

Be Aware Of These Common Scams

Scams are attacks used by cybercriminals to deceive victims into giving away sensitive and financial information which can lead to significant monetary losses. As the world becomes increasingly digital, scams are growing rampant, resulting in the loss of billions of dollars annually.

Cybercriminals will use various tactics to commit scams, such as creating a sense of urgency or fear to pressure victims into acting quickly without thinking. They use social engineering to build rapport among victims by exploiting human psychology and emotions using information they've gathered on the internet. Once they exploit a victim's weakness, they will attempt to steal money through different methods of payment like cryptocurrency, gift cards, or even direct wire transfers. It's important to stay vigilant on the tactics and scams bad actors will use to commit fraud and steal information, so you can be prepared and know how to mitigate the risks associated with these scams.

Different Types of Scams

Impersonation Fraud

Impersonation fraud occurs when a scammer poses as a legitimate person using stolen or fabricated credentials, photos, and contact information to appear credible. The scammer may initiate contact via email, social media, or even SMS text messages. They will direct the victim to communicate through a third-party messaging app like WhatsApp or Facebook Messenger. After contact is made with the victim, the scammer will attempt to build trust by providing seemingly legitimate advice or information. Once trust has been established, the scammer will manipulate the victim and request sensitive information such as account login credentials, financial details, or even direct payments. Continue to educate yourself on the risks of impersonation scams and importance of verifying communications from unknown sources.

Ways to Avoid this Scam:

- Verify the identity of the person contacting you through official channels (e.g., the website or direct phone call).
- Be cautious of anyone who insists on using third-party messaging apps for communication.
- Encourage use of secure, official communication channels.
- Regularly monitor accounts and communications for signs for fraudulent activity.

Toll Text Scam

Have you received a text message saying that you have an unpaid toll that you need to pay immediately? The goal of this scam is to trick the victim into paying the fake toll or clicking on a malicious link, which can lead to financial loss or identity theft. The victim receives a text message claiming they have unpaid toll or road fees and is designed to create panic or urgency. This prompts the victim to act quickly without verifying the claim, leading the victim to a website designed to look like an official toll payment portal.

Ways to Avoid this Scam:

- Do not click on links or call numbers provided in unsolicited text messages.
- Contact toll authority directly using their official website or phone number to verify the claim.
 - Their official website will typically have a license plate searcher to check if you have an unpaid toll.
- If you believe you owe a toll, pay through the official toll authority's website or app and don't click the link in the text message.

Investment Scam

An investment scam involves cybercriminals luring victims into investing in fraudulent or non-existent opportunities. These scams typically promise high returns with little to no risk, exploiting a victim's desire for financial gain. Scammers will create fake investment platforms, website, or social media profiles that appear to be legitimate. Additionally, they can also contact victims via email, social media messaging, or cold calls with offers of exclusive, high-return investment opportunities. Victims are then persuaded to invest money, often through wire transfers, cryptocurrency, or other untraceable methods for the scammer to take advantage of.

Ways to Avoid this Scam:

- Thoroughly research any investment opportunity before committing funds.
- Be wary of investments that promise high returns with little to no risk.
- Verify credentials of the individuals or company offering the investment.
- Only invest through well-known and trusted platforms or financial institutions.

Call Forwarding Scam

A call forwarding scam is an attack where cybercriminals trick victims into activating call forwarding on their mobile phones. Once call forwarding is activated, all incoming calls to the victim's number are redirected to a number controlled by the scammer. This allows the scammer to intercept sensitive information, such as one-time passwords, verification codes, or other confidential communications. A scammer will typically impersonate a trusted entity, such as a bank, cellular provider, or tech support. The scammer will then reach out to a victim through call, text, or email claiming there is an urgent issue with their account, device, or service. The message will instruct the victim to dial a specific code followed by a phone number to "resolve" the issue, and once the number is dialed, call forwarding is activated and all incoming calls to the victim's number are redirected to the scammer's number.

Ways to Avoid this Scam:

- Treat unexpected calls, texts, or emails with caution, especially those claiming urgency.
- Do not dial codes or numbers provided in unsolicited messages.
- Regularly review your phone's call forwarding settings to ensure they're configured correctly.
- Enable MFA for your accounts but avoid using SMS-based one-time passwords if possible.
 - Opt for app-based authentication if available.

Predatory Loans and Loan Scams

Oftentimes, scammers rely on their victims to be at their most vulnerable to commit fraud and will use loan scams to promise funds to victims after paying an upfront fee. Scammers will target individuals seeking a loan for a new house, car, or medical fees by promising to disburse the loan once a deposit has been made. They often target individuals with poor credit or those in urgent need of funds, promising guaranteed approval or no credit checks. They will often impersonate a legitimate entity such as a bank to build credibility and requests upfront fees for various reasons like insurance or taxes. Once the deposit goes through, the scammer disappears, and the victim never receives the loan they were expecting.

Ways to Avoid this Scam:

- Legitimate lenders do not guarantee approval without reviewing your credit.
- Be wary of offers that promise loans with no credit checks or instant approval.
- Verify the legitimacy of the lender by checking their credentials, reviews, or complaints.
- Only borrow from well-known and reputable financial institutions or lenders.
- Avoid using unverified online platforms or apps.

This material is for general information only and is not intended to provide specific advice or recommendations for any individual. This material was prepared by LPL Financial, LLC

Tracking #703378

Exp 03/2027