Many of us open our hearts and our wallets to those in need during the holidays. But beware of fraudsters who may contact you by phone or mail seeking to exploit your good intentions. (UBS)

Keeping cyber safe this holiday season

19 December 2022, 3:35 pm CET, written by UBS Editorial Team

The holiday season is a time for shopping, giving and family festivities. It's also a time for heightened vigilance about cybercrime and fraud. We share common scams to look out for and tips on how to avoid them.

Scammers and cyber thieves come up with new ways to steal your money, data, and identity every year, and many of these schemes are rampant during the holidays. Some of these schemes leverage the increase in online shopping that began in 2020 due to global pandemic.

"Even though you're in the holiday spirit, you need to be cautious," says Roseanna Blum, Tech Cyber Security Specialist, UBS Regional Chief Information Security Office. "We're all rushing around, trying to get a lot done, cyber attackers and fraudsters are aware of it and exploit it, so we need to be even more careful."

"It's really important to think about your next click before you act" added Jeff Meshberg, Wealth Management Americas Divisional Information Security Officer.

Here are five common holiday scams and tips on how to avoid them:

1. Online shopping scams: Online shoppers hunting for bargains or great deals be warned: Fraudulent shopping websites abound with many advertising unusually deep price cuts or exclusive offers that are meant to lure you into providing your personal or financial information or clicking on malicious links that can infect your computer.

How to stay safe: Remember, if an offer seems too good to be true, it likely is. Shop only with reputable retailers and only transact on secure websites with "https" in the URL. Also be sure to have the latest anti-virus software running on your device. Avoid using payment to payment (P2P) cash transfer services, such as Zelle or Venmo, to purchase items over the Internet, as those services are only meant to transact cash with people that you know.

2. Malicious e-mail links: From bogus e-cards to malware-laden advertisements, e-mail scams are a major problem during the holidays. Phishing schemes involving package-delivery notices are especially prevalent. An e-mail, purporting to be from the US Postal Service or a common carrier delivery service, instructs customers to click on a link that promises a shipping-status update. Instead, it unleashes a virus or other malware on their device that could end up stealing usernames, passwords, and other private information.

How to stay safe: Unless you know the sender, never click on a link in an e-mail, and never open attachments. You should also never send personal or financial information by e-mail. If anyone asks you for that it's a red flag.

3. Wi-Fi hotspot risks: Think twice about using the unsecured Wi-Fi in an airport, coffee shop or other public space to order that last-minute gift from your laptop, tablet, or smartphone. Mobile devices make it convenient for us to shop almost anywhere at any time, but they also make it easier for crooks to carry out a wide variety of cyber schemes—from phishing to "evil twin" hacks that use bogus Wi-Fi signals to access your device and plunder your data.

How to stay safe: Keep in mind, the information you transmit or receive on unsecured wireless networks may be accessible to other users on the network. Avoid using unsecured networks in general—and never use them to send or receive personal or financial information. Consider using your own secured personal hotspot instead.

4. Gift card scams: One common scam this time of year involves a victim receiving a threatening call or voicemail saying that a family member needs help to pay for an emergency need or will soon be arrested for crime unless a fine is paid immediately. The victim is then told to make the payment with gift cards and provide the imposter with the codes to redeem and use them. Fraud seeks to exploit one emotion or another—this one being love and trust. Criminals prey on that sense of family support during the holidays.

How to stay safe: Note that no legitimate government entity, bank, attorney, or bail bondsman should ask for payment via pre-paid gift cards. If you receive one of these calls and find it suspicious, never provide your personal or financial information. The best thing to do is simple: hang up.

5. Charity fraud: Many of us open our hearts and our wallets to those in need during the holidays. But beware of fraudsters who may contact you by phone or mail seeking to exploit your good intentions. There are criminal enterprises masquerading as charitable organizations to steal your money. Such scams tend to increase in response to significant events like the holidays, natural disasters or climate change initiatives.

How to stay safe: Learn to recognize the warnings signs of charity scams, and only donate to charities you know and trust. Ratings on Charity Navigator's website can help you find trustworthy charitable organizations. The IRS also has an online tool that lets users search for legitimate charities to which donations may be made tax-deductible.

Taking steps to avoid these common scams around the holidays is important, but so is protecting yourself from fraudsters all year round. You can do your part by adhering to the security measures that financial institutions, like UBS, have put into place to protect your personal information and financial data. Where possible, opt in to multi-factor authentication, maintain strong password protocols, and update your devices with the latest software updates and antivirus/malware software for all of your online activity.

These best practices can help ensure that you stay cyber safe during the holiday season and every day.

Expiration: 12/31/23
Approval date: 12/19/2022
Review Code: IS2207231