Common Scams

In our ongoing commitment to improving your online security, and in light of October being Cybersecurity Awareness Month, we're focusing on common scams that are catching people off guard. Even the smartest folks can get scammed, so being aware is your best defense. Here are some scams to watch out for and tips to keep you safe:

1. For Sale, Hot Deal

Scammers are posting fake deals on social media marketplaces. You pay, but the item never arrives.

Be cautious of deals that seem too good to be true. Scammers often use enticing offers to lure victims into a false sense of security. Once you send the money, not only is it likely you'll never see the item, but it might also be impossible to get your money back. Always verify the legitimacy of the deal and the seller's credibility before making any payments. Check for reviews, and if possible, use secure payment methods that offer buyer protection.

2. Hire Us, Special Offer

Some ads on social media offer deep discounts on services like house repairs and cleaning. After you pay, the service providers never show up.

Always research the company and hire licensed contractors. Ask for references or recommendations from friends and family, verify their credentials, and check online reviews or testimonials. Request a written contract detailing services and payment terms. Avoid paying the full amount upfront; use a phased payment plan to ensure work satisfaction before the final payment. These steps can help you avoid fraudulent service providers.

3. Bank Impersonation

Scammers might text, email, or call, pretending to be from your bank, saying there's an issue with your account to trick you into sharing sensitive information.

If you're not 100% sure it's your bank, contact them using the number on the back of your card. Additionally, be cautious of any communication that asks for sensitive information like your password, PIN, or Social Security number. Banks will never ask for this information via email, text, or phone call. Always verify the authenticity of such requests by contacting your bank directly through official channels. Be wary of links or attachments in unsolicited emails, as these could lead to phishing websites designed to steal your personal

information. If in doubt, it's always better to err on the side of caution and consult with your bank's customer service.

4. Cute Puppies for Sale

Ads for adorable pets often ask for a deposit, but the pet never existed once you pay.

Never share personal details or make payments before seeing the pet in person. It's also a good idea to request a live video call for verification of the pet and the seller's authenticity. Genuine breeders and pet sellers will readily offer more information or arrange a meeting. Be cautious of any excuses or delays when scheduling a viewing, as these could signal a possible scam. Always use secure payment methods that provide buyer protection and avoid wire transfers or gift cards as forms of payment. Stay alert to protect both your heart and your finances.

Want to read up more on scams like these? Check out the links below!

Common Scams | Office of the Attorney General

What are some classic warning signs of possible fraud and scams?