  - Verify requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.
  - Secure credit card accounts, even rewards account, with strong passwords. Change passwords and check accounts routinely.
  - Be wary when replying to unsolicited emails for work-at-home employment.
  - Be cautious of exaggerated claims of possible earnings or profits.
  - Beware when money is required up front for instructions or products for employment.
  - Do not give out personal information when first interacting with a prospective employer.
  - Be leery when a job posting claims "no experience necessary."
  - Be cautious when dealing with individuals outside of the country.
  - Only donate to known and trusted charities; legitimate charities do not solicit donations via money transfer services or ask for donations via gift cards.
  - Make contributions directly, rather than through an intermediary, and pay via credit card or check; avoid cash donations, if possible.
  - Beware of organizations with copycat names similar to reputable charities; most legitimate charity websites use .org (NOT .com).
  - Follow the Federal Trade Commission's tips for online charity research. (https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams)

- ***Consumers who believe they are the victim of a scam should:***
  - Contact their financial institution immediately upon suspecting or discovering a fraudulent transfer.
  - Ask their bank to reach out to the financial institution where the fraudulent transfer was sent.
  - Contact law enforcement.
  - File a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov, regardless of dollar loss. Provide all relevant information in the complaint.


Holiday Caution