



Cybercrime Support Network

Giving victims of cybercrime a voice.

Adrianna Cuellar Rojas
President and CEO
United Ways of Texas

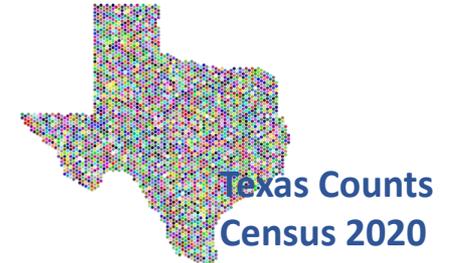




United Ways of Texas

ALICE IN TEXAS:
Asset Limited Income
Constrained Employed

**State Employee
Charitable Campaign
(SECC)**



Vision: United for a Future where all Texans thrive.



Overview

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

Report.



Recover.



Reinforce.



PRESIDENT
Kristin Judge
CEO, Cybercrime
Support Network



VICE PRESIDENT
Barbara Hiemstra
Privacy
Engineer, Steelcase



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



Ben de Bont
VP, Chief Information
Security Officer,
ServiceNow



Aric Permitter
Chairman and
Founder, Lynx
Technology Partners



Ralph Johnson
Chief Information
Security Officer,
County of Los
Angeles



Tim Smith
Executive
Director, Ottawa
County Central
Dispatch Authority



Kelley Bray
Director, Security
Culture and Training,
Splunk Inc.



Aaron Cohen
Cybersecurity
Entrepreneur



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



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



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



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



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

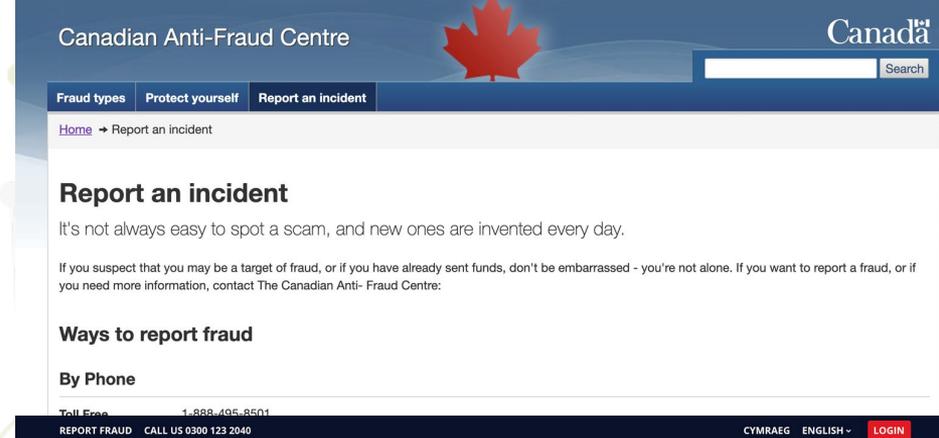


International Solutions



UK, Canada and Israel Solutions

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



Canadian Anti-Fraud Centre

Fraud types | Protect yourself | Report an incident

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:

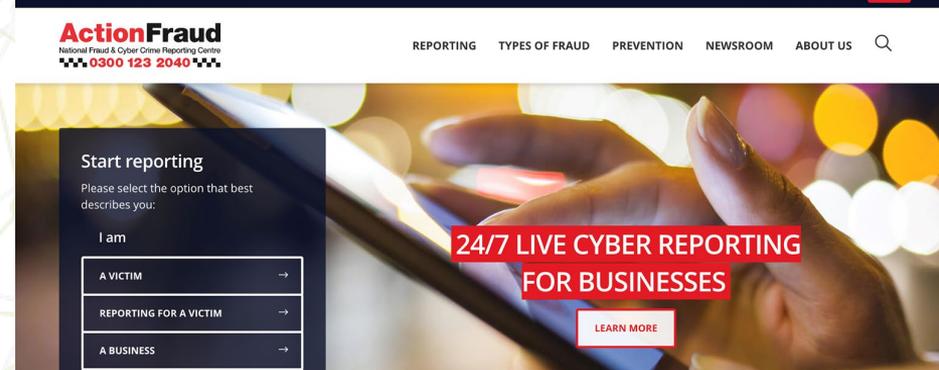
Ways to report fraud

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



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

Description: Screenshot of FraudSupport.org homepage to click on help for businesses or individuals.



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...



Financial/Purchase Scams

Hacked Account/Devices

Identity Theft

Cyberbullying/Harassment /Stalking

Imposter Scams

Feedback

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

Feedback

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

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

Cybercrime and Online Fraud Can Happen to Anyone

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

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



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.



211 Cybercrime Victim Services

Implemented Programs

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

Upcoming Programs

- North Carolina
- New Jersey

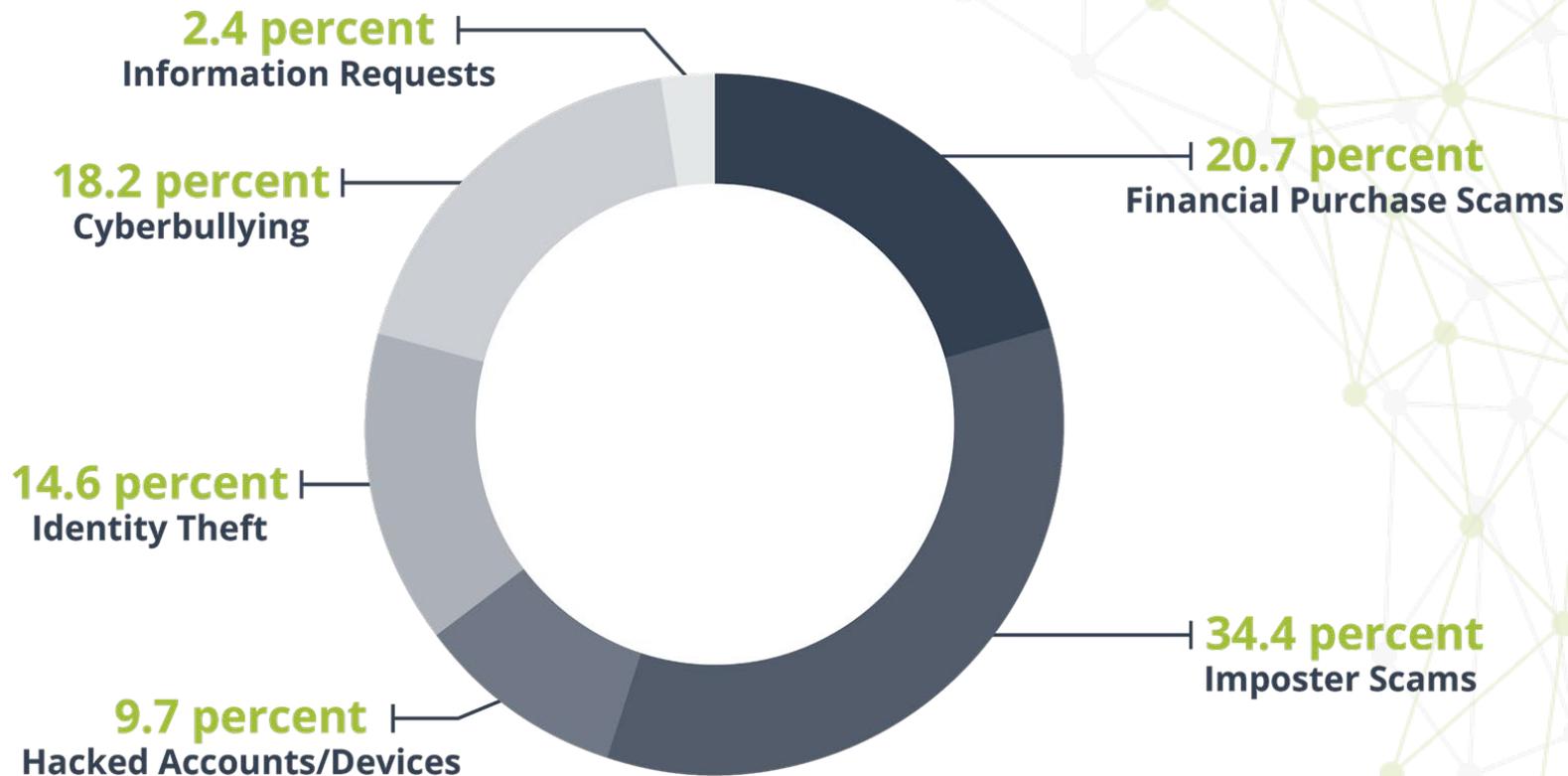
Applications Completed

- Texas
- California
- Florida





Crime Categories Served by 211



What does success look like?

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



CSN team and partners will not stop
until **211 is the national number** serving
cybercrime and online fraud victims.



Sponsors & Funding



Craig Newmark
Philanthropies



Federal Grant Funding
U.S. Department of Justice
Office for Victims of Crime

Federal Grant Funding
U.S. Department of Homeland
Security

Thank you.



Kristin Judge
CEO/Founder
Kjudge@cybercrimesupport.org

[Cybercrimesupport.org](https://www.cybercrimesupport.org)
[FraudSupport.org](https://www.fraudsupport.org)

YouTube:
Cybercrime Support Network

Twitter:
[@FraudSupport](https://twitter.com/FraudSupport)
[@CyberSupportNet](https://twitter.com/CyberSupportNet)