Venture Out at Mesa
— AN ACTIVE ADULT COMMUNITY —

SCAMS
Be Informed

Presented by:
Nephi Williams
CISSP, CISA
VO Resident and Electronics Club Member
Dave Halver
President of Safety & Security Committee

Agenda

- Phishing, Smishing & Vishing
- Malware – Malicious Applications
- Identity Theft
- Internet Scams – Malicious Web sites, Online shopping, Investment, Romance & Tech Support
- How to recognize a scam
- What To Do If You've Been Scammed
- Questions and Answers
- Contact information

Phishing, Smishing, & Vishing

Phishing is when a bad actor (scammer) uses an **email** to **entice the victim to provide personal information** (i.e. credit card information) or to install malicious code on the victim's desktop, laptop or tablet.

Smishing is when a bad actor (scammer) uses **a text message (SMS)** to entice the victim to provide personal information (i.e. credit card information) or to install malicious code on the victim's phone.

Vishing is when a bad actor (scammer) uses a **phone call** to entice the victim to provide personal information (i.e., credit card or bank account).

Phishing – What to look for!

Graphic by Freepik.com

- **Sense of Urgency** – *Bad Actors will use* ***scare tactics*** *to make the victim respond without thinking. (i.e. Your power is going to be shut off, your order won't be delivered, you prize will given to someone else.)*
- **Email Verification** – *Who really sent the email, Bad Actors try to make you think they are a* ***Known Brand****. But in fact, are not even close when you hover of the sent from information.*
- **Misspelled Words or Poor Grammer** – *Bank of Annerica can look like Bank of America when you look at it on a phone or small screen.*
- **Not addressed to you** – *No title or name in the body that would suggest it was meant only for you.*
- **Links** – *The words that appear are legit, but when you hover of the link, you see that is a completely different address.*
- **Attachments** – *Zip files, PDF files, etc. that are not expected.*

Smishing – What to look for!

Graphic from Freepik.com

- **Sense of Urgency** *(overdue, account no longer valid)*
- **No number, unknown phone number, foreign #, or spoofed number** *(# appears to be legit, but is not)*
- **Request for information** *(personal information, credit card, etc.)*
- **A link to a website** (most likely malicious)

Vishing – What to listen for!

Graphic from Freepik.com

- **Since of Urgency** – You are going to be fined, cut-off, arrested.
- **An Authority Impersonation** – Police, IRS, Fire Department
- **Reference to a family member or friend** – Your daughter, grandson, Bettie Joe
- **A family member in need** (Grandparent Emergency Calls – I am traveling and have lost me travelers checks, I need you to wire me some funds.)
- **An offer for a Free Estimate -** Painting, siding, new windows
- **A Software Vendor or Tech Support Call** – "This is Microsoft and we have identified an issue with your Windows computer. We need to help you correct the problem."

Robocalls & how to minimize them

- To minimize robocalls, you should register on the **DO NOT CALL list** (donotcall.gov)
- Answer hello once, **if no response** – hang up!
- **If asked, is this "Your Name"**, do not respond with "yes", but respond "who is calling".
- **Silence Unknown Callers:** Use smart phone settings (iPhone: "Silence Unknown Callers"; Android: "Spam and Call Screen" to send unknow numbers directly to voicemail.
- **Block Specified Numbers:** Use your device's built-in block feature for numbers that repeatedly call.
- If so inclined, **file a complaint** with the FTC at reportfraud.ftc.gov or the FCC at consumercomplaints.fcc.gov to help law enforcement.

Viruses and Malware

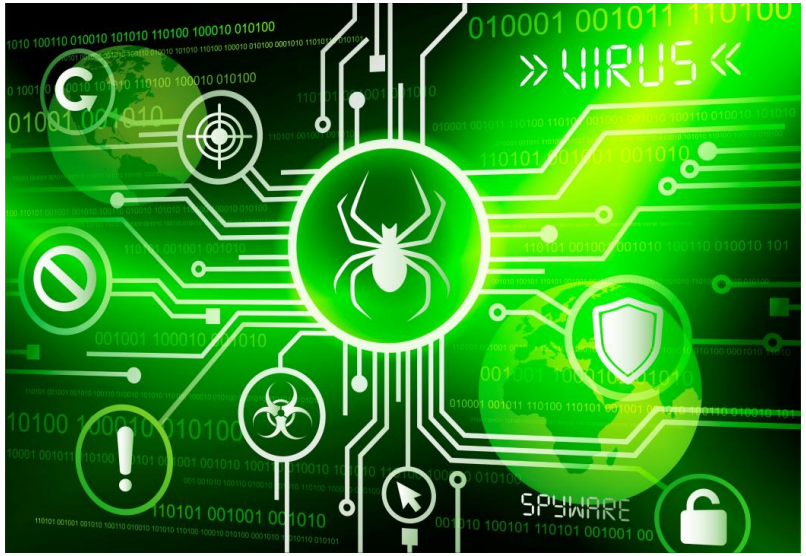


Image by rawpixel.com on Freepik

Virus infections can come from many sources:

- **Malicious websites** - Use of a good browser extension/add-in can help identify potential malicious websites – i.e. Malwarebytes, Bitdefender)
- **An unexpected email attachment** (Photo, Word/Excel, PDF, Zip file)
- **A text message link** – Link that can appear legit but goes to a malicious site where a virus or malware is sent to your device.
- **Social Media link** – Hey Patty, check out this photo, recipe, document, etc.
- **Phone Notification** – Your phone has virus, click here to install an antivirus application to remove the virus

Identity Theft

Malicious Actors use information from:

- **Social Media** (Personal information you've entered or shared)
- **Data Breaches** (Information from the vendor that you have shared to do business)
- **Social Engineered Phone Calls** (Information that you may have given over the phone)
- **Public Records** (Birthdates, Phone #'s, Home Address, etc.)

They use this information to:

- Impersonate the victim
  - Obtain a credit card in the victim's name
  - Trick a victim's friend or relative to buy tickets that don't exist, send funds, open malicious links, or provide personal information about the victim)
- Compromise the victim's account(s) (Bank, Email, Social Media, etc.)

Micro-Deposit Scams

Micro-deposits are small amounts of money – generally under $1 – that are transferred from one account to another.

But how micro-deposit scammers operate is by linking online accounts with strings of random numbers, just hoping to get a valid bank account.

When a deposit is verified from a bank account, the fraudsters will use information about the account holder to withdraw funds from their account.

The best way to combat this type of fraud is to monitor your account regularly. If you notice a micro-deposit, DO NOT verify it if you didn't initiate it and DO NOT click on any links that are embedded in a verification request message or download any attachments in a verification email.
If you've been the victim or a target of a micro-deposit scam, contact your bank to ensure it won't happen again. And then contact the Federal Trade Commission at https://reportfraud.ftc.gov/.

Internet, Social Media, Tech Support Scams!

- **Online Shopping** – If it looks too good to be true, it probably a scam. (Cheap knock-off, Used, Non-functioning,
- **Investments** – Again, if it looks too good to be true, it is probably a scam to get your money.
- **Romance** – Someone befriends you on Social Media. Their picture indicates that they are young beautiful young woman or handsome young man. They are really scammers playing on your loneliness and trick you into sending money, gift cards, etc.
- **Tech Support** – When you need technical support, go to a trusted source, like Best Buy (Geek Squad). Don't Google Support, there are many tech support scamming sites, where the individual on the other end will want to remotely access your device and can install malware. Tech Support doesn't initiate support calls!

SIM Swap or Jacking Fraud!

SIM Swap Fraud is when a bad actor tricks your mobile provider into transferring your phone # to a SIM card they control, thus cutting off your phone service and gain control any accounts linked to your number.

How to avoid or become immediately aware of the swamp or jacking:

- Add a SIM lock and other account passcodes. Most **Apple** and **Android** devices have setup instructions available.
- Enable a “port freeze” or similar feature. This is done through your carrier.
- Setup alerts for account changes – Check to see if you carrier has an email or text alert when you account changes.

Popular Scams that are use against Seniors

- **Grandparent Emergency Calls** – Urgency, scare tactic, request for money, gift cards, etc.
- **Fake Utility Workers** – Some one shows up at your front door saying that they need to enter your home to address a utility issue (i.e. water leak, telephone line issue, gas leak, etc.) – Sense of Urgency
- **Free Estimate** – We are in the neighborhood, and we would like to give you a free estimate on installing pavers, windows, window blinds cleaning, window washing.
- **Fake Checks** – You have won the Publisher's Clearing House Sweepstakes. Just deposit this check. Verify before depositing an unexpected check.

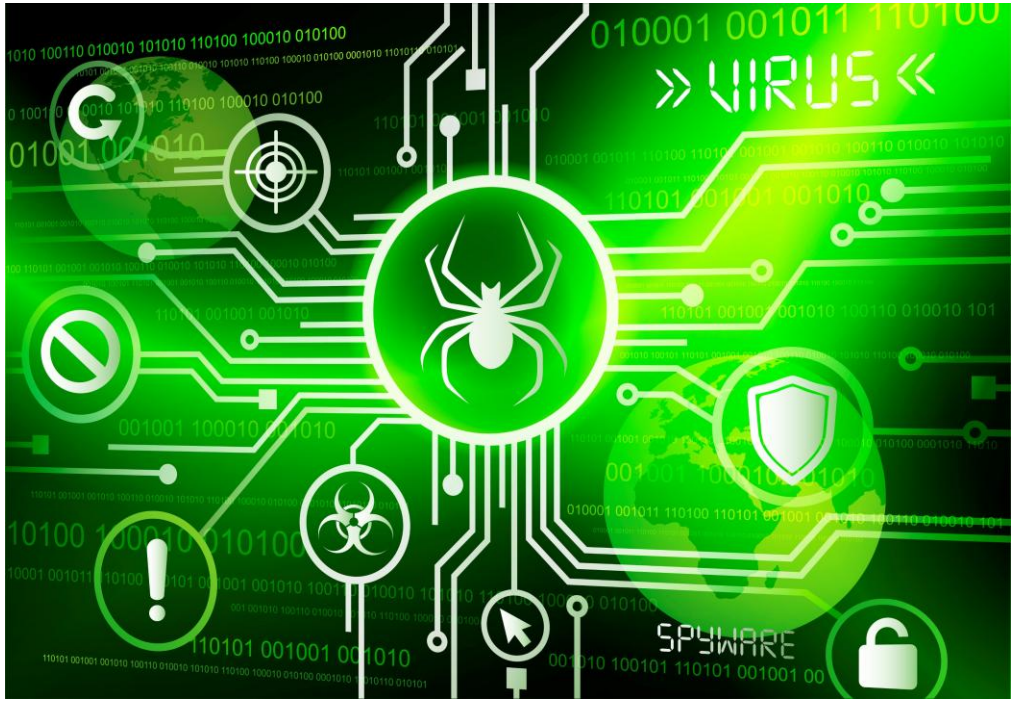
What To Do If You've Been Scammed!

- **Report it immediately to Local Law Enforcement**
  - Local Law Enforcement will assist you in determining next steps (i.e. which other government agency need to be contacted, etc.)
- If you **suspect a virus on your phone**, take your phone into your carrier's local office.

References:

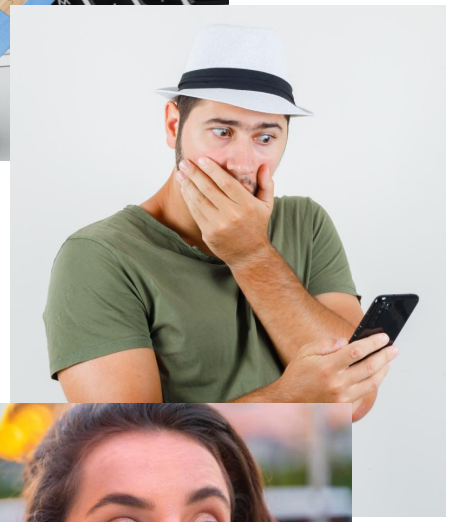
Mesa Police Department -
https://www.mesaaz.gov/Public-Safety/Mesa-Police
Non-Emergency Phone #: 480-644-2211

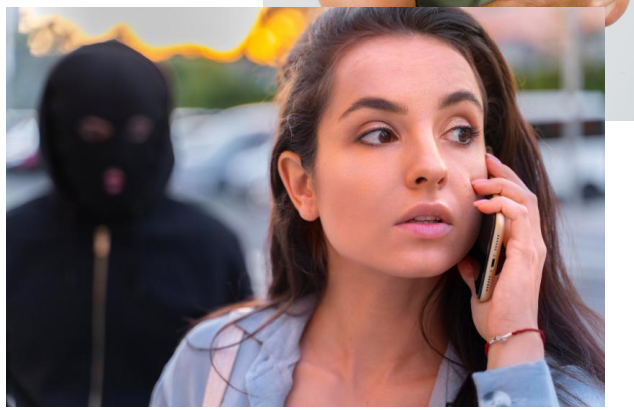
What To Do If You think your computer or phone has been compromised!



- If you think you have a **virus or that a malicious application** has been installed, you should seek professional help at a Legitimate Store . *(i.e. Geek Squad)*
- If you suspect a virus on your **phone**, take your phone into **your carrier's local office**.

Summary





Phishing, Smishing, Vishing

Don't click on any attachment, *unless you are expecting it. Even then, use an antivirus application to scan it. Your friend or family member's computer or device may have been compromised.*

If in doubt about an email, *contact the sender directly (not from contact information in the email, but from your contact list or vendor's phone number) to confirm the email's legitimacy.*

Block any suspicious text messages – *You can always unblock a phone number, if you determine it to be legit.*

Install an antivirus application – *Microsoft Defender is a decent Antivirus, but you can use a site like VirusTotal.com to check a file before downloading or opening it.*

Summary (Continued)

Phishing, Smishing, Vishing

Turn off Auto Download of Attachments

Key Email Clients:

Gmail (Mobile): Open menu > Settings > Select Account > Scroll to Data Usage > Uncheck "Download attachments".
Gmail (Desktop): Settings gear > See All Settings > General > Images > Select "Ask before displaying external images".
Apple Mail (Mac): Mail > Settings/Preferences > Viewing > Uncheck "Load remote content in messages".
Outlook (Classic): File > Options > Trust Center > Trust Center Settings > Check "Don't download pictures automatically".

By turning these off, you reduce the amount of data used on your phone and you aren't confirming to the sender that they have a legitimate email address. You can always select "Load" to see the remote content".

Summary (Continued)

In a Nutshell...Don't Be a Victim!

- If it's **too good to be true**, it's probably is a scam!
- **NO company will ever accept gift cards as payment!**
- Foreign lotteries are illegal. **You didn't play and you didn't win!**
- If you are looking to buy or sell a house, **use a licensed realtor**.
- **Don't use your Debit card where it will leave your hands** into the hands of someone else.
- **If your computer has a virus, take it to a legitimate store**. To test it, turn it off for a few minutes. If the message continues to appear, take it in. **NEVER pay on-line for someone to remotely fix your computer.**
- **Grandparents - your grandchildren are all safe and if you have any doubt, call them**. As a courtesy to their parents, let the parents know about the phone call. Don't get scared and start wiring money.
- **Don't ever wire or send money to someone you don't know.**
- **Don't get manipulated or scared into thinking the police or anyone else will arrest you** if you don't pay for something. You will not be arrested for non-payment. If in doubt, ask a friend or relative to help you
- **If you want to buy something on-line, like tickets to an event, or items, make sure it's a legitimate company**, not one found on a search engine site because the cost is less. Anyone can create a website.
- **If you receive a check you did not expect, don't cash it**, unless you read the small print! Take it to the bank if in doubt and NEVER write a check to cover a discrepancy that was not your fault!

Summary (Continued)

In a Nutshell...Don't Be a Victim!

- **NEVER give out your bank account, social security, or credit/debit card** information unless YOU made the initial contact and know who is receiving that information.
- **NEVER send gift cards as payment!**

*Just for good measure, if you are **requested to send money to someone you don't know** (even if it is a company you are used to dealing with) please call your crime prevention officer. We will help you verify if it is legitimate or not.*
On a side note, if you have a friend or relative who is lonely, they may very easily be targeted and fall for these scams. Many of our victims had no one to confer with or run it by, and reacted quickly. Please touch base with them on a regular basis. This problem affects ALL ages. Many of our victims are in their 20's, 30's, and 40's!

For more information, or for a group presentation, please contact your crime prevention officer.

Info is from the Mesa Police Department's website.

Reference Sites

Identity Theft and Online Security - https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security

Canadian Centre for Cyber Security - https://cyber.gc.ca/en

How to Recognize and Avoid Phishing Scams - https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

How to Spot, Avoid, and Report Tech Support Scams - https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

Beware of Micro-Deposit Scams - https://rcbbank.bank/learn-beware-of-micro-deposit-scams/

Stop Unwanted Robocalls and Texts - https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

Charity Navigator - https://www.charitynavigator.org/

AARP Scam & Fraud Guidance - https://www.aarp.org/money/scams-fraud/

What To Know About Romance Scams - https://consumer.ftc.gov/articles/what-know-about-romance-scams

Malwarebytes Browser Guard - https://www.malwarebytes.com/browserguard

Bitdefender Traffic Light - https://www.bitdefender.com/en-us/consumer/trafficlight

Reference Sites

Test a site or application before you install it - https://www.virustotal.com/gui/home/upload

Have I been Pwned? - https://haveibeenpwned.com/

Malwarebytes - https://www.malwarebytes.com/

Norton's Power Eraser (only valid thu 4/30/26) - https://support.norton.com/sp/static/external/tools/npe.html?inid=nortoncom-free-online-tools_card32_support

How to Prevent SIM Swapping - https://www.aura.com/learn/how-to-prevent-sim-swapping

Con Games, Fraud Schemes & Sweepstakes Scams - https://www.mesaaz.gov/files/assets/public/v/1/publicsafety/police/publications/consfrauds.pdf

Scams - https://www.mesaaz.gov/Public-Safety/Mesa-Police/Crime-Safety/Crime-Prevention-Safety-Publications/Scams

Questions?

My Contact Information

- Email – hnephiwill@pm.me
- Phone – 206-931-4283 (Texting is fine)