

# 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.**

# Board of Directors



**PRESIDENT**  
**Kristin Judge**  
CEO, Cybercrime  
Support Network



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



**Dr. Ernest L. McDuffie**  
Founder and CEO  
The Global McDuffie  
Group



**Joyce Brocaglia**  
CEO, Alta Associates  
Founder, Executive  
Women's Forum  
CEO, BoardSuited



**Ben de Bont**  
VP, Chief  
Information Security  
Officer, ServiceNow



**Ralph Johnson**  
Chief Information  
Security Officer,  
County of Los  
Angeles



**Mari Galloway**  
Sr. Security Architect, Casino  
CEO & Founding Board  
Member, Women's Society  
of Cyberjutsu



**Tim Smith**  
Retired, Executive  
Director, Ottawa  
County Central  
Dispatch Authority



**Kelley Bray**  
Security Culture and  
Training Professional



**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

GALLUP What We Do ▾ Who We Are Locations Careers Store

News Business ▾ Politics ▾ World ▾ Education ▾ Social & Policy Issues ▾ More ▾ SUBSCRIBE

f t in e

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.



# 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





**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](https://econsumer.gov)
- FTC US Complaints  
[ftc.gov/complaint](https://ftc.gov/complaint)
- National Consumers League  
[fraud.org](https://fraud.org)
- FTC report Identity Theft  
[identitytheft.gov](https://identitytheft.gov)
- Call for Action  
[Callforaction.org](https://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
- Need social workers
- **Over 50% no law enforcement response**

The image displays two website screenshots and a news headline. The top screenshot is from the Canadian Anti-Fraud Centre website, featuring a blue header with a red maple leaf logo and navigation tabs for 'Fraud types', 'Protect yourself', and 'Report an incident'. The main content area is titled 'Report an incident' and includes a search bar, a 'Home' link, and a 'Report an incident' button. Below this, it states 'It's not always easy to spot a scam, and new ones are invented every day.' and provides contact information for reporting fraud. The bottom screenshot is from the ActionFraud website, showing a 'Start reporting' section with a form to select the user's role (Victim, Reporting for a Victim, or Business). A red banner on the right side of the screenshot reads '24/7 LIVE CYBER REPORTING FOR BUSINESSES' with a 'LEARN MORE' button. The bottom headline reads 'Israel Launches Cybersecurity Hotline for Suspected Hacking' and mentions that the center is the first such emergency response line in the world.

Canadian Anti-Fraud Centre

Canada

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 1-888-495-8571

REPORT FRAUD CALL US 833 123 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

Reuters | Send me email alerts



# 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](mailto: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](#)

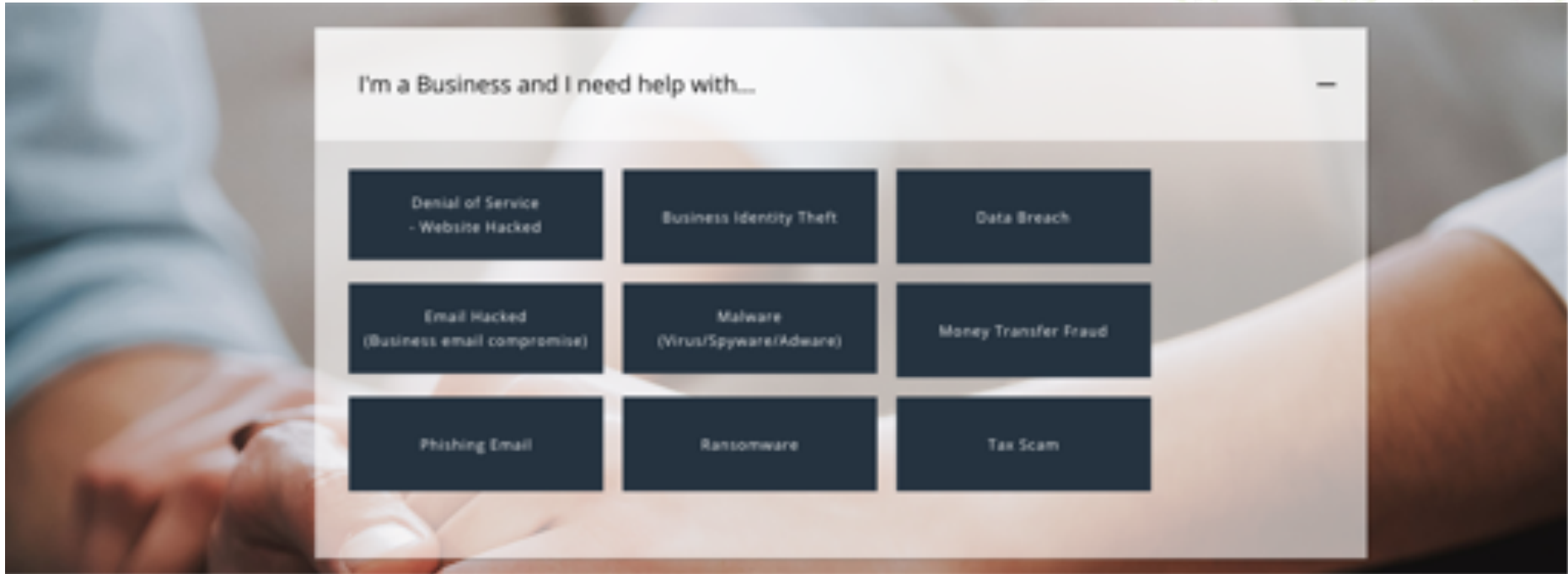


## Reinforce

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



# 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.



## Implemented Programs

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

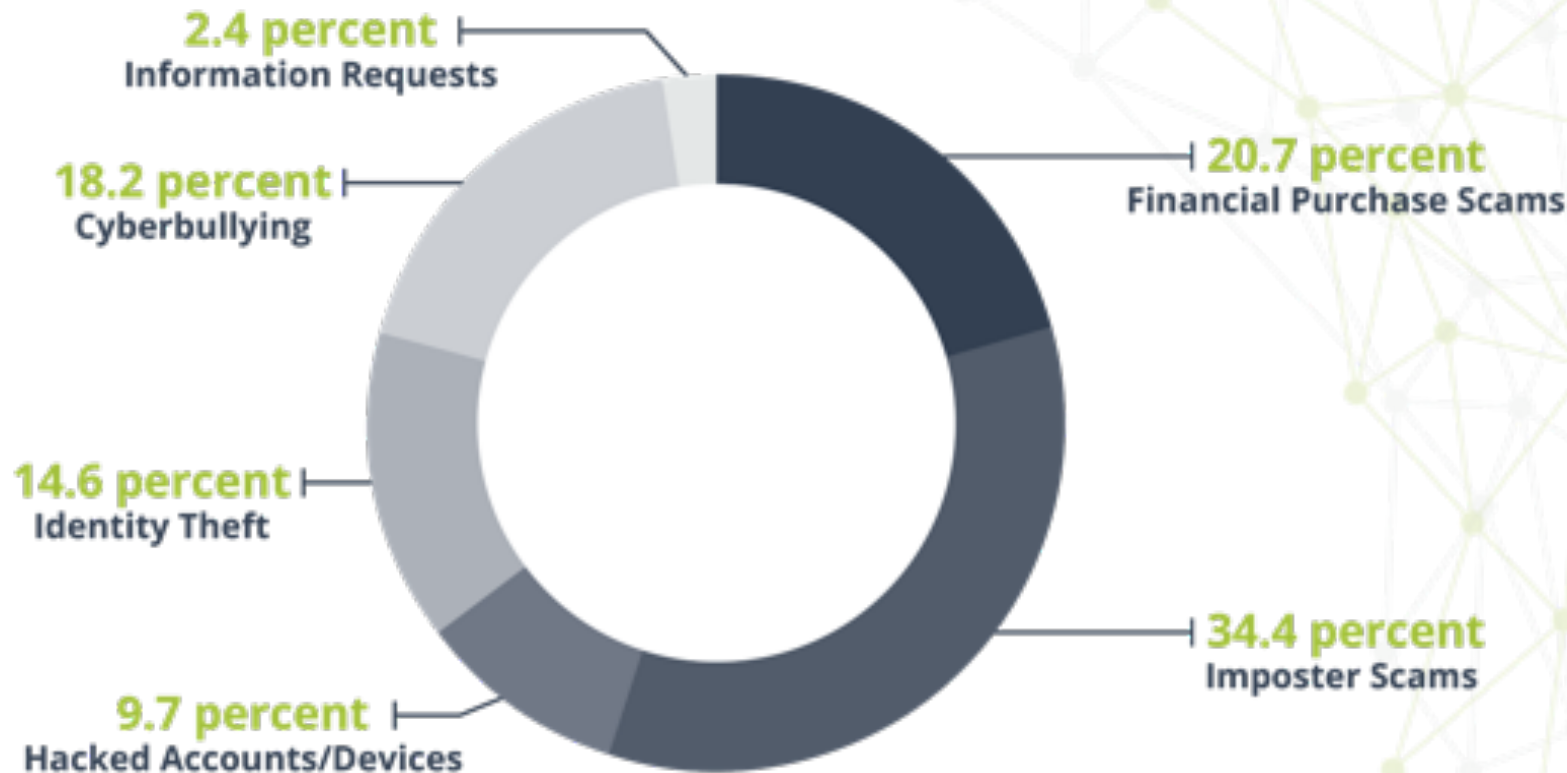
## Upcoming Programs

- North Carolina
- New Jersey

## Applications Completed

- Texas
- California
- Florida

# Crime Categories Served by 211



# The Three Golden Rules

Scam Spotter



Stay scam-free with these  
three golden rules:

- ✓ Slow it down  
Take your time and ask questions to avoid being rushed into a bad situation.
- ✓ Spot check  
Always look up the bank, agency or organization that's supposedly calling and get in touch directly.
- ✓ Stop! Don't send  
No reputable person or agency will ever demand payment on the spot—especially not gift cards.

With the three golden rules, ScamsSpotter.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.

## 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.*

### 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



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](#)

## 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

236 subscribers



YouTube

Search



## Tips

Cybercrime Support Network - 1 / 10



-  5 Steps if Your Social Media Account is Hacked  
Cybercrime Support Network  
0:58
-  5 Steps if Your Social Media Account is Hacked  
Cybercrime Support Network  
0:58
-  5 Steps to Take if a Phishing Email is Clicked at Your Business  
Cybercrime Support Network  
0:54
-  Charity Scam Warning Signs  
Cybercrime Support Network  
0:53
-  5 Immediate Action Steps if You

# 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](mailto:info@cybercrimesupport.org)

**Cybercrimesupport.org**

**FraudSupport.org**

**Scamspotter.org**

**YouTube:**

Cybercrime Support Network

**Twitter:**

@FraudSupport

@CyberSupportNet