Protecting Your Finances

Protect Yourself From Online Identity Theft

What You Should Know About Online Scams

(NAPSA)—With forethought, you may be able to prevent becoming a victim of online thieves who can collect billions of dollars every year using a variety of schemes to steal the personal information—even the entire identities—of unsuspecting people. Take the time to learn the risks now to prevent the months, even years, of bad credit and legal hassles that can result from online scams.

What you should know about online scams

Online scammers typically focus their efforts on gathering the sort of information that may appear on a loan application or other financial transactions: names, Social Security numbers, birth dates, credit card and bank account numbers—as well as passwords and personal identification numbers (PINs). Thieves use this information to create fraudulent accounts for their own use and then go on spending sprees that end up on your credit report.

One of the most popular ways by which thieves steal personal information is through a scam called phishing. A phishing scam begins with an e-mail to potential victims that appears to come from a legitimate business, such as a bank or software company. The message asks you to submit credit card information, Social Security numbers, bank account information or other personal data under a false pretense. This pretense is often a moneymaking opportunity, but it might also be a seemingly routine request to verify personal information. The scammer's e-mail may even include a link to a legitimate-looking Web site to capture this information.

According to the Federal Trade Commission, an estimated 9 million Americans have their identities stolen each year, and about a third of all reported victims of identity theft are teenagers. They make attractive targets because they have good credit, seldom carry much debt and may be less savvy about keeping their personal information secure.

As many as 9 million Americans have their identities stolen each year, according to the Federal Trade Commission.

Signs of a scam

- You don't know the person who has sent you the message.
- You are promised large sums of money for little or no effort on your part.
- The request contains a sense of urgency.
- The sender repeatedly requests confidentiality.
- You're asked to provide money up front for a processing fee or to pay the cost of expediting the process.
- You're asked to provide your bank account number or other personal financial information, even if the sender offers to deposit money into it.
- The scammer offers to send you copies of banking information or other evidence to prove his or her activity is legitimate—but this evidence is easily faked.

Learn More

You can find additional fraud-fighting tips from Comcast at www.comcast.net/security.