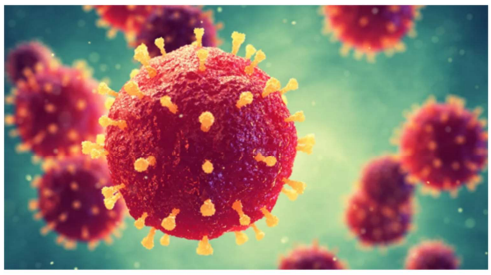
Viruses, Phishing, and Scams, Oh My



by Mike Quinn

March 9, 2023

Types of Threats

- **Malware**
  - Virus
  - Worm
  - RootKit
  - Adware
  - Trojans
  - Bots
  - Ransomware
  - SpyWare
- **Scams**
  - Phishing

Malware = Malicious Software
Virus – attaches to something on the host. Spreads by some action of yours (clicking a link in an email, opening an unknown file or document).
Worm – similar to viruses, but don't need your action to spread.
Rootkit – software installed on your computer that gives an outside party access to everything on your computer. They hide at the lowest levels of your operating system, and are very difficult to get rid of
Adware – Type of virus or worm that puts ads up on your computer
Trojans – a way to sneak one of the other threats onto your machine – it looks like legitimate software, but also infects you with something else
Bots – self-propagating malware that uses your machine to infect other hosts, then do whatever else they are designed to do (relay Spam, open backdoors on your machines, launch DOS attacks, log keystrokes, etc).
Spyware – software installed on your machine to spy on you – gets keystrokes, sees web visits, etc…. Can be installed by almost any of the other types of threats.
Ransomware – software that encrypts all of your files, and requires you to send them money to get the key to unencrypt your files.

Scams: This is a more psychological attempt to get information and/or money out of you. There are thousands of types of scams (dating/romance, charities, employment, etc)

Phishing: A scam where the scammer attempts to get information out of you via email and/or phone calls by pretending to be someone or something that you know.

Malware

- Most viruses infect by you visiting a “bad” website, clicking a link in an email, or downloading an attachment in an email.
- Scammers can also get you to download viruses by using one of the “tech support scams”

So, obviously, don’t visit “bad” websites, or click links in emails, or download attachments in emails. This should stop most viruses from getting to you.

Tech support scams are either calls from “Microsoft” or “Apple” (not really, but they pretend), telling you you have a problem and they need to remote into your machine. Then they place their viruses on your machine when it happens.

They also happen if you go onto a website that will pop up “Virus alerts, please call Microsoft at XXX-XXX-XXXX” – when you do they’ll do the same as above. These pop-ups are NEVER legitimate.

Malware "Whys"

- Using your computer resources
  - Network for BotNet attacks, phishing your friends (by using your contact list)
  - Compute resource to mine Crypto
- Bombard you with ads
- Get bank account info (keyloggers)
- Convince you to call bogus tech support

Some of these uses are "multi-stage". You might get a simple malware that puts up a dialog box that your computer has a virus and to call Microsoft tech support at this number. When you call the number, they convince you to let them to remote access to your computer. If you let them, they can put a much more sophisticated virus on your computer….

Protecting against Malware

- Bitdefender is a highly rated antivirus for Mac or PC
- Windows Security (aka Defender) is pretty good for Windows
- Malwarebytes is great for what the antivirus miss – it will stop you from visiting a bad website, and is a great complement to the antivirus software
- Use a password manager

So, obviously, don't visit "bad" websites, or click links in emails, or download attachments in emails. This should stop most viruses from getting to you.

Highly recommend getting the paid version of Malwarebytes. It will keep you from getting Malware installed, whereas the non-paid version just detects it after it's already installed. You really want antivirus and anti-malware programs that work in the background keeping you safe, not just detecting the problem after the fact.

Quite often, Malware and Viruses are difficult to remove from your computer. I know if you call us to help you with a virus or malware issue, we usually won't do it. It's extremely time consuming, and often you must just reinstall your operating system, which takes quite a while. Geek Squad is probably the way to go for this case.

It's best just not to get a virus or malware in the first place.

Guiding Principles of Malware Protection

- Use real-time Antivirus and anti-Malware software.
- Never click on a link where you're not sure of the source.
- Emails can be spoofed. Be wary even of email from friends if they have links in them.
- Never provide remote access to your computer, unless you're dealing with a known tech support person.
- Keep your important documents backed up somewhere so that if you ever get ransomware, you don't care.
- If your computer acts weird, close your browser (Chrome, Firefox, Edge, etc) and reboot your computer.

They'll try to gain your trust by looking like someone you know, a friend, a company you know, etc…

They may send you to a website to "verify"yourself. It may look genuine, but you need to make sure it's the real deal.

Emotionally, fear is the easiest to prey on – safety of a loved one, fear of being jailed, even fear of missing out (FOMO) can be used

If they create a sense of urgency, it will keep you from thinking too hard about the situation.

It's a Scam if:

- They contacted you
- There's urgency involved
- They ask for personal information
- If you're asking, "is this a scam?"
- They tell you to keep something secret from others
- You're supposed to purchase gift cards or wire money
- It sounds too good to be true

Gift cards and wiring money are the number one thing scammers go for because they're untraceable and cannot be stopped. Once you've given someone a gift card number or a wire transfer, the money is gone….

If a phone call is important – they'll leave a message (make sure you keep your inbox clear, however).

I once got an email from my next-door neighbor claiming she was sick and needed to get a birthday gift for her nephew. She wanted me to get a Nike gift card and she would reimburse me later.
I emailed her back and asked why her "reply-to" email was different than the email she sent from, and let her know that she could buy Nike gift cards online.
I actually thought about doing it, but finally went next door and ultimately found out that she was at the exercise class in the clubhouse, not home sick in bed. Clearly, her contact list had been stolen via malware of some kind. Later found out that several of her other friends had gotten the email too.

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

This checks all the boxes – it gets you to call a support number, where they will verify your information to "cancel" the order.
It preys on your fear that you've been charged for something you actually didn't buy.

But if you think about it for 2 seconds, you're protected from fraud by your credit card company. Also, just go log onto your credit card account and see if the charge actually hit your account (hint: it didn't). Also, why is this from MCOOKE@spellman.com – shouldn't it be somedepartmentorperson@walmart.com. Also – they "used" your credit card, but don't know your name – just "Walmart Customer".

Lastly, you've bought stuff from Walmart before, right? Did they EVER send you an email like this?

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

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.

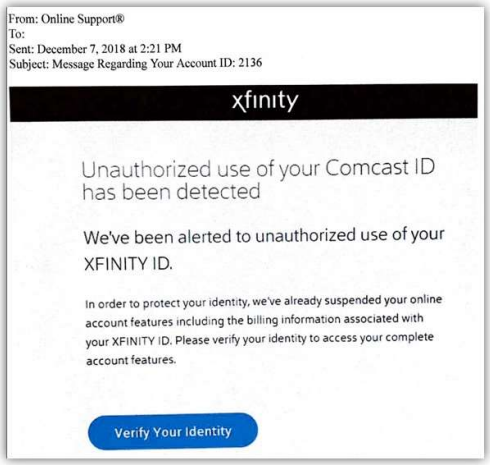
Your Grandson calls to say he is in Trouble …

- **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

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.

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
- Double-check information in an independent manner…
- NEVER be in a hurry to respond

If your grandkid is in jail in Mexico – talk to the parents and see where he really is, or if they have a phone, call them directly. If you want to be really bad, tell the person calling that it's probably good for them to sit in jail for a bit, and see what they do – they'll double-down on trying to get money out of you.

Check with your bank or broker or dealer by using their app or website directly.

Quite often, in an email, you can see where a link is really going by hovering over it (it normally shows where it's going at the bottom of the email window). If it doesn't look right, it's a bogus email.

Turn on "show reply-to" in your email client. Often, an email is "from" a legitimate looking address, but the Reply-To address is totally bogus.

The Smartphone Problem

- If you have a pin code on your smartphone AND you save passwords with the built-in password saving (browser saving or Apple Keychain) you are at risk.
  - If someone gets your pin code, they can get your passwords, change your google or apple passwords, use your bank apps, etc.
- **Solutions**
  - Don't use a pin code
    - Problem on iPhone because Apple requires a pin code if you want to use Apple Pay
  - Don't let keychain or browsers save passwords – use a password manager.
  - Use Face ID or Touch ID when in public – don't enter passcodes
  - Use AlphaNumeric passcodes (harder for someone to see what you're typing)
  - Insure no one can see you enter your passcode when you enter it.

Some Useful Anti-Scam tips

- Shred documents with account information.
- Don't post on public social media when you're away from home
- Never be rushed into a decision
- Gift cards are NEVER the answer to a problem. Neither is Zelle, Venmo, or Cash App.
- Freeze your credit

You don't need to worry about phone numbers or addresses. That information is almost surely already available on the web.

If you're on vacation, it's ok to make posts that are ONLY visible to your friends, but NEVER do a public post indicating that you are away from home.

Forcing you to make a fast decision is one of the hallmarks of a scam. It's to keep you from logically thinking about the problem. Salesmen use this technique as well. One of the reasons for the 3-day recission rules on a lot of sales situations.

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

Thanks for attending

If you have any questions, or would like to see some specific apps or app types demonstrated, please email

mike@mquinn.org

computerclub.summerset2.org