cybercrime SUPPORT NETWORK

Report. Recover. Reinforce.

Giving Victims of Cybercrime a Voice

The impact of an online scam or attack can be devastating, and knowing where to go for help can be confusing.

Millions of American consumers and small businesses are affected by cybercrime each year and struggle to find resources to respond, recover and report the incident. An estimated 15 percent of these victims – roughly 351,000 people – reported a crime to the FBI Internet Crime Complaint Center in 2018. Those who reported lost approximately $2.7 billion in just one year, and the incidents of cybercrime continue to grow.

1 out of 3
Number of U.S. adults impacted by a cybercrime

351,936
Number of victims reported to FBI/IC3 in 2018

$2.7 billion
Victim losses reported to FBI/IC3 in 2018

The Cybercrime Support Network is a voice for those affected by cybercrime.

Founded in 2017, CSN is the first organization to connect victims to resources, increase cybercrime and online fraud reporting, and address the lack of information available to law enforcement and industry with a national reporting structure.

Resources for addressing cybercrime and online fraud are scattered among various organizations, resulting in inconsistent information and details about how to report a crime or who to turn to for resolution. Most cyber incidents are not reported to federal, state or local law enforcement, resulting in missing or understated data. Moreover, law enforcement and 9-1-1 dispatchers are short on resources and often do not have tools to support the current cybercrime calls they receive. With many hackers and cybercrime perpetrators based overseas, prosecution is difficult, or the amounts stolen per incident are too small for some agencies to address. But the victims still need help.

The Cybercrime Support Network fosters collaboration, provides training, compiles resources and works within the law enforcement and consumer protection ecosystem to ensure cybercrime victims are supported in a coordinated manner. As a public service organization, CSN raises awareness about available resources for victims and educates legislators about the need for cybercrime victim services.

FraudSupport.org: A Resource Database for Victims and Law Enforcement

As a public-private nonprofit, CSN is building 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. Through this platform, CSN provides guidance on where to call and how to reach the appropriate resource to recover. In Phase 2, the website will provide a reporting platform that will enable sharing of up-to-date threat intelligence with government, industry, and federal, state and local law enforcement. Partnering with the threat information sharing organizations to share data with the private sector will increase the ability of technology companies to thwart attacks and improved security.

Using CSN’s online resource, FraudSupport.org, victims of cybercrime will now have a central and standardized system for reporting crimes, accessing recovery tools and reinforcing their networks so they are safer and more secure. Law enforcement officials will be able to easily access these reports through federal agencies, improving investigations and determining best practices for detection and response.

Harnessing 2-1-1 Community Information and Referral Services

Fraudsupport.org is just one tool available through CSN's work. Utilizing funds from the Department of Justice Office for Victims of Crime, CSN is piloting a call/text/chat program to support cybercrime victims in West Michigan, Central Florida and Rhode Island that utilizes the existing 2-1-1 national network — a toll-free, human services phone number and chat line supporting over 95 percent of Americans — as a reporting and triage line for victims of cybercrime. CSN is training 2-1-1 referral specialists in the pilot areas to assist victims with reporting and referring them to response and recovery resources.

Working with our 2-1-1 partners across the country, CSN is applying for federal victim support funding to make 2-1-1 a well-recognized tool that all consumers and small businesses use for reporting and resource referral when impacted by cybercrime.

The Cybercrime Support Network assists cybercrime and online fraud victims – both individuals and small businesses – and improves the plight of Americans facing the increase in cybercrime by providing support before, during and after a potential crime occurs.

91%

U.S. adults that believe in the importance of reporting cybercrime to law enforcement

15%

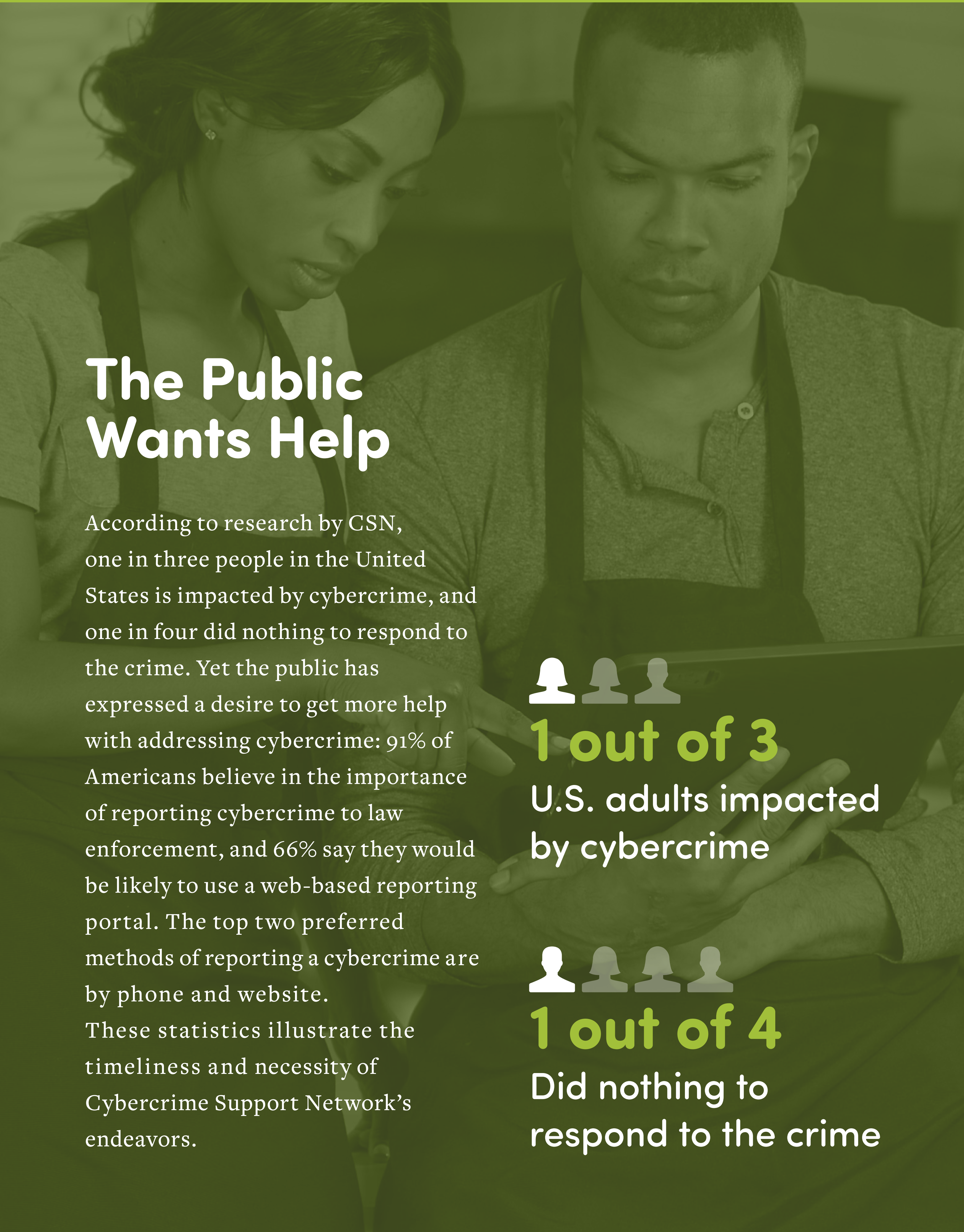
Estimated number of victims who report cybercrime to FBI/IC3

2 out of 3

U.S. adults who are likely to use a reporting portal. With preferred reporting methods being:

1. Phone | 2. Website

3. Smartphone app or in person



The Public Wants Help

According to research by CSN, one in three people in the United States is impacted by cybercrime, and one in four did nothing to respond to the crime. Yet the public has expressed a desire to get more help with addressing cybercrime: 91% of Americans believe in the importance of reporting cybercrime to law enforcement, and 66% say they would be likely to use a web-based reporting portal. The top two preferred methods of reporting a cybercrime are by phone and website.

These statistics illustrate the timeliness and necessity of Cybercrime Support Network's endeavors.

1 out of 3

U.S. adults impacted by cybercrime

1 out of 4

Did nothing to respond to the crime

Who's Most at Risk?

A cyberattack can cause great financial and emotional harm, particularly to more vulnerable groups. CSN helps all individuals impacted by cybercrime, with a keen eye on assistance for special populations:

Small Businesses

Hackers frequently attack small businesses who may not have the resources or experience to implement cybersecurity measures.

Older Adults

Seniors are often impacted by cybercrime due to isolation and accumulated wealth. CSN is working with State Attorneys General to implement programming that helps combat elder fraud and prioritizes help for victims.

Military Personnel and Families

Members of the U.S. Armed Forces and their families are often targeted by cybercriminals by exploiting distance from family members, overseas withdrawals, and the military's vibrant social media community.

CSN's Mission is to Support Cybercrime and Online Fraud Victims...

...Before

by pointing consumers and businesses to the best prevention information

...During

by enabling a one-stop access point to find federal, state and local resources

...After

by providing key contacts to guide in recovery and tools to prevent revictimization

Sponsors

The Cybercrime Support Network's sponsors advise and support CSN to ensure outcomes meet the needs of victims, law enforcement and nonprofit victim service organizations. Their commitment to supporting cybercrime victims is vital to CSN's mission.

Foundational

Craig Newmark Philanthropies

AT&T

Capital One®

COMCAST

Google

KnowBe4
Human error. Conquered.

LYNX
TECHNOLOGY PARTNERS

NordVPN®

TREND MICRO™

verizon✓

Strategic Partners

The Cybercrime Support Network's strategic partners provide invaluable support in helping it achieve its goals in developing a national reporting and referral program for cybercrime victims.

CYBER THREAT ALLIANCE

THE NATIONAL CENTER FOR
Victims of Crime

NW3C

APWG

NCFTA®

United Way

cybercrime
SUPPORT NETWORK

Board Members

President: Kristin Judge, CEO, Cybercrime Support Network

VP: Barbara Hiemstra, Privacy Engineer, Steelcase

Secretary/Treasurer:
James Ellis, D/F/Lt. Commander of Michigan Cyber Command Center (MC3), Michigan State Police

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

Ben de Bont, Chief Information Security Officer, ServiceNow

Aaron Cohen, Cybersecurity Entrepreneur

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

Aric Perminter, Chairman and Founder, Lynx Technology Partners

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

Tim Smith, Executive Director, Ottawa County Central Dispatch Authority

Leadership

Kristin Judge, CEO/Founder: Kristin was elected to serve as a Washtenaw County Commissioner in 2008 and supported the U.S. Department of Homeland Security in growing cybersecurity outreach to state and local government officials. After elected office, she worked at the Center for Internet Security focusing on connecting state and local governments to federal services and technology needed to improve cybersecurity.

As Director of Government Affairs at the National Cyber Security Alliance (NCSA), Kristin worked with Google, FTC, FBI, SBA, DHS, NIST, congressional leaders and other key stakeholders across the country to educate consumers and businesses on how to protect sensitive data.

A thought leader, Kristin has been seen on the C-SPAN Network, local news outlets and called on by technology publications like SC Magazine and Government Technology to share best practices for online safety. She was named an SC Media "Women in IT Security Influencer" in 2017. She is a national speaker, sharing cybersecurity best practices with elected officials, businesses and consumers. Her first LinkedIn Learning Course, "Cybersecurity for Small and Medium Businesses: Essential Training", teaches cybersecurity to SMBs based on the NIST Cybersecurity Framework.

In 2017, Kristin was chosen for the third cohort in the Presidential Leadership Scholars program, which is a partnership between the presidential centers of George W. Bush, William J. Clinton, George H.W. Bush, and Lyndon B. Johnson, to bring together a select group of leaders who share a desire to create positive change across the nation.

To address the needs of cybercrime victims, Kristin founded the nonprofit Cybercrime Support Network (cybercrimesupport.org) and works with federal, state and local law enforcement and consumer protection agencies to help consumers and small businesses affected by cybercrime.

Rachel Dooley, Chief Marketing Officer: Rachel Dooley has been Chief Marketing Officer at the Cybercrime Support Network since 2018. She leads the CSN team in developing communication strategies that help advance the organization's efforts to help cybercrime victims. These strategies include creating publications, web marketing and social media, as well as media relations and developing partnerships.

Prior to joining CSN, she was the marketing coordinator for new home builder Lamar Smith Signature Homes, where she developed and implemented strategic initiatives to promote new home sales. Previously, she was the Brigade Family Readiness Support Assistant for the 170th IBCT located in Baumholder, Germany. She created and published Family Readiness Group material including books, flyers and guides to navigate volunteers and family members through the deployment cycle.

As a graduate of the School of Equine Business at the University of Louisville, she was driven by her love of horses and her desire to bring about change in the industry as a whole. While earning her bachelor's degree, she worked as a youth field coordinator for the Kentucky Equine Education Project, where she became energized by the work of non-profit companies. Rachel brings to CSN her never-ending passion to bring about real change and to help people in a time of need.

Robert Burda, Chief Strategy Officer: Robert supports CSN's mission by developing and maintaining programs and relationships with key stakeholders. Robert is responsible for the implementation of grant programs in Rhode Island, Michigan and Florida. He is the liaison to law enforcement (LE) partners at the federal, state and local level. He ensures programming is consistent nationwide and advises the CEO on LE issues.

Mr. Burda retired from the FBI in 2018 as a Unit Chief at the National Joint Terrorism Task Force at FBI Headquarters. He was responsible for the administration of the 184 Joint Terrorism Task Force (JTTF) locations as well as the Agency Coordination Team, Correctional Intelligence Program, Special Administrative Measures Program, and the Military Operational Support Team.

After completing FBI new agent training in 1998, Robert was assigned to the Charlotte Division, Fayetteville Resident Agency (RA), where he worked a wide variety of criminal investigations. In 2005, Robert was assigned to the JTTF and served as the coordinator for the Fayetteville RA. Prior to joining the FBI, Robert served in the U.S. Navy as a Naval Flight Officer achieving the rank of Lieutenant Commander. Robert has a B.S. in Mechanical Engineering from Clarkson University.

Keith Tresh, Chief Security Officer: Keith has over 15 years of experience in cybersecurity and over 25 years of experience in Information technology. Mr. Tresh was appointed by Governor Jerry Brown on October 6, 2016 as the commander of the California cybersecurity integration center (Cal-CSIC) within the Governor's Office of Emergency Services where he served until he retired from the State of California in November of 2018.

A retired Army colonel, Mr. Tresh is also a veteran C-level IT management professional and an educator with a passion for information assurance and awareness. From 2014 to 2015 Keith was assigned as the chief information security officer (CISO) for the County of Orange, California where he had oversight of over 50 security professionals and their programs.

In 2011, Governor Brown appointed him to serve as California's chief information security officer and director of the Office of Information Security (OIS) at the California Technology Agency, responsible for protecting statewide information systems and assets against intrusion. Prior to this appointment, Keith was the J6/Chief Information Officer for the California National Guard.
Keith Tresh served in the Army and the California National Guard (CNG) for more than 33 years including a combat tour in Iraq from 2005-2006. Among his many assignments at the CNG, he was the CIO and designated approval authority from November 2006 to June 2011. Keith retired from the military in November of 2014.

Keith holds a Master of Science degree in computer information systems from the University of Phoenix and a Master of Science in national security and strategic studies from the United States Army War College.   He currently lives and resides in Boise, Idaho where he teaches cybersecurity curriculum at Boise State University.