Call us:
800.545.4442

Email us:
info@towneley.com

Visit us online:
www.towneley.com

NOVEMBER 2021

PROTECT YOURSELF FROM IDENTITY THEFT AND CYBERCRIME (3-PART SERIES)

PART 3: AVOIDING CLEVER TRICKS AND SCAMS

THIS ARTICLE IS THE THIRD in a 3-part series on protecting yourself and your loved ones from identity theft and cybercrime.

- PART 1 outlined some steps you can take to protect your identity.
- PART 2 focused on protecting your computer and online accounts from cybercriminals.
- PART 3 identifies clever tricks and scams to avoid.

As we learned in Parts 1 and 2 of our Cybercrime series, it's more important than ever to shield your personal information and your computer and online presence from nefarious identity thieves who use technology to aid them in their thievery. In this final installment of our series, you will learn of some common scams to be aware of so that you can avoid being taken advantage of by these cybercriminals.

PROTECTING YOURSELF FROM PHONE SCAMS

While the number and types of phone scams are growing every day, here are three of the most common ways that a fraudster will attempt to steal your information over the phone.

They pose as a government official. Using a "spoofed" caller ID (the incoming call appears to be coming from a government agency such as the IRS or the Social Security Administration), the fraudster will give a compelling reason why you must immediately send money or provide personal information, with grave consequences if you don't comply.

They impersonate your grandchild. Aging adults in the U.S. are the most likely group to be targeted by telephone scammers because they ae more likely to have substantial savings, own a home, and have good credit. In a grandparent scam, the imposter, posing as your grandchild, frantically explains that she's in trouble and needs money. Often, these scammers say they are stuck in a foreign country and that you must wire money immediately to get them out.

They 'robocall' you. The dreaded "robocall" isn't just annoying. In many cases, the calls facilitate identity theft. Robocalls are computer-generated telephone calls that often start with a recorded voice of someone posing as a representative from a commonly used company, such as Amazon. If you stay on the line (or call back) to inquire

about the "problem," you will be transferred to a real-life scammer who will try to swindle your personal information and money from you.

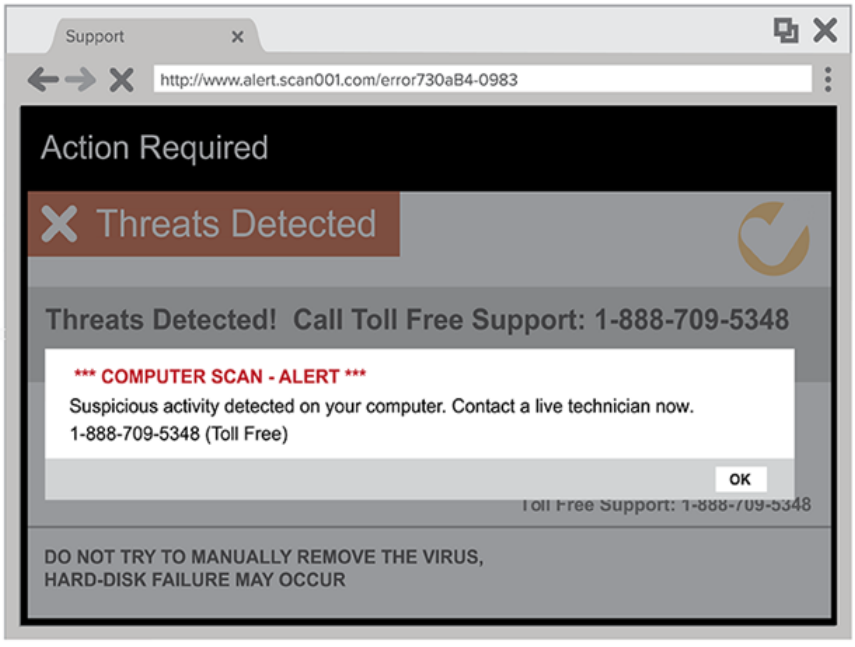
Fortunately, there are some ways to defend yourself from these and other types of phone scams. The best protection is to train yourself to avoid answering calls from numbers you don't recognize. If the contact is necessary and legitimate, the caller will leave a message.

If you do happen to pick up the phone, don't respond to the caller (or the robocaller) asking who you are or asking you to confirm your name. They could record your response and use it to authorize purchases. Also, if the caller or a recording asks you to hit a button to stop getting calls from them, hang up instead – scammers often use this trick to identify potential targets. Also, be cautious about caller ID numbers that appear legitimate and about calls that appear to be from a local number – the scammer could be using software that "spoofs" a local or known phone number. Likewise, it's improbable that a government agency such as the IRS or the SSA will contact you by phone unexpectedly – if a caller is posing as a government official, hang up.

And, if someone is calling posing as your grandchild or another family member who's desperate for money, don't panic – put them on hold, or find another phone, and call your family member on their known phone number – hopefully they'll answer, and you'll know the caller is a scammer. If your loved one doesn't answer, contact other family members or friends to ensure the emergency is fake. But, of course, the charlatans on the other line will tell you not to say anything to anyone because they don't want you to confirm that the person they're posing as is okay.

Protecting Yourself From Tech Support Scams

Tech support scammers lure you with a pop-up window appearing on your computer screen. The message warns of a security issue on your computer and provides a phone number for you to call to get help. If you call, the fraudster will ask you to pay them for tech support to fix a problem that doesn't exist. They may ask you for remote access to your computer, or they may ask you to pay them by gift card because that's virtually impossible to reverse. If you see a pop-up ad on your computer, don't ever call the phone number on the screen. Instead, to remove the pop-up ad safely, start by holding down three keys: CTL + ALT + DEL (Windows) or CMD + Option + Escape (Mac). Next, select the browser window(s) you want to close, then click "End Task" (Windows) or "Force Quit" (Mac).



23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604

Protecting Yourself From Email Extortion Scams

As mentioned in Part 2 of our Cybercrime series, it's essential to safeguard your email account from hackers. Cybercriminals can use your email account as a base for committing multiple types of fraud, including sending malware or malicious links to your contacts who think the email is coming from you. For this reason, don't click on links or attachments in emails from an unknown or suspicious sender, and make sure you "hover over" seemingly familiar senders' email addresses to help ensure it's coming from them.

However, you should also be aware of email extortion scams. Defrauders email you, claiming they have access to your computer or webcam (which they do not have access to), and will release personal information about you and your online habits if you don't pay them. They may even go a step further by proving to you that they know one of your old or recent passwords by including it as part of their message to you.

The fraudsters may have obtained your information via a third-party data breach (as we discussed in Part 1 of our Cybercrime series), not by directly accessing your computer. If you get an email like this, don't engage with them – instead, change your password on the account(s) that correspond to the password they gave you in their email, and then report the incident to the FTC at ReportFraud.ftc.gov.

Protecting Yourself From Ransomware Scams

Ransomware is a form of malicious software that encrypts your computer's files or data so that you can no longer access them. It typically begins with you unsuspectingly opening an email that's addressed to you and clicking on an attachment that seems genuine, such as notice of a pending package delivery. Clicking on the attachment installs the ransomware code on your computer. The ransomware encrypts your files and opens a window on your screen advising you of the attack and demanding you provide a ransom payment in exchange for a decryption key to recover your files and data. To prevent this from happening to you, be very diligent about not downloading attachments from an unknown source, and make sure you back up your files regularly. It's a good idea to use either an external hard drive or a cloud-based service to back up your files. That way, if you fall victim to a ransomware attack, your data can be restored.

Protecting Yourself From Real Estate Scams

According to the FBI's Internet Crime Complaint Center ("IC3"), real estate fraud was responsible for more than $221 million stolen from U.S. victims in 2019. Attempts at real estate wire transfer fraud are prevalent today more than ever, with a recent survey of title insurance professionals reporting that a third of all 2020 real estate and mortgage transactions included some attempt at wire fraud .

It begins with a cybercriminal gaining access to the email accounts of real estate agents, title and escrow companies, lenders, and real estate attorneys and using that access to obtain the details of real estate transactions that are about to close. The criminal, posing as a professional who's somehow related to the transaction, will then email the buyer with fraudulent wire instructions for where to wire the money for the closing. The buyer, who erroneously believes the wire instructions are legitimate, then sends the wire as instructed (unknowingly to the criminal's account). Unfortunately, wire transfers are almost impossible to

23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604

reverse once completed, and it can be tough to recover the funds if the theft is not quickly discovered.

To prevent real estate wire fraud from happening to you the next time you're buying a home, make sure that you know the phone numbers and the voices of all the parties in your real estate transaction. If you've received wire instructions via email, take a moment to call the sender directly using the phone number you already have for them, not the number in the email. Then, verify the wire instructions line by line over the phone before you send your money. Also, if there's been a last-minute change to the wire instructions, be suspicious – wire instructions for escrow, title companies, and lenders rarely change. Finally, listen to your gut – if you feel that something is "off," take the time to investigate it – you're probably right, and there's too much money at stake for you not to address your suspicions. And, if you're not buying a home anytime soon, warn family and friends who are – you may end up saving them from losing thousands of dollars to this despicable crime.

Once you own your home, criminals can also use your identity to forge paperwork that transfers your real estate into their name. While the transfer would not be legitimate because the documents are forged, they could attempt to sell the property before the fraud is discovered. If they are successful, unwinding the mess will undoubtedly result in hours of stress and probably legal fees to get it straightened out. The best defense against this type of fraud is to check with your county to see if they offer automatic notification if there's a record change tied to your property and sign up for that service if available.

As you can see from the examples mentioned (as well as from our earlier Parts 1 and 2 of this series), cybercriminals are always diligently searching for new ways to separate people from their private information and money. Unfortunately, scams have always been a part of history, and today there are more ways than ever for crooks to leverage technology and the information superhighway for successful thievery.

Thankfully, by knowing some common tricks to keep an eye out for, in addition to always trusting your gut (if it feels odd, it probably is), you can keep yourself and your loved ones safe from these devious villains.

23197 La Cadena Drive, Suite 103 | Laguna Hills, CA 92653
Direct: 800.545.4442 | Fax: 949.837.3604