ACCOUNTING & AUDIT

How Online Scammers Target Their Fraud Victims

Scams and con artists are everywhere and they'll do just about anything to gain access to your personal information and steal your hard-earned money. One of your best defenses against fraud is learning to recognize scammers' more common tactics and ...

Oct. 15, 2015

Scams and con artists are everywhere and they'll do just about anything to gain access to your personal information and steal your hard-earned money. One of your best defenses against fraud is learning to recognize scammers' more common tactics and how they work. AARP Fraud Watch Network has compiled tips on what to watch out for and what to do should you find yourself in a scam.

"It's important as consumers to be aware of the most common tricks used by scammers," said AARP Illinois Communications Manager, Gerardo Cardenas. "While scams might change from time to time, the foundations of the scams stay the same. If you know about common tactics used, you can spot a fraud before they have the chance to take anything of value."

Trusting your instincts is always a smart decision, but you need to be aware of these common tactics:

Phantom Riches: A scammer dangles the prospect of wealth, but can't provide it because the prospects they're selling you don't actually exist.

Profiling: Scammers develop a victim profile by asking a series of personal questions to find your emotional trigger. Once they know what that trigger is, they can hone in on specific types of scams that work best on you.

Scarcity: Another way to play with emotions, scammers will offer a product or service that's only available for a limited amount of time "for someone special, like you; so don't miss out." If something is rare or scarce it tends to be more valuable—but these offers are usually fake.

Credibility: In efforts to build your trust, con artists will claim to be affiliated with a well-known celebrity, reputable organization, or by speaking of a special credential or experience. The IRS is the government agency most commonly mimicked in fraudulent attempts to get your personal information.

Another common company mimicked is Microsoft with the con-artist trying to gain access to your computer to fix an issue that they installed through malware ridden folders, links, or emails.

Try to keep these tactics in mind if you're being pitched to from an individual or organization, especially ones you've never heard of. Doing your research and finding out who you're dealing with is important, particularly when it concerns an investment product.

Check to see if the seller you're working with is registered with the Financial Industry Regulatory Authority or if the product/financial advisory is registered with the Securities and Exchange Commission or your state securities regulator. Should you encounter a scammer contact your local Attorney General's office to report it.

For more information on resources and tips to keep you safe, contact the Federal Trade Commission for identity theft related resources or visits aarp.org/FraudWatchNetwork for tips and alerts on new scams.

Accounting & Audit • Advisory • AARP • News • Charity Scams • email scams • Financial Scam • fraud • internet scams • mortgage scam • scam • scammers • Scams • tax scam • Tax Scams

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.