

# Things You Should Know About...**ONLINE SCAMS**

The Internet and online services are convenient and useful. However, they also provide con artists with endless ways to scam consumers. Be on the lookout for these tactics (and other similar schemes) when conducting transactions online.

## **Phishing Scams**



Phishing is the fraudulent practice of sending emails or other messages claiming to be from reputable companies in order to convince individuals to reveal personal information, such as passwords and credit card numbers.

You may receive an email that appears to be from a well-known source like a bank, mortgage company, creditor, etc. The fraudster will trick the person into thinking there is a problem with their account that needs their attention. The goal is to gain personal information so they can steal your identity or financial information.

## **Pyramid/Ponzi Schemes**



Pyramid schemes will promise money or valuables in exchange for soliciting new members in a "business venture." If no new members join, the pyramid eventually falls, and those at the bottom lose their initial investment. These schemes are typically promoted as games, buying clubs, motivational companies, mail order opportunities, or investment organizations.

## **QR Code Scam**



QR code scams, also known as "quishing," involve scammers prompting individuals to scan fake QR codes that redirect to malicious websites or applications designed to steal sensitive information or install malware.

## **Package Delivery Scam**



Scammers send text messages with links that claim information about package shipments or deliveries from well-known entities like Amazon or UPS. When you click the link, it leads to fake websites designed to steal your personal information or gain access to your account.

## **Quizzes, Surveys, and Polls**



While they may seem fun and harmless, the quick surveys, personality tests, and other types of online quizzes ask questions that could lead to fraud. Scammers can use your quiz answers to try and reset your accounts, letting them steal your bank account information and other private information.

## **Fake Gifts and Giveaways**



Fake gift and giveaway scams often promise prizes or free items, but require upfront fees or your personal information to claim the giveaways. Your financial data could be compromised and you could lose the money you paid or risk other unauthorized charges.

## Fake Job Offers



Scammers may approach victims with job offers promising high pay with minimal effort, often on messaging apps or social media. Many times, a job seeker has to click on a link that can put their computer and personal information at risk.

## Health Care Offers



Consumers are lured into buying equipment, vitamins, treatments, or “cures” with the promise of better health, fitness, or appearance. However, products and treatments may not be regulated by the FDA or may be ineffective or harmful. Some purchases may not be covered by insurance as promised, leaving the individual on the hook for the payment.

## Social Media Scams



Social media platforms are ripe for several scams that could involve phony profiles, fake ads, investment scams, and online shopping scams. Be cautious of clicking on links that could put you at risk of identity theft. Look for another digital presence on the social media platform. Try to find independent reviews before you commit to a transaction.

## E-commerce Scams



Scammers may create fake online stores or use fake listings on platforms to steal money and/or personal information. Be cautious of online shopping, especially with new stores and sites. When using online marketplaces, check out the seller's profile and transaction history. Use secure platforms to transfer funds. Also, be safe and use public spaces to view or pick up items.

## TIPS FOR AVOIDING ONLINE SCAMS

- **Always Be Wary** of offers marketed as “too good to be true,” “inside information,” or “hot opportunities.”
- **Don't Give Your Personal or Financial Information** in Response to a Request that You Didn't Expect or Initiate. If you aren't sure if the request is valid, call the business or organization directly.
- **Never Judge a Book by Its Cover.** A website may look professional and be aesthetically pleasing, but that doesn't ensure that the company is legitimate or operating lawfully. Remember, when making online transactions, use as many sources as possible to verify the company's legitimacy and quality of the products or services offered.
- **Always Use a Secure Browser.** To ensure you are using a secure browser, look for a web address that begins with “https:” instead of “http:” on the page that asks for your personal information and look for an icon of a locked padlock on the status bar at the bottom of your page.
- **Always Investigate a Company's Reputation.** Ask a company for a verifiable street address and telephone number before doing business with them. To further verify the company's legitimacy, check with your local Better Business Bureau or the Attorney General's Consumer Fraud Helpline.

## ATTORNEY GENERAL'S CONSUMER FRAUD HELPLINES

**Chicago**  
1-800-386-5438

**Springfield**  
1-800-243-0618

**Carbondale**  
1-800-243-0607

Individuals with hearing or speech disabilities can reach us by using the 7-1-1 relay service.