Preventing Phone Fraud

Source material taken from:
https://mind4survival.com/phone-fraud-dont-be-a-victim/

Contents

The #1 Thing to do When a Scammer Calls

Relax

The first thing you need to do is relax. Criminals, in this case, the phone scammers bank on the fact that nervous people tend not to be as cautious as people who are relaxed. With that in mind, phone scammers try to make you nervous by adding a sense of urgency to their scam.

So, remember, if someone calls you with what at first sounds to be bad news, relax and avoid getting upset and sucked into the scam. Think about it likes this, if a stranger called you and politely asked for $500, what are the chances you'd give it to them? That's why the phone scammers try to make the call sound urgent, or an emergency.

An excellent way to shift your mindset to help you relax when answering the phone is to accept the fact that any incoming call could be someone committing phone fraud. With that, the likelihood of a call being a scam goes up exponentially if the person on the other end asks you for personally identifiable information, also known as PII.

Personally Identifiable Information (PII)

Often, when asking for your PII, phone scammers will add in that sense of urgency to make you nervous with the hope you'll give up your information. Also, the person committing phone fraud may ask you to confirm some information that they know, as in when a company representative will ask you to provide the last four of your social security number for security reasons. It's always good to remember that it's easy to be manipulated, so you have to pay attention and maintain your situational awareness.

Now, if you accidentally give your PII to the scammer, they can use it for things like opening bank accounts, applying for loans and credit cards, renting property, purchasing cars, etc., in your name.

One easy to play tactic that defeats phone fraud is to hang up and look up the information for the organization the phone scammer said they were calling from. Then, determine if you think the call was legitimate, or not. If you think it was legitimate, call the customer service number for the organization if it was an organization you are familiar with. If not, do some more research and look into it before calling and giving anyone your information.

Nine Defences Against Phone Scammers and Telemarketers

The best way to avoid being scammed by phone fraud, it too not get calls from the phone scammers in the first place. There are many ways you can use to help limit the number of calls that you receive from scammers.

1. Don't Advertise

Be careful about who you give your phone number out to. Once you give your phone number out online or to a company, you run the risk of telemarketers and phone scammers getting a hold of it.

2. Sign-up for Silence

Sign up for the Do Not Call Registry, which you can do by going to www.donotcall.gov.au.

3. Adios Anonymous

Your phone may also have the ability to block anonymous phone calls. If your phone doesn't have the option, give a call to your phone provider, and they may be able to help you.

4. Block the Bums

If you continuously receive calls from the numbers, go ahead and block them. Some phones can block incoming numbers built into the phone itself, while others don't. If your phone can't block numbers, do a Google search, because there are a variety of apps and other services out there that will help block calls.

5. Pay for Silence

Another way to stop calls is to sign up for a third-party service like Nomorobo. Services like Nomorobo uses blacklisting software to identify robocalls and phone fraud calls and block the numbers from calling any of the phones on its network.

6. Can't come to the phone, Please Leave a Message

Practice your situational awareness and check the caller ID when your phone rings. It's straightforward. Your phone rings, (play phone ring), you look at it and see a number you don't recognize. Then, rather than answer it, you let it go to voicemail. Usually, if it's a telemarketer, they'll hang. If it's not a telemarketer, and the person making the call wants to speak with you, they'll leave a message.

7. Punt the Pause

If, after you answer your phone, you hear a silent pause, hang up. A pause after answering is often a sign that the person on the other end is a computer making you a robocall. Sometimes you will hear an odd, electronic 'click' noise, these are usually people calling from a VoIP service like Skype, punt it straight away.

8. Pass on the Push

Should you answer the phone and hear a robocall start, which could be a phone fraud call, hang up. DO NOT push any buttons, even if the recording on the other end tells you to. When you push a button, the electronic tone it sends lets person or computer on the other end know they hit a live number.

9. Dive into the Directory

Once you have avoided a possible robocall, open your browser to Google, or WhitePages.com and enter the number that called you into the search bar. Often, you'll find a robocall number, or a phone fraud number is listed on the internet and may even have some discussion about it so you will be able to increase your situational awareness about the phone number calling you.

Tactics and Strategy to Avoid Being a Phone Fraud Victim

Maximize Your Situational Awareness

It's great to use the defensive measures we went over. However, as we all know, no plan is 100% guaranteed to work. So, you need to be ready in the event you end up on the phone with a scammer. To be prepared, you need to know about as many possible phone scammer tactics as possible. That way, when you hear the phone scammer start their pitch, you can hang up and shut them down.

Yank the Yes

Never, ever, ever say the word "YES" to an unidentified caller. Instead, if you want to be polite, say, "May I ask who's calling?" or, you can simply ask "What do you want?" The trick the phone scammer is trying to pull is to get you to say the word "YES" to a simple question. They want you to say "YES" because they are recording the call and will edit your yes response as an answer, into another recording that you never hear. That recording asks if you agree to accept charges for some random service, or whatever else the can come up with to take your money.

Oops, Wrong Name

Another tactic the phone scammers use is to call and ask if they're talking to some random name. So, for example, you answer the phone and the person on the other end say, "Hi, is this Joe Smith?" Then your response is to answer "no." Next, they sound confused and ask, "Is your number blah-blah-blah" repeating your number to you, remember, since they called you, they have your phone number, you are inclined to saw "yes, that's my number."

Oh, My Headset is a Mess

Along the same lines, phone scammers use the tactic of calling and asking you to hang on for a second while they adjust their headset. Once they supposedly get their headset adjusted, the person or computer calling you then asks "Can you hear me now?" To which many people will innocently respond "YES.".

One Ring Bait and Switch

Phone scammers also like to use a bait and switch type of scam. In this scam, the caller calls from a standard, AUS looking number, and hangs up after one ring. Where the fraud comes in is if you call back to see who called. When you call back, the person on the other end will try to keep you on the phone as long as possible. The reason being, the person on the other end, is in a foreign country.

Smishing

Similar to phishing email scams, where the scammer works to have you click on a link that infects your device with a virus so that they can steal your PII. You combat smishing scammers by never clicking on a link from an unknown source. Even if an unsolicited link comes from somewhere that seems to be legitimate, you should avoid clicking on it. Instead, call the company through a number you have or find. Do not call from the phone number the text came from, and ask if there are any issues, or if they sent you the text.

You've Won!

A super happy person calls, letting you know you've just won something fabulous, like the lottery. After some back and forth, and big congratulations, the person works in that to get the winnings to you; you'll first have to pay the tax on it. Once you do, the bad guy makes off with your "tax" money, and you never see a dime or the trip to the Caribbean the person promised you.

Grandkid Scam

This scam starts off with a call, from a phone that sounds like it has a bad connection. The person on the other end that you can barely make out due to the static says "Grandma/pa, I screwed up and am in serious trouble." Most likely, sometime during this part of the conversation, the scammer, either due to the static or through other means will get you to give up the name of one of your grandkids.

They Got a Name, Now What?

After they get a name, the scammer will pass the phone off to a supposed attorney who is there to help out your sweet grandkid. The lawyer will then tell you that your sweet grandchild is in a heap of trouble and needs money for legal costs to keep them out of jail.

Keep the Lights On

You receive a call from someone claiming to be a representative of a utility company. The person then tells you that your bill is overdue and that your service is going to be turned off. Once this happens, the call usually goes one of two ways. The first way is that the person calling from the utility company tells you he/she can accept payment over the phone to keep your service going. The second method is that the person says they're on the way to cut the power and that you can pay when they arrive to avoid a disruption in service.

Unfortunately, when they show up, their ability to process credit or debit cards just stopped working, but they can take cash to keep your utilities on. Often this scam is played dependent upon the season. So, if it's in the middle of a heat wave, the phone scammer may tell you they have to shut off your power and are sorry that the AC will be off, but again, you can pay, and they'll keep your power on.

Spoofing

Is when someone uses software or a spoofing service like SpoofTel or SpoofCard to make their caller ID look like an official phone number. Looking like a legitimate number, they will then proceed with their scam to try and part you with your money.

The Pop-Up

This scam comes at you through your computer after it's infected with a virus from the scammers. Once infected your computer will lock up and a pop-up window opens. The window has a phone number to call to get your computer repaired. DON'T CALL THE NUMBER! Instead, call a local and reliable computer repair service. Have them fix the computer and, once ready, stop clicking on the websites!

You've Been Google Earthed

This is a scam that uses intimidation. In this case, the scammers hop onto Google Earth and look up your property. Once they find your property, they look for anything that is distinguishing. Then, armed with their new information in an attempt to extort money from you. So, for example, they may notice that you have a red and blue table in the yard. Next, they call you saying that they're going to throw the cool red and blue table through the window unless you pay them.

ATO Scams

Many ATO scams are always going around, especially during tax season. Always remember, the first rule of anti-phone scam club is, the ATO never calls looking for past-due taxes. The ATO will ALWAYS, I repeat ALWAYS, here, I'll repeat it. The ATO will always send you a letter in the mail. They won't text, send carrier drones, text, call, e-mail, drop a telegram, nothing. The ATO will always send a letter informing you of tax debt, or other issues.

So, remember, if anyone from the ATO calls to tell you that you owe money, they are NOT the ATO. If that happens, hang up. Then, if you're worried and want to make sure the ATO didn't call, give them a call. When you're sure you're talking with the ATO, confirm and make yourself feel better. Remember, don't forget about spoofing, when you look at the phone number calling in.

Please Help

Mr. and Mrs. Phone Fraud people love to use charities, disasters, etc., as a reason to separate you from your money. The scammers say they're "XYZ" charity. They're calling asking if you would like to make a small donation to help the people affected by "ABC" disaster. Never give any other PII over the phone to an unknown caller.

Can We Help You?

This is a tactic that phone scammers use where they pretend to be tech support. Their ruse is to call to do an update or fix a possible glitch in your computer. Often, this is the type of scam where the scammers try to get your PII from you. They will often try to make a connection to your computer by asking you to follow a series of instructions.

Never forget, tech support is not going to call you, without you first calling them. If you get an unsolicited call from tech support, hang up, it's a scam.

Five Universal Phone Fraud Prevention Truths

1. You do NOT have to answer your phone.

Regardless of who shows up on your caller ID, there is no mandate that you must answer your phone. You can ignore a phone call or send it to voicemail whenever you choose to.

2. There is no law against hanging up on a phone fraud scammer. I

f you have even the slightest suspicion that someone is a scammer, hang up immediately. Don't engage them.

3. Don't talk to them. Just hang up.

Whenever you suspect a call is from a scammer, block the phone number immediately after the call. If you don't, there's a chance they will continue to call back.

4. If you don't have a mobile phone and instead use a home landline you aren't safe.

Don't think for one second that phone scammers only target mobile phones. Phone scammers target phone numbers and will try to get money or PII from you regardless of whether your device.

5. Do not mess around with the scammers.

Some people like to goof around and talk trash to the phone scammers. Never forget, the people who commit phone fraud are criminals! And, many criminals who are phone scammers are also involved in cybercrime that includes computer hacking. There have been cases where people played games with phone scammers. Once they did, they ended up as the cybercriminals pet project. So again, hang up, go about your day without antagonizing the criminals on the other end of the phone.

Wrap Up

Always remember, that no matter what precautions you take or defensive tactics you use, phone scammers are continually evolving. In today's social media driven society, criminals can research you through any number of other ways. They can find out who your friends are, where you live, what you like to eat, where you work, etc.

Remember, all of those cute pics you post on Facebook? Well, hackers can see them too. So, think about it before you make a post.

Once scammers have your information, your life, friends, etc., they can they can use it to scam you, and others. So, be wary when people you don't know call you, or when you FEEL something isn't right about a call.

Also, remember, when in doubt, hang-up

Fraud Alert Reference Card

Keep me near your phone so you are ready when the phone scammers ring

- Relax any phone call could be a scammer, don't let them get you stressed
- Don't say "YES" when answering the phone, it can be recorded and used against you
- Do say "Hello"
- Don't give out your PII (Personally Identifiable Information)
- You have not won anything
- The ATO/ Microsoft/ Telstra/ any bank, will never call you and demand money, your PII or to update details
- Tech support never calls you
- Don't allow unknowns to connect to your PC
- Say no to Crypto and gift cards
- When in doubt, hang up, find your own contact details and call them

Created by Paul
HobStar Computing Solutions
hobstar@protonmail.com
www.hobstar.io
0401 268 321

Scan to find all the ways to connect with me.

Keep me near your phone so you are ready when the phone scammers ring

- Relax any phone call could be a scammer, don't let them get you stressed
- Don't say "YES" when answering the phone, it can be recorded and used against you
- Do say "Hello"
- Don't give out your PII (Personally Identifiable Information)
- You have not won anything
- The ATO/ Microsoft/ Telstra/ any bank, will never call you and demand money, your PII or to update details
- Tech support never calls you
- Don't allow unknowns to connect to your PC
- Say no to Crypto and gift cards
- When in doubt, hang up, find your own contact details and call them

Created by Paul
HobStar Computing Solutions
hobstar@protonmail.com
www.hobstar.io
0401 268 321

Scan to find all the ways to connect with me.