



6/2/2023 Popular Payment Scams

In today's digital age, protecting your financial information is crucial. Scammers are constantly evolving their techniques to exploit unsuspecting individuals and unfortunately, they're very good at what they do. To help you safeguard your finances, we've put together a list of some popular payment scams to be aware of and avoid. By familiarizing yourself with these popular scams, you can minimize the risk of falling victim to fraud. Remember to always prioritize secure payment methods, be skeptical of unsolicited requests, and regularly monitor your accounts for unauthorized activity.

- **Phishing Emails, Calls, and Messages:** Phishing is a technique where scammers send deceptive messages or make phone calls pretending to be from legitimate organizations, aiming to obtain your personal and financial information.
 - Be cautious of unsolicited messages or calls requesting sensitive information.
 - Avoid clicking on suspicious links or downloading attachments from unknown sources.
 - Independently verify the legitimacy of the company by contacting them directly using only official contact details.
- **Card Skimming:** Card skimming involves criminals stealing your card information by using devices or methods to capture your data during transactions.
 - Always keep an eye on your card during physical transactions.
 - Use ATMs located in well-lit and secure areas, inspect them for any suspicious devices, and remain at the terminal until your transaction is completed.
 - Regularly monitor your bank statements for any unauthorized charges.
- **Fake Online Sellers:** When shopping online, be cautious of fraudulent sellers who may take your payment without delivering the promised goods.
 - Purchase from reputable and secure websites.
 - Read reviews and check the seller's rating before making a purchase.
 - Use secure payment methods or services that offer buyer protection.
- **Bogus Online Payment Processors:** Some scammers create counterfeit payment processors that mimic legitimate ones to deceive you into sharing financial details.
 - Only use trusted and well-known payment processors for online transactions.
 - Double-check the website's URL and look for secure connections (padlock symbol and "https") during the payment process.
 - If in doubt, research the payment processor independently or contact customer support using official contact information to verify their legitimacy.