Since the start of the year, we have noticed an uptick in notifications from clients who have been preyed upon by scammers via email, text, and telephone. Unfortunately, scamming attempts are on the rise. The Federal Trade Commission recently issued its 2022 report which showed, among other things, that Americans lost $8.8 billion last year alone to scammers. This was a 33% increase over 2021! [i]

We encourage you to make every effort to protect yourself from becoming a scam victim in 2023 and beyond. You must remain vigilant and not let your guard down at any time – even if the person on the other end of the phone, email, or text is pressuring you, rushing you, or threatening you. This is all part of their scam tactics designed to get you to act quickly without thinking through what is really happening. Do not worry about being rude to or offending this person – remember they are most likely trying to take advantage of you! Also, you are your own best and first line of defense against scammers. Do not ever let the scammer gain the upper hand on you.

There are often many red flags and telltale signs that something is a scam – but all too often, we only see them with the benefit of hindsight. Here are some of the most common:

1. **Impersonation of a government agency:** A person reaches out to you via telephone, email, or text and represents themselves to be from a governmental agency such as the IRS, the Social Security Administration, or Medicare/Medicaid. They may threaten you and demand you give them personal information or that you send them money to pay off "penalties and fees". Also, your caller ID may even make it look like the caller really is from a governmental agency. Do not trust your caller ID, as this is easily faked by a scammer. STOP. Do not be tempted to do anything. These calls, emails, and texts are never legitimate. Our government agencies do not operate in this manner. Immediately hang up the phone, delete their text, or block their number. Do not purchase any gift cards to send to them and do not provide any personal or financial information to them.

www.BLBB.com
215.643.9100
Mailing address
P.O. Box 1010, Montgomeryville, PA 18936
Street address
103 Montgomery Avenue, Montgomeryville, PA 18936

2. **Surprise communications:** You are unexpectedly contacted and told you have won a prize, someone in your family/friend circle needs immediate financial assistance, or there is a problem with one of your financial accounts or credit cards. In most instances, the person contacting you creates a sense of urgency and/or threatens you with serious repercussions if you do not act immediately. For example:
    a. they may tell you your grandson was just arrested on spring break in the Bahamas and you must immediately pay his fine or else he will be sent to jail;
    b. they may get your hopes up by announcing you just won a large lottery prize and in order to collect you just need to pay a small fee first; or
    c. they may tell you there is a problem with your credit card or cell phone account and ask you to pay a fee or fine asap or face immediate loss of the use of your card or phone.

3. **Overly Friendly Message from an Unknown individual:** You receive a random text that appears to be directed to you in error asking something innocent, like if your plans to get together are still on, if you have heard from a friend or relative, if you had a nice trip, etc. You feel obligated to let them know they have reached your number in error and a pleasant "conversation" follows. This is not your friend and may be someone trying to get you to let your guard down with a motive of obtaining personal information, such as your name, where you live, if you own a pet, if you did in fact go on a recent trip. Note that much of our personal information can be used to guess passwords to some of our accounts. They may also try to use the personal connection made to create a sense of trust that they will then use to have you send them funds or buy fake financial products. Delete the text, block the number and don't look back.

4. **Manufactured sense of great urgency:** The person who contacts you creates a sense of grave urgency and threatens you with serious consequences if you fail to take immediate action. They will make you feel like you MUST ACT NOW so that you can avoid losing access to your phone, financial accounts, government benefits, or computer. For example, Amazon or Microsoft will not call you about viruses or updates for your computer or your accounts. If you are on the receiving end of an urgent phone call, email, or text, do NOT respond or engage with the caller/sender. Instead go to the legitimate website of the entity that is supposedly reaching out to you and confirm for yourself whether or not your credit card has been hacked or your phone service is about to be severed. Do not click on any links in any unknown texts or emails – even if they appear to be legitimate. Those too are usually scams and the links they include are malicious and not legitimate.

There are several easy ways to protect yourself from scammers:

1. Do not answer unknown/unwanted/unexpected telephone calls, emails, and texts – block them instead.
2. Be extremely wary of any prerecorded or robocall. Do not "press 9 to speak with a representative" and do not provide any personal, financial, or payment information in response to any such call.
3. Do not provide <u>any</u> information – especially personal identifying or financial account information (like your full name, birthdate, Social Security number, passwords, account numbers, etc.) – in response to any unknown or unexpected request.
4. Do not click on any links or call any phone numbers included in any unexpected phone call, email, or text. Those are most likely fake although they will appear to be "real". Instead, if you want to confirm the legitimacy of a call/text/email you receive, go to the known website of the organization or call their known and legitimate telephone number.
5. Do not trust your caller ID.

6. Do not be fooled into thinking you recognize the voice on a call or voicemail – especially when the call is unexpected and involves an urgent demand for money or your personal/financial information. Believe it, or not, some sophisticated scammers now capture another person's voice electronically and then manipulate and use it to trick that person's relatives into thinking a call demanding money is legitimate.
7. Remember, government agencies and legitimate businesses do NOT call, email, or text you demanding personal/financial information or immediate payment for anything.
8. Do not buy any gift cards or prepaid credit cards to give to anyone who demands payment from you in this manner.
9. Resist the desire to please, or be nice to, a potential scammer and do not give in to any sense of urgency or fear they try to develop in you. Recognize those devious tactics for what they really are – deceptive and sinister – and immediately end the conversation.
10. Consider signing up with a reputable fraud protection company that monitors usage of your personal information like your social security number, home address and email.

What if you fall victim of a scammer?

1. Check bank and credit card statements for any unusual activity and report it immediately
2. Call the number on the back of your credit card to question any suspicious charges
3. Report the incident to the Federal Communications Commission
4. Enlist the help of a lawyer if funds or identity need to be recaptured
5. Alert the major credit bureaus (Equifax, Experian and TransUnion)
6. Consider freezing your credit card and bank accounts
7. Cancel your credit card and ask for a new card to be issued

We hope these tips help you protect yourself from scams. As always, if you have any questions or concerns about this information, please reach out to your BLBB Financial Advisor at (215) 643-9100.

[1] https://www.ftc.gov/business-guidance/blog/2023/02/ftc-crunches-2022-numbers-see-where-scammers-continue-crunch-consumers