PUBLIC SERVICE ANNOUNCEMENT

TLP:CLEAR
21 November 2024

2024 Holiday Scams and Phishing Awareness

This product draws from the FBI's 2021 and 2023 Public Service Announcements

As you're doing your online shopping this holiday season, scammers are busy looking for victims, too! While you shop online, especially during the holiday shopping season, you may encounter shopping scams in many forms. Scammers are often aggressive and creative in their efforts, and there are many red flags and common schemes that holiday shoppers should be aware of during this holiday season. The following is an overview of the most common scams encountered during the holiday season, and best practices that may reduce the likelihood of falling victim to these prevalent scams.

Online Shopping Scams

Over the last five years, a reported $37.4 billion has been lost to online shopping scams; $12.5 billion during 2023.[1] Scammers often offer "too-good-to-be-true" deals via phishing e-mails or advertisements. Such schemes may claim to 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 advertised.

- Avoid use of untrustworthy sites or ads offering items at unrealistic discounts or with special coupons. Victims of these scams end up paying for an item, give away personal information and credit card details, and receive nothing in return except a compromised or stolen identity.

A recently observed phishing campaign is impersonating brands such as IKEA, L.L. Bean, North Face, and Wayfair. The campaign is utilizing websites that have top-level domains (TLDs) as .top, .store, and .vip – often with a website address that very closely resembles the legitimate website address.[2] The following is a list of the known malicious websites associated with this campaign:[3]

- Northfaceblackfriday[.]shop
- Lidl-blackfriday-eu[.]shop
- Bbw-blackfriday[.]shop
- Llbeanblackfriday[.]shop
- Dopeblackfriday[.]shop
- Wayfairblackfriday[.]com
- Makitablackfriday[.]shop
- Blackfriday-shoe[.]top
- Eu-blochdance[.]shop
- Ikea-euonline[.]com
- Gardena-eu[.]com

Social Media Shopping Scams

- Beware of posts on social media sites that appear to offer vouchers or gift cards. Some may appear as a holiday promotion or contest. 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 designed to steal personal information.

- If you click an ad through a social media platform, do your due diligence to check the legitimacy of the website before providing credit card or personal information.

Gift Card Scams

- Consumers should be careful if someone asks them to purchase gift cards for them or requests gift cards as a method of payment for goods. In these scams, the victims receive either a spoofed e-mail, a spoofed phone call, or a spoofed text from a person in a position of authority or familiar to them requesting that the victim purchase multiple gift cards usually for an urgent personal or business reason.

- For example, a victim receives a request to purchase gift cards for a work-related function or as a present for a special 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)[a] scenarios.

Charity Scams

- Fraudulent charity scams, in which fraudsters setup fake charities and profit from individuals who believe they are making donations to legitimate charitable organizations, are common after disasters, which the FBI has seen during the COVID-19 pandemic. Charity fraud also rises 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

[a] Business Email Compromise: A form of phishing attack where a criminal attempts to trick a senior executive or budget holder into transferring funds or revealing sensitive information.

scams can be challenging to monitor due to their extensive reach, short-lived nature, and, when conducted online, minimal oversight.
- Charity scam solicitations may come through cold calls, email campaigns, crowdfunding platforms, or fake social media accounts and websites. They are designed to make it easy for victims to give money and feel like they're making a difference. Perpetrators may divert some or all the funds for their personal use, and those most in need will never see the donations.

Reshipping Scams

- These scams involve fraudsters who use stolen credit cards to buy items—usually expensive items—online. Instead of having the items shipped to the billing address, the fraudster sends them to what's called a "reshipper." At the "reshipper" location, the items are repackaged and usually sent overseas. There, they can often be sold at a high price on the black market.
- Scammers will convince unwitting individuals to be money mules and accept the deliveries and become the "reshipper." That person has now become part of a criminal enterprise without knowing it. Don't be a money mule!

Holiday Phishing Email and Social Media Security Best Practices

- Safeguarding yourself against various types of scams requires adopting accepted online best practices that should be incorporated not only during the holiday period, but year-round. Remember, if it seems too good to be true, it's probably a scam.

Email

- Don't click the link in the e-mail. Manually enter a trusted website's address into your browser.
- Enable multi-factor authentication on your email, online banking, and online shopping accounts, if available.
- Check the sender's email address to see if it matches the company email.
- Don't click on weblinks provided via social media; even if they are shared from legitimate accounts. They could have been hacked.
- Do not click on links contained within an unsolicited email or respond to them.
- 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.

- Verify requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.
- Only open attachments from people you know and that you are expecting an email attachment from.
- If you are expecting the sender to send you something, scan the attachments for viruses prior to opening.

Credit Card/Payment and Donation Security

- Check credit card statements routinely. If possible, set up credit card transaction alerts, and regularly monitor checking account 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.
- Secure credit card accounts, even rewards accounts, with strong passwords. Change passwords and check accounts routinely. See NIST Best Practices for expanded recommendations.
- Beware of purchases or services that require payment with a gift card.
- Never provide credit card information when requested through unsolicited emails.
- Make charitable 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 that mimic reputable charities; most legitimate charity websites use .org (NOT .com).

What To Do If You Become a Victim

If you are a victim of an online scam, the FBI recommends taking the following actions:

- Report the activity to the Internet Crime Complaint Center at https://www.ic3.gov , regardless of dollar loss. Provide all relevant information in the complaint.
- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This PSA was produced from information obtained from multiple opensource articles written by cybersecurity professionals and is based extensively on two Public Service Announcements produced by the FBI.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Online Article; Security Boulevard; 20 November 2024; "Black Friday Scammers are Hard at Work: Security Experts"; Date visited: 21 November 2024; Black Friday Scammers are Hard at Work: Security Experts - Security Boulevard

[2] Online Article; The Hacker News; 18 November 2024; "Fake Discount Sites Exploit Black Friday to Hijack Shopper Information; Date visited: 21 November 2024; Fake Discount Sites Exploit Black Friday to Hijack Shopper Information

[3] Online Article; Forbes; 20 November 2024; "New Chrome, Safari, Firefox, Edge Warning – Do Not Shop On These Websites"; Date visited: 21 November 2024; New Chrome, Safari, Firefox, Edge Warning—Do Not Shop On These Websites