TOWN OF MANLIUS POLICE DEPARTMENT

IDENTITY THEFT INFORMATIONAL SERIES

SERIES 3 | 06.11.2018

TOPICS


What is a phone Scam?

Phone Scams

Warning signs

Phone Scam Security


Phone Scam Prevention


A look at Series Four

What is a Phone Scam?

Phone scams have been sweeping across the nation. More and more scam artists are coming up with clever ways to dupe unsuspecting citizens out of their personal identifying information. Phone scams range in type and style. Some scams are automated services or robocalls which use the internet to make phone calls. These calls normally are from randomly generated numbers and may appear as a local number. This technique is called "masking" where the scammer uses a computer or similar device to literally mask the true number they are calling from. In most cases this 'masking' makes the number untraceable and calling the number back often leads to out of service dial tones. Some scammers simply call unsuspecting citizens pretending to be a telemarketer, a trusted person or institution. Many mobile phone scams happen over texting. In all these cases the scammers are trying to lure your personal information out of you. This term is often referred to as "Phishing".

Phone Scams

Here is a list of some of the more popular current phone scams sweeping the nation:

- The Imposter: A person poses as a trusted institution and demands money or asks you to verify your information without you first prompting the call. The most notable imposter scams are someone pretending to be from the IRS (internal Revenue Service), a utilities company or a government official.

- The Romantic Interest: A seemingly innocent person poses as a romantic interest at first just wanting to chat and get to know you. This person starts professing their love to you quickly and starts asking for gifts, funds or money.

- Loved one in Danger: A seemingly legitimate law enforcement official or lawyer calls you saying a loved one has been arrested and needs bail money in the form of prepaid credit cards or a wire transfer. Another version of this scam is that your loved one or someone else's loved one has been taken captive and you need to pay a ransom.

- Prize or Vacation: An automated response tells you that you just won some prize or vacation getaway. Once connected you are then told that you must pay out of pocket fees and expenses for a tax of some kind to receive your "free" item or offer.

- Can You Hear Me: A voice does not say a greeting when you answer but instead asks if you can hear them and hangs up after you've responded with a "yes" or "okay." The person then uses your recorded confirmation as authorization for accessing your accounts or opening unauthorized accounts in your name.

- Unsolicited Texts from Institutions: An institution claiming to be your bank or credit card company begins to text you without you prompting a text first. Demanding your PIN (personal identification number) and/or account number to confirm your identity.

- Charitable Causes: Some scammers take advantage of recent disasters, by unlawfully soliciting people for money over the phone. These phony charities demand that donations come in the form of prepaid credit cards, gift cards or wire transfers.

- Tech Support: Someone calls you and tells you that there is something wrong with your computer and they need to remotely access your computer to fix it. This happens without you ever contacting an Information Technology or "I.T." service. The mission of this scam is to gain full access to your computer and all your personal identifying information that may be on it.

To stay up to date on the most recent scams go to: https://www.consumer.ftc.gov/features/scam-alerts

Warning Signs

When you are answering phone calls here are some warning signs you can look out for that will notify you right away if you are dealing with a potential scammer trying to steal your identity:

- Most scammers will try to invoke fear or a need for urgency, regardless of what scam they are trying to pull off. Legitimate companies and trusted institutions will never try to use scare tactics to get you to fork over funds, services or charitable donations. If you feel you are being pressured into making a decision or the caller is rude or abusive, it is most likely a scam. In the case of a loved one in danger' scam that provokes an enormous amount of urgency, take the time to check all the facts and contact that loved one at a trusted number first before making a hasty decision. You can always contact your local police to do a welfare check on a loved one if you cannot get ahold of them and are truly concerned that they may be in danger.

- Companies will never demand payment in the form of prepaid credit cards, gift cards, wire transfer or money order. These forms of payment are accepted most places, but are never demanded as the only form of payment. These forms of payment are the least likely to be able to dispute from their parent companies, and you will most likely not be able to get those funds back.

- The IRS (Internal Revenue Service) will never call you and demand immediate payment. The true IRS will contact you several times by mail before ever trying to contact you by phone, so you will have known in advance of any issues with the IRS. They will not ask for credit or debit card numbers and they will not threaten to bring the police to arrest you. If you get a call from the IRS that involves any of these things, it's a scam. To check out more need to know tips for staying alert on IRS scams, follow the link below: https://www.irs.gov/newsroom/irs-urges-public-to-stay-alert-for-scam-phone-calls

- If a solicitor calls you with a free product or service but requires some form of payment for said product, it's a scam. Remember that if you must pay for a product or service it is not free and is a purchase. If a marketing prize or product seems to good to be true, then it normally is. If a lottery or other prize agency is calling to let you know you've won big, take a moment to ask yourself if you signed up for such a prize. If you never initiated the sweepstakes or lottery, it's a scam. Also, if the lottery or prize agency is requesting that you pay any type of fee or amount due it's a scam. In series two under mail fraud we covered that the Deceptive Mail Prevention and Enforcement Act of 1999, states that a legitimate sweepstakes must provide rules that no purchase is necessary, and a purchase does not improve your chances of winning. This is also true for sweepstakes telemarketing.

- The Federal Trade Commission "Telemarking Sales Rule" (TSR) requires that telemarketers not call you before 8:00am or after 9:00pm. They must also immediately identify the seller or organization that they are calling from and that this is a sales call or a charitable solicitation. They must also disclose all information about the goods or service and the terms of sale. If these rules are not being followed, your telemarketer may be a scammer. If you want to know more about the rules that telemarketers are required to follow, click the link below: https://www.consumer.ftc.gov/articles/0198-telemarketing-sales-rule

- A few warning signs to look out for on your mobile device are simple things like apps randomly crashing, text or calls from unknown numbers. Popup adds on your phone are also a sign that your mobile security may be at risk. Receiving calls from people claiming you just called them may be a sign that your phone number is being used in a scamming process known as "wire cloning". This process is where a scammer is using your number to mask the true number they are calling from.

Phone Scam Security

Using the warning signs above, here are some things you can do if you happen to be in a call with someone who may be a potential scammer. The first thing you can always do is hang up and terminate the call. There is no rule saying you can't hang up on someone especially if they are being pushy or rude to you. If they call back, let your answering machine or voicemail system retrieve the call. Know who you are speaking with, callers should always identify themselves and the organizations that they work for. Even when a caller does provide information on the company, be skeptical. Something as quick as an online search will let you know if their business is legitimate. Consumers can always use the Better Business Bureau or the Yellow Pages to check the legitimacy of an organization. The Better Business Bureau website has the "BBB Scam Tracker™", where you can view current scams by zip code using an interactive map. You can also search scams by keyword or type. Check out their link below. Feel free to tell the person on the other line that you will call them back, and when provided with a call back number, double check it. Quick research before making a hasty decision is another step in helping you protect your identity. Don't ever feel pressured into giving out personal information during a call unless you initiated the call and have checked the validity of the person you are calling.

https://www.bbb.org/scamtracker/us

Phone Scam Prevention

The easiest and simplest solution is to allow your voicemail or answering machine service to pick up the call and let the caller leave a message. Don't answer calls from numbers you don't know and don't trust, even if they appear to have a local area code. This allows you to screen your calls for scammers. Screening is where you can evaluate and asses every call that you receive. This allows you to research calls for legitimacy without being pressured into making a hasty decision. The next step to unwanted calls, is putting yourself on the National Do Not Call Registry from the Federal Trade Commission. You only need to sign up for the National Do Not Call Registry once per phone line for the life of the phone line. Most telemarketers are still calling after thirty-one days of being on the registry then they are most likely a scam. Some calls not included in the registry that you may still receive are legitimate political organizations, charities and telephone surveyors. The FTC takes telemarketers who do not adhere to the National Do Not Call Registry very seriously and you can report them to the FTC. You can also contact your service provider and see if there is a way to block calls for free. For mobile phone users remember to check use of your phone's security features and to update those features regularly.

https://www.donotcall.gov/

A look at Series Four

The most proactive thing you can do to help against scammers of any kind is to help promote awareness of the identity theft problem. Tell your family, friends and co-workers the dangers of giving out their personal identifying information. Stay up to date on the most current scams. This series will attempt to educate individuals on the different types of scams, prevention strategies to protect your identity, warning signs to be on the lookout for and what you can do if you're a victim. Be on the lookout for the fourth installment in the Identity Theft series, "Cyber scams and Security". Where we take a look at cyber scams, computer security and some prevention methods you can do today to start protecting your identity. The Town of Manlius Police Department reminds citizens if they are ever a victim of Identity Theft to call 911.

Town of Manlius Police Department
1 Arkie Albanese Avenue
Manlius, NY 13104
(315) 682-2212

If you are ever a victim of Identity Theft call 911.