

This Holiday Season, Skip the Scams!



The festive season means fun with friends and family, goodwill and giving. Sadly, it's also a prime time for cybercrooks to cook up nefarious schemes. According to AARP Fraud Watch, three-quarters of U.S. consumers have experienced or been targeted by at least one form of fraud that can be tied to the holidays, including requests from (often fake) charities, online shopping scams and fraudulent communications about shipping problems

1

This Holiday Season, Skip the Scams!

- During the holidays we may be more trusting, we let our guard down and we can become victims to many of the classic scams. We are more generous during this “time of giving” and the scammers are out in full force. We always need to be vigilant but even more so during this season.
- It was only a few years ago that staying safe online meant having a good virus program and having a full backup. Today psychological manipulation in the form of social engineering and phishing emails require that we are constantly vigilant and contain our trusting nature.
- Your best defense is to recognize the symptoms of being scammed. AI and spam filters have not yet devised foolproof methods to stop scams.
- Our goal today is to turn you into scam hunters and give you the tools to spot and stop these scams

3

Learning About Cybercrime and Scams

Knowledge is the Best Defense



5



It's been around a long time
Trojan War 1260–1180 BC



Trojans rely on a user unknowingly downloading a program because they appear to be legitimate files or apps.

6

Tools of the Scammers




11

The jury duty manager: "Hi, I'm calling from the courthouse, and you have won \$1 million! Pay \$400 or go to prison."	The big-winner announcer: "I'm from the Canadian lottery, and you have won \$1 million! Pay the import tax and fee, and we'll send you your winnings"
The puppy breeder: "As a dog lover, you should know we just got a beautiful litter of purebred golden retriever puppies. Just \$200 each!"	The doctor representative: "Research shows conclusively that these new capsules will stop your disease in its tracks."
The utility company: "We will be shutting off your electricity in 24 hours if you don't pay the past-due amount on your bill immediately."	The police or fire department: "We're raising money for officers (or firefighters) injured in the line of duty. How much will you be donating today?"
The government clerk: "You have unclaimed property with our state. Simply pay this fee, and we will release it to you."	The Internal Revenue Service: "You owe taxes and are at grave risk of large fines or jail time if you do not settle this situation immediately."
The ticket seller: "As an affiliate of a major ticket vendor, we can get you seats for your dream concert for a discount, if you act quickly."	The long-distance lover: "In these weeks of chatting, I've fallen so in love with you. Send money for a plane ticket, and oh, the magic that will happen!"
The bank verifier: "There's a data problem with your checking account. Please verify this information so we can confirm things and fix the error."	The military rep: "I'm from the Veterans Administration, and you are entitled, as an ex-soldier, to benefits from this program. I just need to know ..."

When a Con Man Calls



12

 This is a post from one of your local agencies

 **Montgomery County Police Department** ✓
Police Officer Dana Stroman • 2 days ago

Hurricane Ian Scams. Florida residents, friends and family are facing one of the most catastrophic weather events in the history of this country. As hard as this storm is churning, fraudsters are already churning up their schemes as well. Playing on the sympathy of people who want to do right and help their fellow man, these individuals see this as an opportunity to operate criminal enterprises to fraudulently obtain well intentioned donations.

Only donate to charities you know and trust
The State of Florida has set up the Florida Disaster Fund to respond to relief efforts. The money will be distributed to different organizations for disaster relief and recovery
Other legitimate charities include the American Red Cross, the Salvation Army and Catholic Charities
Research any charitable entity to determine their legitimacy
Do not donate to anyone wanting cash donations, gift cards or by wiring money
Do not respond to emails seeking donations.
Some scammers use names very similar to legitimate charities
Some scammers "spoof" telephone numbers to make it look like a real charity calling

REPORT FRAUDULENT ACTIVITY TO THE FEDERAL TRADE COMMISSION
FTC Fraud Website: <https://reportfraud.ftc.gov/>

13



Telephone Scam. Phone Scam Alert! Over the last several weeks, Montgomery County have received calls from a person stating that he/she is a Montgomery County Police (MCP) Officer. The scammer has "spoofed" (disguised) his number to make it appear that the call is coming from a Police Station.

There are variations of this police impersonator scam but generally the "officer" states that the resident has to make payment – for a bond, warrant, missed court hearing, or fine. The scammer instructs the resident to send money through a wire transfer, pre-paid cards or internet transaction.

It is important to remember that the Montgomery County Police Department will never call residents to collect payment for fines or bonds nor solicit money.

If you receive this type of call, hang up and call the Montgomery County Police non-emergency number at 301-279-8000.

Posted to **Subscribers of Montgomery County Police Department** in 1 area

14

Anatomy of a Scam



15

How To Recognize a Phone Scam

<https://consumer.ftc.gov/>

- There is no prize
- You won't be arrested
- You don't need to decide now
- There's never a good reason to send cash or pay with a gift card
- Government agencies won't call to confirm your sensitive information
- You shouldn't be getting all those calls

16

Social Engineering and Phishing



Use of psychological techniques to persuade someone to do something not in their best interest

- Time Pressure and illusions of scarcity
- Authority Bias
- Greed and Status

Today most common tool for social engineering is a phishing email

17

Renewal Payment Reminder . Auto-Debit

Mary June <snowtravel@blackandwhitecompany.be>
To victor.reznovic@blackandwhitecompany.be

snowtravel@blackandwhitecompany.be

2 attachments View Download

.BE is country code for Belgium



Dear User,

You are kindly informed that, you signed up for a subscription product when you purchased it on Oct 27, 2021.

This subscription ends today, Oct 28, 2022.

Your subscription will automatically renew on Oct 28, 2022, and \$399.00 will be charged to your account. This indicates that you don't need to take any action to keep your membership valid.

If you wish to not use your subscription, you may cancel it at any time. You will be charged \$399.00 for your subscription if you don't cancel it by Oct 28, 2022.

Please mention your reference ID #GK28102987 when contacting us.

We're ready to help.

Geek Squad 24/7 Support.



Options for assistance

Any order or payment related issue will be resolved by our Customer Support. Kindly, contact us at +1(808)797-2708

Sincerely,

18

<https://www.consumerfraudreporting.org/>

- Did you receive an email from Geek Squad, claiming your annual subscription with GeekSquad is renewed? Did they then instruct you to call a number in the email or something similar?
- Well, don't fall for it. It is a scam, and if you call them back or follow their instructions you will lose money and possibly your identity! The people behind this are the worst kind of human scum; willing to do anything to scare, threaten, lie, cheat and steal money from anyone, including the elderly and poor. They usually operate out of Nigeria, China, Russia and even some developed western countries. **Attachments typically include malware to infect your computer, tablet or phone and allow the scammer to capture your passwords.**
- One thing for certain: This is NOT from Best Buy and has nothing to do with their Geek Squad service. Do NOT call the numbers in the email. Just ignore the email.

19

Ways to Recognize a Phishing Email

Legit companies don't request your sensitive info via email

Legit companies usually call you by your name

Legit companies have domain emails

Legit companies know how to spell

Legit companies don't force you to their website

Legit companies don't send unsolicited attachments

Legit companies links match legitimate URL's

Sense of urgency, authority and greed

20

Are you smarter than a scammer? Play this game.

Take this quiz to find out if you can spot what's real and what's fake

<https://www.washingtonpost.com/technology/interactive/2023/identify-scam-quiz-zelle-email-text/>

21

Wait, Wait, Don't Scam Me!

You will now see a series of emails. The emails will remain on the screen for 10 seconds. Decide if the email is legit, a scam or unsure. Keep score for yourself

FEDERAL TRADE COMMISSION

Got a text from Costco or Home Depot about a survey?

Don't click on the link!

It's a scam.

Learn more: ftc.gov/phishing

Answer Questions About Your Experience With Us For Your Chance To Receive a Brand-New Power Drill! click OK to Begin.

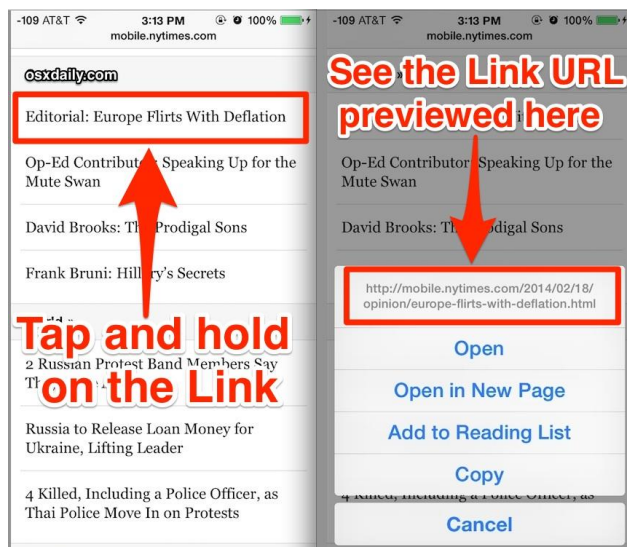
22

The Most Important Tool for Suspicious Links

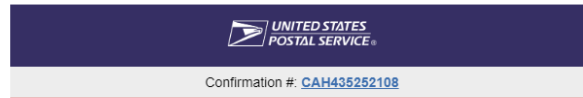


23

Mobile Devices



24



Hello VICTOR REZMOVIC,

We've received your USPS Hold Mail® request for 07/20/2022 - 08/03/2022. If your mail is currently being held, you cannot cancel this request, but you can change the end date.

[Edit this USPS Hold Mail request](#)

USPS Hold Mail Details

Confirmation #: [CAH435252108](#)

Hold Mail for:

VICTOR REZMOVIC

[REDACTED]

Phone: [REDACTED]

Email: [VICTOR.REZMOVIC@\[REDACTED\]](#)

Start Date: 07/20/2022

End Date: 08/03/2022

Delivery Option: Post Office delivers accumulated mail.

25

Hello {victor.rezmovic}
You have (1) SUSPENDED PACKAGE
waiting for delivery



DELIVERY OF THE SUSPENDED PACKAGE



You have (1) package waiting for delivery. Use your code to track it and receive it.

Schedule your delivery and subscribe to our push notifications to avoid this from happening again!

[Schedule your delivery](#)

26

✉ Spencer Jangn <spencerjangn@gmail.com>

To undisclosed-recipients;; Blind copy vrezmovic@[REDACTED]

Reply Forward Delete ☰

AMAZON

Dear Customer,

Your AMAZON Prime subscription has expired.

And, the card associated with your account has been determined to be invalid.

To update your card, please call our Customer Care team at +1 (814) 888-0801.

Kindly,
Team AMAZON

27



Order Confirmation

Hello JEFFREY [REDACTED],

Thank you for shopping with us. You ordered "Echo Dot (2nd Generation) ...". We'll send a confirmation when your item ships.

Details

Order #112-2607104-3111416

Arriving:
Wednesday, October 4

Ship to:
Victor Rezmovic

[View or manage order](#)

Total Before Tax:	\$49.99
Estimated Tax:	\$3.00
Order Total:	\$52.99

We hope to see you again soon.

[Amazon.com](https://www.amazon.com)



FREE 2-hour delivery

Groceries, electronics, and daily essentials
available in 30+ cities nationwide
Get \$10 off your first order

28



Your Bill

Unfortunately, We have an issue with your billing profile

It has come to our attention that your billing information records are out of date. That requires you to check your billing information.

Please view your billing profile to solve this issue.

[View Billing](#)

© 2022 Comcast. All rights reserved.

29



[My Account >](#)

Helpful information about your Xfinity TV services

Each year, we'll send you information to keep you up to date with the latest Channel Lineup and Xfinity TV Services & Pricing available in your area.

View or print our Xfinity TV [Channel Lineup](#).

See our Xfinity TV service options and other offerings with our [Services & Pricing](#) list.

To request print versions of this Services & Pricing list or Channel Lineup in the mail, please [click here](#). To receive future Services & Pricing lists or Channel Lineups in print, [click here](#). For either of these options, you can also call 1-800-Xfinity.

You can always find our current [Channel Lineup](#) or [Services & Pricing online](#).

Thank you for being an Xfinity customer.

30

Microsoft account team <account-security-noreply@accountprotection.microsoft.com> 7/7/2022 11:03 AM MT

To victor.rezmovic@██████████

Reply Forward Delete

Microsoft account

Verify your account

We detected something unusual about a recent sign-in for the Microsoft account [v***c@comcast.net](#). For example, you might be signing in from a new location, device, or app.

To help keep you safe, we've blocked access to your inbox, contacts list, and calendar for that sign-in. Please review your recent activity and we'll help you secure your account. To regain access, you'll need to confirm that the recent activity was yours.

[Review recent activity](#)

Thanks,
The Microsoft account team

31

Apple <no_reply@email.apple.com> 6:23 AM

To victor.rezmovic@██████████

Reply Forward Delete



Receipt

Save 3% on all your Apple purchases with Apple Card.¹ [Apply and use in minutes²](#)

APPLE ID victor.rezmovic@██████████	BILLED TO Visa ... 0589 (Apple Pay) Victor Rezmovic 10505 Democracy Lane Potomac, MD 20854 USA
DATE Oct 28, 2022	
ORDER ID MNHY1YG5J1	DOCUMENT NO. 187597077630

iCloud+



iCloud+ with 50 GB of Storage
Monthly
Renews Nov 29, 2022

\$0.99

TOTAL

\$0.99



Save 3% on all your Apple purchases.



[Apply and use in minutes](#)

32

WelcomeTo SpeedyNetLoan  Inbox x

SpeedyNetLoan info_1yZOvkQ8pFvc@msaayhb.gotocro.com via 02150.fulfree.com
 to victor.rezmovicB.df, victor.rezmovicjl.di

7:!

 French > English [Translate message](#)

[Get up to 5000 USD victor.rezmovic let us help.](#)

You'll be thrilled you looked inside! Finally ease your stress and make a change

Would \$5,000 brighten up your autumn?

Cover your monthly expenses, payments and bills with funds in your account as soon as tomorrow.

Request up to \$5,000

Enter Amount

Or choose an amount below

\$500

\$1,000


\$1,500

\$2,500

\$5,000

34

Att: vrezmovic@comcast.net

 **Billing.Support-Paypal** <suajalsinghh6527@gmail.com>

4/18/2022 11:38 AM



B

To vrezmovic@comcast.net

[Reply](#) [Forward](#) [Delete](#) 

Billing Customer Care +1 (801) 895-4816

You've authorized a payment of \$ 399.89 to Coinbase.

Dear user,

Thank you for using PayPal for your recent purchase.

We wanted to let you know that you have authorized a transaction of \$399.89 for bitcoin. The amount will be debited from your Bank/Credit card/PayPal Wallet.

The charge will appear on your Bank/Credit card statement as *PAYPAL-COINBASE* by next 24 to 48 hrs.

Transaction ID
248745-856740-54864

Order ID
745K2J

Payment Mode
Online Authorized

Transaction Date
April-18-2022

Description	Unit prices	Quantity	Amount
BTC	\$399.89 USD	1	\$399.89 USD
Subtotal			\$399.89 USD
Total			\$399.89 USD

35

@Comcast 2018

Comcast Service <olivebranchins@windstream.net>

3/29/2018 6:07 PM

CS

[Reply](#) [Forward](#) [Delete](#) [⋮](#)

Dear Comcast User

Your account has exceeded the storage limit, You can not send or receive new messages until you validate your account.

Kindly [CLICK HERE](#) to Validate your account..

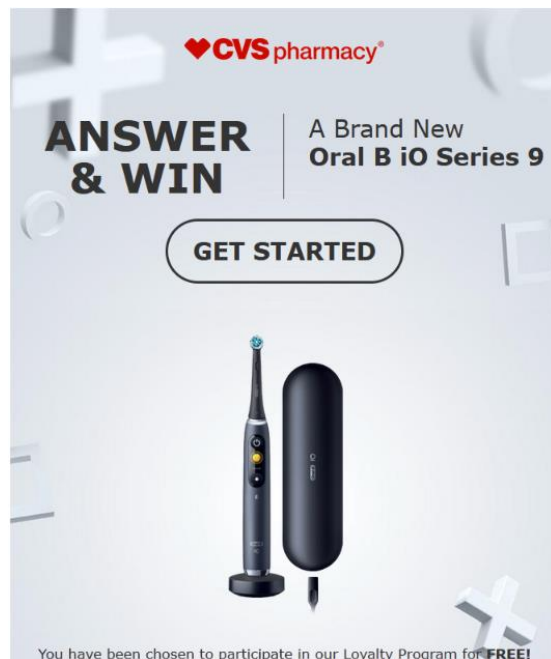
Thank You,
Comcast Communications

36

Fw: Acknowledging Your Loyalty with an Oral B iO Series 9

CVS_Pharmacy <azqazqmolver@incarnation.org>

11/

To vrezmovic@~~comcast.net~~
[Reply](#) [Forward](#) [Delete](#) [⋮](#)


37

Pop Ups and Scareware Warning Signs

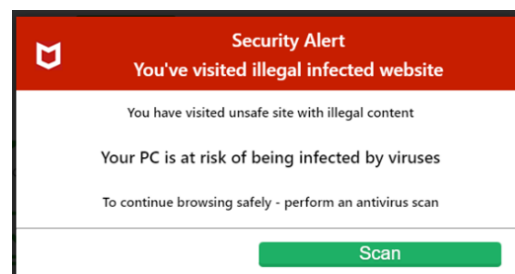
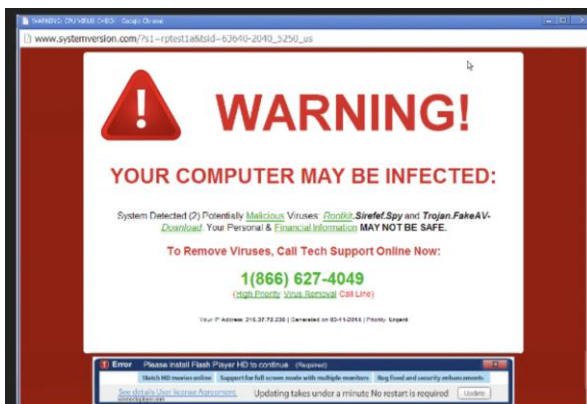


Malicious Software

- Designed to frighten; play on your emotions
- Ask you to ACT FAST
- Hard to close

38

Pop-ups



39

Types of Malware

Malware is any [software](#) intentionally designed to cause disruption to a [computer](#), [server](#), [client](#), or [computer network](#), leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.

Ransomware

- Access to your files/data is blocked through encryption
- Data is held hostage in exchange for a ransom
- May steal files from computers rather than encrypting them
- Demand for ransom appears as a pop-up



40

Types of Malware

Spyware

- May collect information from your device or through observation
- May be installed on your device via software such as keyboard logger or via video surveillance
- Information may include sites visited, downloads, passwords



41

Scams

Smishing



Basically, it's phishing by another means, namely text messages on mobile devices.

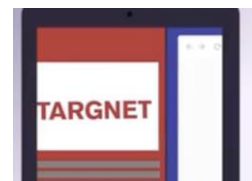
An attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone.

42

Scams

Online [Shopping](#)

- Deals appear too good to be true such as “bargain-basement” deals
- Look like real logos—check closely
- Messages saying to confirm a purchase you never made



43

Scams

Tech Support

- Received via unsolicited telephone call or a pop-up which may include a phone number to call
- Claim to provide tech support for fake computer problems
- Caller or pop-up may claim to be from a company you know such as Apple or Microsoft
- May offer to run diagnostic tests and claim you have malware installed
- Play on fear and demanding quick action

44

Scams

Online Banking

- Fake sites may be set up with similar name to your bank
- Banks will not contact you out of the blue and ask for your Social Security number, online account password or other personal information



45

Scams

Grandparents [Scam](#)

- Call, text or email from someone pretending to be your grandchild who is in trouble
- Asks for money such as to help pay medical bills for a hospital
- May ask you to call someone (lawyer, doctor) who may ask for money to be wired immediately
- Stories are usually very convincing



46

Scams

Social Media



- Be careful where you click: Fraud is prevalent on popular social networks like Facebook, Instagram and Twitter
- Types of scams
 - Fake ads
 - Looking for romance
 - Offers of financial help

48

Scams

Jury Duty

- Phone call or email saying you failed to report for jury duty and warrant issued for your arrest
- If an email: Don't click links or download attachments!
- Asks to provide:
 - Identifying information such as SSN
 - Pay a fine:
 - Credit card
 - Prepaid cards

49

You Can Protect Yourself



AARP Fraud Watch Network

877-908-3360

Call our free helpline if you or a loved one suspect a scam

Sign Up for Free 'Watchdog Alerts'

Look Up and Report a Scam in Your Area

How AARP Helps You Combat Fraud

aarp.org/fraudwatchnetwork

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

50

FRAUD RESOURCE CENTER*Learn how to spot and avoid the common scams listed below*

Apartment Rental Scams	Gift Card Scams	Obituary Scams	Social Media Scams
Business Email Compromise	Government Grant Scams	Online Banking Scams	Social Security Scams
Car Warranty Scams	Grandparent Scam	Online Pharmacy Scams	Spear-Phishing
Caregiver Fraud	Greeting Card Scams	Online Shopping Scams	Student Loan Scams
Celebrity Impostor Scams	Health Fraud	Package Scams	Survey Scams
Census Scams	Health Insurance Scams	Pet Scams	Sweepstakes and Lottery Scams
Charity Scams	Holiday Scams	Phishing	Tax ID Theft
Coronavirus Scams	Home Improvement Scams	Phone Scams	Tax Preparation Scams
Credit Card Interest Rate Scam	Identity Theft	Political Scams	Tech Support Scams
Credit Repair Scams	Impostor Scams	Ponzi and Pyramid Schemes	Time-Share Resale Scam
Cruise Scams	Investment Fraud	Psychic Scams	Travel Scams
Cryptocurrency Fraud	IRS Impostor Scam	Public Wi-Fi Scams	'Update Account' Scams
Debt Collection Scams	Jury Duty Scams	QR Code Scams	Utility Scams
Debt Relief Scams	Medical Equipment Scams	Ransomware	Vacation Scams
Dietary Supplement Scams	Medical Identity Theft	Reverse Mortgage Scams	VA Pension Poaching
Disaster Scams	Medicare Card Scams	Robocalls	Veterans Charity Scam

Caption

51

Resources for Protecting Yourself Online

- General safety tips
- Passwords and password managers
- Avoid Public Wi-Fi
- Virus protection
- Updating software, OS, devices etc
- VPN's and encryption
- Backups
- Choosing the right browser
- Two Factor Authentication
- Passkeys (Authenticator App)



52

Learning About Cybercrime and Scams



RESOURCES FOR PROTECTING YOURSELF ONLINE

General

AARP FRAUD RESOURCE CENTER—General Starting Point

<https://www.aarp.org/money/scams-fraud.html#frc>

OASIS Resource: <https://connections.oasisnet.org/oasis-connections-guide-to-online-safety/>

FCC Site: <https://www.fcc.gov/general/frauds-scams-and-alerts-guides>

https://www.youtube.com/watch?v=M--Yk6_f8MU

<https://www.marylandattorneygeneral.gov/CPD%20Documents/Tips-Publications/ConsumerGuideForMarylanders.pdf>

Holiday Scams

<https://www.forbes.com/advisor/personal-finance/common-holiday-scams/>

<https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/holiday-scams>

Specific Cybersecurity Topics

Ransomware

<https://www.aarp.org/money/scams-fraud/info-2021/ransomware-protection-tips.html>

IRS Scams

<https://www.aarp.org/money/scams-fraud/info-2017/fake-irs-scammers-fd.html>

Protecting Financial Accounts

<https://www.aarp.org/money/scams-fraud/info-2021/account-takeover.html>

<https://www.aarp.org/money/scams-fraud/info-2019/online-bank-account-security.html>

Shady Telephone Calls

<https://www.youtube.com/watch?v=Exf4iUD7gRo>

Unwanted Calls and Texts

<https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts>

Passwords and Password Managers

<https://www.aarp.org/home-family/personal-technology/info-2021/use-a-password-manager-for-online-security.html>

<https://www.youtube.com/watch?v=BoyeFozmAXk>

WiFi Safety

<https://www.aarp.org/money/scams-fraud/info-2019/public-wifi.html>

Protecting Privacy

<https://www.aarp.org/home-family/personal-technology/info-2021/protect-your-devices.html>

If You Are a Victim of a Scam

<https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>

<https://www.fbi.gov/contact-us#I-would%20like%20to%20report%20an%20online%20scam%20fraud%20or%20crime>

<https://fightcybercrime.org/>

<https://www.ic3.gov/>

<https://www.identitytheft.gov/#/>