March 2019

How to Spot and Avoid Common Scams

Metropolitan Government of Nashville and Davidson County

Have you ever gotten an email from someone claiming to be royalty? In their email they tell you that they will inherit millions of dollars, but need your money and bank details to get access to that inheritance. You know this email isn't legitimate, so you delete it, yet there are many more scams being perpetrated by criminals that sound more believable and aren't as easy to spot. Learning to identify and avoid these scams is the first step in protecting yourself from these schemes. Senior Citizens are often particularly vulnerable to some of these fraud campaigns.

The world today is full of cybercriminals launching both phishing emails, and the tried and true phone scams that never fell out of fashion. Protecting not only your finances, but also your data from these scams is more important now than ever.

Phone Scams

Scammers who operate by phone can seem legitimate and are typically very persuasive! To draw you in to their scam, they might:

- Sound friendly, call you by your first name, and make small talk to get to know you
- Claim to work for a company or organization you trust such as: a bank, a software or other vendor you use, the police department, or a government agency
- Threaten you with fines or charges that must be paid immediately
- Mention exaggerated or fake prizes, products, or services such as credit and loans, extended car warranties, charitable causes, or computer support
- Ask for login credentials or personal sensitive information
- Request payments to be made using odd methods, like gift cards
- Use prerecorded messages, or robocalls

If you receive a suspicious phone call or robocall, the easiest solution is to hang up. If you experience this at home, then you can block the caller's phone number and register your phone number on the National Do Not Call Registry (https://www.ftc.gov/donotcall).[1]

Email Scams

Phishing emails are convincing and trick many people into providing personal data. These emails tend to be written versions of the scam phone calls described above. Some signs of phishing emails are:

- Imploring you to act immediately, offering something that sounds too good to be true, or asking for personal or financial information[2]
- Emails appearing to be from executive leadership you work with requesting information about you or colleagues that they usually do not request (for example, W2s)
- Unexpected emails appearing to be from people, organizations, or companies you trust that will ask you to click on a link and then disclose personal information.[3] Always hover your mouse over the link to see if it will direct you to a legitimate website
- Typos, vague and general wording, and nonspecific greetings like "Dear customer"[3]

Beware that many scam and phishing emails look legitimate! An email pretending to be a company might contain pictures or text mimicking the company's real emails. If you're unsure about an email you received, there are some steps you can take to protect yourself:

- Do not click links or open attachments in emails you were not expecting[3]
- Do not enter any personal, login, or financial information when prompted by an unsolicited email [3]
- Do not respond to or forward emails you suspect to be a scam[3]
- If in doubt, contact the person or organization the email claims to have been sent by using contact information you find for yourself on their official website[3]

If you get scam phone calls or phishing emails at home, hang up or delete the emails. If you get scam phone calls or phishing emails at work, please contact Metro ITS (615-862-HELP, metroitshelpdesk@nashvillle.gov) so they can help protect others from these scams! Additionally, please educate your parents and grandparents on these scams, as they are becoming only more and more common.

Resources:

1. https://www.consumer.ftc.gov/articles/0076-phone-scams
2. https://www.stopthinkconnect.org/tips-advice/general-tips-and-advice
3. https://staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.