Investigator Insight

Anatomy of a Scam

There is no single group of people who is more likely than any other to be the target of a scam. Kroll's Investigators talk to people from all walks of life who have fallen victim.

To avoid a scam, it is helpful to understand how one is put together. Here we take a look at the basic components:

Contact information is collected. The scammer has obtained some of your personal identifying information (PII) which might include name, email address, phone number, address, and/or other information they will use to reach you. If contact information is not first obtained by the scammer, then they will lay out a bait of some sort—fake employment ad, for example, that might cause you to contact the scammer first and then willingly provide your personal identifiers.

A compelling story is presented. This is where the scammer gives the reason they need PII and/or money from you. The fake reason may be one of the following:

- A caller claims he is a Microsoft representative and can see that your computer has a virus.
- An email claims our credit card or bank account is in danger of being closed or your access to it restricted.
- A person in a foreign country needs your help getting a great fortune transferred to the United States.
- A caller claims he is an IRS agent who must collect payment from you or you will be arrested.

The target of the scam gives up personal information or money. This is where the trouble starts—you give them your personal identifiers, access to your computer, access to your bank account, or accept a bad check presented to you by the scammer.

The scammer is rewarded. Now the scammer gets to work using information provided by the scam victim to steal money, open new credit accounts, or trick the victim into giving money to the perpetrator of the fraud.

Use these tips to avoid falling victim to a scam:

- Hang up on anyone that you believe is a scammer. Do not push any buttons on your phone or speak to the caller.
- Understand that legitimate businesses will not send email or text messages asking for your PII. Delete such messages without responding.
- Don't trust Caller ID. Scammers can mask their number.
- Think about what you are asked for before providing your PII whether by phone, clicking on a link in an email, answering an ad, etc.
- Be cautious when using a search engine. The first links listed are paid advertisements and may not be the site you seek.