Fact Sheet
October 2023

PURDUE UNIVERSITY
Extension - Health and Human Sciences

Don't Let Scams Scare You This Halloween

Treat yourself to safety instead of tricks this Halloween and follow these tips!

- Don't believe the caller ID or email address. These can be changed to reflect what the scammer wants you to believe or where they are calling from.
- Hang up! Remember you don't have to be friendly. Be sure that you have signed up for the do not call list. To do this, visit donotcall.gov, or call 888-382-1222 from the phone you want to register.
- Don't pay in advance for something you expect to receive (sweepstakes, loan, grant, etc.).
- Don't deposit money into your account and then pay it back to someone else. You could lose your money if the check doesn't clear.
- While there are people you undoubtedly trust, keep in mind that they could have had their identity stolen. Even those who appear to be your friends and family could be scammers in disguise.

Many people enjoy a little spine-tingling sensation as Halloween approaches, but no one wants to experience the fright of financial fraud!

People reported losing $2.4 million to fraud in 2022, according to the Federal Trade Commission (FTC).

Scam artists are getting smarter and smarter these days with tools like Artificial Intelligence (AI) voice generation. It is important to watch out for scams whether it is online or on your phone!

The following are the scams that continue to happen in 2023, according to the Better Business Bureau. Brush up on these bad guys so you don't become a victim.

Hoosiers are receiving scam text messages and emails falsely claiming shipping-and-delivery issues orders. The fraudulent communications, purportedly from well-known companies such as Amazon, FedEx, the U.S. Postal Service, UPS, and others, have inundated inboxes throughout Indiana. These deceptive emails and texts contain links that allegedly assist recipients in tracking their packages, but in reality, they redirect users to malicious websites designed to compromise their security.

People have reported paying for items online, but never receiving the items that they purchased in the mail. Sellers also have asked for additional money for shipping, or other cash up front. These same tricks are used in advance fee scams and government grant scams. These are called online purchase scams.

Quick Tip: Research and verify online businesses before paying. Also, make sure the site is encrypted – look for the "s" in https.

Social Media Verified Scam
You receive a direct message or email that appears to come directly from Twitter, Instagram, or another social media platform. It states that your verified account has been flagged, and you must re-verify it. You could allegedly lose your verified account badge if you don't respond. For example, some social media users have reported receiving direct messages or emails stating that their blue verified badge has been marked as spam and, if they don't appeal the decision, it will be deleted. The scam message asks you to click on a link or download a form to start the appeal process and re-verify your account. You may download malware onto your laptop or mobile device if you click. This can collect your personal data without your knowledge. If you fill out forms or reply with the requested information, scammers may be able to hack your account or use your personal information to commit identity theft.

Quick Tip: Look for signs of a scam. Poor spelling, bad grammar, pressure to act now, and scare tactics are all red flags that indicate a scam.

Family or Grandparent Scam
This scam often targets seniors. A caller on the phone claims to be a relative and makes up an urgent situation, and plead for help, and money. The scammer could say that they have been arrested or stranded and needs money wired to them immediately. The relative stresses urgency and secrecy, not wanting to upset their "family member." Recognize that anytime someone wants you to make a quick decision, it may be a scam. If this situation happened to you, you could call the relative to check on them to see if they really need your assistance.

Quick Tip: Always check it out before parting with your cash.

What should you do if you are a victim of a scam?

The first thing you need to do is report the potential fraud to the Attorney General at 888-432-9257 and the Better Business Bureau at https://www.bbb.org/scamtracker/reportscam. There will be a series of questions that you will need to fill out. This is a free tool that anyone can use to report suspected crimes. Reporting these crimes will warn others so they can avoid similar cons.

This website also allows you to lookup current scams that are occurring in a database. In 2022 alone, this tool helped consumers avoid losing $21 million to scammers, according to the Better Business Bureau.

Don't forget:

- Don't ever wire money or send a gift card to a stranger.
- Remember, if it sounds too good to be true, it probably is.

References:

BBB Institute for Marketplace Trust. "BBB Scam Tracker." (Data retrieved Sept. 26, 2023) https://www. bbb.org/scamtracker

Federal Trade Commission Protecting America's Consumers. "FTC Imposter Scams." (Data retrieved Sept. 26, 2023) https://www.consumer.ftc.gov/ blog/2019/02/top-frauds-2018

Indiana Attorney General Todd Rokita. "Consumer Protection Division." (Data retrieved Sept. 26, 2023) https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/

Resource: Safe Wise & University of Kentucky Extension - Money Wise - Volume 10 Issue 10