

THIS & THAT

by
Bob Lunaburg



I'm not sure that seniors are more vulnerable to scams and fraud than any other group is, but it seems like we are a group the media likes to report on. Regardless, a wise person needs to be aware of the warning signs that a crook is after our identity, and our money.

The Identity Theft Resource Center (<http://www.idtheftcenter.org>) is a not for profit organization that is loaded with great advice and information on this subject, and is worthy of your attention.

I never read "Dear Abbey" in the AJC, but someone I am extremely fond of reads it religiously every day. Recently (Sunday, December 5) my special someone turned to me and said, "You've got to read this. You need to tell the Seniors about it too." She handed me the paper.

In the back of my mind I thought, "Here we go. This must be something about an overly risqué old coot who was two timing his lady of fifty years, with a twentysomething sweetie." With that thought in mind, I took the paper and read the column. Boy, was I wrong. The stuff in that article is perfect for us, and for that matter, anyone who has a trusting heart.

Linda Foley, coexecutive director, Identity

Theft Resource Center, offered the following six items to watch for when guarding against email, web, and any other form of identity theft. She uses the term "phishing" to describe this fraud. Don't you just love these new terms? Anyway, here are her six points, and thank you Dear Abbey, the Atlanta Journal Constitution, and especially Linda Foley.

(1) No company is going to call or e-mail you to verify an account, ask for your Social Security number, or any bank or credit card numbers, *period!* This is called "phishing." Account verification scams look very real, but are *all* scams. Do not answer them no matter how convinced you are that it is a real company.

(2) You have *not* won a lottery in the Netherlands, or Canada, or anywhere else, if you didn't first buy a ticket here in the U.S.A.

(3) Question any company that offers you a prize but asks for a fee or your Social Security number, and verify the existence of that company through the Better Business Bureau, and confirm independently that the prize is real.

(4) A stranger did not die and leave you money.

(5) The Nigerian scam has now morphed into a creative writing exercise about all kinds of people needing your help to transfer money from one account to another. This practice is called money laundering, and it is illegal.

(6) You may also be telephone-scammed with similar offers. Be on the alert for suspicious callers, and never give out your Social Security number or a credit card number to anyone who calls you.

I will add one more item to this list. It

pertains to your computer passwords.

(7) Never give anyone any of your account pin-numbers or passwords unless you are using them to gain access to the thing you created them for. They are designed to protect against unauthorized access, and as such *need to remain secret*.

Finally, if this kind of thing concerns you, you are not paranoid. You are just being a responsible citizen who, like all of us, lives in an imperfect world.