ARMY CRIMINAL INVESTIGATION DIVISION

16 December 2024

Cybercrime Prevention Flyer

Holiday Scam Awareness

While shoppers and revelers are preparing for the holidays, scammers are too. Tantalizing job offers, fake charities seeking donations, or unbelievable online deals that never materialize are recurring scams reported every year. Read on for a refresher to spot and avoid common holiday scams. Stay aware, stay informed, and protect yourself and your loved ones this holiday season.

Temporary Holiday Employment Scams

During the holidays, retail businesses often increase their staff numbers temporarily to manage the shopper rush. To match the online shopping demand, shippers and delivery services also advertise for temporary employees during the busy season. Students on winter break, retirees, and individuals looking for supplemental income are often well-suited for seasonal holiday jobs, as they can provide a flexible and temporary source of employment. Follow these tips when assessing any prospective holiday jobs.

- **Research the company before applying.** Look for official websites, reviews, and contact information to confirm legitimacy.
- **Avoid jobs requiring upfront payments.** Real employers will not charge fees for training, equipment, or other expenses.
- **Verify job offers from email or social media.** Scammers often use fake profiles or unverified accounts to send false opportunities.
- **Be cautious of offers promising high pay.** Scams often claim large rewards for minimal work to lure victims.

Charity Scams

Charity scams exploit goodwill during the holidays. Scammers pose as real organizations or create fake ones to solicit donations. They use phone calls, emails, or fraudulent websites to target victims. Signs include high-pressure tactics or vague details about how donations are used. Research charities to ensure your gift goes to a real cause.

- **Donate through trusted websites**. Visit the official website of the charity instead of clicking links from emails or ads.
- **Verify the organization's legitimacy**. Use platforms like Charity Navigator to check if the group is registered and credible.
- **Avoid paying with gift cards or wire transfers**. Legitimate charities accept secure, traceable payment methods.

Too Good to Be True Deal Scams

Ninety-eight percent of Americans reported they expect to shop online during the holidays. Scammers target these shoppers with fake discounts and false offers that often appear on unreliable websites or in phishing messages. Victims risk losing money or receiving counterfeit goods. Always verify offers that seem unrealistic and shop from trusted sources to avoid falling victim to fraud during the holiday season.

- **Verify website authenticity.** Check for secure domains and online reviews before shopping.
- **Avoid unknown advertisements.** Scammers use pop-ups and fake ads to lead to fraudulent sites.
- **Stick to well-known retailers.** Established sellers reduce the risk of scams or fake deals.
- **Use safe payment methods.** Credit cards and secure apps offer buyer protections.

Department of the Army Criminal Investigation Division: Submit a Tip - Report a Crime

FBI Internet Crime Complaint Center (IC3): File a Complaint

How to spot and avoid job scams this holiday season

Protect your donations from charity scams

Online Fraud 2024 Study Update

Holiday Scams

Authorized for widest release, without restrictions.

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134

SUBMIT A TIP
REPORT A CRIME
WWW.CID.ARMY.MIL

CPF 0111-2024-CID461

CID LOOKOUT
ON POINT FOR THE ARMY