Protect yourself from Scams

by Mike Quinn & Jeff Hensel

May 12, 2022

https://www.usa.gov/common-scams-frauds

Some Scary Scams

- Cold Calls or Pop-up Warnings are NOT legitimate
- Tech Support Scams
- Pay to Unfreeze your Computer
- Remote Access Scams
- IRS Scams
- "Grandpa, it's your Grandson and I'm in trouble!"
- Suspended Xfinity Account ID.
- You've Won! Just Give Me …

How to Identify Scams

If they contact you – it's a scam.

- Don't believe someone just because you are not certain or unknowledgeable.
- Ask someone you know to validate.
- Do a quick internet search.

Start from the position that it is a scam right away.
The number of valid contacts that are just like scams are so few that it is very safe to first start from the point of view that the contact is a scam

Guiding Principles of Protection

- Just hang up on them
- Do NOT give personal information
- Close the window or unplug the computer (even if they say not to)
- Do NOT give remote access to your computer
- Ask someone you trust
- Do a little investigation on the internet
- Make them contact you via mail
- Make them come to you so you can see credentials

Tech Support Scams – I'm from …

- **SCAM!**
- They pretend to be from a well-known company like Microsoft or Apple
- They use lots of technical terms
- They ask you to get on your computer and open some files and those files show there are problems on your computer
- They ask you to give them remote access to your computer
- Trick you into installing some software or convince you to purchase software or a service

https://consumer.ftc.gov/articles/how-spot-avoid-report-tech-support-scams
https://us.norton.com/internetsecurity-online-scams-how-to-recognize-and-avoid-tech-support-scams.html
https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams

Video of an actual scam tech support call:
https://www.youtube.com/watch?v=neQCTEHh8XM

A “scary” popup says your computer is infected and call this number immediately

- **SCAM!**
- Close the window or browser.
- These occur when you are on the internet
- They are simply advertisement windows
- They are NOT your computer giving you are warning unless it is your Anti-Virus program that you installed
  - Or is Windows Defender that comes FREE with Windows 10
- Or a computer voice sounds off

Simply close the window or the browser tab. That’s it!

If there is no ‘x’ in the upper right corner that allows you to close the window, you can “force” close the program by using the Task Manager.
Use Control + Alt + Delete key -> Select Task Manager -> Click on the name of your browser and click on “End Task” in the bottom right corner.

Worst case – shut down your computer and restart (either pull the plug, or hold down the power button for 5-10 seconds)

Remote Access – You Give Someone Control of Your Computer …

- **SCAM!**
- **Don't Do it!**
- Only if you personally know who it is.
- Remote access is physically possible and is a valuable service but only YOU can give permission.
- Don't do it UNLESS you know the person.

https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/remote-access-scams

"This is the IRS and We're Going to Arrest You Unless…"

- **SCAM!**
- Call to demand immediate payment, nor will we call about taxes owed without first having mailed you a bill..
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Threaten to bring in local police or other law-enforcement groups to have you arrested for not paying.
- The IRS only makes initial contact via mail.
- Just hang up!

https://www.irs.gov/newsroom/scam-phone-calls-continue-irs-identifies-five-easy-ways-to-spot-suspicious-calls

https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams
Microsoft does NOT reach out to you in person for any reason.
Virus notifications from from Windows Defender ONLY or your currently installed anti-virus program.

Amazon Scams

- **Don't provide personal information!**
- If you have an Amazon account, they already have your personal information.

https://money.usnews.com/money/personal-finance/spending/articles/2018-08-24/3-amazon-scams-to-avoid
Amazon Scam. Email saying "Your recent order cannot be shipped". Click a link to re-enter your information and credit card.
If you think it's real – right click on the link, choose "copy link" and paste it into your browser or notepad – it WON'T be an amazon.com address.

Brushing scams – you receive an unsolicited package. #1 – you get to keep it, #2 – you will probably find your name used in a glowing review of the product online. Not much you can do about these, and I don't think they're as scary as the media likes to make you think – yes, someone got your name and address from somewhere, but let's be real – your name and address and probably phone number are all over the place, typically.

Fake Social Security Administration Call

- **Martinez, Calif. –** Today, the Contra Costa County District Attorney's Office is issuing a consumer protection scam alert to notify residents of fraudulent phone calls from callers pretending to be from the Social Security Administration. These scammers are claiming you need to pay a fee to unlock your Social Security number as a result of criminal activity. The callers are specifically asking for the individual to confirm their Social Security number.
- Recently, the Federal Trade Commission confirmed an increase activity of these scammers. These telephone scams are attempting to collect personal information from unsuspecting residents.
- The Social Security Administration will never call and ask for your Social Security number.
- To report this fraudulent activity please contact the Social Security Administration at 1-800-772-1213. To file a complaint with the Federal Trade Commission please visit their website.

You will never be asked to pay anything over the phone by an authorized member of the Social Security Administration.
Do not give out your Social Security number or the last four digits to anyone contacting you.
If anyone asks you to pay them with a gift card, cash or a wire transfer, this is evidence of a scam.

Your Grandson calls to say he is in Trouble …

- **SCAM!**
- "Hi grandpa, this is your grandson and I'm in need help."
- The person wants a wire transfer of some type.

Don't volunteer information (i.e. don't give them the name of your grandson/husband/wife/son, etc)
https://www.cnbc.com/2018/06/12/you-think-its-your-friend-calling-but-its-actually-this-growing-phone-scam.html

You Win! We Just Need Some Information …

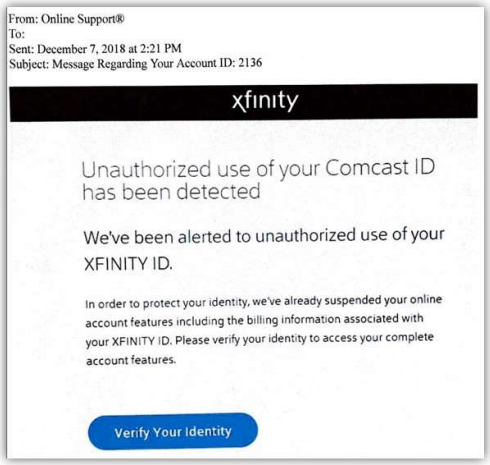
- Once the victim has handed over remote control of their computer, the fraudster will tell the victim that they may be entitled to compensation, or put them through to a supervisor who will appear to make an offer of compensation.
- The scammer will say that they are sending the money and ask the victim to log into their bank account to check that it has arrived.
- But the fraudsters will put up a fake screen to make it appear that the money has arrived. Meanwhile they will be working away in the background to empty your bank account.

http://home.bt.com/tech-gadgets/computing/security/beware-the-new-breed-of-computer-takeover-scams-11364015789542

There are also scams where you win a large sum of money but need to pay the taxes up front……

Xfinity Email – Unauthorized Use of Your Comcast ID has been detected

- **SCAM!**
- Your account has been suspended including billing
- Please Verify your identity


From: Online Support®
To:
Sent: December 7, 2018 at 2:21 PM
Subject: Message Regarding Your Account ID: 2136

xfinity

Unauthorized use of your Comcast ID has been detected

We've been alerted to unauthorized use of your XFINITY ID.

In order to protect your identity, we've already suspended your online account features including the billing information associated with your XFINITY ID. Please verify your identity to access your complete account features.

Verify Your Identity

Total Scam – no need to respond until you lose your internet or TV – then call comcast directly!
This is an example where going to a trusted source (as much as Comcast can be trusted, anyway) – call Comcast directly and see if there's a problem.
Use a number you look up on your own, not one provided in the email.

Also, you can right click on the "Verify Your Identity" and copy the link address – you will see it does not go to a Comcast/Xfinity website.
Sometimes scammers get clever and try to fool you with something like https://comc.ast.com/comcast_verification – don't fall for it – the domain here is "ast.com", which is not Comcast/Xfinity.


STOP
DON'T BE THE VICTIM OF A GIFT CARD SCAM!
For your protection:
• Is someone calling claiming to be a family member in trouble?
• Are you being asked to purchase large sums of gift cards?
• Is someone claiming to be the IRS?
• Are you being pressured to buy gift cards to pay your taxes?
Remember:
• Gift cards cannot be used to pay for legal fees or bail.
• Gift cards cannot be used to pay taxes OR to fix computer viruses.
• Do not share card numbers or PINS with anyone.
• Do not get scammed. Report any of the above to local authorities.

Latest Scams

- Online friend
- DMV “help” – dmv.com
- Found money that belongs to you
- “virtual kidnapping”
- Fake online dog breeders
- Broker cold calls
- Family fraud/abuse

Freeze your Credit

- https://www.nerdwallet.com/article/finance/how-to-freeze-credit
- You can call or do this online
- Make sure you save the code they give you to unfreeze your credit

USA.gov says...

The US Government warns of many scans. Just say NO!

- Find information on common scams and frauds that can happen to you.

https://www.usa.gov/common-scams-frauds

Summary – what to do

- Assume it's a scam
- Hang up
  - Even better, don't answer numbers you don't know
- Close the window, popup, or application
- Do not give personal information
- Do not give remote access
- Never use gift cards, cryptocurrency, Zelle, Venmo (or similar) or wire transfers to solve issues – this should be an immediate red flag
- Always type the url yourself and insure it's from who you think it is (at least if you click on it, verify that where you go is where you expect, although at this point you may have been given a virus).

Quiz (Text)

- Chase Fraud: We declined $10000.000 with card ending in 213 at GOFNDME *HELP SUPPORT. Was this you? Reply YES or NO

This is legitimate. However, even if it's not – answering YES or NO does not give the texter any information that matters.

Quiz (email)

- From TrustWallet notifications@sg.graphy.com

TrustWallet requires all users to verify their wallets in order to comply with KYC regulations this must be done before 14/05/2022 as a regulated financial services company, we are required to verify all wallets on our platform.

We require all customers to verify their wallets to continue using our service.

What if I don't complete the wallet verification ?

Verify your wallet

If you don't verify your wallet,your wallet will be restricted and your assets will be frozen.

Best, TrustWallet Support

For further assistance with this issue,please contact our support team here

Extra info – if you hover over “Verify your wallet”, the email client shows https://oyoshop.easy.co

Definitly a scam – the “from” address, and the “Verify your wallet” address are not from TrustWallet.

Quiz (Text)

- Wells Fargo: We have detected unusual activity in your account, and have put your account on hold. Please go to https://wlsfrgo.com/verification in order to remove the hold from your account.

Scam – wellsfargo.com is Wells Fargo's legitimate internet address. "wlsfrgo.com" is an attempt to fool you.

My Favorite (email)

From Cooke, Matthew MCOOKE@spellman.com

CREDIT CARD PAYMENT INVOICE
Bill To
Walmart Customer
Invoice # 419373570

$874.90
Payment Terms Debit/Credit

Amount Due $874.90
Issue Date May 09 2022

If you dont recognise this order please call immediately at +1-855-533-1430.

Product/Service-Name: Iphone 13 Pro Max 1tb
Thankyou For Making Your Purchase From Walmart.
Your Order Id Is 678368.
Subtotal $874.90
Tax
Misc
Amount Due $874.90
Note: This is an Auto-generated message please call us for any query or to cancel this order.
Customer Support: +1-855-533-1430

Scam- Clearly not from Wallmart – Does not know your name (“Walmart customer”). It’s an attempt to scare you into thinking someone ordered a bunch of stuff on your credit card.
Notice that it doesn’t even give the last 4 digits of the credit card. Googling the phone number does not yield “Walmart”, either.