



Montgomery County Department of Police



Financial Crimes Section
Detective Cindy Miranda
CFCI, CFE

Police Headquarters
100 Edison Park Drive
Gaithersburg, MD
(240) 773-6330

Make a report by calling (301) 279-8000 or visiting your
local police district station

Disclaimer



This presentation is an educational tool and while names, photographs, cartoons and other information may be included – it is not meant to cause injury, embarrassment or harm to any individual or entity.



The information is based on the presenters own personal and professional experience.



Information was obtained from cooperating law enforcement agencies, financial institutions, businesses, victims and other numerous sources.

MCPD Financial Crimes Section

The financial crimes section is comprised of:

- 1 Sergeant –
- 5 Sworn Fraud Detectives –
- 1 Civilian investigator
- Handful of interns and volunteers



What we do:

Follow-up Investigations:

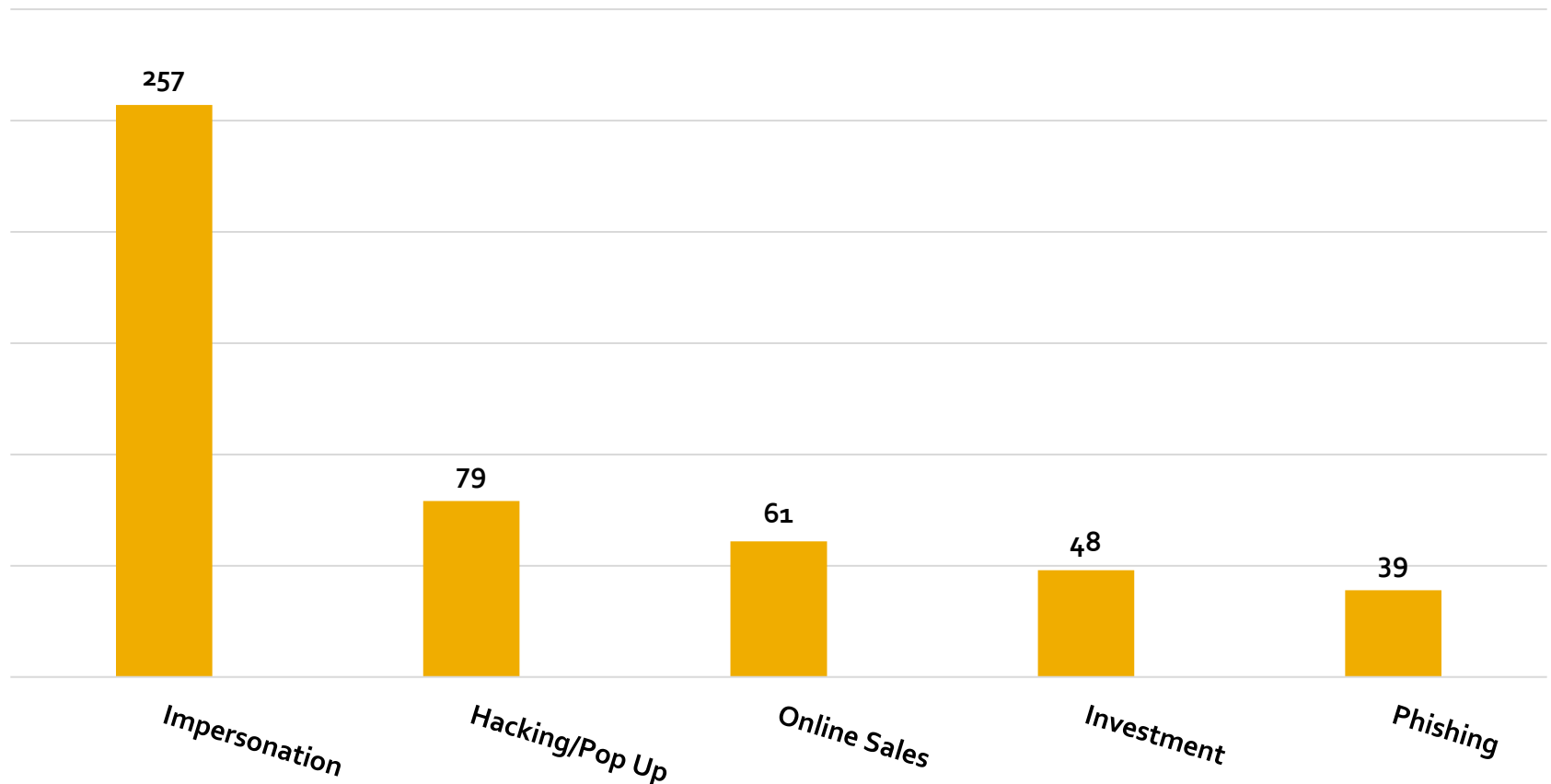
- Receive over 400 reports a month
- 4,000 to 5,000 reports a year
- 3-4 reports are assigned to a Detective per month
- Our cases involve: Substantial monetary loss, multiple victims, those involved with manufacturing money, credit cards, fake ID's, etc.



Montgomery County Cases

April 2024-2025

TOP 5 SCHEMES & SCAMS



Current Fraud Trends

Elder Fraud / Exploitation

- Family , Healthcare provider, Home Repair, Telephone / Internet scams, Account Take Over

Phone scams/requesting money

- Romance scams, computer virus (Microsoft pop up), courier pick up scams , lottery scams, government imposter scams, “Pig Butchering” scams, distress scams

Pig Butchering

What is it?

- "Pig butchering" refers to a type of online investment scam where criminals build trust with victims, often through romance or fake investment opportunities, before luring them into fraudulent schemes to steal their money.

How?

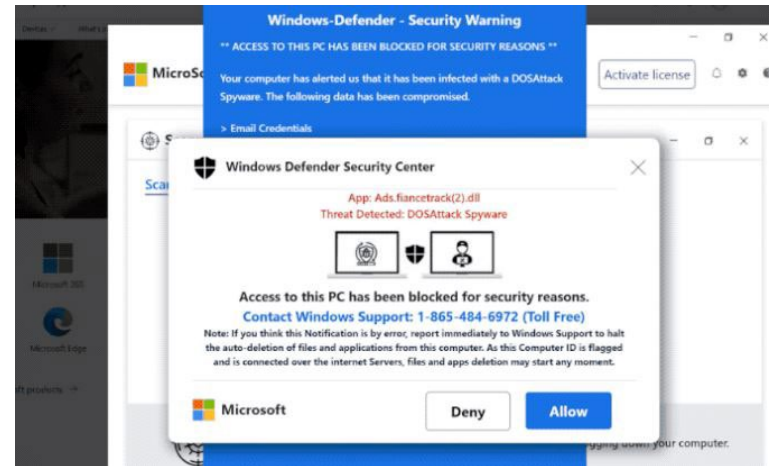
- Download an APP on their phone
- Monitor the investments going up (this if fake)
- Make the victim pay more money to withdrawal the "investment"
- "Investments" are made through Cryptocurrency



Phishing

Microsoft Pop Up Scams

- ❑ Message appears
- ❑ Victim contacts number
- ❑ Allows suspect to gain access
- ❑ Another person calls & tells victim she/he needs to secure funds (imposter scam)



How not to become a victim of Phishing

- Do not reply to unsolicited or pop-up information which request “personal identifying information.”
- Find a legitimate number to call to verify (do not use the number to call on the screen)
- If you receive a Pop Up on your computer, turn off your computer by doing a “hard shut down”



Government imposter scams aren't new



Taxes are overdue
& you need to pay
via gift cards



...stated & you've
been called up for
service




There's a warrant for
your arrest & you must
pay to have it recalled



Government imposter scams just evolve

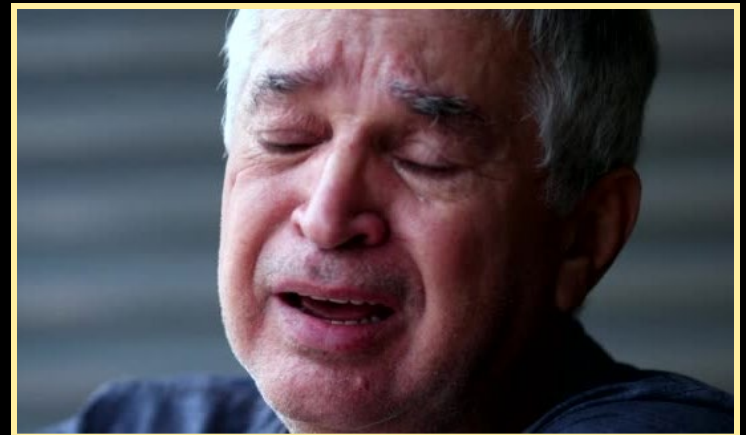
A current trend involves couriers picking up gold bullion and other precious metals, gold coins, and US currency (bulk cash)





The typical sequence of events:

1. Notification
2. Initial contact
3. Secondary Contact
4. Secrecy
5. The Realization
 - the scammer “agent” disappears
 - the victim realizes they’ve been scammed
 - the victim faces financial consequences, emotional and psychological trauma, and potential re-victimization





Montgomery County Police Department Financial Crimes Section

FCS has successfully prevented over \$3.3 million in potential losses related to gold bars.

The smallest recorded loss by a victim is \$20,000, while the largest is over \$2.3 million.

Some victims have lost additional money to cash pickups and cryptocurrency deposits.



Credit Card Data Breach

- What is a data breach? Intentional or unintentional release of secure information to an untrusted entity.
- Some examples include Target, Kmart, Home Depot, Harbor Freight, etc.



What happens with your info?

- Sold in the dark market (dark web)
- Buyers then use your info to open up credit cards, steal IRS return money, open up bank accounts to commit fraud



How you can protect yourself.....

Don't open emails or links from people you don't know

Review your credit report annually

Report lost checks, credit/ATM cards and/or suspicious activity
on your bank account immediately

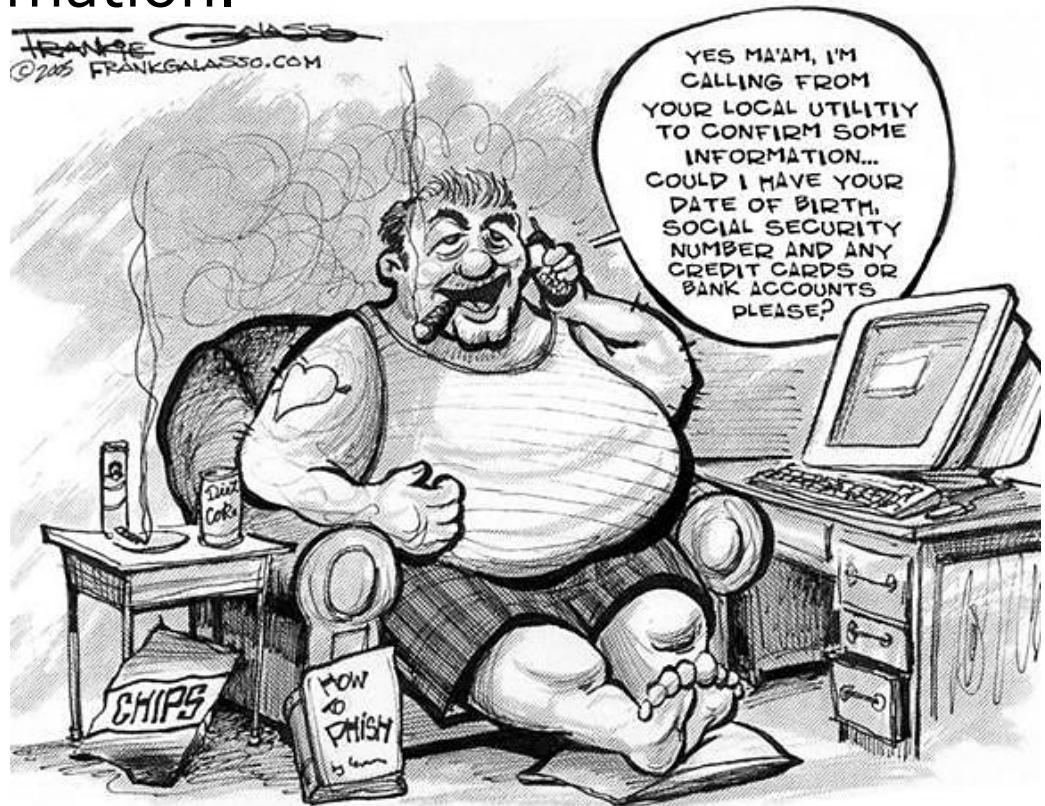
Check your credit card charges and bank account
frequently

Do not let someone rush you into making quick money decisions

If you don't understand cryptocurrency, then don't use it

More easy protections

- **Do not give out financial information** (account numbers, credit card numbers or your Social Security number) unless you know the organization or person requesting this information.
- **Notify your bank or credit card company** of any suspicious phone inquiries asking for account information.



Prevention

Solicitations:

If you did not initiate the contact no matter who the contacting individual says they represent, do not react to the solicitation through the channels the solicitor set up.



Scammers may use cryptocurrencies because the transactions are irreversible and hard to trace.

Urgency:

Think before you withdrawal cash, buy cryptocurrency or wire large amounts of money. Do not let the scammers urgent request allow you to become a victim. Contact a friend/police department/family member first!

WARNING SIGNS THAT YOU MAY BE A VICTIM

Failure to receive bills, statements or cyclically arriving financial information

Denial of credit or vendors who question your credit worthiness

Receive credit cards, checks or any other financial instrument that you did not apply for

Unusual solicitations from vendors outside of your normal pattern

WARNING SIGNS THAT YOU MAY BE A VICTIM

- ❑ Failure to receive tax refunds or you receive an audit or tax bill that is unfamiliar to you
- ❑ Unfamiliar bills, invoices, lack of receiving your tax return, ACH debits mortgage or rental statements
- ❑ Bill collectors start calling/write referencing debt you did not accumulate
- ❑ Pinging (1 or 2 dollar charges on your statement often to charities)

FRAUD ALERT

Three Credit Bureaus:

Equifax

Transunion

Experian



Different requirements for the bureaus

There are alerts, temporary freezes and a long-term freezes for victims of identity theft

IF YOU ARE A VICTIM

- Make a police report by calling 301-279-8000 or going to your local district police station
- Immediately notify affected creditors, vendors and close all fraudulent accounts
- Get a copy of your credit bureau reports and dispute all unauthorized or unknown transactions
- Request a copy of any fraudulent records created by the imposter, you will need to provide the business with an FTC identity theft affidavit or another acceptable affidavit and your Identity Theft Report (police report). The business should send copies of the records to victims within 30 days.
- File an ID theft complaint with FTC

Free Credit Report/Monitoring

- Make sure you apply for your free annual credit report at annualcreditreport.com, call 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Take advantage of free credit monitoring from companies that have been breached

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

[Home](#)[All about credit reports](#)[Request yours now!](#)[What to look for](#)[Protect your identity](#)[Frequently asked questions](#)[Contact us](#)

One of these things is not like the others.

You may think you have one credit report and one credit score. But you really have several, and they may differ. You should check all three reports regularly.

[Request your free credit reports](#)[PAUSE](#) ||[SPOT IDENTITY THEFT](#)[GOOD CREDIT](#)[DON'T BE FOOLED](#)[MORE THAN A SCORE](#)[NOT LIKE THE OTHERS](#)

Your credit reports matter.

- Credit reports may affect your mortgage rates, credit card approvals, apartment requests, or even your job application.
- Reviewing credit reports helps you catch signs of identity theft early.

[Request your free credit reports](#)

FREE Credit Reports. Federal law allows you to:

- Get a free copy of your credit report every 12 months from each credit reporting company.
- Ensure that the information on all of your credit reports is correct and up to date.

BROUGHT TO YOU BY

TransUnion 

EQUIFAX

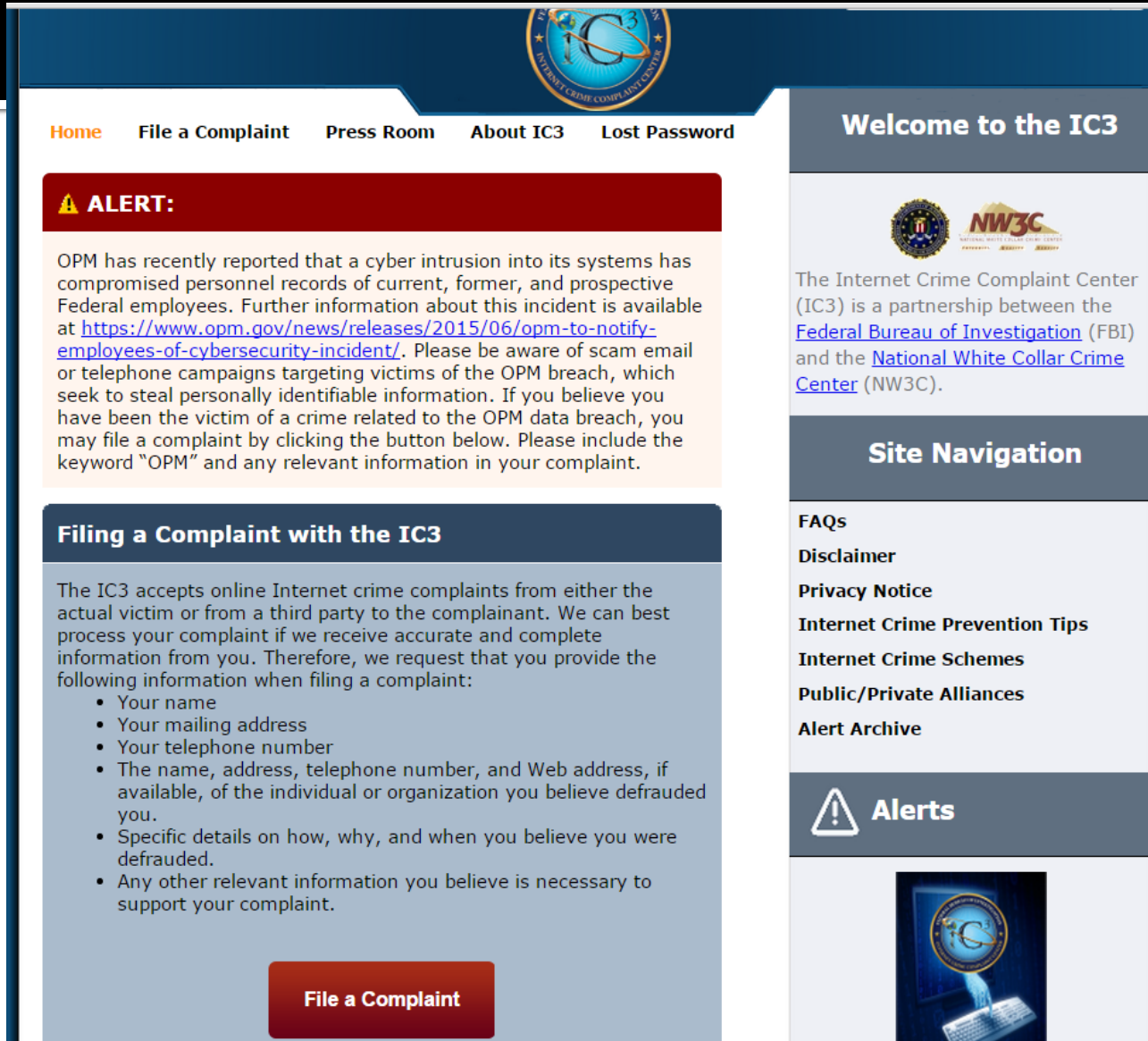
 **Experian**

MONITORING

- Early detection significantly reduces the damage and time spent on resolving issues
- Closely review each statement to make sure they accurately reflect all legitimate charges.
- Review your credit report at least once a year preferably twice a year. Look for accounts and inquiries of any kind that seem strange or do not belong to you.
- Check your bank accounts daily

Computer Prevention

- If you have been a victim of an internet scam or fraud please report the crime to the
- [Internet Crime Complaint Center \(IC3\) | Home or \(www.ic3.gov\).](https://www.ic3.gov)



The screenshot displays the official website of the Internet Crime Complaint Center (IC3). At the top, a navigation bar includes links for Home, File a Complaint, Press Room, About IC3, and Lost Password. A prominent red alert banner states that OPM has reported a cyber intrusion into its systems, affecting personnel records, and provides a link to further information. Below this, a section titled 'Filing a Complaint with the IC3' explains the process and lists the required information for a complaint, such as name, address, telephone number, and details of the crime. A 'File a Complaint' button is visible at the bottom of this section. On the right side, a 'Welcome to the IC3' section introduces the partnership between the FBI and the National White Collar Crime Center (NW3C). Below this is a 'Site Navigation' menu with links to FAQs, Disclaimer, Privacy Notice, Internet Crime Prevention Tips, Internet Crime Schemes, Public/Private Alliances, and Alert Archive. An 'Alerts' section at the bottom right features a warning icon and a small image of a computer monitor displaying the IC3 logo.

Home **File a Complaint** **Press Room** **About IC3** **Lost Password**

ALERT:

OPM has recently reported that a cyber intrusion into its systems has compromised personnel records of current, former, and prospective Federal employees. Further information about this incident is available at <https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/>. Please be aware of scam email or telephone campaigns targeting victims of the OPM breach, which seek to steal personally identifiable information. If you believe you have been the victim of a crime related to the OPM data breach, you may file a complaint by clicking the button below. Please include the keyword "OPM" and any relevant information in your complaint.



Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.

File a Complaint

Welcome to the IC3


 

The Internet Crime Complaint Center (IC3) is a partnership between the [Federal Bureau of Investigation](https://www.fbi.gov) (FBI) and the [National White Collar Crime Center](https://www.nw3c.org) (NW3C).

Site Navigation

- FAQs
- Disclaimer
- Privacy Notice
- Internet Crime Prevention Tips
- Internet Crime Schemes
- Public/Private Alliances
- Alert Archive

Alerts



Do Not Get Depressed

- After listening to this presentation it may seem hopeless at times when dealing with scammers and con-artists. Rest assured the system has greatly improved with servicing victims needs in a timely manner. As always making yourself a less desirable target than others will go a long way to keeping you and your identity safe.

Resources.....know who to call

Equifax:

1-800-525-6285 or www.equifax.com

Experian:

1-888-397-3742 or www.experian.com

Trans Union:

1-800-680-7289 or www.transunion.com

Federal Trade Commission (FTC)

1-877-438-4338 or www.ftc.gov

Social Security Administration

1-800-772-1213

Internet Fraud Complaint Center (IFCC)

www.ifccfbi.gov

Annual Credit Report

<https://www.annualcreditreport.com/index.action>





REALITY

If it is too good to be true, it probably is.

Any Questions?
Montgomery County Police Financial Crimes
240-773-6330



Safeguarding Yourself Against Fraud

Presented by:

Dennis Chapman, Manager, BSA & Vendor Compliance

Risk Management Department

April 22nd, 2025

Presentation Overview

- How can I detect and protect myself and family members from fraud?
- What resources does NIHFCU offer to help mitigate my fraud risk?
- Additional Fraud Resources

“Trust, but verify” - Ronald Reagan

How can I detect and protect myself and family members from fraud?

- **How do Fraudsters gain access to Victim information:**

- Phishing - Email or malicious Website
- Vishing - Voice Communication via VoIP service
- Smishing - SMS or Text Message
- Quid Pro Quo - Service in Exchange for Access or Information
- Honey Trapping - Fake Relationship and Exploits Connection
- Baiting - Temptations and False Promises



- **Social Engineering** - non-technical malicious intrusion that relies on human interaction and often involves tricking people into breaking normal security procedures and divulging confidential information.
- Over **90%** of Cyberattacks involve Social Engineering tactics
- **56%** increase in Fraud manipulating Authorized Individuals

How can I detect and protect myself and family members from fraud?

- When experiencing an unexpected communication from any channel, think:
 1. Is the sender or caller familiar?
 2. Are there oddities in the communication? (voice, spelling)
 3. Unexpected/Unfamiliar links?
 4. Is there heightened urgency for the request?
- Always treat requests for sensitive information with skepticism.
 1. Does this request make sense?
 2. What is the source of the request?



How can I detect and protect myself and family members from fraud?

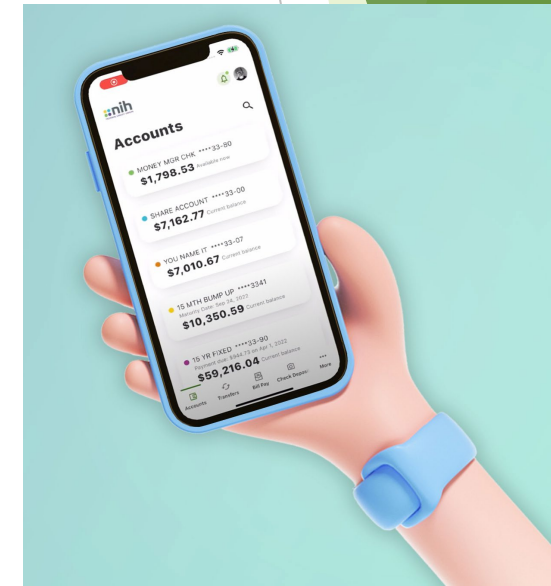
- **Cybersecurity Tips:**

1. Strong Passwords - Don't Share or Use Just One!
 - 12+ Characters in Length
 - Passphrases
 - Uniqueness
2. Multi-Factor Authentication
3. Think Before You Click!
4. Keep Devices and Software Up-to-Date
5. Avoid Public USB Stations and Wi-Fi
6. Social Media/Dating Application Awareness
 - Disinformation/Misinformation
 - Data Mining
 - Fake Profiles
 - Phishing



What resources does NIHFUCU offer to help mitigate my fraud risk?

- **Online and Mobile Banking**
 - Change Notifications (Credentials, Personal Information)
 - Transaction Notifications
 - Custom- accounts, balance, login
 - Zelle & Bill Pay
 - Debit/Credit Card Freezes
 - Fraud Prevention Monitoring
 - Multi-Factor Authentication & Biometric Login
- **E-Statements**
 - Reduce risk of mail fraud
- **My Credit Rx**
 - Monitor credit reporting to detect potential ID Theft



NIHFCU Fraud Resources



Federal Worker
RIF Support

CLICK
NOW

LOGIN

MENU

My Credit Rx – Credit Monitoring

Monitor your credit score and pull on-demand credit reports for free.

OVERVIEW

IMPROVE YOUR CREDIT

MONITOR YOUR CREDIT

GET STARTED

FAQs



%
Rates

Locate

Book

Check your credit score for free

My Credit Rx powered by SavvyMoney® is available in online banking and our mobile app. Easily check your credit score, view your credit report, set up credit monitoring updates and much more. With **My Credit Rx**, you can:

- Check your credit score daily
- View your full credit report
- Monitor your credit for unusual activity
- Get alerts for changes to your credit
- Visualize what affects your credit score
- Simulate how future actions may impact your score
- Dispute items on your credit report
- Get tips on rebuilding credit & saving money

GET STARTED TODAY



NIHFCU Fraud Resources

Digital Security Center

Secure Your Accounts and Reduce Fraud

OVERVIEW

PROTECT YOURSELF

COMPROMISED ACCOUNT

USEFUL LINKS

Your account security is our priority

NIHFCU uses advanced fraud prevention technology to monitor accounts for fraudulent activity 24/7/365. Systems like our 2-factor authentication process provide your accounts with even more security. For more protection, review the suggestions below to reduce your risk of fraud.

>>>Security Update for Online and Mobile Banking<<<

We are adding a new feature to your login page experience. This new addition, Cloudflare Turnstile, attempts to seamlessly confirm that the user logging in is a real person and not a bot attempting to login via scripted, brute force attempts. It will provide a visual "authentication" during your login.

During most logins you will not have to interact with this tool at all, as it will conduct automatic verification when possible. Some users may need to click a dynamically generated "Verify you are human" checkbox to complete verification if they are using a different device or connection.

If you encounter an error message, please [contact us](#) at 800.877.6440 but here are some tips on how you may address the situation:

- Restart your browser or close and re-open the mobile app.
- Clear your cache and cookies.
- Update your browser to the latest version.
- Disable browser extension(s).



Let's Chat!

NIHFCU Fraud Resources



Federal Worker
RIF Support

CLICK
NOW

LOGIN

MENU

%
Rates

📍
Locate

📖
Book

Fraud & Security Hub

Protect Yourself Against Fraud

TIP OF THE DAY: Regularly check your financial statements for any unfamiliar or suspicious transactions.

Support • Identity • Business • Finances • News • E-Learning •

Search All Safety Tips Search EN ^

What To Protect +



Popular Topics +



Your Identity +



Scams +



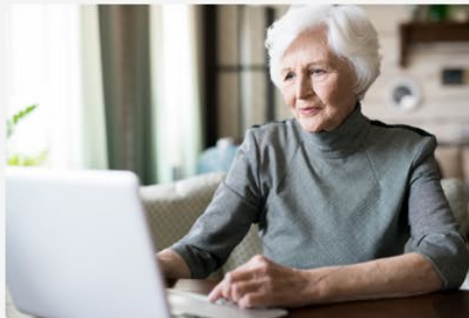
How-to Guides +



Money +



Senior Citizens +



Internet +



Let's Chat!

Additional Fraud Resources



If you or a loved one were solicited through a computer pop-up, social media site, dating site, text, email, or phone call by someone you have never met, and answer "YES" to one of the following questions, **you may have been targeted by a SCAM.**

- Have you been asked to invest in cryptocurrency or in gold futures?
- Has someone claiming to be a bank or government agency requested money, or for you to liquidate your accounts, in order to clear you of a crime or secure your accounts?
- Has someone claiming to be a tech or customer support representative requested money to remove a virus or child pornography from your computer or secure your account?
- Has someone contacted you claiming a family member is in danger or jail, and you must send money now to avoid further harm?
- Has someone you never met claimed to be romantically interested in you but requests you send them money or something else of value?
- Have you ever been directed to withdraw cash to purchase gold or silver bars to give someone else?
- Has someone sent individuals to your home or directed you to meet in a public place to drop off or pick up money, or other items of value, to deliver to an unknown person?
- Has someone asked you to obtain cash to either purchase gift cards or deposit in a cryptocurrency ATM—or given you a QR code to deposit money into an ATM?

If you answered "YES" to any of these questions, please go to www.ic3.gov

for additional resources or to file a complaint with the FBI
INTERNET CRIME COMPLAINT CENTER (IC3).

Persons 60 and older may call the National Elder Fraud Hotline at [\(833\) 372-8311](tel:833-372-8311) for assistance in filing with IC3.

Additional Fraud Resources



CRYPTO INVESTMENT SCAMS

WHAT YOU SHOULD KNOW

Crypto* investment scams, commonly referred to as "pig butchering" by scammers, cost consumers billions of dollars. Criminals befriend people to entice them to make crypto investments through phony apps and websites. The investments may start out slowly with small sums of money, but it's a scam aimed at stealing tens of thousands to millions of dollars.

*Crypto is also referred to as cryptocurrency by users

HOW DO CRIMINALS TARGET PEOPLE & HOW DOES THE CON START

HOW DOES THE CON START?

Criminals often pose as people interested in:

- Friendship,
- Romantic relationships, or
- Business investments.

Using fake profiles, they take time and build connections with their targets. They claim to be, or to know, experts who can help investors make money. To mask their identities, they:

- Use fake phone numbers (spoofing)
- Rely on deepfake videos, voices or images
- Employ artificial intelligence

They target people through texts, dating sites, social media channels, professional networking platforms and/or other apps. After establishing trust with their victims, criminals move conversations to encrypted messaging apps and introduce crypto.

They coach victims into investing using fake platforms. Websites might look legitimate, but it's all phony and controlled by criminals. Once people begin "investing," criminals manipulate the sites/apps to show fake profitable returns. Victims might even be allowed to make initial withdrawals, but it's a ploy to encourage further investments.

HOW DOES IT END?

When victims try to withdraw larger sums of money, they are told they need to pay a fee or taxes. But there's no getting the money back, even if they pay the supposed fees or taxes. In the end, victims lose everything they invested.

PROTECT YOURSELF

- ✓ Research before you invest in anything.
- ✓ Recognize that pressure to "act fast" might be a sign of a scam.
- ✓ Do not send money to anyone you meet online or via apps, and don't make investments based on their advice.
- ✓ Do not download or use any unfamiliar apps.
- ✓ Do not pay for services that claim they can recover lost funds.
- ✓ Do not trust anyone who offers a "sure bet." All investments involve risk.
- ✓ Recognize that even video chats and online trading platforms which appear real can be fake.

WARNING SIGNS

- Unexpected contact by an unknown person.
- Requests to limit contact with financial institutions or advisors.
- New online friends sharing "can't-miss" investment opportunities.
- Sense of urgency to invest more money or pay fees.
- Misspelled web links.

IF YOU HAVE BEEN VICTIMIZED

- Stop sending money to the criminals.
- Contact your bank.
- Keep records and communications relating to the scam.
- File a report with the FBI Internet Crime Complaint Center at [IC3.gov](https://www.ic3.gov).

ABA Foundation is proud to work with the following agencies on this infographic





Thank you for your attendance!