

How Phone Scammers Try to Manipulate You

We all know phone scams are out there, so let's review some ways phone scammers try to manipulate you into giving them information.

But first, let's be clear. End Elder Fraud's #1 piece of advice for you is to NEVER answer phone calls if you don't know the caller. Period. End of story. If it's a legitimate call, the person will leave a message, and you can then decide—in a relaxed and centered manner—if you wish to return the call.

But we get it. Sometimes you're waiting for an important call-back. And in this day-in-age when employees/contractors are often required to use their personal cell phones for contacting customers, it isn't as black and white as we wish it was. And isolated, trusting seniors--who grew up with phone calls generally being a "positive" (or at least truthful) in their life--are often quick to pick up the phone. It can be a tough habit to break.

So, let's say you do answer that call. Here are some things to watch out for.

Scammers may:

- Open the call by placing you in a vulnerable, emotional place, such as causing you to feel fear or even greed. They often couple those emotions with the need for urgent resolution. They use these techniques to decrease your ability to think clearly and logically. (How do they do this? They tell you something horrible happened or may soon happen, or that you have an opportunity to receive a lot of money, a prize, a great deal, etc.)
- Act authoritatively and state they have your personal information and just need you to verify pieces
 of data. Much of your personal information IS available online, and scammers often lead with this
 correct information.

While many people will not give out their personal information willingly, sometimes when a scammer tells a person correct information they have, but then parts of the information are wrong, it feels somehow natural for the person to jump in and correct the scammer. And what happens if a person does that? S/he gives the scammer exactly what they wanted in the first place.

An example is a scammer saying to someone, "I see you were born in November 1955." If a person is not aware, they can easily and mindlessly reply, "No I wasn't. I was born in February of 1954." And now the scammer has what s/he needed.

- Feed you bits of information for verification one at the time—spaced out through the conversation. They may start with general facts to gradually lull you into the rhythm of the call. For instance, starting with a bank name early in the call (seems harmless, right?), perhaps moving to the type of credit card you hold a bit later in the call (still pretty generic), then after more "rapport" has been established, moving on to your card's expiration date, and finally to your account number.
- Say "We already have your account information, and we'd like to review your recent charges. Can you confirm your credit card number beginning with the number "5"? This technique makes a person believe the caller already has their credit card number. However, earlier in the conversation with the scammer, the scammer may have asked if the caller has a Master Card, Visa, or AMEX. Knowing which card you have gives them the first digit. (https://www.forbes.com/advisor/credit-cards/what-does-your-credit-card-number-mean/)
- Ask "Are you still at [one of your previous addresses]?" As we noted above, it is easy to find information on most people via a simple google search. Free online records will reflect nearly accurate information about where people live and work. However, these records can become stale, so the scammer asks if you are still living at that address to show you how informed he is and instill a false sense of security in you. He wants you to believe you are dealing with a professional for valid business reasons.
- Refuse to give you a call-back number, to try and pressure you into completing the call.
- Transfer you to many different departments, so you feel your issue is being escalated for resolution.

If at any time in a phone conversation you feel unsafe or wary, do not hesitate to end the call—politely or otherwise. Scammers are criminals after all.

To hear examples of some of the above ploys, check out our YouTube videos on the "Bulletins and Tips" page of our website https://endelderfraud.org/

If you have any questions or comments on this information, please email us at info@endelderfraud.org.

End Elder Fraud is dedicated to ending cyber fraud amongst the seniors in our community.

If you'd like to help, please support us at endelderfraud.org

Stay safe through awareness