Beware of these common scams

Nigerian Scams

People claiming to be officials, businessmen or surviving relatives of former government officials in countries around the world send countless offers via e-mail, attempting to convince consumers that they will transfer thousands of dollars into your bank account if you will just pay a fee or "taxes" to help them access their money. If you respond to the initial offer, you may receive documents that look "official." Unfortunately, you will get more e-mails asking you to send more money to cover transaction and transfer costs, attorney's fees, blank letterhead and your bank account numbers and other sensitive, personal information.

Tech Support Scams

A tech support person may call or email you and claim that they are from Windows, Microsoft or another software company. The person says your computer is running slow or has a virus and it's sending out error messages. Scammers will ask you to visit a website that gives them remote access to your computer. If the caller obtains access they can steal personal information, usernames and passwords to commit identity theft or send spam messages. In some cases, the caller may even be asked for a wired payment or credit card information.

Lottery Scams

In foreign lottery scams, you receive an email claiming that you are the winner of a foreign lottery. All you need to do to claim your prize is send money to pay the taxes, insurance, or processing or customs fees. Sometimes, you will be asked to provide a bank account number so the funds can be deposited. In reality, your bank account is likely to be depleted. You end up shelling out your hard earned money for "winnings" you will never receive.

Phishing Emails

Phishing—also known as carding or brand-spoofing—is a type of deception designed to steal your identity. In a phishing scam, a thief tries to get information like credit card numbers, passwords, account information, or other personal information from you by convincing you to provide it under false pretenses.
In a phishing scam, the messages often look very authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes.

Overpayment Scams

In check overpayment scams, the con artist responds to an item you may have for sale online. They send you a check payable for more than the agreed upon price along with a reason why they are writing the check for more. They ask that you deposit the amount in your bank account and wire or transfer the extra amount to a foreign account. The scammer vanishes after the money is deposited. At that point, the check bounces and you are required to pay for the entire amount.

Disaster Relief Scams

Every time there is a disaster like the tsunami, a tornado or an earthquake, millions of do-gooders want to do something to help the victims. Scammers take advantage of this by setting up scam charity institutions which rob the money that you wanted to send to the victims of the disaster. Scammers also attempt phishing by sending you donation requests via email where you can click on a link which then leads you to website designed to steal your passwords and other details.

"Free" Trial Offers

Misleading free trial offers online for diet supplements, penny auctions and money making schemes blanket the internet resulting in thousands of complaints ever year. The free trial offers seem no-risk but complainants state they were repeatedly billed every month and found it extremely difficult to cancel.