BEWARE OF THESE 6 COMMON WAYS CRIMINALS STEAL FROM YOU

Scams have certainly changed over the years but the goal of the scammer remains the same—to separate you from your hard-earned money. Previously, scams usually came in the form of phone calls and snail mail. Currently, scams can take many forms but most come from phone calls, email, texts, social media and other technology. At times it is very difficult to distinguish between legitimate interactions and those that are illegitimate. The FTC Consumer Sentinel reports that for 2020, 18,739 frauds cases were reported in Oklahoma. That's why, in October 2020, the FTC launched ReportFraud.ftc.gov, a new site for consumers to report fraud and other illegal business practices.

Here are the six most common ways swindlers rob you with scams:

1. **Phone calls:** Smart phones are equipped with caller ID, but crooks still find ways. The best way not to get scammed is to not answer the phone unless you recognize who is calling. This option may not always be practical as you may, for example, be expecting a call about an order from an online retailer or it may be the doctor's answering service confirming your appointment. If you are fairly certain it is an unsolicited call, let it go to voicemail. Scammers are most likely not going to leave a message, as it takes away from their next target. If you do answer and determine it is a solicitation, it still may or may not be a scam. If in doubt, get a call back number and do some research to see if the number is associated with the company. Charitable-sounding organizations may not be legitimate, so use caution. One way to stop or at least slow down unsolicited calls is to block the number on your phone. The process will vary from phone to phone. In any event, never give out personal information unless you initiated the call and know with whom you are communicating. A consumer can also place his or her mobile number on the National Do Not Call Registry to notify marketers that they do not want to get unsolicited telemarketing calls. The Do Not Call Registry accepts registrations from both cell phones and land lines. To register by telephone, call (888) 382-1222 (TTY: (866) 290-4236). You must call from the phone number that you want to register. To register online, visit donotcall.gov. You will be asked to respond to a confirmation email.

2. **Internet:** Most of us have seen inquisitive posts from friends on social media that tell about their high school mascot, where they were born, favorite teacher, first car, etc., and then ask you to share the post and input your answers. Unfortunately, these are the very security questions many companies ask if you need to reset your password. By sharing this personal information, you may have potentially given thieves the information they need to reset your password and take over your on-line banking. Plus, there are multiple crowdfunding sites that request donations for various reasons. If you do not know the organization or person, be cautious. Research before donating money. Additionally, many consumers often accidentally misspell a word or type the wrong web address. Scammers are aware of this fault and purchase domain names with these misspellings. Check to see the site you have has "https:\." This means the site is secured with a Secure Sockets Layer (SSL) Certificate. Secure sites will also display an icon, such as a padlock or an unbroken key, to let consumers know their credit card information is protected. Enable two-step verification if available. Whenever you or someone else logs in to a website with your user name and password from a device that is not recognized you will be sent a code via text message to your phone. The code must be entered in order for anyone to log in. Without the code you cannot log in. Avoid using the local coffee shop or other public Wi-Fi for online purchases. Thieves use Wi-Fi sniffers to capture the information you send on unsecure wireless networks including your credit card and banking information. The sniffer only needs to be within range of the Wi-Fi network to steal your information.

3. **Email:** Phishing has been around for years, but scam artists continue to come up with new angles, so it is wise to be on guard. Phishing generally involves a fake email or other communication that is designed to look like it came from your bank or another financial institution or even a government agency. They may also come from a company making a payment to you. The message urges you to click on a link where you will be told to reveal some confidential financial information. Always check the sender of the email. At first glance the email may look authentic but look at the details of the sender to see who actually sent it. The email domain address will not match the senders. Also look at the spelling of the domain name as it may be very similar but not an exact match to the real company. What can you do? Use an email filter provided by your service provider, software or app to send unwanted mail to your junk mail folder. Never open an attachment unless you are 100 percent positive you know where it came from and even then, be suspicious and make sure the email sounds like the person you think is sending it. Your friend may have been hacked and the scammer is using his or her email account to send you a message.

   The Nigerian prince email scam is a familiar example. However, a new twist on this is emerging. A new version poses as military officers stationed overseas needing someone to talk to or asking for financial help. Scammers will create a fake Facebook page with pictures of an officer they have stolen from that person's actual Facebook page. Never respond to unsolicited email or click on links that are provided.

4. **Apps and software:** There are a number of software and apps available for free. These freebies are also a wonderful way for scammers and others to install malware on your devices or take your information. For instance, why would a flashlight application need access to your contact list? Before installing a new screen saver, background or free game, check to see who developed the application. Is the developer legitimate? Was that app or software

you're investigating actually created by that developer? Look to see what permissions will be granted with this access. Does it seem reasonable for this app?

5. **Text spam:** Plain and simple—spam sent via text message is illegal. There are exceptions for companies for whom you have established a relationship and non-commercial messages such as political surveys and fundraising. Do not reply or click on any links provided since it may install malware on your phone. What you can do? You can register your phone with the National Do Not Call Registry and most major carriers will allow you to report the spam by forwarding the message to 7726 (SPAM) free of charge.

6. **Skimmers:** Credit/debit card skimmers account for more than $350,000 of stolen funds every day. Skimmers are devices that fit over the credit card reader of an ATM, gas pump or any reader that is not watched on a regular basis. The device will be innocuous and difficult to detect. Previously, thieves would need to return to the scene of the crime and retrieve the skimmer with your data recorded. Now, however, many skimmers transmit your stolen information through text messages. (To see good examples of sketchy skimmers, visit krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/.) You need to take a common-sense approach to this scam. If the skimmer does not look right, do not use it. The color may be a little different or stick out more than you think it should. Stay away from machines that are not located in publicly visible and well-lit areas. Your best bet is to go to your financial institution and withdraw your cash with a teller.

We certainly will never be able to rid ourselves of all the scams, phishing and other tricks people use to harm us, but there are certainly steps we can take to reduce our exposure. Install anti-virus protection on your devices and keep them up to date. Always update your operating system with the latest security patches. Never get in a hurry clicking on a link or responding to an email. Check and double check its authenticity. Check the privacy settings on your social media accounts to limit access. Use two-factor authentication if available. Only provide personal information on encrypted websites. Never use public Wi-Fi. Backup your data to an external drive or cloud. That way, if you do need to wipe your device clean due to malware, your personal files will be secure.