

Cybercrime Support Network

Giving victims of cybercrime a voice.

Cybercrime Support Network is a national nonprofit whose mission is to assist individual and small business cybercrime victims before, during, and after a cybercrime incident.

Report. > **Recover.** > **Reinforce.**

SLTT Board Members



**SECRETARY/
TREASURER**

James Ellis

D/F/Lt. Commander of Michigan
Cyber Command Center (MC3),
Michigan State Police



Tony Sager

Senior Vice President and
Chief Evangelist, Center for
Internet Security, CIS



Ralph Johnson

Chief Information Security Officer,
County of Los Angeles



Tim Smith

Retired, Executive Director, Ottawa
County Central Dispatch Authority

Partners



The Problem

- Millions of Americans are victims of cybercrime and online fraud each year with no clear path to reporting and recovery.
- The true rate or cost of cybercrime and online fraud to individuals and SMBs is unknown.

FBI Internet Crime Complaint Center (IC3) 2019 Annual Report

2019 Overall Statistics

IMPORTANT STATS



of complaints
reported since
inception (2000)

4,883,231

Approximately 340,000
complaints received
per year on average

\$3.5 billion
victim losses in 2019

Over 1,200
complaints received
per day on average



POLITICS DECEMBER 11, 2018

One in Four Americans Have Experienced Cybercrime

BY RJ REINHART

Actual losses could be
\$338 billion per year
for 50M American consumers and SMBs.

How do you define cybercrime?

- A device is the object of the crime
(Ransomware and DDOS Attacks)
- A device or the internet is used as a tool to commit an offense
(Credit Card Fraud)



36+ Cybercrime Categories (IC3)

Advance Fee

Auction

Business Email Compromise

Charity

Civil Matter

Confidence Fraud/Romance

Copyright/Counterfeit

Corporate Data Breach

Credit Card Fraud

Crimes Against Children

Criminal Forums

Denial of Service

Duplicate

Employment

Extortion

Gambling

Government Impersonation

Hacktivist

Harassment/Threats of Violence

Healthcare Related

Identity Theft

Lottery/Sweepstakes

Malware/Scareware

Misrepresentation

No Lead Value

Non-payment/Delivery

Phishing/Smishing

Ransomware

Real Estate/Rental

Re-shipping

Social Media

Terrorism

Virtual Currency

Virus

Cybercrime Categories

International Discussion

| A | B | C |
|-----------------------------|---|--|
| | <p>Layman Taxonomies for Reporters</p> <p>This is the most simple of levels, used by victims and the first responders who receive victim reports about cybercrime related incidents to ensure accurate classification of incidents with minimal inaccuracy</p> | <p>Technical Taxonomies for Investigators and Analysts</p> <p>These are used by investigators and analysts to more accurately classify cybercrime related incidents, primarily for investigative, prosecutorial, and high-level trend/data analysis. Some of the taxonomies in this classification enable the user to fully understand and communicate what happened, who did it, why for any cyber related incident.</p> |
| dictionary | | <p>NICCS Glossary of Common Cybersecurity Terminology - https://niccs.us-cert.gov/about-niccs/glossary</p> |
| dictionary | | <p>ISACA - https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf</p> |
| dictionary | | <p>NIST - https://csrc.nist.gov/glossary?index=A</p> |
| Incidents/IR | <p>Europol Common Taxonomy for LE and CSIRTS: https://www.europol.europa.eu/publications-documents/common-taxonomy-for-law-enforcement-and-csirts</p> | |
| Incidents/IR | | <p>DNI Framework: https://www.dni.gov/index.php/cyber-threat-framework and https://www.dni.gov/files/ODNI/documents/features/ODNI_Cyber_Threat_Framework_Overview_UNCL_20180718.pdf</p> |
| Incidents/IR | | <p>Lockheed Cyber Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html</p> |
| Incidents/IR; Defining Harm | | <p>VERIS: http://veriscommunity.net/</p> |
| Incidents/IR | <p>FraudSupport.org - https://fraudsupport.org/</p> | <p>FraudSupport.org - https://fraudsupport.org/</p> |
| Incidents/IR | <p>USA.gov - https://www.usa.gov/online-safety</p> | |
| Incidents/IR | <p>IdentityTheft.Gov - https://identitytheft.gov/Assistant</p> | |
| Incidents/IR | <p>FTC Consumer Sentinel</p> | <p>FTC Consumer Sentinel</p> |

Cybercrime Classification Compendium



Cyber Classification Compendium v0.9; 20 April 2020

To provide a consistent language across cyber taxonomies and jurisdictions in an effort to increase cyber event and incident reporting, intelligence sharing, file deconflation, further legislation, and enable comparability

| Layman Classification (for reporters and call takers) | Layman Description | Technical Classification (for investigators and analysts) | Alternate Terms | Technical Description | Legal Correlations | | | |
|--|---|--|---|--|---|--|--|--|
| | | | | | European | Canadian | | Federal |
| | | | | | | Federal Criminal Code | Regulatory Schemes | |
| Malware | Software that is intentionally included or inserted in a system for a malicious purpose, without the user's approval. | Malware infection | Virus, worm, Trojan, spyware, scareware, dialler, rootkit, exploit kit, ransomware. | Software that is intentionally included or inserted in a system for a malicious purpose without the users approval. | System(s) or softwares(s) infected with malware allowing remote access, monitoring of system activities and gathering of information: -Art 2 and 6 [A] -Art 3 and 6 [F] | 342.1 - Unauthorized use of computer 430 (1.1) - Mischief to data 342.2 - Possession of device to obtain unauthorized use of computer system or to commit mischief | CASL section 8 - in the course of commercial activity, instal or cause to be installed a computer program on any other person's computer system without express consent. | Computer Fraud § 1030(a) intent without authori access, including With respect t extortion mal extortion associa computer and commerce with i to injury p |
| | | Malware distribution | malspam | Malware attached to an email message, social media post, text message, or other message format, or any of the above formats containing a link to a malicious URL or IP address with malware on it. | Dissemination of malware through various communication channels: - Art. 7 [F] - Art. 6 [A] | 342.1 Unauthorized use of computer Competition Act 52.01 (1-3) - False or misleading representations in: sender, subject matter, body and locator (URL). | The message is covered by CASL section 6 - send, cause or permit to be sent a commercial electronic message sent without consent. The malicious link is covered by CASL section 7 - in the course of commercial activity, alter or cause to be altered transmission data such that it is delivered to a destination other than specified by the sender (user who clicked on the link). Any resulting installation is covered by CASL section 8. Also Competition Act 74.011 (1-3) - False or misleading representations in: sender, subject matter, body and locator (URL). | CFAA 18 USC § 11 a computer with authorized acces re |

Cybercrime Classification Compendium

Crosswalk to NIBRS

Crosswalk to NIBRS Offense Codes (US)

Cyber Classification Compendium
v0.9; 6 April 2020

| Group A Offenses | | | | | |
|---------------------|----------|--|---------------|-----------------------|---|
| Offense | IBR Code | Offense Description | Crime Against | Layman Classification | Technical Classification |
| Extortion/Blackmail | 210 | Extortion/Blackmail | Property | Malware | Malware infection |
| | | | | Frauds | False representation |
| Fraud Offenses | 26A | False Pretenses/Swindle/Confidence Game | Property | Frauds | False representation |
| Fraud Offenses | 26B | Credit Card/Automated Teller Machine Fraud | Property | Frauds | Misuse or unauthorized use of resources |
| Fraud Offenses | 26C | Impersonation | Property | Information Gathering | Phishing |
| | | | | | Other Information Gathering |
| | | | | Intrusion | Compromised Account |
| Fraud Offenses | 26E | Wire Fraud | Property | Frauds | Misuse or unauthorized use of resources |
| | | | | | False representation |
| Fraud Offenses | 26F | Identity Theft | Property | Information Gathering | Phishing |
| | | | | | Other Information Gathering |
| | | | | Intrusion | Compromised Account |
| | | | | Frauds | Misuse or unauthorized use of resources |
| | | | | | False representation |
| | | | | Malware | Malware infection |
| | | | | | (Successful) Exploitation |

Cybercrime Classification Compendium

Crosswalk to State Criminal Codes

| Technical Classification (for investigators and analysts) | Alternate Terms | Technical Description | American | Alabama | Alaska | Arizona | Arkansas |
|--|---|---|---|---|---|---|---|
| | | | Federal Criminal Code | Criminal | Criminal | Criminal | Criminal |
| | | | | | | | |
| Malware infection | Virus, worm, Trojan, spyware, scareware, dialler, rootkit, exploit kit, ransomware. | Software that is intentionally included or inserted in a system for a malicious purpose without the users approval. | <p>Computer Fraud and Abuse Act (CFAA) 18 USC § 1030(a) intentionally accesses a computer without authorization or exceeds authorized access, including government and restricted data.</p> <p>With respect to wiper, ransomware, and extortion malware: 18 USC § 1030(a)(7) extortion associated with causing damage to a computer and 18 USC § 875(d) interstate commerce with intent to extort through threat to injury property or reputation</p> | <p>Not a crime if no access occurs.</p> <p>Alabama Digital Crime Act (ADCA) 13A-8-112 § 3(a)(1-5, 7) - accessing/altering /damaging system; specifically to (4) - introduction of computer contaminator/virus, and specifically to (7) obtaining confidential/non-public records.</p> | <p>Alaska Statutes 11.46.740 (a)(1)(A-E) - access or exceeds authority to access computer, computer system, computer program, or network; introduces false information to computer, system, network with intent to damage / criminal negligence</p> <p>AS 11.46.740 (a)(2-3) - installation and use of key logger</p> | <p>Arizona Revised Statutes (ARS) 13-2316 (A)(1-8) - knowingly access computer, comp. system, network, software, programs/data; ARS 13-2316(A)(3) specific to introducing malware to system</p> | <p>Arkansas Code Annotated (A.C.A.) § 5-41-104. Computer trespass. (a) A person commits computer trespass if the person intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer</p> |



WHERE
DO I
START



We asked the public what they thought...

1 out of 3
impacted by a cybercrime

1 out of 4
did nothing to respond
to the incident

91%
believe in importance of
reporting to law
enforcement

2 out of 3
likely to use a reporting portal

Preferences:

1
Phone (911/211)

2
Website

3
Smartphone app or
physical



Philadelphia Police 

@PhillyPolice

Follow



Yes, our [@YouTube](#) is down, too. No, please don't call 911 - we can't fix it.

6:30 PM - 16 Oct 2018

8,659 Retweets 22,495 Likes



 460

 8.7K

 22K

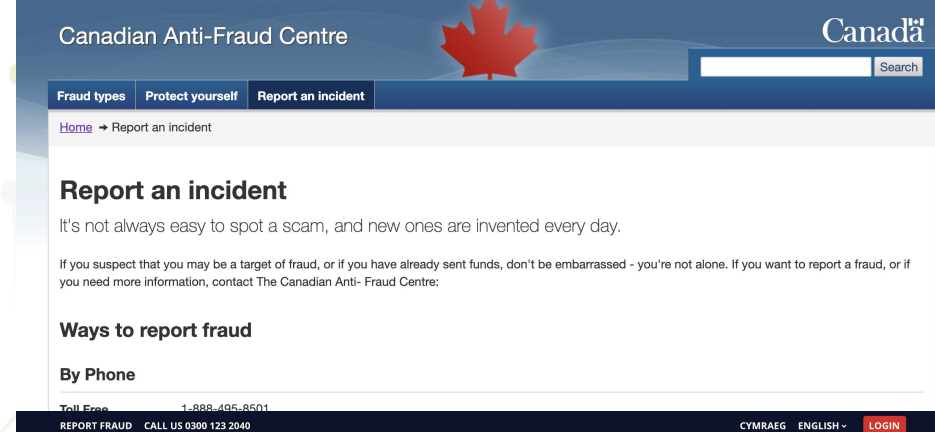
The Hotline Issue

- AARP Fraud Watch [Scam-Tracker](#)
- Office of Inspector General Dept. of Transportation <https://www.oig.dot.gov/hotline>
- U.S. Treasury [IRS Impersonation Scam Reporting](#)
- National Center for Missing and Exploited Children [Cyber Tip Line](#)
- Internet Crime Complaint Center FBI (IC3) [Complaint Form](#)
- U.S. Senate Special Committee on Aging's Fraud Hotline 1-855-303-9470 [2017 Committee Report](#) Pages 43-47 have lists of potential places to report
- International in cooperation with FTC econsumer.gov
- FTC US Complaints ftc.gov/complaint
- National Consumers League fraud.org
- FTC report Identity Theft identitytheft.gov
- Call for Action Callforaction.org
- Better Business Bureau [BBB Scam Tracker](#)
- US Cert for Business [Report an Incident](#)
[Report Malware](#)
[Reporting Phishing Email to APWG](#)
- Consumer Financial Protection Bureau (Gov) [Report a Complaint](#)
[Complaint Categories](#)
- Anti-phishing Working Group (APWG) <https://www.antiphishing.org/report-phishing/overview/>
Forward phishing email as an attachment to:
reportphishing@apwg.org.
- Identity Theft Resource Center 888-400-5530
- AARP Fraud Watch Helpline Call 877-908-3360 to share your story and receive assistance from our call center

International Solutions

UK, Canada and Israel Solutions

- One national number to call
- Jurisdiction legislation
- Needed social workers
- Only responding to 15% of complaints
- **Over 50% no law enforcement response**



Canadian Anti-Fraud Centre

Home → Report an incident

Report an incident

It's not always easy to spot a scam, and new ones are invented every day.

If you suspect that you may be a target of fraud, or if you have already sent funds, don't be embarrassed - you're not alone. If you want to report a fraud, or if you need more information, contact The Canadian Anti-Fraud Centre:

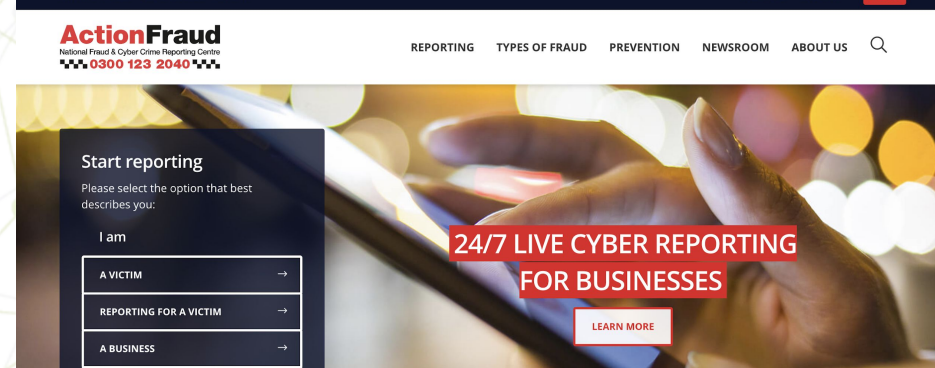
Ways to report fraud

By Phone

Toll Free 1-888-495-8511

REPORT FRAUD CALL US 0300 123 2040

CYMRAEG ENGLISH LOGIN



ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

REPORTING TYPES OF FRAUD PREVENTION NEWSROOM ABOUT US

Start reporting

Please select the option that best describes you:

I am

- A VICTIM →
- REPORTING FOR A VICTIM →
- A BUSINESS →

24/7 LIVE CYBER REPORTING FOR BUSINESSES

LEARN MORE

Israel Launches Cybersecurity Hotline for Suspected Hacking

The center is the first such emergency response line in the world and aims to help businesses and individuals

CSN Solutions

FraudSupport.org



[Donate](#) [Resource Library](#) [ScamSpotter.org](#) [Stay Informed](#) [Security Tools](#) [COVID-19 Alerts](#)

Cybercrime and Online Fraud Can Happen to Anyone

I'm a Business and I need help with...



I'm an Individual and I need help with...



Resources for
Children, Teens,
and Young Adults

Resources for
Older Adults
and Caregivers

Resources for
Military Personnel
and Families

FraudSupport.org for Individuals

I'm an Individual and I need help with... —

Identity
Theft

Financial/Purchase Scams

Hacked Account/Devices

Cyberbullying/Harassment
/Stalking

Imposter Scams

FraudSupport.org

Financial /Purchase Scams

Financial/purchase scams are common and come in many forms. In these types of scams, you lose money when paying for something you never get, invest in a fake company or program, are promised help with debt that doesn't come, or send money in advance with a promise for a big payout.

We have identified nine major categories of financial / purchase scams. Click on each button to find specific information on how to **Report**, **Recover** and **Reinforce** yourself from any financial cyber-criminal activities.

Which of these applies to your situation?

Advance Fee Scams

Credit Card
Bank Account Scams

Debt Management Scams

Extortion Scams

Investment Scams

Online Shopping Scams

Real Estate
/Mortgage Scams

Tax (IRS) Scams

Timeshare/Travel Scams

Online Shopping Scams

Did you buy something online but never got it? An online shopping scam is when an online transaction is made, but the item or service you paid for never arrives or does not exist as described.

If you think you are a victim of an online shopping scam, we recommend that you act immediately by following our guidelines below, and then proceed to our **Report**, **Recover**, and **Reinforce** sections for further assistance.

Some Immediate Action Steps to Take

- ✓ Collect all relevant documentation related to the scam and keep them in a secure file. You may need to provide this documentation when you file a report.
- ✓ If you paid with a credit card, dispute the charge with your credit card provider right away:
 - [Visa](#) 800-847-2911
 - [American Express](#) 800-528-4800
 - [MasterCard](#) 800-307-7309
 - [Discover](#) 801-902-3100
 - [Capital One](#) 800-227-4825
 - [Chase](#) 800-432-3117
- ✓ If you paid with a debit card, call your bank or financial institution.
- ✓ Report the scam to the online platform where you purchased the good or service:



Report

Reporting cybercrime incidents to the [FBI Internet Crime Complaint Center \(IC3\)](#) is very important! The more national reporting data that is collected, the better the chance law enforcement has to catch the criminals and decrease online crime. Although the FBI does not resolve individual complaints directly, they will make your report available to local, state and other law enforcement partners. The FAQs about reporting can be found [here](#). Please read the FBI/IC3 privacy policy [here](#). (If you believe that you've received a phishing email, please forward the email directly to reportphishing@apwg.org.)



Recover

These resources have been gathered, selected and vetted to help simplify the process of recovering after a cybercrime incident has taken place. You may need to contact organizations outside FraudSupport.org. Results will vary depending on your circumstances.

- [Find local victim services near you](#)
- File a complaint with the [Better Business Bureau](#)
- Report international scams to [econsumer.gov](#)
- Contact your [State Consumer Protection Office](#) for help.
- [Get your money back](#)



Reinforce

Once you have notified the appropriate organizations and you are on the road to recovery, it is time to reinforce your cybersecurity using these resources and tools.

- [Sign-up for FTC Scam Alerts](#)
- Before shopping, [check to see if a site is safe](#)
- [Remove your name from email lists](#)
- FTC.gov: [Shopping Online](#)
- [FDIC Cybersecurity Awareness Basics](#)
- [Improve Your Security](#): Find cybersecurity tools to enhance your online safety.
- CSN: [Black Friday and Cyber Monday Scams](#)

FraudSupport.org for SMBs

I'm a Business and I need help with...

Denial of Service
- Website Hacked

Business Identity Theft

Data Breach

Email Hacked
(Business email compromise)

Malware
(Virus/Spyware/Adware)

Money Transfer Fraud

Phishing Email

Ransomware

Tax Scam

Utilize existing national 211 infrastructure

- Victims call for support to report, recover and reinforce their security.
- 211 call specialists provide referrals to organizations or law enforcement that can help.



Get Connected. Get Help.™

211 Cybercrime Victim Services

Implemented Programs

- Rhode Island
- Orlando, FL
- West Michigan
- Mississippi

Upcoming Programs

- North Carolina
- New Jersey

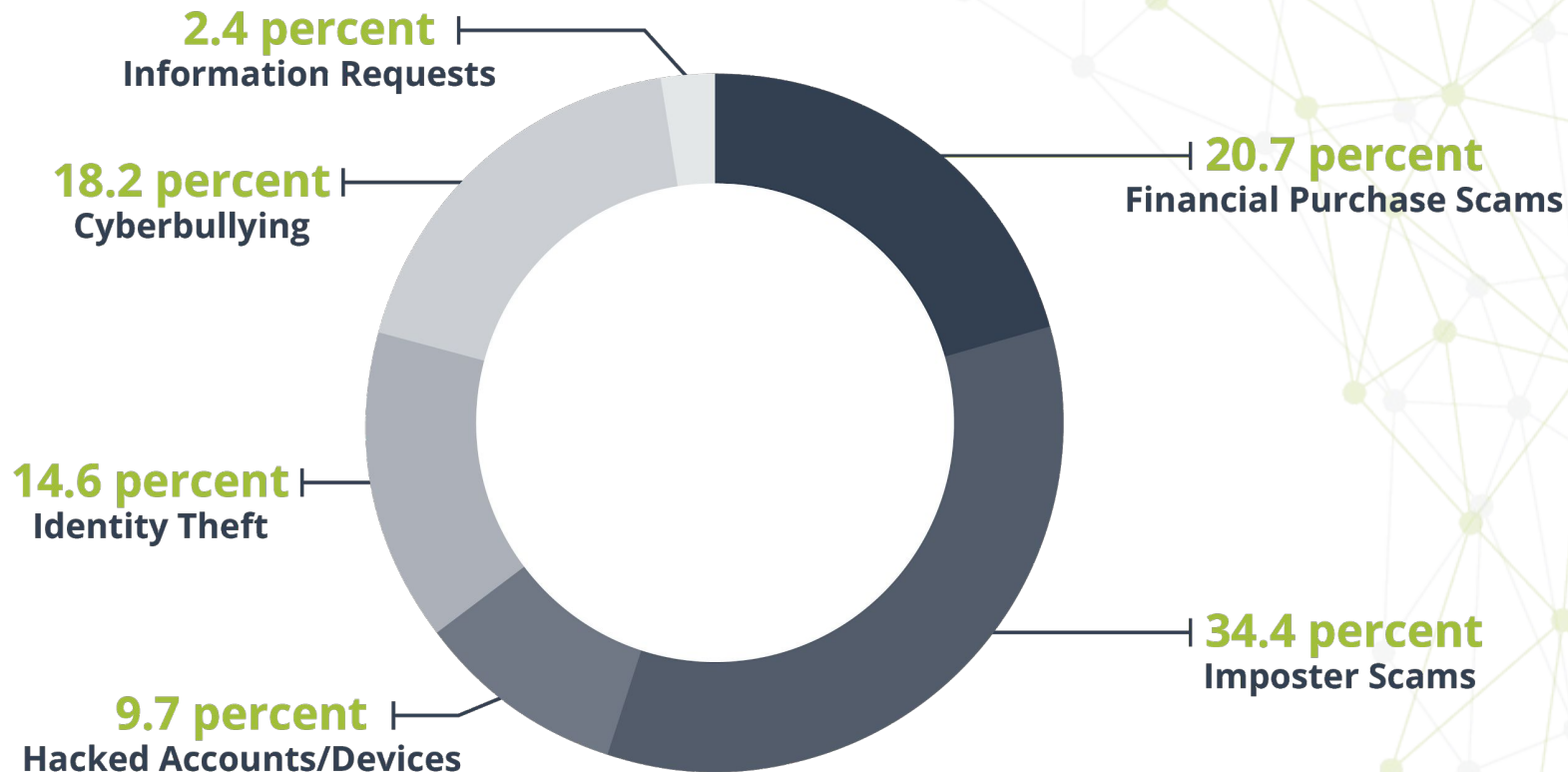
Applications Completed

- Texas
- Arizona
- California
- Florida



Get Connected. Get Help.™

Crime Categories Served by 211



ScamSpotter.org

BROUGHT TO YOU BY



The Three Golden Rules

Scam *Spotter*



Stay scam-free with these three golden rules:

- ✓ Slow it down
- ✓ Spot check
- ✓ Stop! Don't send

Take your time and ask questions to avoid being rushed into a bad situation.

Always look up the bank, agency or organization that's supposedly calling and get in touch directly.

No reputable person or agency will ever demand payment on the spot—especially not gift cards.

With the three golden rules, ScamSpotter.org offers easy-to-follow help to prevent cybercrime.

1. *Slow it Down.*
2. *Spot Check.*
3. *Stop! Don't Send.*

CISA Cooperative Agreement

| Working Group | Purpose |
|-------------------------|--|
| Incident Collection | Identify and refine requirements for a national cyber incident collection system focused on individuals and SMBs. |
| Information Sharing | Research and map existing cyber threat information sharing processes related to consumer and SMB cyber incidents to current needs. Explore and evaluate the most effective methods for cybersecurity information sharing focusing on regional sharing model. |
| Response Directory | Research existing directories and/or information sources of Federal, SLTT, and other professional entities that support cyber incidents/crimes and evaluate the need/feasibility and design the framework to create a new centralized Response Directory. |
| Victim Resource Catalog | Build a catalog of cyber education and awareness resources that would be provided to consumers and businesses impacted by cyber incidents. |

National Reporting Form

PLEASE SELECT THE OPTION THAT BEST DESCRIBES YOU:



I AM THE VICTIM



I AM REPORTING FOR A VICTIM



I AM REPORTING FOR A BUSINESS

Save & Continue

National Reporting Form

FraudSupport.org



VIEW MOBILE CONCEPT

[File an Incident](#)

[Donate](#)

[Resource Library](#)

[Stay Informed](#)

[Who We Are](#)

[Security Tools](#)

[Feedback](#)

PLEASE SELECT THE OPTION THAT BEST CATEGORIZES YOUR INCIDENT:



FINANCIAL PURCHASES & SCAMS

Financial/purchase scams are common and come in many forms. In these types of scams, you lose money when paying for something you never get, invest in a fake company or program, are promised help with debt that doesn't come, send money in advance with a promise for a big payout.



IDENTITY THEFT

Your personal information, credit history, medical identification, insurance or other identifying characteristics was used to make purchases, borrow money, open lines of credit, create bank accounts, open a business, or obtain medical / dental / prescription services without your permission.



HACKED ACCOUNTS & DEVICES

Attacks on digital devices and on user accounts occurs every 39 seconds on average. If you have noticed any unfamiliar activity on your computer, smartphone, tablet, email or social media accounts, someone may have gained access and be using your device or account without your permission.



CYBERBULLYING & HARASSMENT

It's easy for bullies to hide behind a computer or device to help them attack and harass someone. Because the bully can hide better on the internet, the seriousness and consequences of cyber harassment can be as severe as, if not more severe than, when you are face-to-face.



IMPOSTER SCAMS

Fraudsters pretend to be someone you trust, contacting individuals by email, text, phone, or other methods and pretending to be a public, private, or government individual that typically requires some type of financial payment to resolve, or pretending to be a friend or loved one in trouble who needs money immediately.

[Back](#)

[SAVE & CONTINUE](#)

National Reporting Form

FraudSupport.org powered by **cybercrime** SUPPORT NETWORK

NEW INCIDENT REPORT

- VICTIM**
- REPORTER
- INCIDENT
- TRANSACTIONS
- OFFENDERS
- WITNESSES
- REVIEW
- SIGN & SUBMIT

VICTIM

*Please provide information about the victim of this incident, in case further information is needed. Fields marked with an asterisk (*) are required.*

First Name: * **Last Name: ***

Age Range:

Address (Line 1): **Address (Line 2):**

Country: **County:**

City: **State:** **ZIP Code:**

Email: **Phone Number:**

FraudSupport.org



COVID-19
SCAM ALERTS

Stay up to date on COVID-19 scams, visit: [COVID-19 SCAM ALERTS](#)



[Donate](#)

[Resource Library](#)

[Stay Informed](#)

[Who We Are](#)

[Security Tools](#) ▾

[COVID-19 Alerts](#)

Cybercrime and Online Fraud Can Happen to Anyone

I'm a Business and I need help with...



I'm an Individual and I need help with...



Feedback



TAKE ACTION AGAINST COVID-19 SCAMS



ROMANCE SCAMS

Cybercriminals will try to capitalize on the heightened internet traffic to lure people into romance scams.

TAKE ACTION

If you find yourself involved in a romance scam, visit [FraudSupport.org](https://www.fraudsupport.org) for recovery help.

They will often ask for gift cards for medical expenses or bills.



SOCIAL MEDIA SCAMS

Social media is a tool that cybercriminals use to distribute false information and capitalize on panic.

TAKE ACTION

If you're looking for information on social media, visit trusted profiles like the [CDC](https://www.cdc.gov), [World Health Organization](https://www.who.int), [Federal Trade Commission](https://www.ftc.gov), and the [Better Business Bureau](https://www.bbb.org).



TAKE ACTION AGAINST COVID-19 SCAMS



PHISHING SCAMS

Emails impersonating the World Health Organization, the CDC, and other reputable sources may hit your inbox. These emails may ask you to click a link or share your sensitive information.

TAKE ACTION

If you've clicked on a phishing link or shared personal information, visit FraudSupport.org for recovery help.



ROBOCALLS

Calls from cybercriminals pretending to be government organizations, family members in distress, or banks/credit card companies are on the rise. These calls will often ask for gift cards as payment.

TAKE ACTION

If you have provided personal information to a robocaller, visit FraudSupport.org for recovery help.



TAKE ACTION AGAINST COVID-19 SCAMS



CHARITY SCAMS

You may see charities that you don't recognize asking for donations in the wake of COVID-19.

TAKE ACTION

If you donated to a fraudulent charity, visit [FraudSupport.org](https://www.fraudsupport.org) for recovery help.

Verify all charities before donating on the [IRS tax exemption site](https://www.irs.gov/charities).



ONLINE SHOPPING SCAMS

Cybercriminals may try to sell you bogus COVID-19 vaccinations and home test kits.

TAKE ACTION

If you have purchased a fake vaccine or home test kit, visit [FraudSupport.org](https://www.fraudsupport.org) for recovery help.

Visit the [FTC website](https://www.ftc.gov) to learn more about companies selling fake coronavirus treatments.

Hacked Video Conference

If you think your video conference has been hacked, we recommend that you act immediately by following our guidelines below, and then proceed to our **Report**, **Recover**, and **Reinforce** sections for further assistance.

Some Immediate Action Steps to Take

- ✓ Take a screenshot of disruptive behavior, then shut down the video conferencing software immediately.
- ✓ Report the incident to the [FBI Internet Crime Complaint Center \(IC3\)](#). Provide a detailed description of the incident and how you were victimized.
- ✓ Review your security settings on the video conferencing software. Check out these [Best Practices for Video Conferencing Security](#) from Palo Alto Networks.
- ✓ If you or someone within your meeting clicked on a phishing link in the chat, visit our [Phishing](#) page for reporting and recovery help.

Resource Library

The FraudSupport.org Resource Library provides tools, resources and collateral for educators, law enforcement, businesses, and organizations to share with their audiences and the general public. Please feel free to print, distribute and share these resources with your audiences.

Resources on this page are the property of the Cybercrime Support Network.



FraudSupport.org Rack Card

A rack card to share information about FraudSupport.org with the public.

Download

Download in Spanish

FraudSupport.org

CYBERCRIME CALLS?



FraudSupport.org

As a public-private nonprofit, Cybercrime Support Network (CSN) built FraudSupport.org as the first nationwide initiative developed specifically to help cybercrime and online fraud victims through a process of "report, recover and reinforce" after an incident occurs.

At FraudSupport.org, CSN provides guidance on where to call and how to reach the appropriate resource to report the crime, recover from and reinforce their own cybersecurity.

Report. Recover. Reinforce.

A Voice for Victims of Cybercrime and Online Fraud



Updated February 2020



CybercrimeSupport.org | FraudSupport.org



RED HEARTS RED FLAGS

Red Flags of a Romance Scam:

- ❗ You meet someone online and after just a few contacts or a short time, they profess their love or strong feelings for you.
- ❗ They ask you to start communicating by text or personal email, away from the original site you met on.
- ❗ Their profile you read on the site might not match everything they tell you.
- ❗ After gaining your trust, they start telling you stories of bad luck or medical illnesses.
- ❗ They indirectly/directly ask for money, gift cards, or funds to pay credit cards.
- ❗ Their messages are poorly written, inconsistent, or sometimes vague.
- ❗ They offer various excuses for why they can't show you more photos of themselves.
- ❗ They delay meeting in person or talking with you on a video chat.
- ❗ When you do agree to meet, they cancel or postpone due to some emergency.



If you notice any of these red flags:

If you or someone you know is in immediate danger, call 911 right away.

- Report the incident to the [FBI Internet Crime Complaint Center \(IC3\)](#)
- To help dating sites provide the best services possible, report the incident by clicking the logo below for the site where the connection first took place:



For more romance scam recovery tips, visit [FraudSupport.org](#)



CybercrimeSupport.org | FraudSupport.org
Facebook | Twitter | YouTube

Cybercrime & Online Fraud Can Happen to Anyone

FraudSupport.org is here to help.



Report. Recover. Reinforce.

A resource database to guide you through the steps to find help after a cybercrime has occurred.



Simple Rules to Stay Safe

- ⚠️ If an offer or opportunity seems too good to be true, it's probably a scam.
- ❌ Never wire money, send gift cards, or send a check to a stranger.
- ⚠️ If someone claims to be from a federal agency, call the office to confirm.
- ❌ Never accept money from a stranger promising you can keep some of it.
- ⚠️ If you suspect you've been hacked, change your passwords immediately.

Help Starts Here: Visit [FraudSupport.org](#)

FraudSupport.org

powered by:





Cybercrime Support Network

190 subscribers



5 immediate action steps if your social media account is hacked






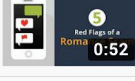
Play (k)

0:07 / 0:57

Tips

Cybercrime Support Network - 1 / 9



-  **5 Steps if Your Social Media Account is Hacked**
Cybercrime Support Network
-  **5 Steps if Your Social Media Account is Hacked**
Cybercrime Support Network
-  **5 Steps to Take if a Phishing Email is Clicked at Your Business**
Cybercrime Support Network
-  **Charity Scam Warning Signs**
Cybercrime Support Network
-  **5 Immediate Action Steps if You Experience Cyberbullying**
Cybercrime Support Network
-  **5 Red Flags of a Romance Scam**
Cybercrime Support Network



5

Red Flags of a
Romance Scam

What does success look like?

- Increased reporting
- Increased recovery
- Increased resources
- ***Decreased crime and re-victimization!***

Sponsors & Funding



Craig Newmark
Philanthropies



AT&T



NordVPN®



TREND
MICRO™

Federal Grant Funding
U.S. Department of Justice
Office for Victims of Crime
U.S. Department of Homeland Security (CISA)

Thank you.



Kristin Judge
CEO/President
info@cybercrimesupport.org

Cybercrimesupport.org
FraudSupport.org
Scamspotter.org

YouTube:
Cybercrime Support Network

Twitter:
@FraudSupport
@CyberSupportNet