Cyber Security Safety:
Recognizing and Avoiding Phishing & Hacking Attempts

Glen Maxson

Center for Learning in Retirement

Fall 2022

Who Am I

- Penn State grad 1977
- Information Technology professional (1978-2011)
- Retired from Intel 2011
- Teach Tech - Del Val CLR and Temple OLLI (http://seniortechadvisor.com/)
- Build electric bikes as a hobby (http://ratelectricbike.com/)
- E-bike advocate

Bucks County Consumer Protection

Michael D. Bannon, Director

Consumer Protection/Weights & Measures

Phone: 215-348-6060

Fraud Alert

Fraud & Scam Alerts

The Bucks County Crimes Against Older Adults Task Force issues regular alerts on fraudulent practices and scams that could impact older adults.

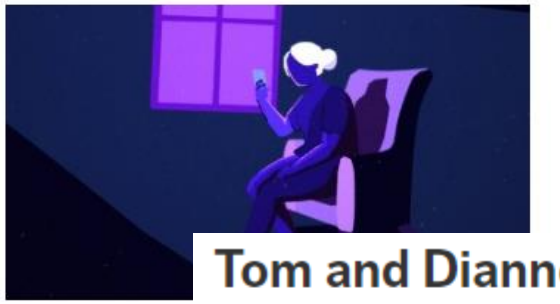
Scammers, Cons, and Fraudsters Booklet (PDF)

The Perfect Scam

Preview: The Perfect Scam

6 Tales of Real-Life Scam Stories

Host of 'The Perfect Scam' podcast shares a few of the most memorable episodes



Scam Turns a Money Mu

Annie believes she's reality, she's being l

Tom and Dianne's Savings Disappear After Seeking Help

In part 2, after a computer hacking, a "bank fraud" investigator disappears with the couple's life savings

THE PERFECT SCAM

Computer Lockout Leads to Loss in Life Savings, Part 2

30 00:00:00 / 00:43:09 30

Computer Hacker Drains Couple's Life Savings

In part 1, a retired couple finds their life suddenly turned upside down when their computer is hacked

THE PERFECT SCAM

Computer Lockout Leads to Loss in Life Savings, Part 1

30 00:00:00 / 00:24:05 30

MONEY

Scams & Fraud

1 in 3 Adults Targeted by Gift Card Payment Scams

AARP survey finds widespread frauds involving store cards

AARP FRAUD WATCH NETWORK

Our team of fraud fighters has the real-world tips and tools to help protect you and your loved ones.

Look Up and Report a Scam in Your Area

Sign Up for Free 'Watchdog Alerts'

How AARP Helps You Combat Fraud

Call Our Helpline If You Suspect a Scam

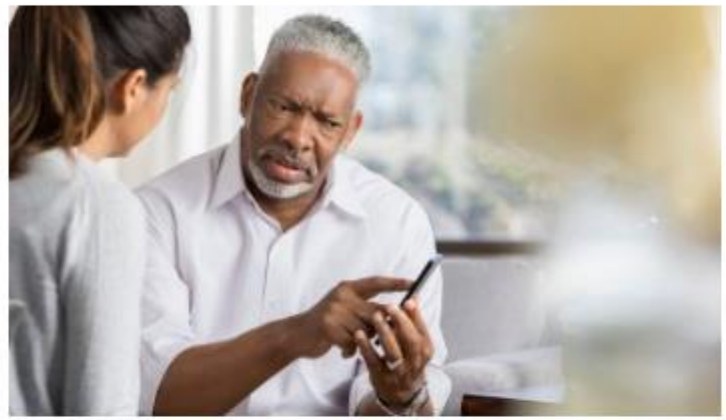
877-908-3360

Toll-free service is available Monday through Friday, 7 a.m. to 11 p.m. ET

Elder Fraud

Tech Tools to Help Guard Against Elder Financial Abuse

Websites and firms that can flag suspicious behavior



How to Spot Elder Fraud by a Financial Professional

Protect loved ones from exploitation by a fiduciary

Safeguard Older Loved Ones From Caregiver Fraud

How to hire wisely and spot signs of financial abuse

Coronavirus Scams

First Federal Criminal Charges for COVID Vaccine Card Fraud

California woman accused of helping others create fake vaccination records

Fraudsters Hit COVID Program Offering Help for Funerals

Beware unsolicited calls, emails offering help with FEMA application

5 Things to Know About the Latest Vaccine Scam

Feds say post-vaccine survey is fake and prize never arrives

Fake COVID-19 Vaccination Cards Put Public Health at Risk

Authorities warn Twitter, Shopify, eBay to stem online sales of sham records

Beware COVID-19 Frauds and Scams

Nearly 500 charged with crimes during yearlong Justice Department crackdown

Stimulus Check Scams

This Is What a Real Paper Stimulus Check Looks Like

Consumers are warned to beware of scammers

Fake Stimulus Checks Drive Traffic to Used-Car Sale

Federal lawsuit alleges deceptive and illegal tactics

First Fraud Charges Involving Stimulus Loans Filed

Feds allege men schemed to get relief money

In the News

Criminals Target Medicare Benefits to Reap Millions

Guard your Medicare number to steer clear of crooks

Beware: 8 Red-Hot Frauds to Watch Out for in 2022

Job frauds, crypto scams and more

Gift Cards Used to Turn 'Dirty' Money Into 'Clean' Cash

Crooks launder the proceeds of crimes in many ways

Cybercrime Cost Older Americans $3 Billion in 2021

FBI elder fraud report tracks soaring cost of scams

Identity Fraud Hit 42 Million People in 2021

Victims lost $52 billion last year

[AARP Bulletin April ‘22 Issue]

AARP Bulletin – April 2022

The Bad Guys: Who They Are and How To Stop Them!

-> On your phone

In your computer

Filling your email

Mining your info

Tracking your loved ones

Impersonating you, and

Plotting their next steal

Summary

Make no mistake: We are at war with a growing, spreading industry of fraud

- Technology – makes it possible
- Greed – makes it profitable

There's hope: You can win every battle against them if you understand who the scammers are, how they manipulate you, and how you are prone to react

Part 1 – The Data Brokers

Fraud starts with information about you. It can be easily and cheaply bought in an underground marketplace.

- Where does the information come from?
  - 1,862 publicly reported breaches of large-organization customer databases last year
  - Hackers gaining access to your computer by infecting it with malware
- Where does it go?
  - Vendors buy stolen data, repackage it and sell it to ‘end users’ (aka scammers)
  - Data point: your SSN is worth $2, SSN + name + birth date is $4 to $5, credit card info is $25 to $35, a hacked Facebook account is $65, and a selfie photo + US driver’s license is $100!

Part 1 – The Data Brokers (continued)

What to do?

- Set up multifactor authentication when available
- Freeze your credit at all 3 credit bureaus
- Don’t save credit card numbers online with merchants
- Activate biometric locks (fingerprints, etc.) on mobile devices
- Use anti-virus software and keep it updated!
- Remove your phone number from online accounts

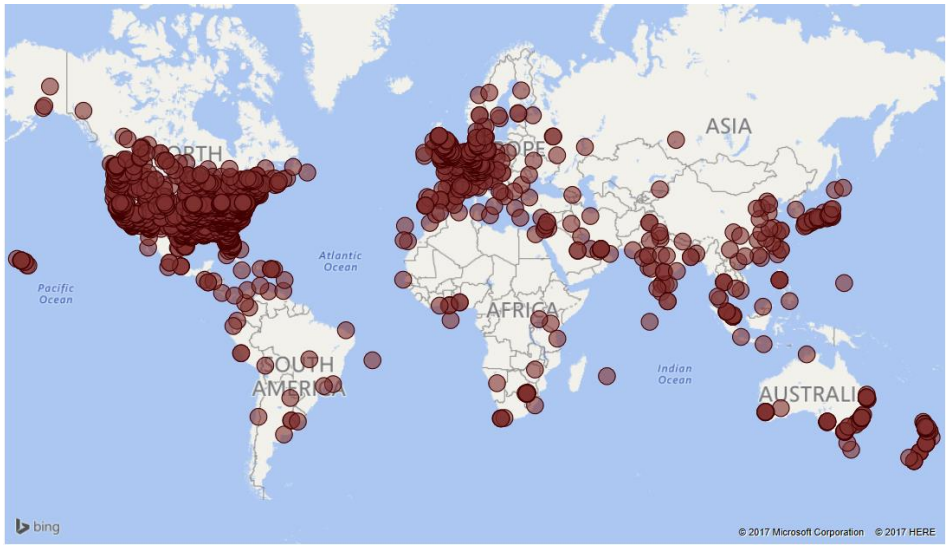
Part 2 – The Boiler Room

Criminal call centers from around the world may be dialing your number soon

- They're bombarding your phones, email accounts, social media feeds and text screens with false pitches, using high-pressure sales techniques
- Boiler rooms are often based in Southeast Asia, Eastern Europe, India, Nigeria, or a Caribbean island
- Phone number 'spoofing' makes the number appear like it's nearby
- Boiler room sales likely have additional information about you before they call, making is possible to target a specific demographic

Who’s doing the scamming?

Who’s being scammed?



Top 10 Scamming Countries in the World

1.Nigeria:
2.India:
3.China:
4.Brazil:
5.Pakistan:
6.Indonesia:
7.Venezuela:
8.South Africa:
9.Philippines:
10.Romania:

Part 2 – The Boiler Room (continued)

Criminal call centers from around the world may be dialing your number soon

- Today they can “drop a fraud request into somebody’s inbox from anywhere in the world, 24/7”
- Expect 2 tiers of salespeople: the openers/fronters making the initial call and establishing that the ‘client’ is ‘good for the money’, then the experienced closer who will use persuasion and emotion to con you out of your hard-earned cash
- This is a money-making machine you want to avoid at all cost!

A short video (link) – 5:25min

Part 2 – The Boiler Room (continued)

What to do?

- Ignore ALL phone calls from numbers you don't recognize
- NEVER make a quick decision when it involves money (~~ACT NOW!~~)
- Listen for tell-tale words like "insider information" or "exclusive deal"
- Look for the same 'red flags' in social media and email
- Before committing to any investment, check the broker's credentials
  - A useful link: brokercheck.finra.org

Part 3 – The Money Handlers

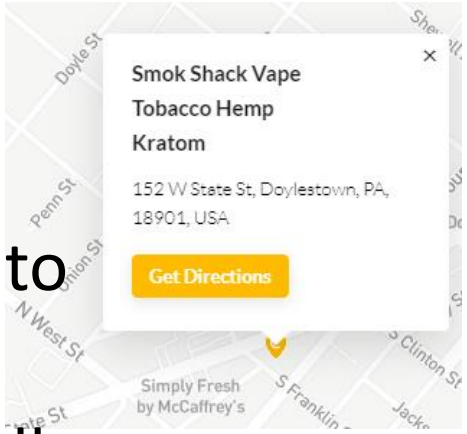
Stealing your money is only half the battle for cybercrooks

- What comes next is how they get your money in an untraceable way
  - Gift cards, wire transfers, cryptocurrency, ‘cash in books’, etc.
- Example:
  - A man was talked into buying a $1000 gift card
  - He read the card redemption code over the phone
  - This information was given to criminals via the messaging app WeChat
  - A runner was dispatched to buy a $862 tablet from a store in California
  - The total time for this transaction beginning to end was 13 minutes!

  PS – The runners were instructed to use self-checkout lanes to avoid scrutiny, and a busy runner could hit a dozen different stores in a day.
  A good day’s work, with a $200 to $300 commission!

Part 3 – The Money Handlers (continued)

Stealing your money is only half the battle for cybercrooks



- When using cryptocurrency like Bitcoin to make tracing transactions more difficult, scammers direct their ‘marks’ to go to a crypto ATM to convert dollars into crypto
- But cash is still king. Money laundering is still alive and well through ‘front companies’ or by smuggling money overseas
- You might also be asked to ‘wire’ money via Western Union
  - Note: <u>It is illegal for a telemarketer to ask you to pay via wire transfer</u>, so if someone asks you to send a wire to buy something, <u>HANG UP</u>!

Part 3 – The Money Handlers (continued)

What to do?

- NEVER buy gift cards for any purpose, other than as a gift
- Use credit cards for ALL online transactions
- Don’t pay for goods or services with cryptocurrency, unless you have a trusted relationship with the seller
- NEVER send cash through the mail to pay for something bought online or from a phone solicitation

Part 4 – The Tech Experts

Fraud requires online sophistication – but it's not that hard to do

- Cybercriminals are motivated by the prospect of 'easy money', and the tech tools are easy to find, buy (if not free) and use – including:
  - The Dark Web – The 'open source' TOR browser helps keep users anonymous
  - Telegram – secure, encrypted, private messaging – great for crooks!
  - PII (Personal Identifiable Information) – Robocheck if you're shopping for SSNs, or annualcreditreport.com, delvepoint, tlo, intelius, or beenverified work
  - *Internet browsing 'fingerprints' – your 'fingerprint' is unique and is worth ~$3
  - Burner phones – need a number to complete a scam, get a phone for $40
  - Spoofing tools – SpoofCard, CallerIDFaker, PhoneGangster, telespoof, and numerous others.PhoneGangster. Spoofmycalls will spoof their caller ID (10¢/min)

**Browser fingerprinting is a powerful method that websites use to collect information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution and various other active settings.*

Part 4 – The Tech Experts (continued)

Fraud requires online sophistication – but it's not that hard to do

- Cybercriminals are motivated by the prospect of 'easy money', and the tech tools are easy to find, buy (if not free) and use – including:
  - SOCKS5 proxies – mask your current location - 30¢/proxy
  - Fake driver's license & docs - $40, plus proof of address docs for $25
  - *Remote desktop protocol (RDP) – a hacker gains control of your computer then grants access to others to commit crimes - $5 per session – untraceable
  - Cryptocurrency expertise – if you have this skill (Alan?), you're in demand to help criminals launder their ill-gotten gains

* "RDP hacking is easy and common enough that almost anyone can learn how to do it"

Part 4 – The Tech Experts (continued)

What to do?

- Change passwords on your ‘important’ accounts every 3 months
- Record your passwords in a secure password manager (I like Roboform) or in a book kept in a secure location at home – NEVER store them in a file on your computer!
- Take alerts about potential data breaches seriously. If you get a message that one involving your information has occurred, immediately review your account and change your password
- Purge your social media account(s) of personal information – anything you don’t want a stranger to have access to including address, photos, etc.

Part 5 – Medicare Scammers

Sometimes, crooks simply use you to steal from the deepest pocket in America: the government

- This scheme manipulates Medicare members, or steals or misuses their private information
- The recent pandemic and loosened telehealth restrictions resulted in billions of dollars in fraudulent claims
- Quote: “In times of crisis, fraud control can be viewed as less important than ensuring access to care” – Malcolm Sparrow

Seems ‘times of crisis’ invite criminals to take advantage…

Part 5 – Medicare Scammers (continued)

What to do?

- NEVER give your Medicare number to anyone who calls – only to your healthcare provider or Medicare (then only if you call them)
- If someone offers free genetic testing in person or online, it's a scam
- If someone calls and promises COVID tests, medical equipment, or medical services in return for your Medicare number, HANG UP!
- If someone calls to help you enroll in Medicare, it's a scam – HANG UP!

Organized Crime

What does the ‘billion-dollar underground economy’ run by criminal syndicates look like?

- Older Americans have become a profitable target (aka ‘elder fraud’)
- Syndicates are located overseas, and use impersonation, intimidation, and sometimes violence to steal from older people
- The grandparent scheme:
  - Your grandchild is in dire legal trouble and needs help
  - ‘Actors’ are then dispatched to your home to retrieve the funds
  - This money is quickly converted into cryptocurrency
  - This scam may also be combined with ‘identity theft’

Fraud Prevention Checklist

- **Clean your wallet** – driver's license, 1 credit card, bus pass…
- **Update your phone contacts** – include only frequent calls, next turn on 'silence unknown callers' (iPhone), or 'block numbers' (Android) – this will block numbers not in your contacts or you haven't been in contact with
- **Review your credit report** – visit AnnualCreditReport.com. Check your report to make sure no one has opened credit in your name
- **Add two-factor authentication** to your accounts (when possible) – this is great protection for your accounts even if someone has your account and password already
- **Refresh your Facebook security** – go to Settings & Privacy, and complete the Privacy Checkup – lock your profile so only friends can see it
- Add this number to your contacts – AARP Fraud Watch Network helpline

  1-877-908-3360, and it's free

2022 Hottest Scams

- **Google Voice Scam** – never share verification codes
- **Rental Assistance Scam** – only apply for legit rental assistance
- **Fake Job Fraud** – use a separate email address for job hunting
- **Fake Amazon Employee** – ignore calls, texts, emails about suspicious activies, raffles, unauthorized purchases
- **Cryptocurrency ATM Payment** – "Nobody from the government, law enforcement, utility company, or prize promoter will ask you to pay in cryptocurrency. If they do, it's always a scam"
- **Local Tax Imposter** – ignore ALL calls! Tax agencies do business by mail and they don't ask for passwords, or bank account or credit card info
- **'Favor for a Friend' Gift Card** – call or text your friend to confirm if the person really needs the favor – ALWAYS double-check BEFORE sending money!
- **P2P Payment Request** – only use P2P apps to send money to friends and family – and turn on the security lock feature that requires a passcode to make a payment

P2P examples: PayPal || Venmo || Zelle || Cash App || Apple Pay Cash…

HEAR THESE WORDS? HANG UP!

Here are seven actual scam phone pitches we've logged recently at the AARP Fraud Watch Network Helpline, with names and details changed to protect privacy. Can you detect the signs that they are fraudulent? Remember: Impostor fraud—in which criminals pretend to be law enforcement, government officials or other authorities—is now the number 1 type of consumer scam in America. The better you are at detecting it, the safer you become.

BY **AMY NOFZIGER**

Scenario 1

"Hello, is this Mrs. Perl? This is Bill from Genetic Testing Services. Your doctor reached out to us because he is concerned with the cancer that runs in your family and would like you to take a DNA swab test. This test is covered by Medicare, and we just need your Medicare number to process and ship out the order."

Scenario 2

"Good morning, this is Apple Inc. We are calling to tell you there is a problem with your phone, and someone has placed malware on it. We will need you to download AnyDesk onto your phone so we can help you."

Scenario 3

"This is Agent McMurphy from the IRS, and I am calling to inform you that you have a federal arrest warrant for not paying your taxes. Please press 1 on your keypad to be connected to my desk so we can clear up this matter."

Scenario 4

"Nana, it's me, Henry. I was away for spring break and got arrested because my friend that was driving was drunk, and we hit a pregnant woman! Please don't tell Mom and Dad. I need your help."

Scenario 5

"Hello, sir. This is Amazon Security calling to inform you that there's been an attempt to order items on your account. But don't worry, we can help with the refund. I just need a few pieces of information from you to get this started."

Scenario 6

"This is Denver Energy Company, and we are notifying you that you have missed your last two payments. And, unfortunately, your electricity will be shut off by the end of today unless you can pay immediately over the phone."

Scenario 7

"This is the Social Security Administration, and your Social Security check has been frozen due to fraudulent activity. Press 1 to take care of this matter."

DID YOU SPOT THE MOMENT WHEN YOU NEEDED TO END THE CALL?

Here's advice AARP Fraud Watch Network experts have gotten from government, financial and other officials on these 7 scenarios.

Scenario 1 Hang up when you hear any request for your Medicare number. This is a scam aimed at billing Medicare for unnecessary tests, many of which it does not cover.

Scenario 2 Hang up when anyone you do not know asks for remote access to your phone. Scammers are looking to steal personal information for identity theft or fraud.

Scenario 3 Hang up on any call you believe is coming in as a computerized robocall. IRS employees never demand money or threaten you over the phone. They may call to set up appointments or discuss audits, but only after trying to notify you by mail.

Scenario 4 Hang up and reach out to your grandchild or another family member to check the story out. This is almost certainly a form of the "grandparent scam" that uses personal information about your grandkid gleaned from social media to deceive you. Don't panic and send money or reveal any banking or financial info.

Scenario 5 Hang up when asked for info to access your bank or other private accounts remotely. If you think there could be a problem, go directly to your Amazon account and contact the company directly through its website.

Scenario 6 Hang up when threatened over the phone, especially by a robocall. Utility shutoffs are not handled that way. You get notification in the mail.

Scenario 7 Hang up when any government official says you need to pay money over the phone or asks for personal information. That doesn't happen. ■

Anti-fraud expert ***Amy Nofziger*** *is AARP's director of fraud victim support.*

Source: [AARP Bulletin June 2022]

Stay up-to-date

- Stay up on the latest scams
  - aarp.org/frc
- Monitor neighborhood scams
  - aarp.org/scammap
- Get updates on the latest scams
  - aarp.org/watchdogalerts
- Hear stories of real scams
  - aarp.org/theperfectscam
- Get support from trained specialists
  - AARP Fraud Watch Helpline – 877-908-3360
- Watch live and on-demand webinars
  - aarp.org/fraudwebinar

Video (5:15min)

Video Notes

Classic Phishing

- You receive an email from your bank that asks you to update your PIN ‘in the next 24 hours’
  - You follow the link provided
  - You enter your PIN
  - The Website becomes unresponsive
  - A short time later, you see an unauthorized charge on your credit card
  - You were just the victim on a Phishing attack
- Response
  - Contact your bank or credit card company immediately to have the charges reversed and report the scam

Video Notes

Better

- Don’t open the email in the first place but contact your bank or credit card company directly to inquire if this request is legitimate
- Or, if you opened the email, NEVER click on the link provided. Go to your bank or credit card website directly if you believe further action is required.
- Or, if you clicked the link provided, NEVER enter confidential information on a website you don’t absolutely trust
- Or, if you did enter the information requested, contact your bank or credit card company IMMEDIATELY to report the incident and have them monitor you account for unauthorized charges. Hopefully you’ll never get to this step!

Some types of Phishing you may encounter

- Phishing - Mass-market emails
- Clone phishing - When copies are just as effective
- Smishing - Phishing via text message
- Spear phishing - Going after specific targets
- Whaling - Going after the big one
- Pharming - redirecting a website's traffic to another, fake site
- Vishing: Phishing over the phone
- Snowshoeing: Spreading poisonous messages
- Etc….

Protect yourself from phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website.

video

Protect yourself from phishing

Learn to spot a phishing message

- **Urgent call to action or threats** - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you.

  > **Tip:** Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.

- **First time or infrequent senders** - While it's not unusual to receive an email from someone for the first time, especially if they are outside your organization, this can be a sign of phishing. When you get an email from somebody you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.

Protect yourself from phishing

Learn to spot a phishing message

- **Spelling and bad grammar** - Professional companies and organizations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.

- **Generic greetings** - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.

- **Mismatched email domains** - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.

Protect yourself from phishing

Learn to spot a phishing message

- **Suspicious links or unexpected attachments** - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message. In the following example, resting the mouse over the link reveals the real web address in the box with the yellow background. Note that the string of numbers looks nothing like the company's web address.

> **Tip:** On Android long-press the link to get a properties page that will reveal the true destination of the link.
> On iOS do what Apple calls a "Light, long-press".

Cybercriminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. Sophisticated cybercriminals set up call centers to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

Protect yourself from phishing

If you receive a phishing email

- Never click any links or attachments in suspicious emails. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. Or call the organization using a phone number listed on the back of a membership card, printed on a bill or statement, or that you find on the organization's official website.
- If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it.
- Report the message (see below).
- Delete it.

Helpful Videos

[Phishing Explained In 6 Minutes | What Is A Phishing Attack? – use this]

- This video on **Phishing** Explained In 6 Minutes explains what is a **phishing** attack, we cover the infamous cyber attack vector which has been ...
- YouTube · Simplilearn · Sep 16, 2021

[Phishing awareness video - YouTube]

- White board style video about **phishing** attacks.
- YouTube · Oliver Muenchow · Jan 29, 2020

[What is phishing? - YouTube]

- **Phishing** is an attack attempting to steal your money or identity by getting you to divulge personal information.
- YouTube · Microsoft Security · Jul 22, 2020