Identity Theft

Protecting Your Good Name

Hosted by

New York University
FEDERAL CREDIT UNION

ID ADVOCATE

Anne Madrid

Annem@idadvocate.org

Id Theft Stats

(Javelin Research 2022)

One out of every three people in the United States will be a victim of ID Theft. 7-10% a year. 1 Every 22 seconds.

While Georgia ranks #1 in reported identity theft cases in the nation per capita (574 per 100K) NY ranks #4 in the nation for the # of cases in 22’

Credit card fraud tops list in 2022, followed by bank and loan fraud.

40 Million victims in 2022 and 43 billion in losses.

Data breach is responsible for most stolen identities. (1,802 breaches in 2022 totaling 422.14M Americans +41.5%)

Social media users are more likely to be victimized.

Hosted by
New York University
FEDERAL CREDIT UNION

ID Theft Losses and Changes 21-22’

(Javelin Research 2022)

-17%
Combined losses
$ 43 Billion

-1%<
Account Takeover
Fraud
$11 Billion

-42%
New Account
Fraud
$3.9 Billion

-7%
40 Million
victims

$1311
Average loss per
identity fraud victim

+84%
Losses to persons
over 60

+7%
P2P
Fraud

The Coming AI Crime Spree!
More Criminals, More Crimes, More Victims

- The criminal world is drowning in stolen data. AI is quickly sorting, analyzing and packaging that data to be sold and used by criminals.
- 1,265% ↑ in phishing/1,000% ↑ credential phishing following the launch of ChatGPT.
- AI has huge success in developing very realistic deep fake versions of real humans used for a variety of nefarious purposes. 24' bank lost 25M to fraudster using AI deep fake technology.
- AI is setting its eye on our passwords. 65% can be cracked in less than an hour. Any 7-character password could be cracked in less than 6 minutes.
- AI is specially suited for exploiting security holes, scanning billions of lines of code instantly for flaws, weaknesses or mistakes, which was previously time consuming and $ for criminals.
- AI can change quickly and automatically to evade antivirus software and it's making malware smarter and more capable.
- AI can forge just about any type of document, making identity fraud easier to commit.

Cryptocurrency Scams Have Become A Major Criminal Scheme

CASH-TO-CRYPTOCURRENCY SCAMS

Criminals convince victims to withdraw cash so that it can be deposited into a criminal-owned cryptocurrency ATM account.

INVESTMENT SCAMS

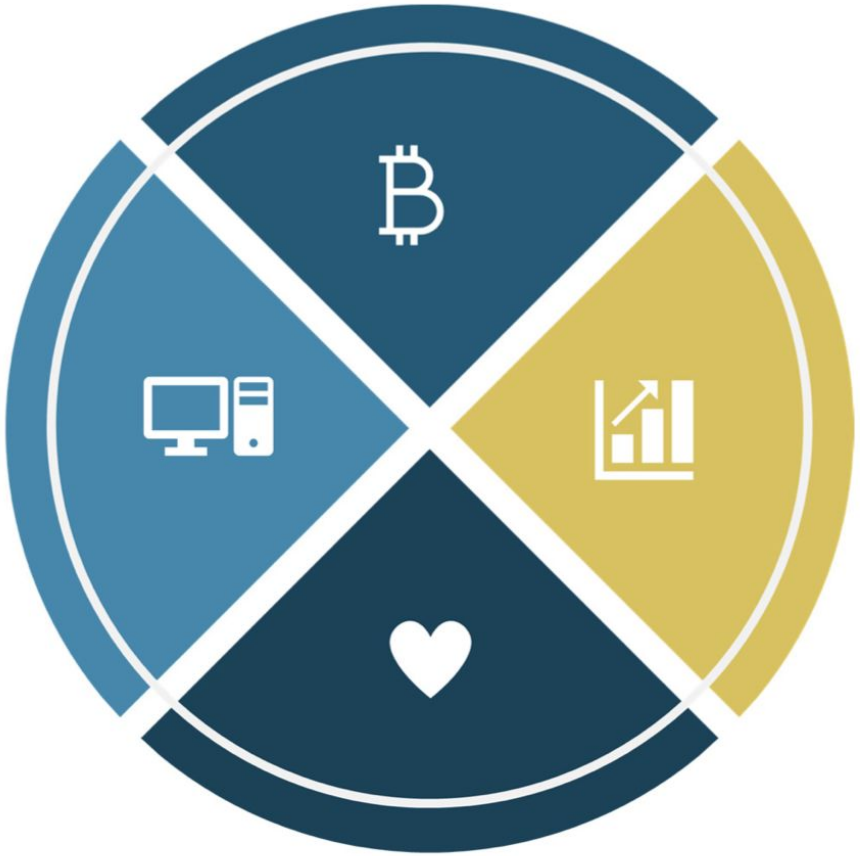
Victims are convinced to co- invest in a lucrative opportunity that may also be a criminal ploy used to build trust and affection with romance scam victims

TECH SUPPORT SCAMS

Victims are directed by criminals to pay huge fees in cryptocurrency to pay for computer repairs that are not even necessary.

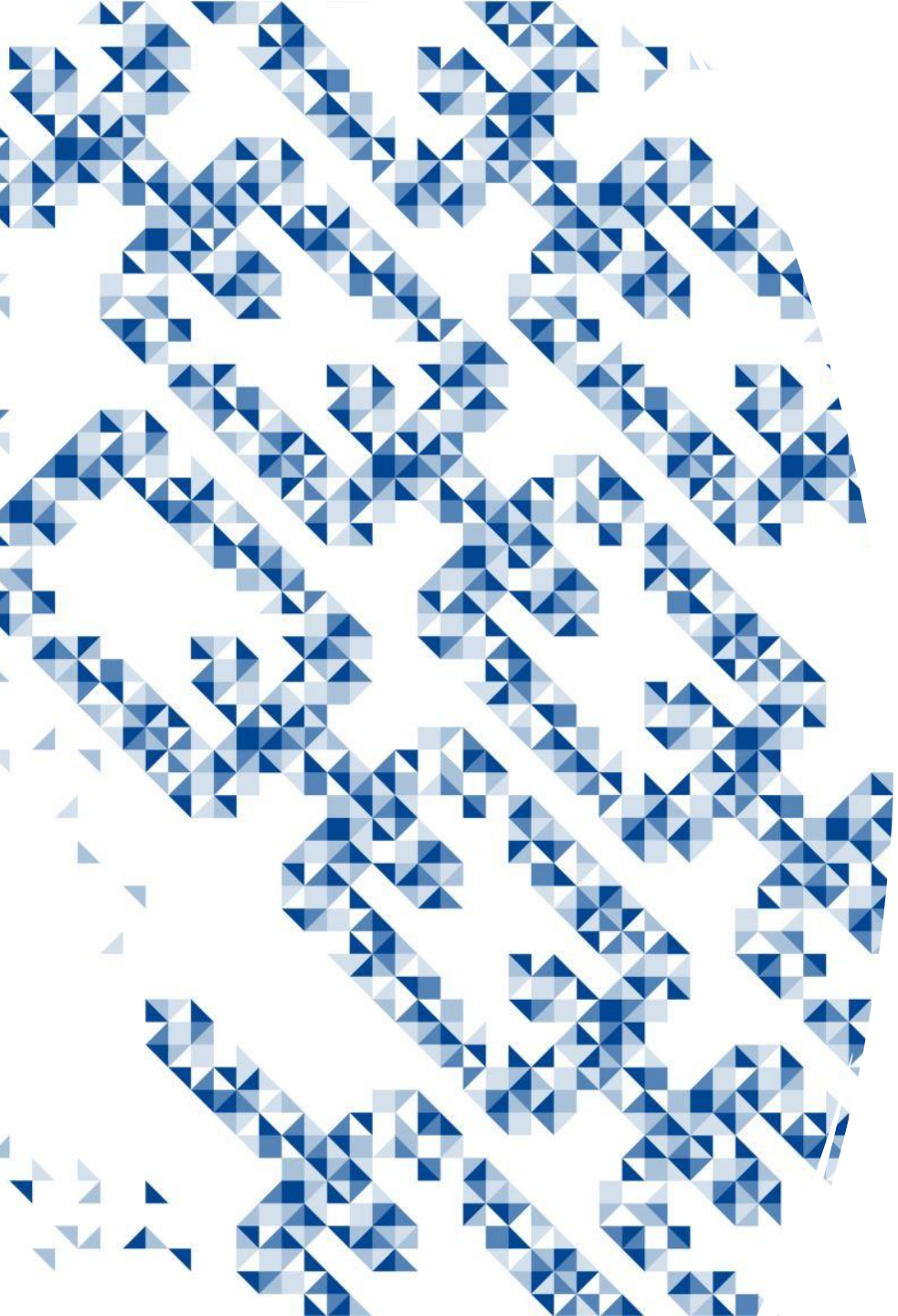
ROMANCE SCAMS

Romance scammers steal funds from their victims by requesting funds via cryptocurrency to pay for fake emergencies.



P2P- payment fraud

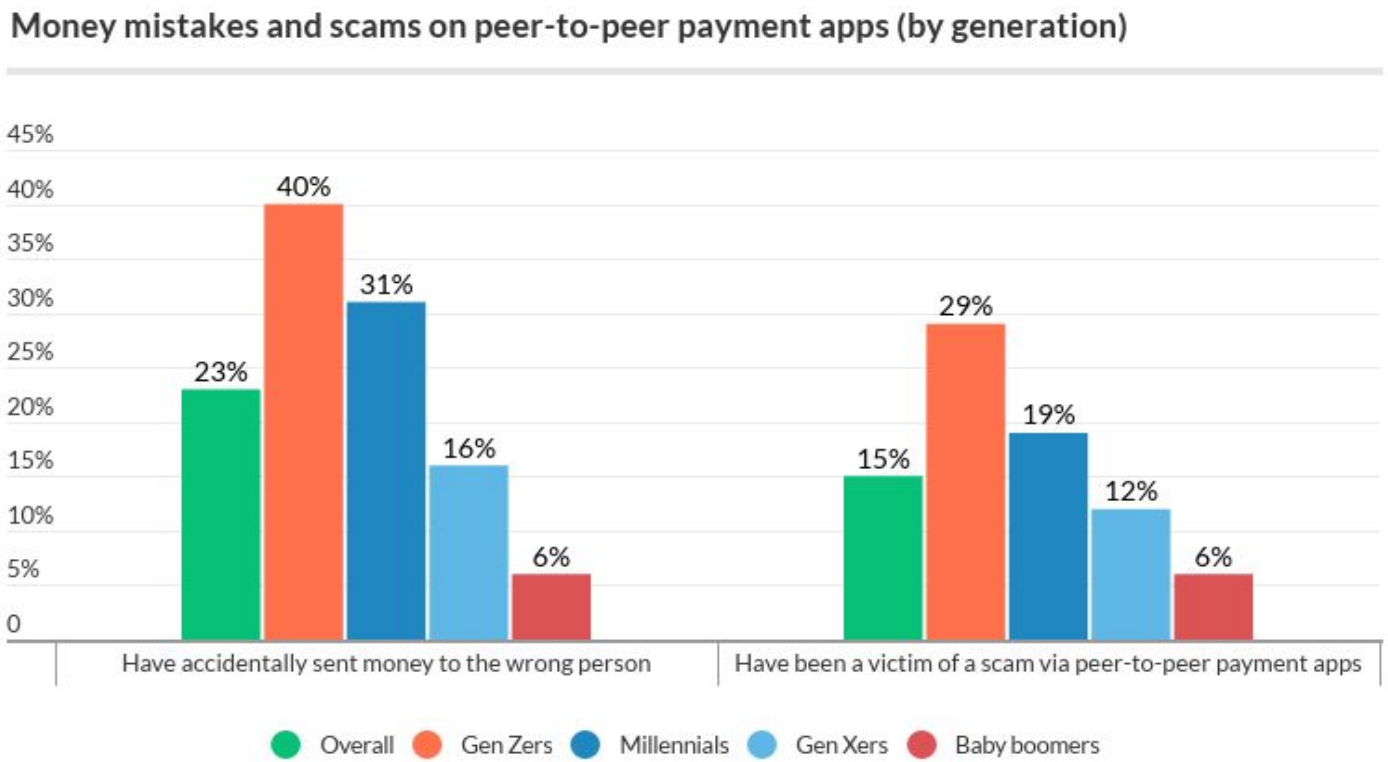
- Losses top $255M and 192,000 cases in 2022.
- Relatively few victims get their money back, < 50% even those that are supposed to have Regulation E protection vs. scam < 10%. (Zelle, Venmo, Cash App)
- Only use with trusted friends, do not use to pay someone you do not know or with any business or online marketplace.
- Link to credit card, for added protection, not bank account or debit card.



P2P- Payment Fraud

- Always verify recipient’s information before sending payment.
- Nearly ¼ of users have mistakenly sent $ to the wrong recipient.
- No government agency will ever ask for payment via P2P app.

Scams on P2P App by generation



Source: LendingTree survey of 972 peer-to-peer payment app users, conducted in May 2022.

lendingtree

IDENTITY THEFT

- Defendant willfully obtains the personal identifying information (pii) of another person with or without authorization.
- Uses the information without your knowledge or under false pretenses.
- Mere possession of information in some states can be a misdemeanor.

Information is used for an unlawful purpose

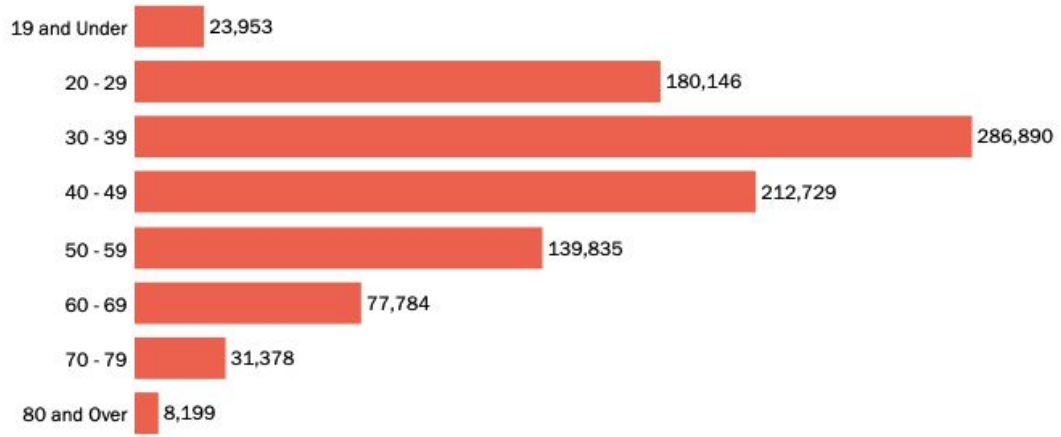
- including: *(but not limited to)*
- Obtaining, or attempting to obtain credit, goods, or services, work, benefits.
- Obtaining/using medical information of another person without the consent of that person.
- Committing criminal acts.

Hosted by
New York University
FEDERAL CREDIT UNION

What is Personal Identification Information ?

- Name, address, telephone number
- Date of birth
- Driver's license number
- Social security number.
- Place of employment
- Employee ID number
- Saving/checking account number
- Mother’s maiden name
- Credit/debit card number
- Health insurance or school ID number
- Biometric data

Identity Theft Reports by Age



Identity Theft Types by Age

Theft Type	19 and Under	20 - 29	30 - 39	40 - 49	50 - 59	60 - 69	70 - 79	80 and Over
Bank Fraud	1,779	20,194	38,144	34,097	26,575	19,090	8,462	2,232
Credit Card Fraud	2,090	71,773	121,654	90,815	58,099	29,193	10,812	2,566
Employment or Tax-Related Fraud	16,900	19,203	19,425	14,676	11,536	9,409	5,400	1,646
Government Documents or Benefits Fraud	1,192	5,045	8,940	7,757	6,871	4,630	1,859	640
Loan or Lease Fraud	744	31,800	49,243	31,964	17,562	7,569	2,282	451
Other Identity Theft	2,153	57,315	91,033	61,334	34,414	15,046	5,127	1,357
Phone or Utilities Fraud	615	15,095	23,001	15,890	10,107	5,496	2,051	540

How easy is it?

Hosted by
New York University
FEDERAL CREDIT UNION

Why
ID Theft ?

STEALING THE OLD-FASHIONED WAY

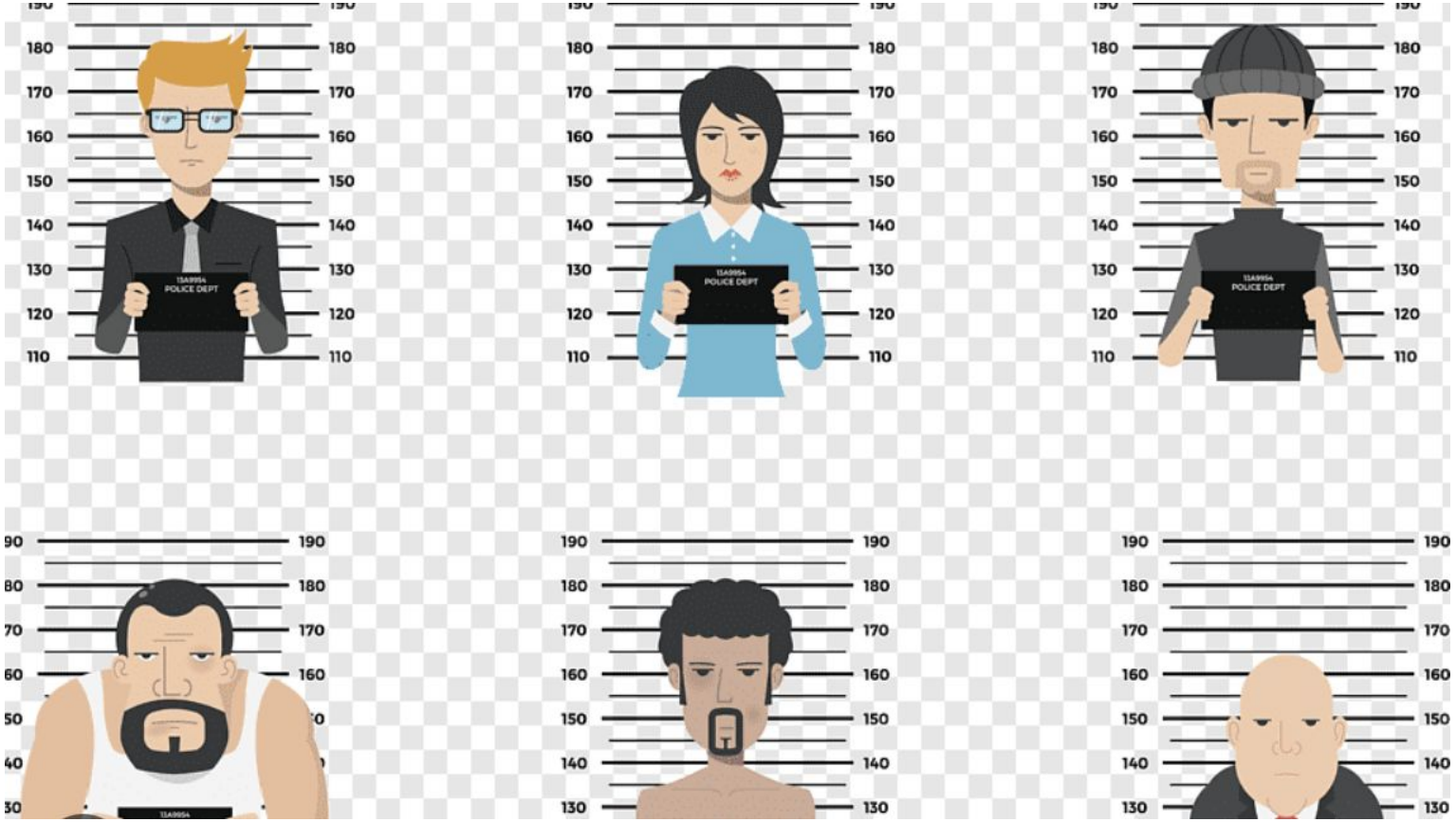
- Small gain, great risk
- Victim can ID you
- Victim can fight back
- Police can chase you
- Gun enhancements
- “Strike” charges
- Long prison terms
- You don’t know what you will get, property, money, nothing?

STEALING VIA ID THEFT

- Rarely victim contact
- No weapon used
- You know what you're stealing
- Police concentrate resources on other crimes (violent crime, gangs, drugs, etc.)
- If convicted-light sentences
- ID theft cases are hard to investigate, hard to prove, & easy to beat in court

The loot is delivered!

Crime Trends In



IDENTITY THEFT

Who is committing Identity Theft?

Drug addicts – To support their habit

Organized crime – To cover trail in other crimes

Street gangs –To support the gang
(buying weapons, housing, drugs etc.)

Career criminals -(Con-Man) - Occupation

Terrorist – To fund terrorist activities

How do they get your information?

- Data breach
- Steal your purse or wallet
- Steal your mail
- Home burglaries
- Auto burglaries
- Get your personal information from inside sources

Hosted by
New York University
FEDERAL CREDIT UNION

- Complete a “change of address” form online and redirect your mail
- Copy or steal your information while working for you (Housekeeper, Valet etc.…)
- Skimming
- Shoulder surfing
- Telemarketing Scams
- Hacking into businesses
- Dumpster diving
- Infected text
- Infected barcode

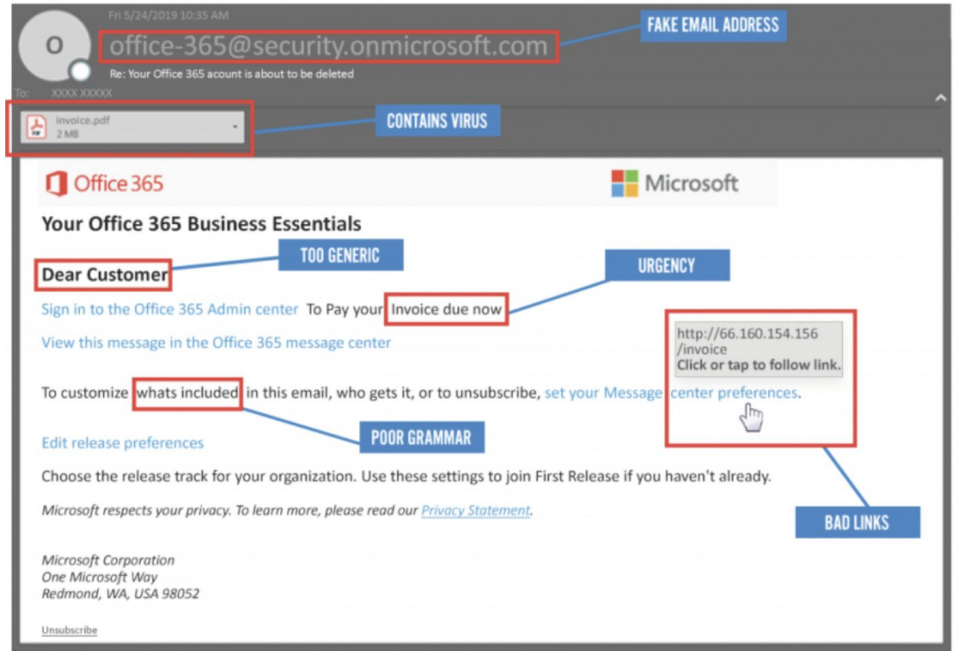
And

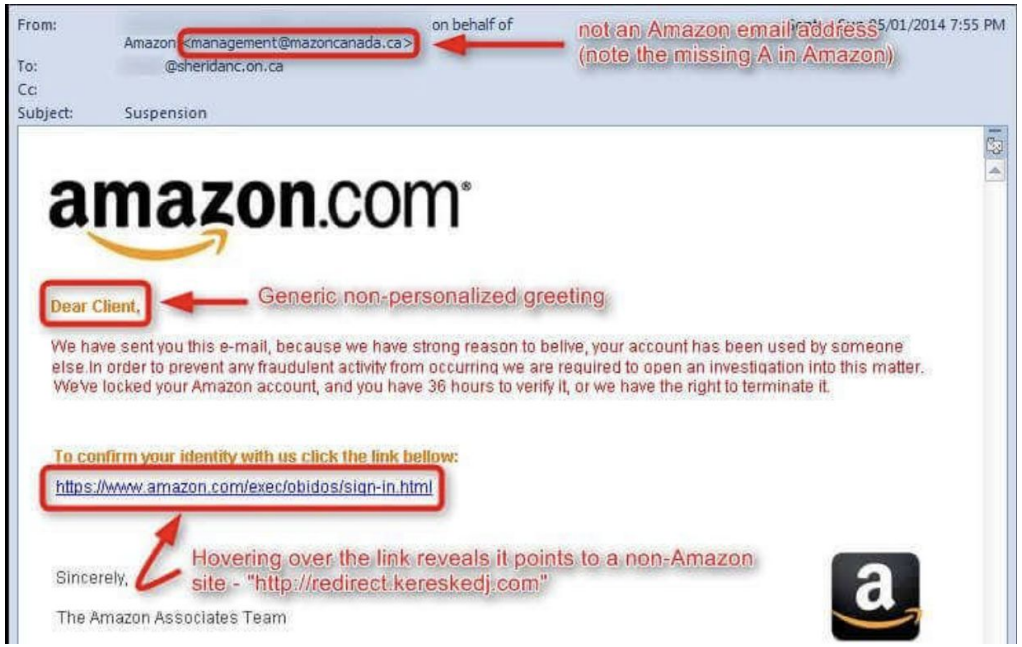
The INTERNET

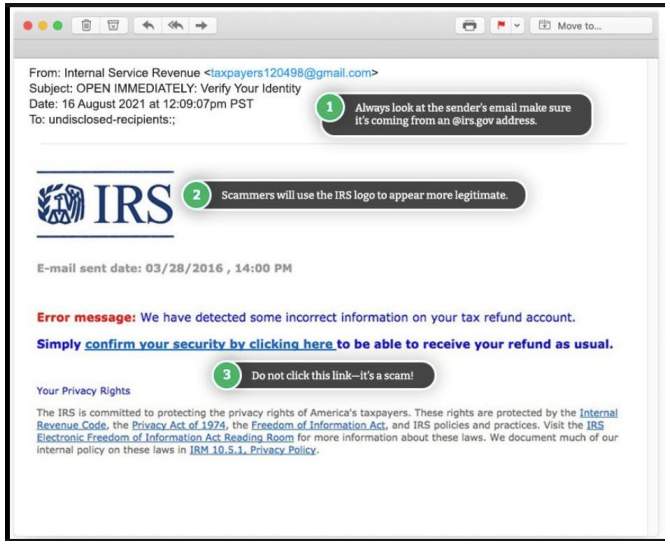
- **Internet data searches**
  - US Search
  - People Finder
  - Google

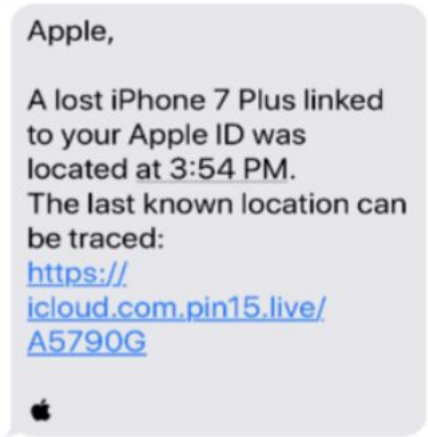
- **E-Mail Ruses**
  - SPAM
  - Spoofing
  - Trojans /Spyware
  - Phishing

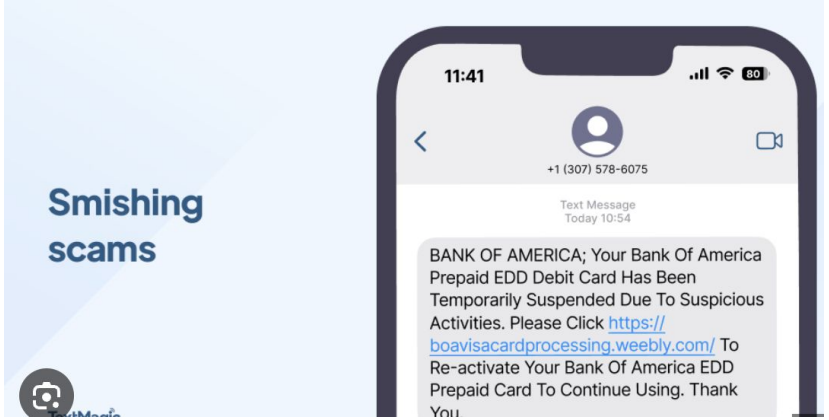
Phishing Emails and Smishing Texts



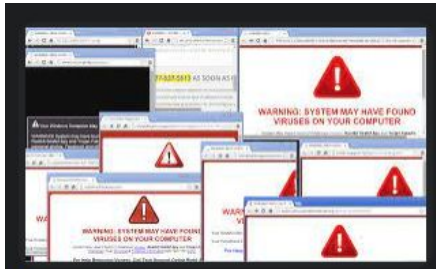








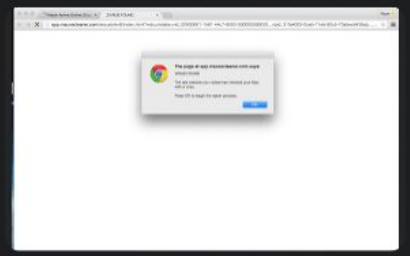
Computer Pop Ups



Malwarebytes
PSA: Tech Support Scams Pop-Ups on the ...

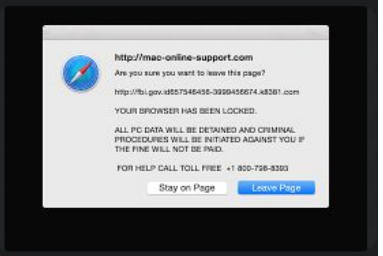
MalwareTips Forums
How To Remove "WARNIN...

Yahoo
Random pop-ups? 5 telltale signs your ...



Information Security Stack Exchange
malware - "Virus Found" Web Browser Pop ...

Cybernews
How to Remove Malware (...



Intego Support
About the Web Browser Pop-up Alert Sca...

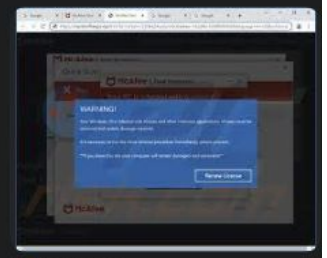
Oasis Institute
Pop-up ads driving you crazy? Try an ad ...

Avast
Scareware: What Is It & How to Avoi...

Lifewire
a Virus Warning Pop-Up on Android

PCrisk.com
Got Corrupted Due To Virus POP-...

Madison County Bank
Fake Website Popup Scams - Scarew...



PCrisk.com
Infected With Viruses POP-UP Sc...

LinkedIn
Unmasking the Tech Support Pop Up Scam

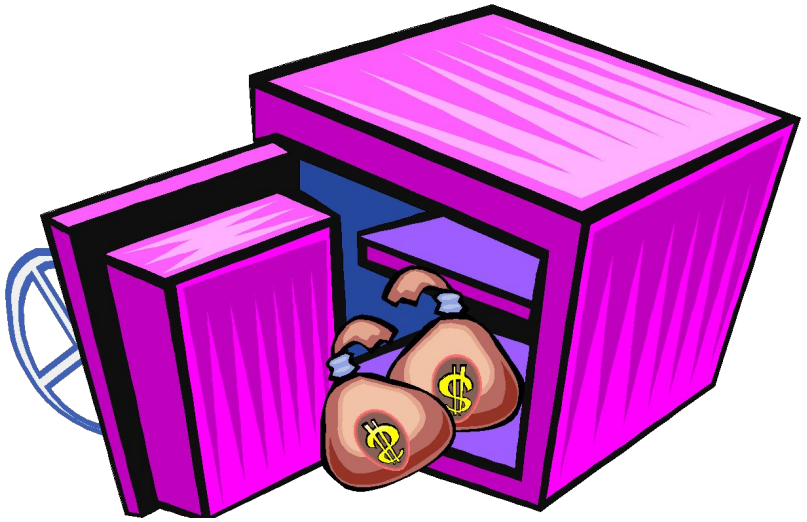
www.tcpalm.com
pop-up warning about viruses ...

East River Federal Credit Union
Federal Credit Union - SCAM WARNING ...

RGB Computer Solutions
Avoiding Virus Alert Popups and Fake ...

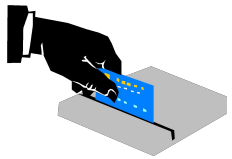
Cybernews
Congratulations you won" Pop-Up Ads ...

Once they have your information what can they do?



Anything!

Hosted by
New York University
FEDERAL CREDIT UNION



- Access your existing: Checking accounts
  - Savings accounts
  - Retirement accounts
  - Credit card accounts
  - Utilities accounts
  - Social media accounts

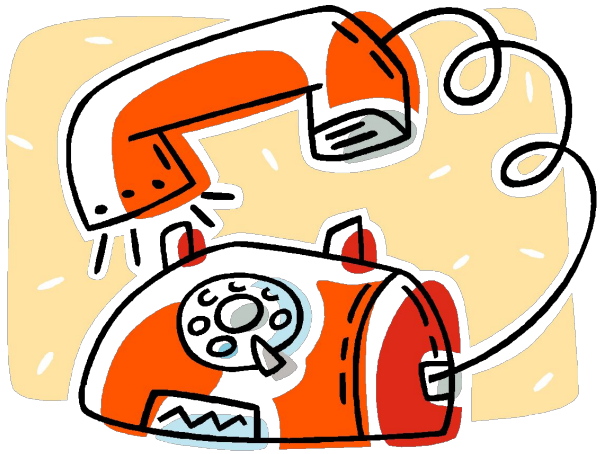
- Obtain loans secured by your property

- Sell your property

- Receive medical services

- Receive government benefits

Signs to look out for



- Your credit card or bank statements show unauthorized charges and/or purchases that you know you did not make
- You fail to receive bills or credit card statements
- You are receiving phone calls from creditors trying to collect debts that are not yours
- You are unable to send/receive emails
- You are unable to make or receive calls on your cell phone

How can I protect myself?

Hosted by
New York University
FEDERAL CREDIT UNION

What You Carry Around

- Do not carry your or anyone else's social security card, birth certificate, or passport, with you unless absolutely necessary
- Only keep a few credit cards in your purse or wallet
- Keep a list of your credit card and bank account numbers in a safe place that you can access in an emergency

What else can I do?

- Always take credit card receipts for all purchases; dispose of by shredding with a confetti shredder. Shred ANY documents with PII before throwing away.
- Do not give out any part of your social security number to anyone over the phone or Internet if you did not initiate the contact. Do not give SSN over a wireless phone.
- Get a locking mailbox or PO Box. USPS informed delivery
- Bring all outgoing mail to the Post Office.
- Do not keep ANY documents in your car.
- Have you checks sent to your bank branch, not your home.
- Do not put your DL #, or phone # or your checks. Consider using only your first initial.
- Invest in RFID blocking cards to carry with your EMV credit and debit cards.

Stop Pre-Approved Credit Offers

- Have your name removed from credit bureau marketing lists. 1-888-5OPTOUT
- Write to your existing creditors/utilities and “Opt-Out” of sharing your personal information with anyone, including their affiliates and ask to be on their non-promotional list. (Stops credit card checks)
- Obtain credit monitoring and check your credit at least twice a year.

Click with Caution

Shield your computer from Viruses and spies. Utilize virus protection, firewalls and a VPN from a reputable seller.

Password protect or use biometric login on all devices. Obtain password manager.

Do not use personal information to create a PIN. Use a mix of letters and numbers, not personal information such as your birth date, spouse's name, children's names, pet's names, address etc. Use different PINS for every site.

Don't click on pop-up windows or SPAM e-mail or text and fall victim to phishing, spoofing or smishing.

Utilize multifactor authentication (MFA) whenever offered.

Ultimate Security

- Catch it quickly by checking your credit report with all three credit-reporting agencies at least 2 times a year. www.annualcreditreport.com provides one free credit report a year. (Obtaining your own credit report does not affect your credit score.)

- Obtain credit monitoring through the credit reporting bureaus or another reputable source. A credit monitoring service, for a fee, notifies you if there are any changes to the credit reporting bureaus under your SSN, including inquiries, offers quarterly or unlimited credit reports, and often provides ID theft insurance. Make sure you sign up for a service that monitors all three credit reporting bureaus, Equifax, Experian, and Transunion.

- Place a "Credit or Security Freeze" on all three credit-reporting bureaus and Chexsystems. Merchants and banks typically will not open accounts if they cannot access your credit/banking history or score. To place a free security freeze on your reports, go to each to each of the credit reporting bureaus websites: www.experian.com, www.equifax.com, www.transunion.com, and www.chexsystems.com and type “credit freeze” or “security freeze” in the search bar.

Criminals Adjust Their Tactics for Each Generation

	Robocalls	Unusual Text Messages	Emails with Suspicious Links	Social Media Requests from Strangers	Emails with Suspicious Attachments	Chatbots
Gen Z	52%	52%	39%	46%	29%	18%
Millennials	60%	53%	46%	46%	36%	24%
Gen X	59%	53%	50%	44%	43%	22%
Baby Boomers	65%	46%	45%	31%	37%	14%

Most Common Scams Targeting College Students

- Fake employment offers- Students provide their personal/ financial information for non-existent jobs or send $ for “work supplies” based on a counterfeit check from their new employer, that then comes back counterfeit. Many end up laundering money or receiving/ sending illicit materials for criminal organizations.
- Fake listing for rental housing- students and their grantors lose millions of dollars in security deposits and first/last months rent and compromise their personal information to fake housing listings each year.
- Scholarship and financial aid scams- encouraging student to provide their bank account number to “deposit” their scholarship or financial aid award solely to steal bank account and personal information.
- Student loan debt relief- scam designed to obtain the personal and financial information of its victims and divert legitimate payments into the scammer's pockets.
- Social media scams- not limited to online romance, sextortion, blackmail.
- Peer to peer App scams- can be used to facilitate any number of scams. Never respond to a request for funds that were mistakenly sent to you.
- Public Wi-Fi Scams- Not only is public Wi-Fi an invitation to have your personal information and passwords stolen and make students susceptible to fraud but Wi-Fi you think is “safe” could be spoofed.
- China Law Enforcement Impersonation Scam- Students from China targeted around the United Stated, threatened with arrest for a variety of crimes, if they don’t provide at times $100,000’s and passport numbers to the scammers

Top Ways to Avoid Identity Scams

- Employment scam red flags- If the job look to good to be true, it probably is. If the employer asks for an unusual amount of personal information or for you to purchase “Work supplies. A suspicious email or company website or being asked to interview in an unusual location. Always go to the company website and check the job listings and email address format for employees.
- Never agree to rent an apartment or home without first seeing it inside and outside and don’t make a deposit or pay rent over the phone or via peer-to-peer app. Safest to rent using a property management company or real estate agency, which will charge a one-time fee and only run your credit once to use for finding you suitable housing.
- If someone calls and offers you a scholarship or financial aid first confirm you have even applied for what they have offered. Visit the Federal Student Aid website provided by the Office of the Department of Education for free resources to help find funds for college.
- If you receive an unsolicited call regarding student loan debt, it’s likely a scam. If you have question about federal student loans visit the US Department of Education website at Studentaid.gov/repay.
- The best way to protect yourself on social media is to limit the amount of information you share and post on ANY form of social media and only add friends you actually know.
- Peer-to-Peer apps were only designed to be used with people that you know, and you have no protections if you use it outside of how it was designed to be used. Do not use it for ANY e-commerce, and no government agency or utility will ever request or require that a payment be made via a P2P app or gift card.
- Obtain a top-rated VPN if you will be using public Wi-Fi.
- If you are contacted by anyone claiming to be Chinese or any other foreign Law Enforcement, immediately hang up, do not provide any other personal or financial information, contact the actual agency they claim to be calling from and report to local LE and FBI.

Top Ways to Avoid Identity Scams

- Do not answer your home or cell phone for any phone number you do not recognize.

  (Do not trust caller ID, it can be spoofed)

- Do not give any personal or financial information in response to contact you did not make. (Phone, email, social media, text)
- Resist the pressure to act immediately. Anyone who pressures you to pay or give them your personal information is a scammer.
- Never pay someone who insists that you pay with cryptocurrency, Western Union or MoneyGram, a P2P payment app, or gift cards and never deposit a check and send money back to someone.
- If it sounds too good to be true, it is!
- Stop, slow down, and talk to someone you trust. Talking about it could help you realize it is a scam.

Financial Impact of ID Theft

- 69% of victims experience re-occurring identity theft
- 75% of victims experience financial problems, difficulty paying rent, turned down for credit, inability to pay bills
- 25% lost employment opportunities
- 30% lost time at work or school
- 63% blame the financial institution and consider leaving (35 % close their accounts)
- 50% were dissatisfied with their financial institution's/law enforcement's response to their fraud report

Emotional Impact of ID Theft

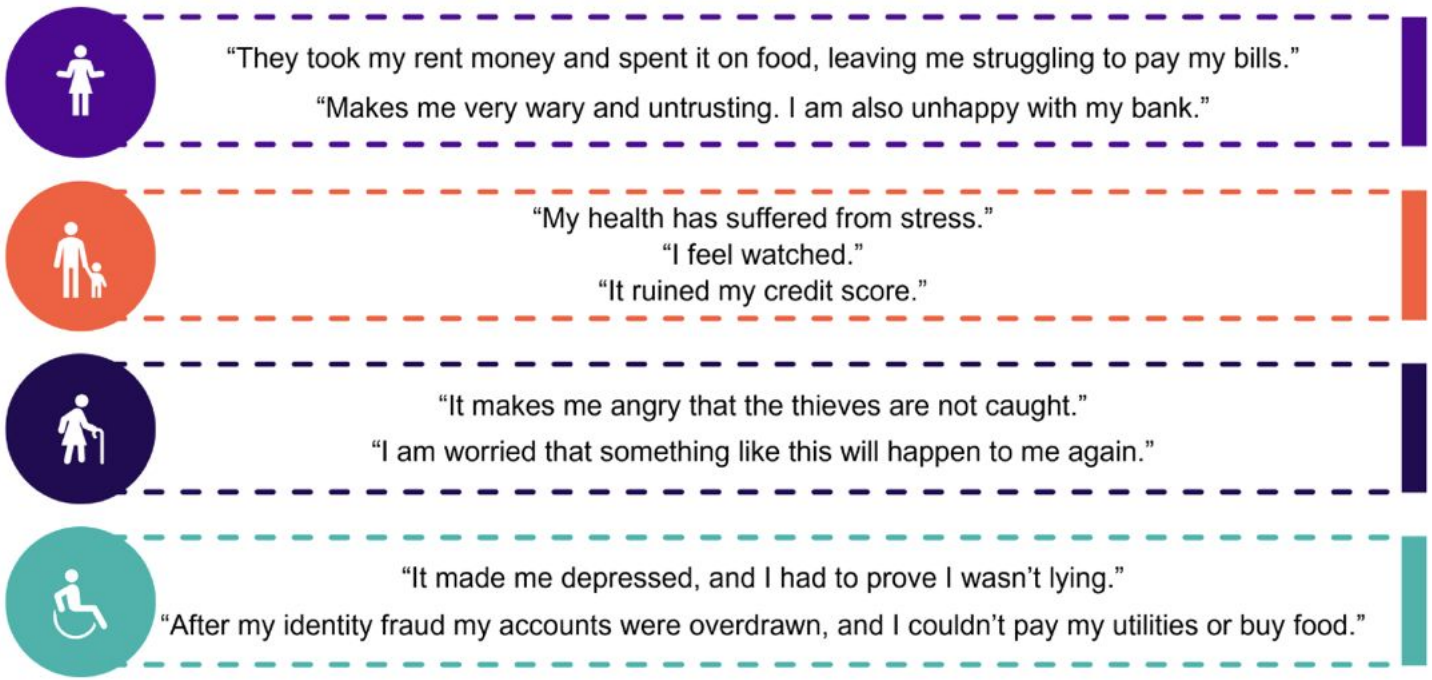
(ITRC 2023)

- 87% worried or anxious
- 78% angry/violated
- 54% sense of powerlessness or helplessness
- 63% sad or depressed
- 52% shame or embarrassment
- 16% suicidal (Call or text 988 for crisis help)
- 5% homicidal thoughts
- 60% lead to problems with family and friends
- 44% experiences physical problems

(sleep, aches, pain, G.I., fatigue, blood pressure, stress, concentration, chest pain, relapse or addictive behavior)

The Indelible Mark of Identity Fraud

Identity Fraud Victim Impact Statements



Source: Identity Fraud Study, Javelin Strategy & Research, 2023

javelin

Roadblocks to Recovery

What if I am a Victim ?

Most Important

Act quickly and assertively to minimize the damage!

What if I am a victim?

1. Obtain a free copy of each of your credit reports at www.annualcreditreport.com.

2. Visit the Federal Trade Commission (FTC) website, report the ID Theft and fill out the FTC ID Theft Affidavit.

3. Go to your local police department and file a report. Provide them with your ID Theft Affidavit.

What if I am a Victim ?

4. In writing, dispute any transactions made to any of your existing accounts as soon as you discover the fraud. Always dispute “new” account fraud in writing after the initial contact.

5. In dealing with financial institutions, keep a log of all conversations, including dates, time spent, and expenses incurred, in case you can request restitution in a later judgment or conviction.

What do I ask for?

- Request a free credit report Annualcreditreport.com. (Also free to ID Theft victims)Review all 3 reports for accuracy.
- Dispute any inaccurate information on your credit reports with the 3 credit reporting bureaus.
- Ask that your three credit bureau files be flagged with a fraud alert. Can be extended to 7 years but must be done in writing.
- Credit Freeze. (A fraud alert is only as good as the merchant who sees it)

CREDIT REPORT CLUES

Look for:

- Any demographic information that is incorrect
- Any account that doesn’t belong to you
- Hard inquiries
- 30/60/90 late indicators on existing accounts that are inaccurate

Law Enforcement Response

66% of states now have mandatory reporting laws

20 % of states have ID theft passports

The FTC report is considered a LE report for ID Theft reporting purposes

Victim's Right to Information

§ 609(e) of the Fair Credit Reporting Act (15 U.S.C. § 1681g)

(within 10 days of legal written request)

What information can the victim get:

- Application
- Record of transactions
- The personal information that was used on the application.

How does victim get it:

- Present police report or Federal Trade Commission report
- Verify their identity