



Watch Out for These Common Fraud Scams

It may seem odd, but the fact that many common scams have a long shelf-life is a good thing. The long shelf life makes it possible for organizations to track scams and warn the public about what to watch for. There are many agencies doing this, including the Federal Trade Commission (FTC) and the Better Business Bureau (BBB). The FTC regularly updates the part of its website that's dedicated to exposing scams and provides a way for consumers to post complaints. The BBB also keeps track of current scams and schemes to keep consumers and businesses on their toes.

The Target

One key item scammers seek is your Social Security number (SSN). By now, we all know it's critical to guard this key piece of information. Yet, one method scammers often use to steal SSNs is to simply phone victims. It goes something like this: You get a call from someone claiming to be from the Social Security Administration, and the caller tells you that your SSN has been "suspended" because of suspicious activity. The story varies, for example, the caller may say that you're due for an increase in future benefits. Then he or she will ask you to verify your SSN, just to be sure you're really the person who owns the account. And that's how they get your number.

No matter what a caller tells you, the Social Security Administration states that it never places such calls. The same is true for the IRS. Don't be fooled by caller ID, which can be part of the scam. Thieves can mimic actual phone numbers, even for government agencies.

What should you do if you get such a call? Hang up and call the number yourself. Or, if you want to be sure everything's in order, end the call. Then look up the general phone number on your own, call it and ask whether someone is trying to reach you. (For the Social Security Administration, the general office number is (800)-772-1213. Don't rely on a phone number that the caller gives you. That number is most likely part of the scam.

How Thieves Use Stolen SSNs

Once a thief gets hold of your SSN, he or she might seek to deepen the scam using one of the following tactics:

Fund wiring request A scammer may call you pretending to be with an organization that you'd expect to already have your SSN. As noted before, this could include the Social Security Administration, the IRS, or an official from your bank or credit card. After the caller convinces you that the call is legitimate, he or she may recite to you your own SSN, to further establish credibility. Then the caller may ask you to authorize a funds transfer for a specific purpose, such as to prevent having your account frozen. Don't fall for it.

Tax identity theft: This seasonal scam involves intercepting a tax refund that should go to you. The early tip-off could be a letter from the IRS stating that the tax return you have just submitted is the second one it has received using your SSN. If you e-file your return, you may get a notice that your filing was rejected because your refund has already been paid. Or the IRS might say it isn't giving you a refund because of you still owe taxes that you didn't know you had to pay. This could indicate that someone was fraudulently using your SSN to work under but not paying the related taxes.

Another Common Scam: the Fake Charity Many Americans are charitably inclined. If you're one of them, thieves may seek to use your generosity against you. Bogus charities pop up like mushrooms after a rainstorm following disasters such as hurricanes, earthquakes and flood. The COVID-19 pandemic is another example. Fraudsters have devised and executed plenty of scams during the crisis. A charity with an unfamiliar name isn't necessarily a sign that it's fake, and a name that does sound familiar isn't necessarily a legitimate charity. Scammers often piggyback

on established charities with names that are close enough to fool casual observers. Give special attention to the spelling. Suppose you get a plea for donations from a group called United Ways. The actual charity is United Way. Thieves are counting on your failure to notice the slight difference. So, outsmart them by taking a moment to check and double-check the proper spelling and existence of a charity.

In addition, before you donate, do some research using charity rating groups such as Charity Navigator and the Wise Giving Alliance. You can also run an Internet search on your own by pairing the charity's name with words like "complaint" or "scam."

Bogus Ads and Not-So-Sweet Sweethearts: Here's a common Internet-based scam that's catching on: Fake ads. You'll be intrigued by an offer for heavily discounted "name brand" goods, and make an online purchase. The problem is, the site is just a collection point for credit card information that will be used by scammers to test the credit limit on your card. Steer clear of ad scams by using a secure Internet connection and checking the website's URL to make sure that it begins with https:// as opposed to http://. The "s" stands for "secure" and indicates that information transferred on that site is encrypted and, therefore, less vulnerable to theft.

Too Hot to Be True: Falling victim to retail fraud might not be quite as emotionally distressing as another kind that's claiming many victims today: The "romance scam." According to the BBB, while social media has made meeting new people and dating easier, "it has made the scammer's work simpler, too." There's even a term for it: "catfishing," a play on the general purpose online "phishing" ploy. The basic formula is that a scammer creates a fake identity, then tricks you into building up a friendship with this phantom. To explain why you can't simply call the individual or meet in person, the scammer may claim to be in the military, living overseas or is always too busy. Next thing you know, you have surrendered enough personal information to be fleeced. In many cases, to elicit sympathy, the scammer claims to be a single parent with a young child. Once you're hooked, your "sweetheart" will most likely begin asking for money. It's "just a loan," but probably the first of many for which you'll never be paid back. As the BBB warns, if someone is "too hot to be true," cut off all contact.

Healthy Skepticism: It would take millions of words to catalog all the scams that are out there. Don't assume that you'll be targeted only if you spend a lot of time online. Some scams and schemes are low-tech and arrive at your home with a simple knock on your door or a ring of the phone. That said, don't let fear and paranoia run your life! Be wary of threats, but don't assume everyone is out to get you. Keep your skepticism healthy.



www.paoli-umc.com



Instagram - @paoliumc

April Birthdays

- 1 Judy Detweiler
- 3 Sarah Windhorst
- 4 Jenna Dittmer
- 12 Libby Newkirk
- 13 Lily Eubank
- 14 Tim Austin
- 17 Callie Mathers
- 30 Melanie Trinkle

Calendam Aparin 2022 aries

- 3 Dave & Margaret Mathers 7:00 AM Tri Kappa Easter Egg Dipping
- 4 7:00 PM Ad Council
- 7:00 PM Choir Practice
- 7 6:30 PM Lenten Bible Study
- 10 50th Anniversary Celebration event with catered meal following worship service

Secretarial Help Needed at Church

Church has been without a secretary since August 2021. We need the congregation's help to find someone to work 20 hours a week. 8-3 PM M-Thursday

Page 3 April Newsletter 2022

Sunday Schedule 8:15 - Worship 9:00 - Sunday School 10:15 - Worship

Essentials Project

organized by the Becomer's Class *Donations can be dropped off in the Sanctuary

Items Needed:
girls' underwear (large sizes
preferred)
Hanes and/or Fruit of the
Loom
4 pk or 6 pk
Gift bags in which to discreetly
take the items home are
needed

March 2022 Unspoken Prayer Concerns

March 6 8:15 - 3 10:15 - 14

March 13 8:15 - 2 10:15 - 13

March 20 8:15 - 2 10:15 - 14

March 27 8:15 - 2 10:15 - 8

Remember Paoli United Methodist Church in you will. Contact Skip Lambdin, endowment chair, skipl1963@gmail.com or 812-345-3873.

50 th Anniversary Celebration Year April 2022