

Federal Information Security Educators (FISSEA)

Winter Forum

February 14, 2024
1:00pm – 4:00pm ET

#FISSEA | nist.gov/fissea

Please Note...

This webinar and the engagement tools will be recorded.

An archive will be available on the [event website](#).

Welcome and Opening Remarks



Marian Merritt

Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology



Brooke Crisp

FISSEA Co-Chair

Get Involved



Subscribe to the FISSEA Mailing List
FISSEAUUpdates@list.nist.gov



Volunteer for the Planning Committee
<https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee>



Serve on the Contest or Award Committees
Email fissea@list.nist.gov



Submit a presentation proposal for a future FISSEA Forum
<https://www.surveymonkey.com/r/fisseacallforpresentations>

Previous FISSEA Award Winners include:

- Best blog
- Best newsletter
- Best website
- Best podcast
- Best poster
- Best innovative solution and more



Opening Keynote

They Give Love a Bad Name: How the FTC Educates Consumers to Spot, Stop, and Report Romance Scams

Lesley Fair

Senior Attorney

Federal Trade Commission





BAD ROMANCE

How romance scammers
give love a bad name –
and what the FTC is doing
to educate consumers
about the risks

Lesley Fair
Senior Attorney
Federal Trade Commission
lfair@ftc.gov

February 14, 2024

Federal
Trade
Commission

For
The
Consumer

Unfair methods
of competition or
unfair or deceptive
acts or practices
in or affecting
commerce are
hereby declared
unlawful.



AN ACT OR PRACTICE IS **DECEPTIVE** IF:

it's likely to
mislead
consumers

acting
reasonably
under the
circumstances

and it would
be material to
their decision
to buy the
product

AN ACT OR PRACTICE IS **UNFAIR** IF:

it causes
substantial
consumer
injury –
financial,
physical, etc.

not
reasonably
avoidable by
consumers
themselves

and not
outweighed
by benefits to
consumers of
competition

FTC DATA SECURITY CASES



**How does the FTC
collect data
about romance scams?**

register.consumersentinel.gov

CONSUMER SENTINEL NETWORK

Law enforcement's source for consumer complaints

Welcome to the Consumer Sentinel Network



Brought to you by the Federal Trade Commission

The Consumer Sentinel Network (CSN) is:

- An investigative cyber tool and complaint database for law enforcement officials only.
- A site that provides immediate and secure access to fraud, identity theft, telemarketing (including Do Not Call), and other consumer related complaints.
- The site is available only to members of law enforcement organizations that have entered into a [confidentiality and data security agreement](#) with the Federal Trade Commission (FTC).

As a CSN member you can



Search



Report



Collaborate & Connect



View

**How does the FTC
report the data it collects?**

CONSUMER SENTINEL NETWORK

DATA BOOK 2022

Federal Trade Commission
February 2023



Consumer Protection

Data Spotlight

FTC reporting back to you

Romance scams rank number one on total reported losses

People looking for romance are hoping to be swept off their feet, not caught up in a scam. But tens of thousands of reports in Consumer Sentinel show that a scam is what many people find. In 2018, Sentinel had more than 21,000 reports about romance scams, and people reported losing a total of \$143 million – that’s more than any other consumer fraud type identified in Sentinel.¹ These reports are rising steadily. In 2015, by comparison, people filed 8,500 Sentinel reports with dollar losses of \$33 million.

Romance scammers lure people with phony online profiles, often lifting photos from the web to create attractive and convincing personas. They might make up names or assume the identities of real people. Reports indicate the scammers are active on dating apps, but also on social media sites that aren’t generally used for dating. For example, many people say the scam started with a Facebook message.

Once these fraudsters have people by the heartstrings, they say they need money, often for a medical emergency or some other misfortune. They often claim to be in the military and stationed abroad, which explains why they can’t meet in person. Pretending to

need help with travel costs for a long-awaited visit is another common ruse.

Scammers can reap large rewards for time spent courting their targets. The median individual loss to a romance scam reported in 2018 was \$2,600, about seven times higher than the median loss across all other fraud types.² People often reported sending money repeatedly for one supposed crisis after another.

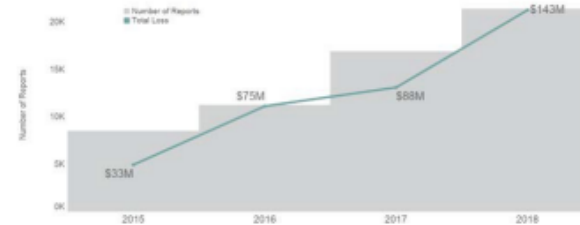
\$2,600

The **median reported loss** to romance scams is about seven times higher than for other frauds (2018)

People who said they were ages 40 to 69 reported losing money to romance scams at the highest rates – more than twice the rate of people in their 20s.³ At the same time, people 70 and over reported the highest individual median losses at \$10,000⁴

Romance Scam Reports Over Time

Reports more than doubled and reported losses increased more than fourfold from 2015 to 2018



Among people who told us how they paid the scammer, the majority said they wired money. The next largest group said they sent money using gift and reload cards (like MoneyPak), and reports of this type of payment increased in 2018. People said they mailed the cards or gave the PIN number on the back to the scammer. Con artists favor these payment methods because they can get quick cash, the transaction is largely irreversible, and they can remain anonymous.

AGE AND FRAUD LOSS IN GENERAL

**FRAUD LOSS REPORTS
PER 100,000 POPULATION**

**MEDIAN REPORTED
DOLLAR LOSS**

20-29

157

\$480

30-39

183

\$460

40-49

170

\$450

50-59

137

\$470

60-69

149

\$500

70-79

158

\$803

80+

87

\$1,450

**What have the reports
taught us about
romance scams?**

2019 ROMANCE SCAM DATA

2019

First year that romance scams first ranked #1 in total reported fraud losses

\$2,600

Median losses to romance scams

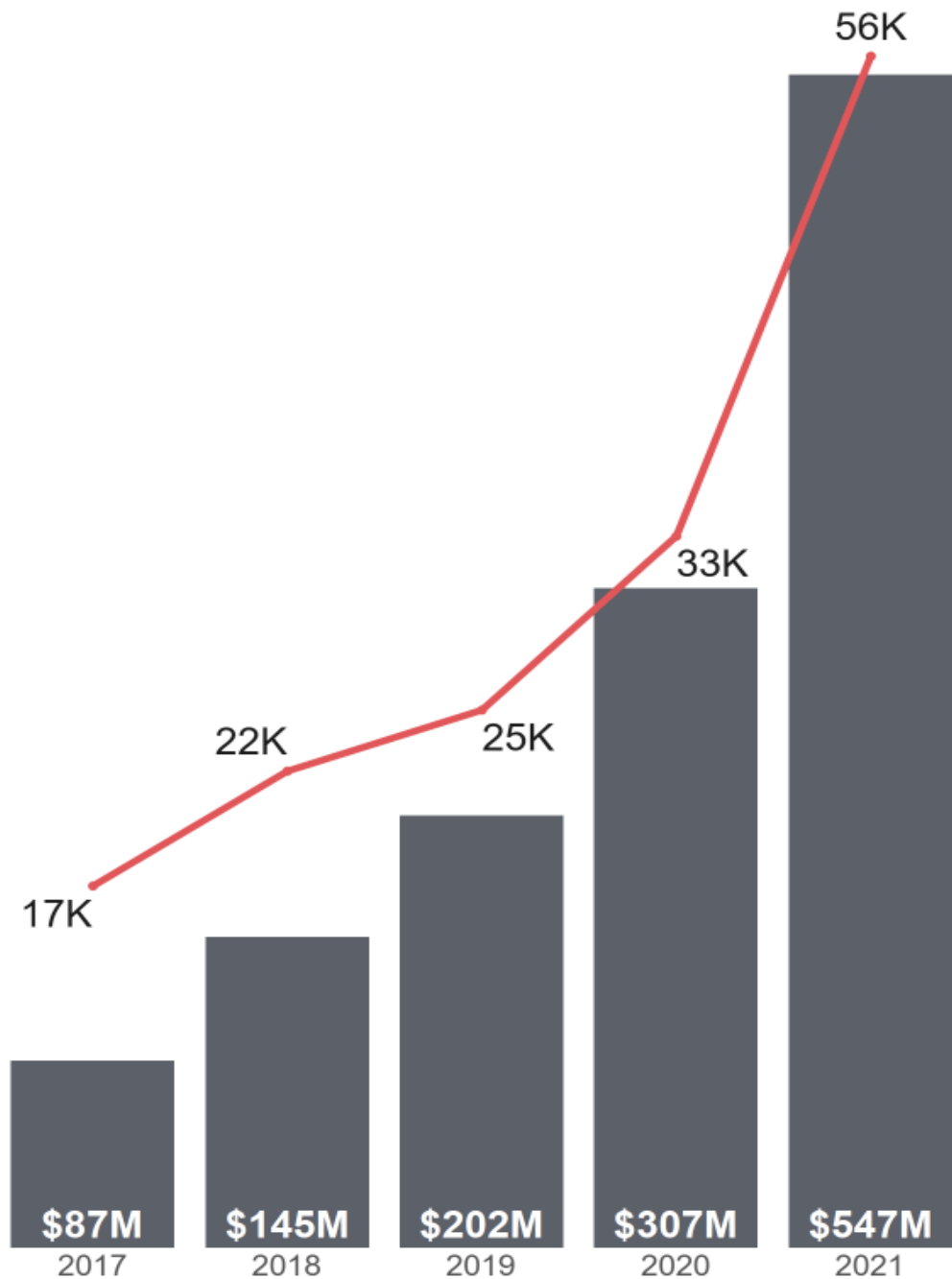
About 7 times higher than other forms of fraud reported to the FTC

40-69

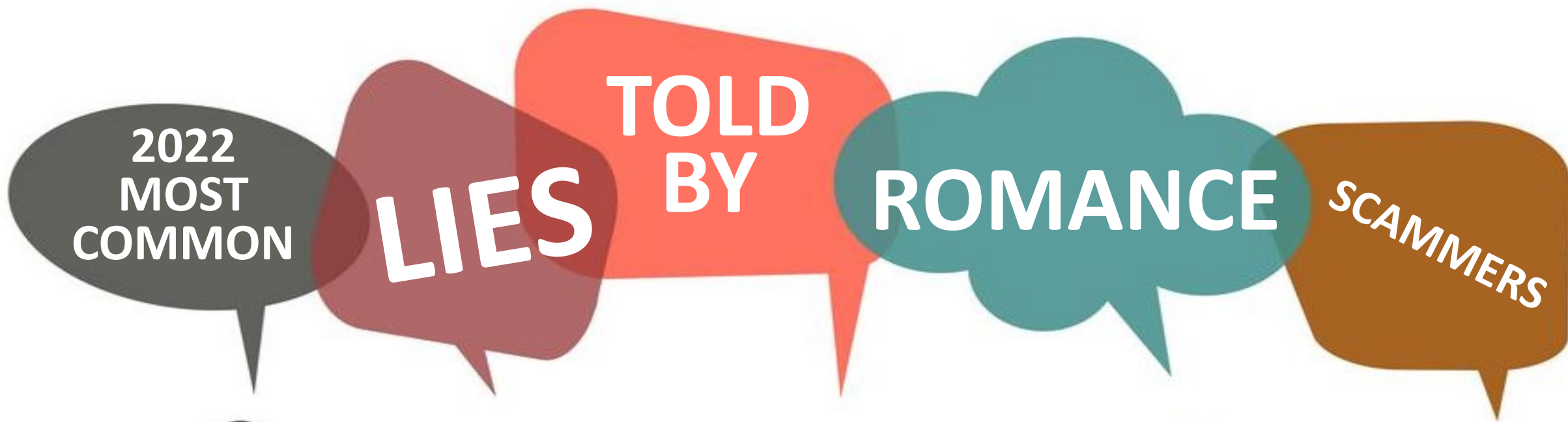
Age range of those who reported losing money to romance scams at highest rate

70+

Age range of those who reported the highest individual median losses: \$10,000



- **2021:** Total financial losses to romance scams were six times what they were in 2017.
- **2021:** Total number of romance scams reports were three times what they were in 2017.



2022
MOST
COMMON

LIES

TOLD
BY

ROMANCE

SCAMMERS

“I (or someone close to me) is hurt, sick, or in jail.” 24%

“I can teach you how to invest – and make big money.” 18%

“I’m in the military far away.” 18%

I need help with an important delivery.” 18%

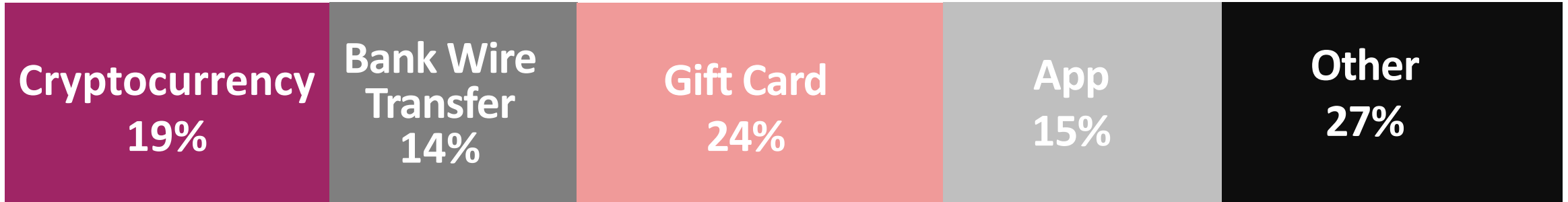
“We’ve never met, but let’s talk about marriage.” 12%

“I’ve come into money or gold and need help getting it.” 7%

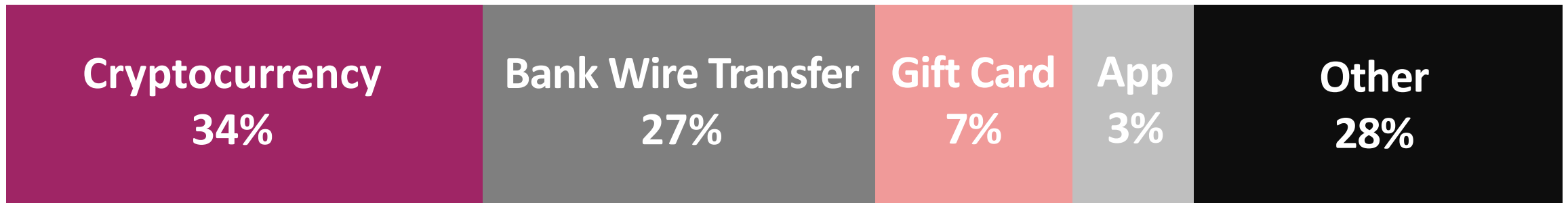
“I’m on an oil rig or a ship.” 6%

“You can trust me with your private pictures.” 3%

2022: Payment methods for romance scams by total reports



2022: Payment methods for romance scams by dollar loss amount



**What does the
2023 Data Book
tell us about romance scams?**

COMPARING ROMANCE SCAM DATA

	2019	2020	2021	2022	2023
NUMBER OF FRAUD REPORTS	39,875	54,213	79,696	69,583	64,003
NUMBER OF REPORTS WITH DOLLAR LOSSES	28,399	35,900	48,495	42,115	39,680
MEDIAN DOLLAR LOSSES	\$959	\$1,300	\$1,870	\$2,000	\$2,000
TOTAL DOLLAR LOSSES IN MILLIONS	\$483M	\$722M	\$1,294M	\$1,339M	\$1,140M

COMPARING IMPOSTER SCAM REPORTS – 2023

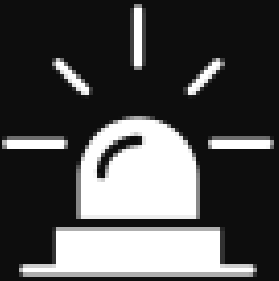
	BUSINESS IMPOSTERS	474,731
	GOVERNMENT IMPOSTERS	228,282
	TECH SUPPORT SCAMS	91,196
	ROMANCE SCAMS	64,003
	FAMILY EMERGENCY SCAMS	33,479

Of the \$2.21 billion imposter
“industry,” which imposters
are inflicting the most
reported financial harm?

IMPOSTER SCAM DATA BY REPORTED \$\$ LOSS

**FAMILY
EMERGENCY
SCAMS**

5



**\$89
million**

**TECH
SUPPORT
SCAMS**

4



**\$242
million**

**GOVERNMENT
IMPOSTERS**

3



**\$617
million**

**BUSINESS
IMPOSTERS**

2

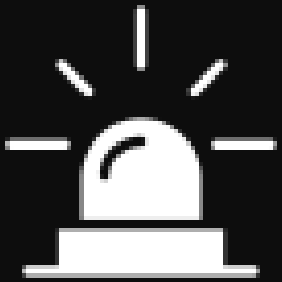


**\$752
million**

IMPOSTER SCAM DATA BY REPORTED \$\$ LOSS

**FAMILY
EMERGENCY
SCAMS**

5



**\$89
million**

**TECH
SUPPORT
SCAMS**

4



**\$242
million**

**GOVERNMENT
IMPOSTERS**

3



**\$617
million**

**BUSINESS
IMPOSTERS**

2



**\$752
million**

**ROMANCE
SCAMS**

1



**\$1.14
billion**

So why is it so difficult to go after romance scammers?



**What can we do to shatter
the stigma of romance scams?**

Rethink the vocabulary



Encourage reporting



⚠ Servicemembers, veterans, and military families: [Report here.](#)

Report to help fight fraud!

Report Now →

Protect your community by reporting fraud, scams, and bad business practices.



**Empower
through
education**



MULTIMEDIA EDUCATION

Articles on
consumer.ftc.gov

Videos on
ftc.gov, YouTube,
and other
platforms

Articles and blog
posts directed to
consumers and
businesspeople

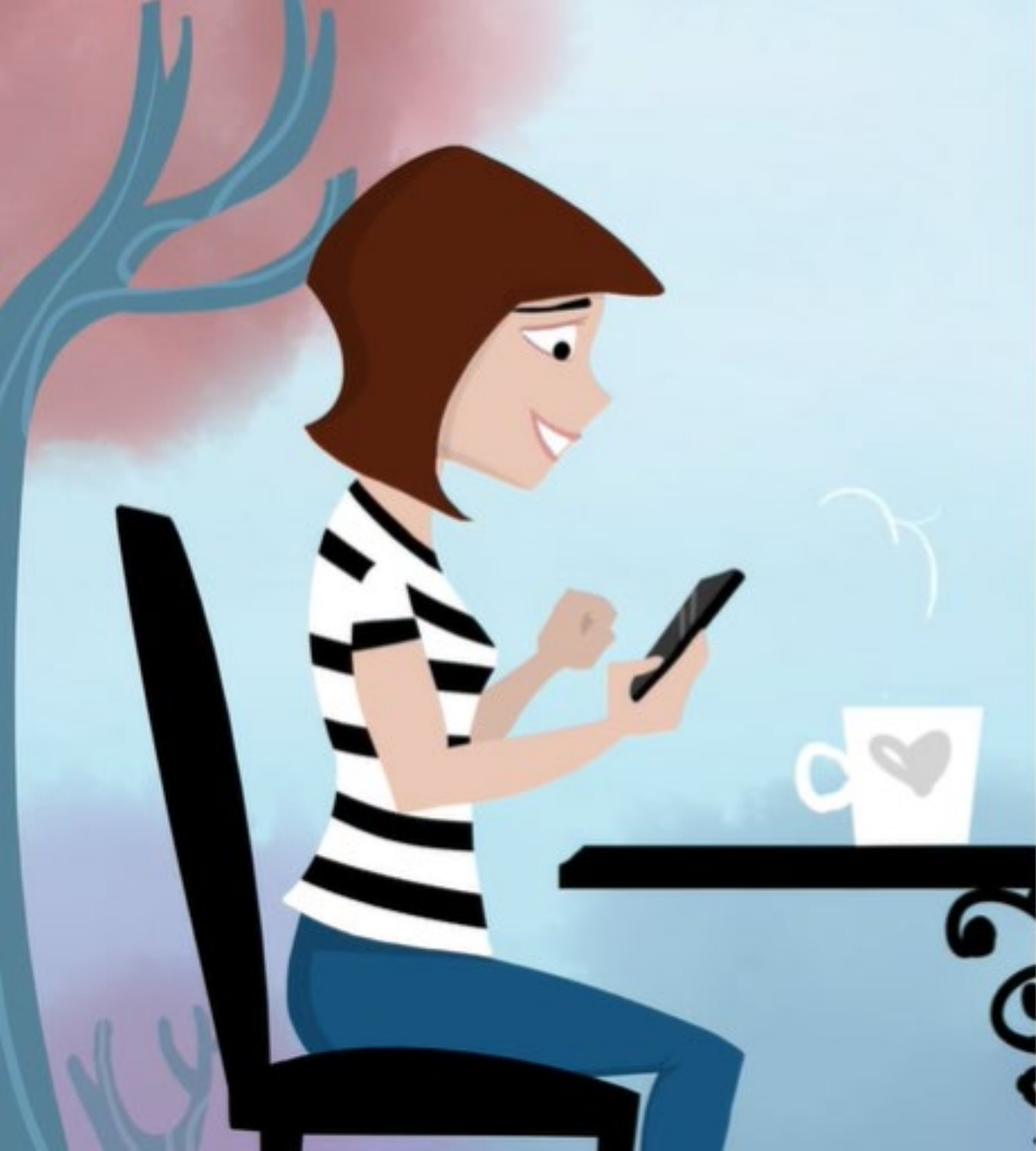
Strategic
partnerships

Social media
content with
sharable
graphics

Articles for
specific audiences
(college students,
military, older
consumers)

Data spotlights
for news media
and others

“Carpe
podium!”



Bad Romance: Top “Love Game” lies told by romance scammers

By: Lesley Fair

February 9, 2023



“Rah, rah-ah-ah-ah. Roma, roma-ma.

Gaga, ooh-la-la. Want your bad romance.”

This Valentine’s Day if you find yourself gaga over an online love, the Federal Trade Commission – yes, the FTC – has advice on ways to tell if you could be caught in a “Bad Romance.”

According to a new [Consumer Protection Data Spotlight](#), in 2022 the [Consumer Sentinel Network](#) received nearly 70,000 reports of romance scams, with reported financial losses hitting a staggering **\$1.3 billion**.

Many people who report losing money say the contact started on a website or app. But the more common approach – according to 40% of reports – was through a social media platform, often as an unexpected message. You know, one of those “Hi, there,” “Loved your post,” or “You’re cute!” comments from an attractive stranger.

From there, the romance scammer may suggest a move to WhatsApp, Google Chat, Telegram, etc. That’s where they may turn to a favorite trick: subtly teasing out their target’s likes and dislikes and then mirroring them back to create what looks like an instant connection. Are you a football fan? They are, too! Is poetry your thing? OMG, let me count the ways! But when it comes time to meet in real life, they have a “Million Reasons” to avoid a face-to-face. According to the [Data Spotlight](#), their



THE MESSAGES

1

LET FAMILY & FRIENDS KNOW YOU'RE LOOKING ONLINE AND PAIR UP WITH A PEER TO COMPARE NOTES.

2

DO REVERSE IMAGE SEARCHES FOR PHOTOS AND LOOK FOR TEXT ON SEARCH ENGINES.

3

A REQUEST FOR MONEY IS A NO.

4

AN "INVESTMENT OFFER" IS A NO.

5

A REQUEST FOR EXPLICIT PHOTOS IS A NO.

6

HELP OTHERS BY REPORTING SCAMS TO THE FTC AND TO THE PLATFORMS.



Sign up to get FTC Business
Blog and Consumer Alerts
at ftc.gov/subscribe.

lfair@ftc.gov

Q&A

Are There Any Questions?

Using OSINT Model to Identify Threats to Critical Infrastructure

Katie Shuck

Lead Cyber Intelligence Analyst
South Dakota Fusion Center





Using OSINT Model to Identify Threats to Critical Infrastructure

FISSEA Winter Forum

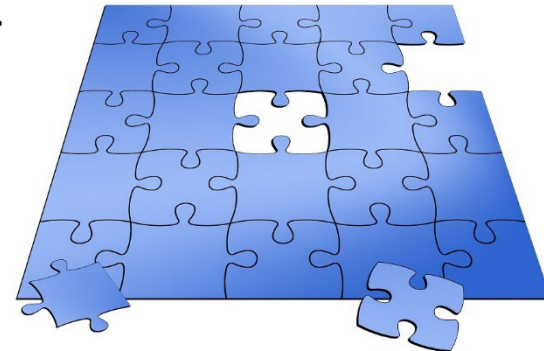
14 February 2024

Open-Source Intelligence (OSINT)

The collection and analysis of publicly available information for an intended audience.

- Public Records
- News Articles
- Social Media
- Data Breaches
- Vulnerability Information
- ...and More

The Internet maximizes the availability OSINT...
and its use by cyber and physical threat actors.



OSINT Physical Threat: Doxing

Revealing and possibly publicizing the personal information of an individual, which was previously private or difficult to obtain, often for the purpose of online shaming, extortion, stalking, harassment/intimidation, and/or vigilante activities.

Including, but not limited to:

Full Name

Address

Phone Number(s)

Email Address(es)

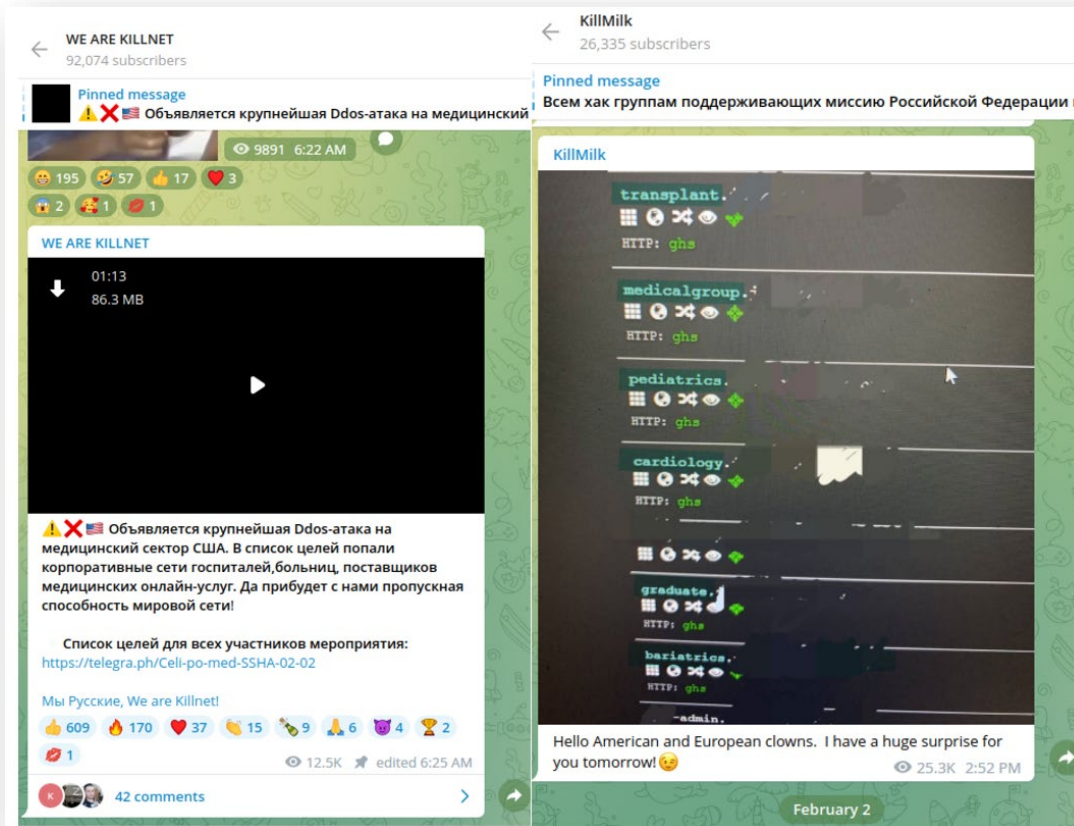
Family Member Information

Social Media Account(s)

Intimate images



OSINT Cyber Threat: The Possibilities are Endless



Phishing
Impersonation
Domain Information
Vulnerabilities
Vulnerable Devices
Credential Leaks
Open Ports
Data Breach Information
Ransomware Victims
Fraud/Scams
And more...

OSINT Techniques

- Google – and non-Google – “Dorking”
- Public Records
- Social Media and Online Communities
- People Search Sites
 - Mapping Services
 - Email Searches
 - Phone Number Searches
- Data Breach Information
- Image Searching
- Vulnerability Posts and Searches
- Dark Web Searching



Google “Dorking”

The most popular search engine – Google works by using web crawlers to generate and index its search results

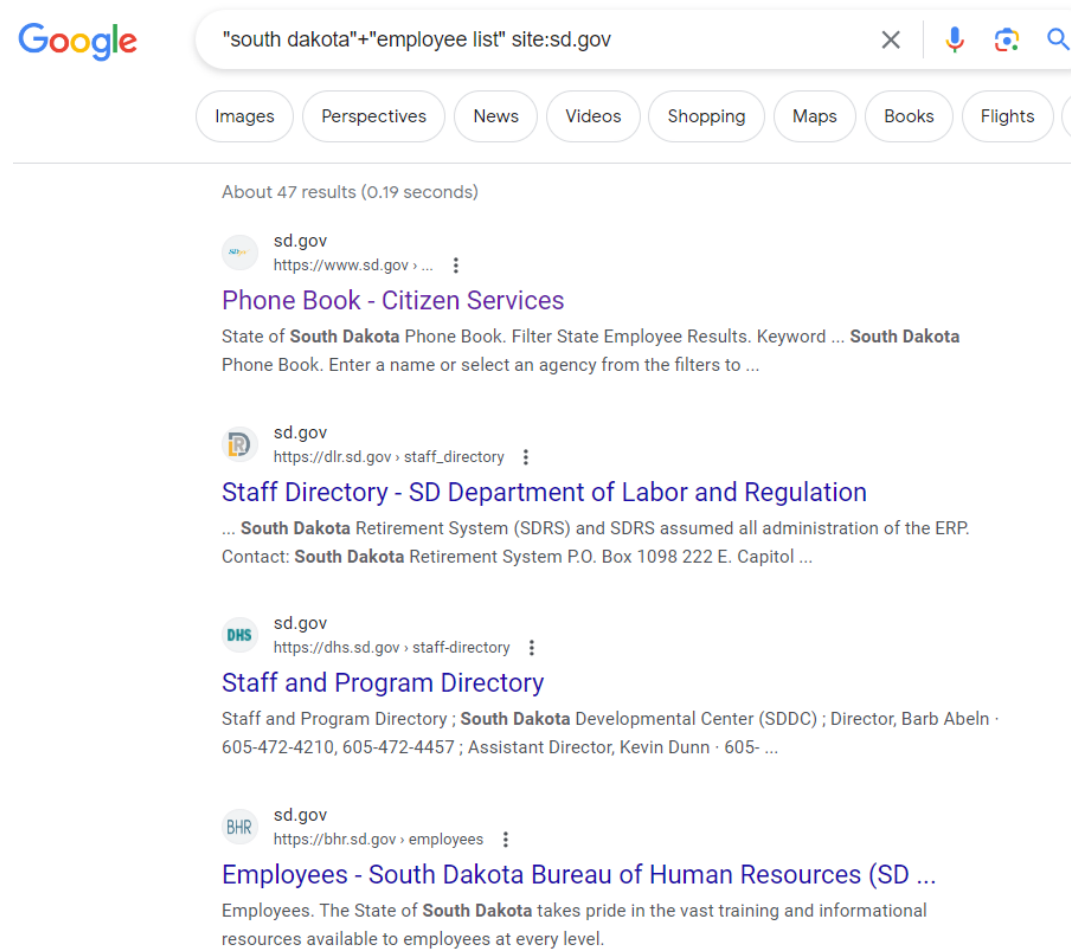
- Advanced search techniques/queries make searching more effective and efficient – and provide better ways to identify hard-to-find information
- Some search strings are Google-specific – some can be used on other browsers and in other search techniques (e.g., searching Facebook)

Advanced Search String Examples	Result
Taylor Swift	The words “Taylor” AND “Swift”
“Taylor Swift”	The exact phrase “Taylor Swift”
“Taylor Swift” –music	The phrase “Taylor Swift” but NOT the word “music”
site:[URL]	Restrict search to one website or domain

Google “Dorking”: Linking Searches

Search parameters, when linked together, can greatly improve search results so that you only see what you really want to see

Example:



The screenshot shows a Google search interface. The search bar contains the query: "south dakota"+"employee list" site:sd.gov. Below the search bar are tabs for Images, Perspectives, News, Videos, Shopping, Maps, Books, and Flights. The search results are displayed below, showing about 47 results in 0.19 seconds. The first three results are:

- sd.gov**
https://www.sd.gov > ...
Phone Book - Citizen Services
State of **South Dakota** Phone Book. Filter State Employee Results. Keyword ... **South Dakota** Phone Book. Enter a name or select an agency from the filters to ...
- sd.gov**
https://dlr.sd.gov > staff_directory
Staff Directory - SD Department of Labor and Regulation
... **South Dakota** Retirement System (SDRS) and SDRS assumed all administration of the ERP. Contact: **South Dakota** Retirement System P.O. Box 1098 222 E. Capitol ...
- sd.gov**
https://dhs.sd.gov > staff-directory
Staff and Program Directory
Staff and Program Directory ; **South Dakota** Developmental Center (SDDC) ; Director, Barb Abeln · 605-472-4210, 605-472-4457 ; Assistant Director, Kevin Dunn · 605- ...

The fourth result is:

- sd.gov**
https://bhr.sd.gov > employees
Employees - South Dakota Bureau of Human Resources (SD ...
Employees. The State of **South Dakota** takes pride in the vast training and informational resources available to employees at every level.

Public Records

- Public records can provide vast amounts of freely available information and are often available online
 - While some records can be requested to be made public, this is dependent on the location of the records

Examples of Public Records:

- *Property Records*
- *Court/Criminal Records*
- *Birth/Death Records*
- *Voter Records*
- *Business Filings*
- *Government Open Records*



Social Media and Mobile Apps

Can provide access to exponential information to identify home, family, friends, patterns of life, background...

Username	Display Name	Birthday
Connections	Images/Video	Phone Numbers
Email	Employment	Schools Attended

Visibility of accounts is often dependent on privacy settings



Facebook
Twitter/X
Instagram
LinkedIn
SnapChat
Tik Tok
Telegram
CashApp
Venmo
And Many More...

Online Communities

- Similar to social media, but usually created for a specific service or lifestyle
- Many online communities won't show up on Google searches because Google doesn't index them – or doesn't index them well.

Some online communities can be searched with a Google site: search but many cannot

- Online communities can include chat forums, blogs, dating and meetup sites, chat applications, eCommerce sites, and more
- Examples:

Reddit	4Chan	Discord
Slack	Craigslist	Amazon
eBay	Match	Meetup
Roblox	Tinder	OnlyFans

People Search Sites

Tool	Description
True People Search (truepeoplesearch.com)	Results include current and previous addresses, telephone numbers (including mobile), email addresses, relatives, spouses, and associates
Fast People Search (fastpeoplesearch.com)	Similar to True People Search, but may produce results if a person removed their information from True People Search
Nuumber (nuumber.com)	Allows for search of a first and last name with results including location and often, full name, age, range, home address, telephone number, and neighbors
Family Tree Now (familytreenow.com)	Targeting for those conducting family history research and specializes in connecting people to their relatives
That's Them (thatthem.com)	Displays information not publicly available elsewhere
Yasni (yasni.com)	Similar to other search engines, but also provides news articles, websites, and social networks related to the person
How Many of Me (howmanyofme.com)	Tells how many people exist with a specific name (may help determine the effectiveness of targeted searches)

People search sites will have opt out pages or contacts to have information deleted from their site – but this isn't always easy and information may repopulate over time

Mapping Services



Phone Searches

Once identified, they can be verified with search techniques, including:

- “Forgot My Password” searching
- Payment application searches
- Adding to device contacts and searching
- Caller ID Databases

- The same databases that identify phone numbers on landline caller ID displays
- Often includes the name associated with the number

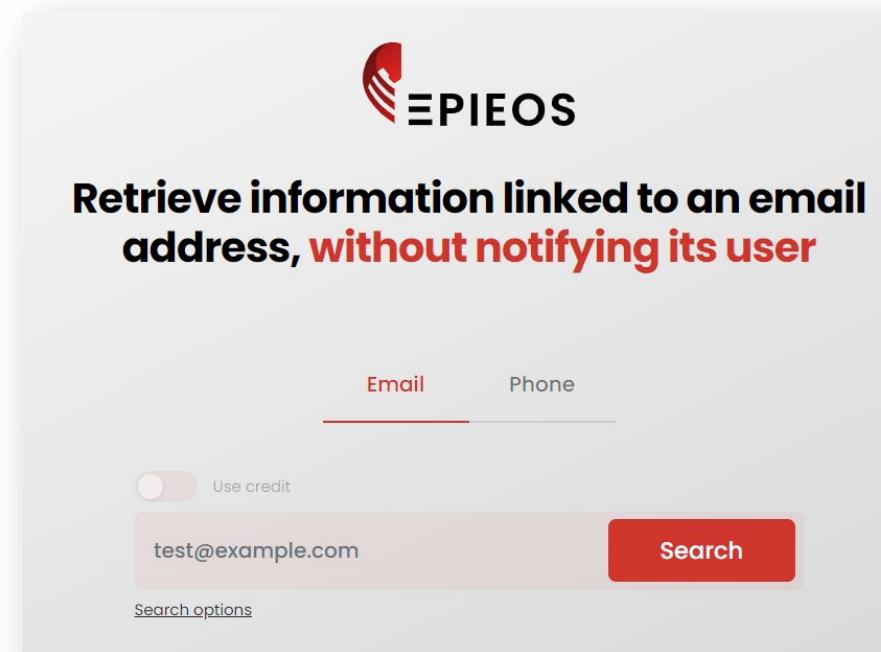
Tool	Description
Twilio (twilio.com/lookup)	Provides VoIP services to many apps, companies, and individuals and allows queries against their database
Open CNAM (opencnam.com)	With the CNAM Query Tool, can receive the carrier and name associated with mobile and landline numbers
Everyone API (everyoneapi.com)	Owned by same company as Open CNAM, but also provides the current address, gender, carrier information, previous carrier, and subscriber name of the owner
Truecaller (truecaller.com)	Uses crowd-sourced information (via users sharing their contact information) to provide results

- Craigslist may post phone numbers

Email Searches

Can search for similar to phone searches

- “Forgot My Password” searching
- Payment application searching
- Adding to Contacts and searching



The screenshot shows the EPIEOS search interface. At the top is the EPIEOS logo, which consists of a red stylized 'E' icon followed by the text 'EPIEOS'. Below the logo is the heading 'Retrieve information linked to an email address, without notifying its user', where 'without notifying its user' is in red. There are two tabs: 'Email' (selected with a red underline) and 'Phone'. Below the tabs is a toggle switch for 'Use credit', which is currently turned off. A search input field contains the text 'test@example.com' and a red 'Search' button is to its right. At the bottom left of the interface, there is a link for 'Search options'.

Image Searching

PimEyes

[Search](#) [Pricing](#) [Blog](#) [News](#) [Opt-Out](#) [FAQ](#)

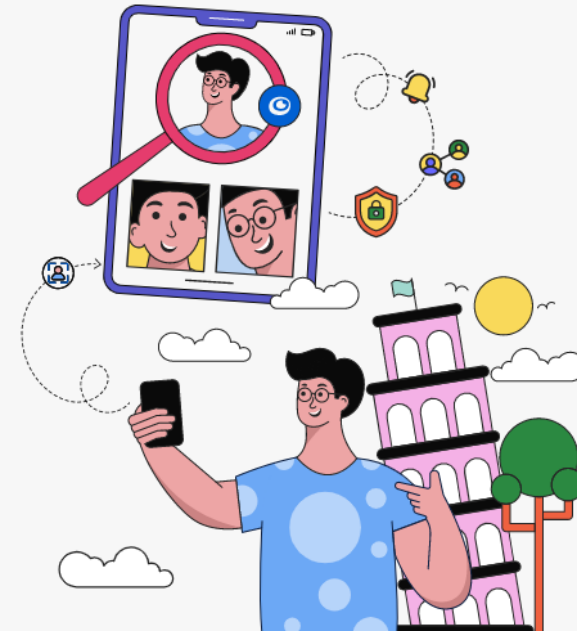


Face Search Engine Reverse Image Search

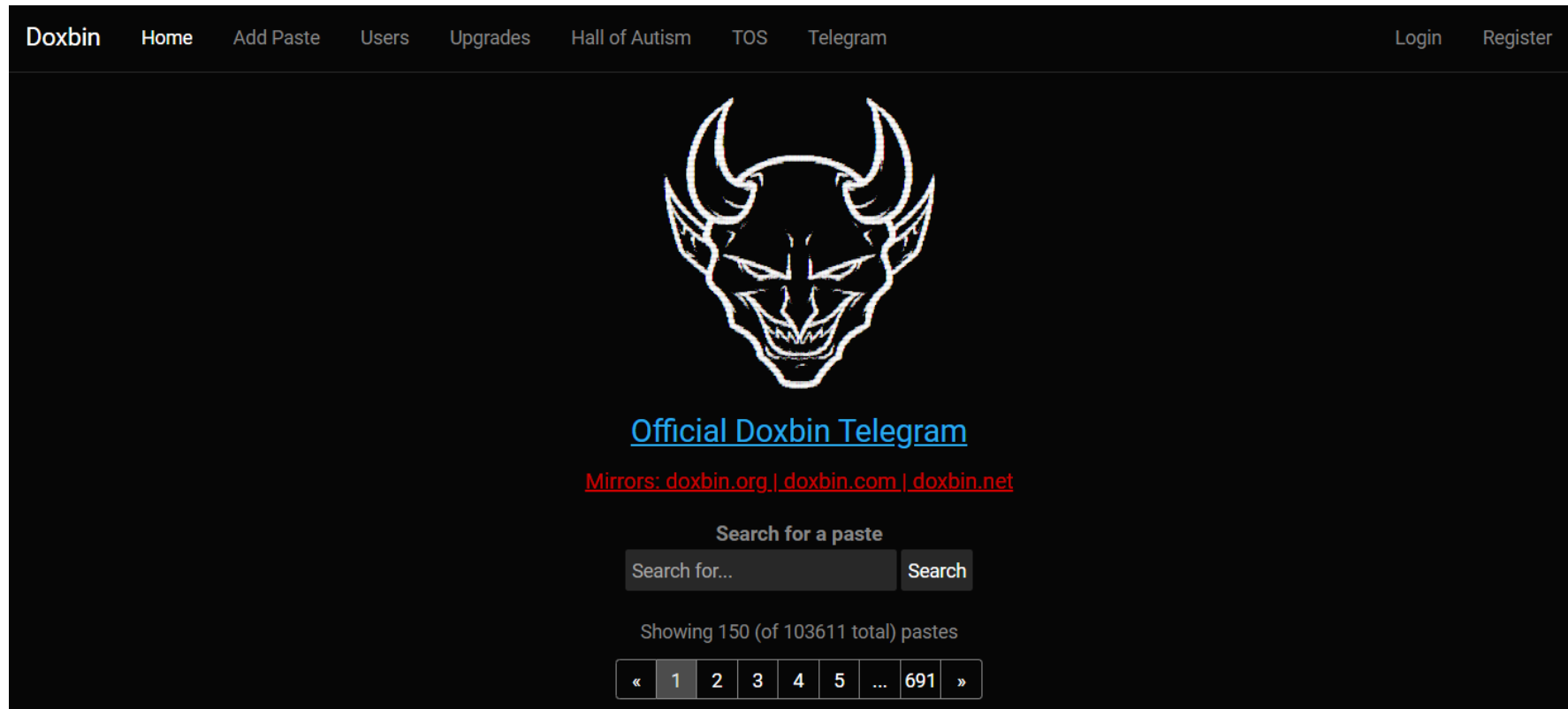
UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED

 Upload a photo 

Or you can take a photo with the device's camera. Don't worry, we will not store it!

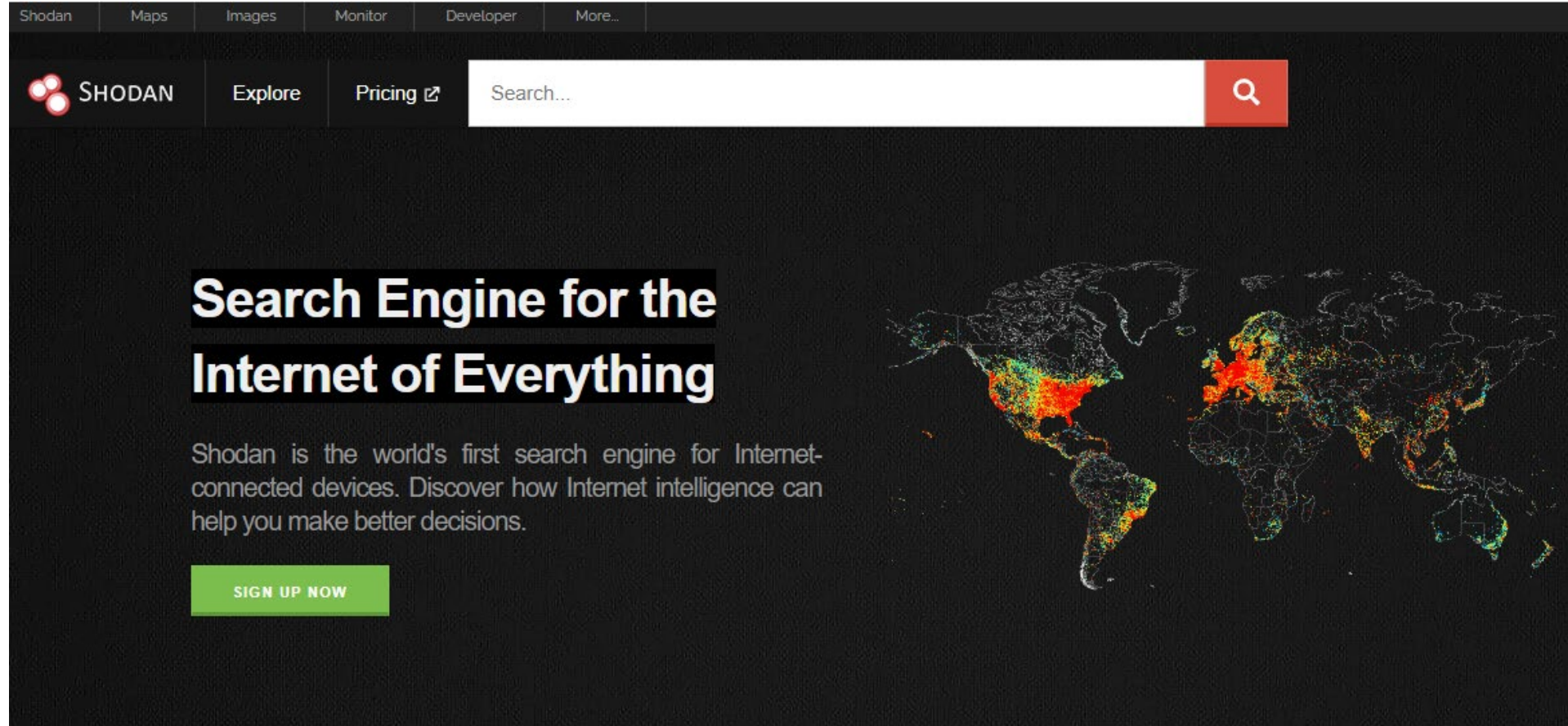


Paste Sites



The screenshot shows the Doxbin website interface. At the top, there is a navigation bar with links: Doxbin, Home, Add Paste, Users, Upgrades, Hall of Autism, TOS, Telegram, Login, and Register. The main content area features a large white outline of a devil's head with horns and a grinning mouth. Below the image is a blue link for the "Official Doxbin Telegram" and red text for "Mirrors: doxbin.org | doxbin.com | doxbin.net". A search section includes the text "Search for a paste", a search input field with "Search for..." placeholder, and a "Search" button. Below the search section, it says "Showing 150 (of 103611 total) pastes" and a pagination bar with buttons for «, 1, 2, 3, 4, 5, ..., 691, and ».

Vulnerability Searches



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More... Below this is a dark header with the Shodan logo (three red circles) and the word 'SHODAN' in white. To the right of the logo are links for 'Explore' and 'Pricing' with an external link icon. A large white search bar with a red search button is positioned to the right of the navigation. The main content area features the headline 'Search Engine for the Internet of Everything' in large white text. Below the headline is a paragraph: 'Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.' A green button with the text 'SIGN UP NOW' is located below the paragraph. On the right side of the page, there is a world map with a network overlay and color-coded regions in red, orange, and green.

Questions?



Katie Shuck

Lead Cyber Intelligence Analyst

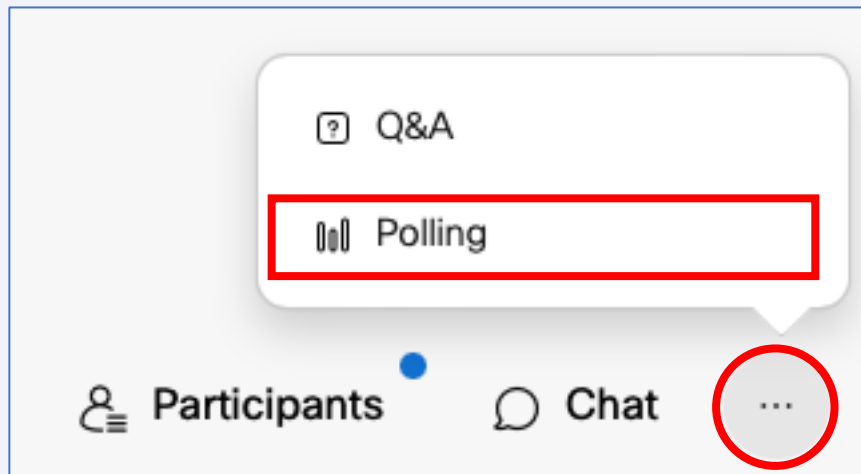
South Dakota Fusion Center

katie.shuck@state.sd.us

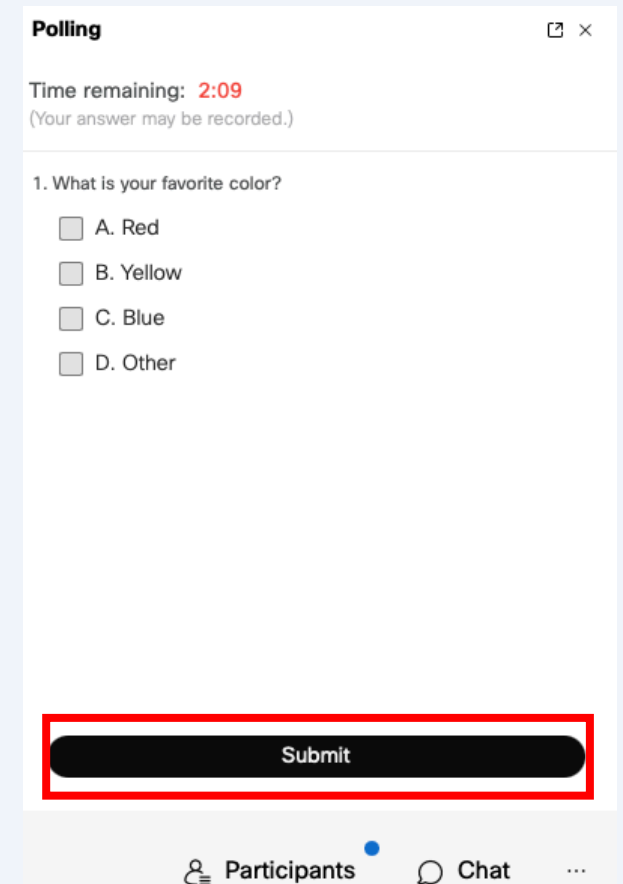
fusion.sd.gov

We want to hear from you!

Select "Polling" in the bottom left of your screen



Complete the poll and click "Submit"



Federal Information Security Educators (FISSEA) Winter Forum

BREAK

The Forum will resume at 2:30pm ET

#FISSEA | nist.gov/fissea

Welcome Back!

Maureen Premo

Cyber Defense Education and Training (CDET)
Cybersecurity and Infrastructure Security Agency



Featured Panel: NIST SP 800-50



Marian Merritt

Deputy Director of NICE/FISSEA Lead
National Institute of Standards and Technology



Susan Hansche

CISA/CSD Training and Development
Department of Homeland Security



Kevin Sanchez-Cherry

Cybersecurity Policy, Architecture
and Training Lead
U.S. Department of Transportation
Office of the Chief Information Officer



Don Walden

Senior Privacy Analyst
Internal Revenue Service

**NIST SP
800-50
update**

Panel:

Susan Hansche, CISA

Marian Merritt, NIST

Kevin Sanchez-Cherry, DOT

Don Walden, IRS

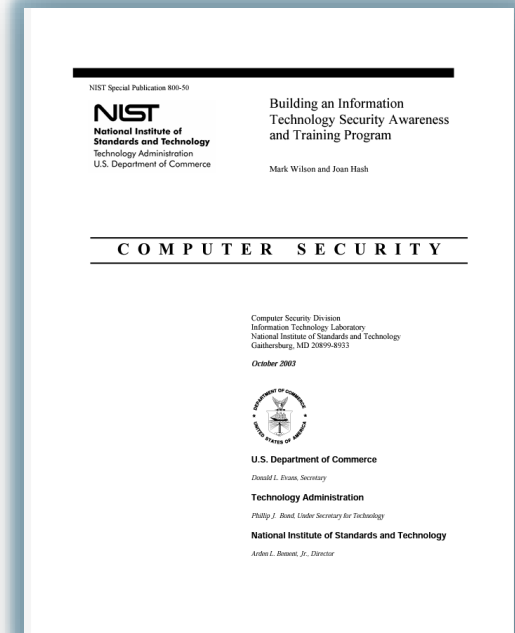
Additional NIST Special Publication 800-50 Authors:

Brenda Ellis, NASA

Julie Snyder, MITRE

NIST SP 800-50 rev 1

- Building an Information Technology Security Awareness & Training Program - 2003 (20 years ago)
 - Revision draft made public August 28, 2023
 - Comments through October 27, 2023
 - Co-authoring team from several Federal agencies
-
- Goals:
 - Leverage NIST guidance
 - Develop consistent language
 - Reflect research from FISSEA community
 - Address challenges such as measuring impact



NIST SP 800-50 rev 1, cont.

- The learning program is a cyclical, iterative model
- Consolidates 800-16, incorporates NICE Framework
- Intended to be collaborative, flexible, scalable

Adding Privacy

- Background to the Privacy Act of 1974
- Requirements of OMB Circular A-130
- Leverage and reference the NIST Privacy Framework

Poll 1

In your current job, do you have privacy-related responsibilities?

- Yes
- No
- Don't know/aren't sure

Poll 2

Do you have responsibility for including privacy topics in an awareness or training program?

- Yes
- No
- Don't know/aren't sure

Poll 3

In your current job, do you participate in or are required to take privacy training?

- Yes
- No
- Don't know/aren't sure

What SP 800-50 r1 is:

- “Building a Cybersecurity and Privacy Learning Program”
- Enterprise-wide awareness, training, and education program - Cybersecurity and Privacy Learning Program (CPLP)
- The learning program supports a culture of respect for employees
- Everyone plays some type of role in managing the organization’s cybersecurity and privacy risk

The Learning Program is...

- a cyclical, iterative model that adapts to each agency's needs and situation
- Intended to be collaborative, flexible, scalable
- A way to encourage cross-functional cooperation with senior leadership



Senior Leadership

- 800-50 r1 recommends forming a Senior Leadership committee or advisory board
 - CIO, CPO, etc
 - Human Resources
 - Communications
- Strategy and Budget Planning
- Regular Program review and discussion
- Program support and participation

What SP 800-50 r1 is NOT

- Details on designing or developing new training elements
- How to create a change management or cultural program
- An enterprise-wide human risk management program
- Who should do what work in the organization
- How to create an enterprise-wide metrics program
- How to identify employees in your workforce according to the NIST

SP 800-181 work roles

What comes next...

- Final editing to incorporate comments
- Internal NIST editorial review
- Publish to the public-facing NIST website

Q&A

Thank you!

Q&A

Are There Any Questions?

How IC3.gov Works

Wes Quigley

Unit Chief
Federal Bureau of Investigation

Rachel Yurkovich

Management and Program Analyst
Federal Bureau of Investigation

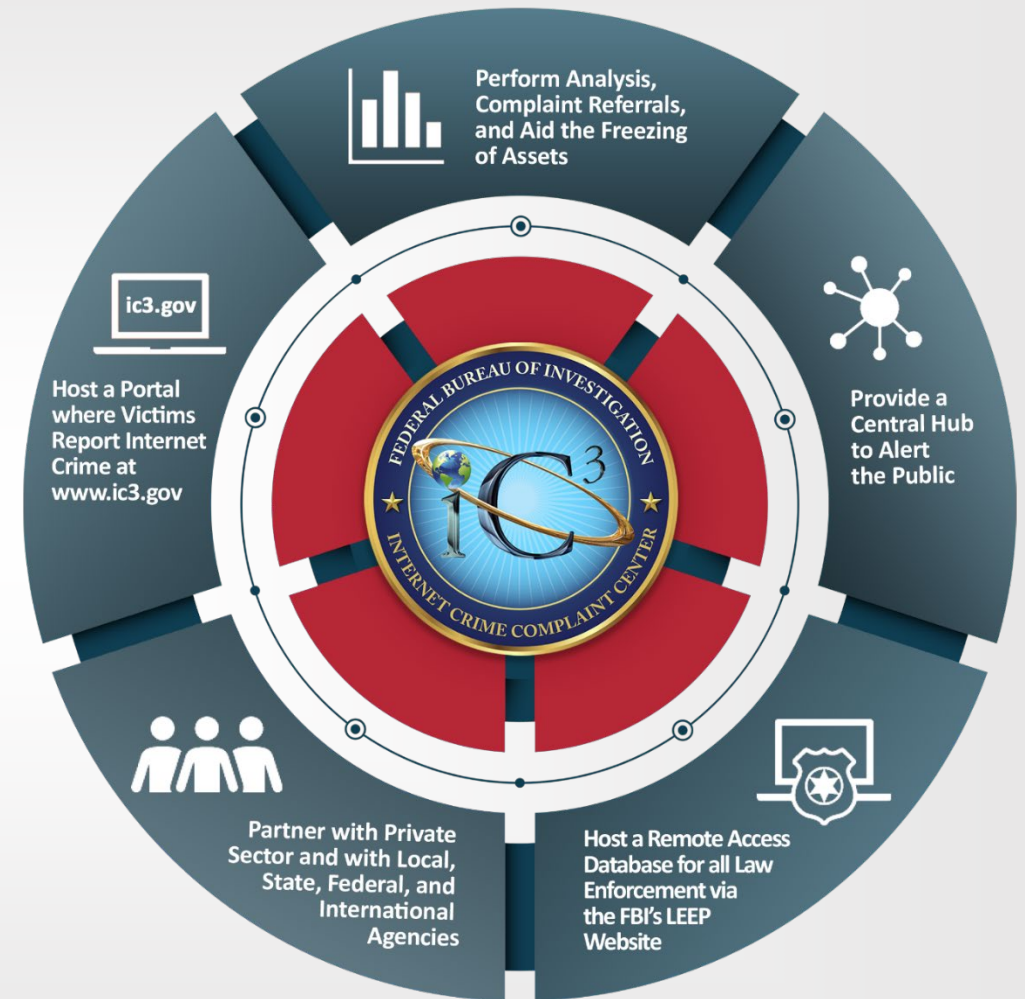




Internet Crime Complaint Center

Internet Crime Complaint Center

The mission of the Internet Crime Complaint Center is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness.



IC3 - or - NTOC

Internet Crime Complaint Center (IC3)



www.ic3.gov

Receives and processes online complaints reporting:

- Frauds, scams
- Elder Fraud
- Intrusions
- Ransomware

National Threat Operations Center (NTOC)



1-800-CALL-FBI

www.tips.fbi.gov

Receives and processes phone calls and e-Tips reporting:

- Threats to Life
- Suspected Terrorism



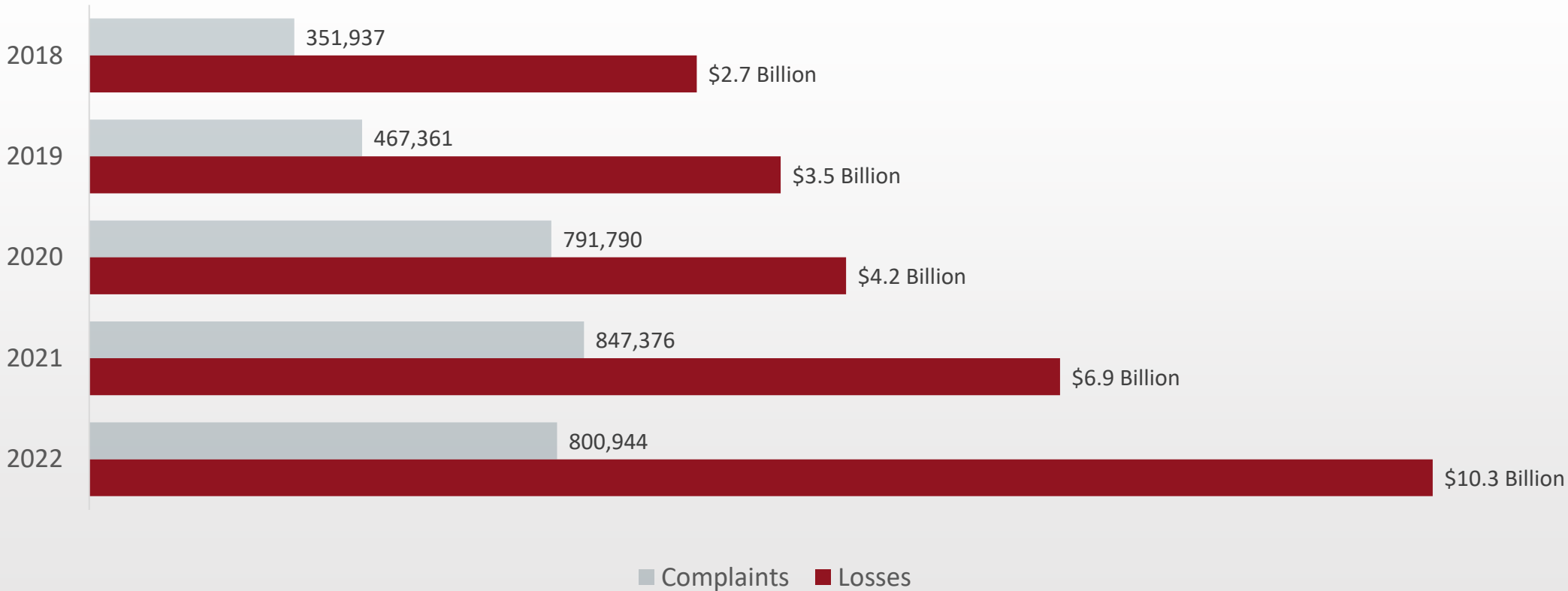
Criminal Investigative
18 U.S Code § 1341, 1343, 1349
Frauds and Swindles
Mail Fraud
Wire Fraud
Frauds and Scams
Cryptocurrency
Elder Fraud

Recovery Asset Team
18 U.S Code § 1349
Wire Fraud
Business Email Compromise
Domestic Financial Fraud Kill Chain

Cyber Division
18 U.S Code § 1030
Fraud and Related Activity in
Connection with Computers
Ransomware
Computer Intrusion
Malware

IC3 Complaints – Past Five Years

Complaints and Losses over the Last Five Years*



Cryptocurrency

52,218

Complaints
with Crypto
Nexus

\$3.853
Billion

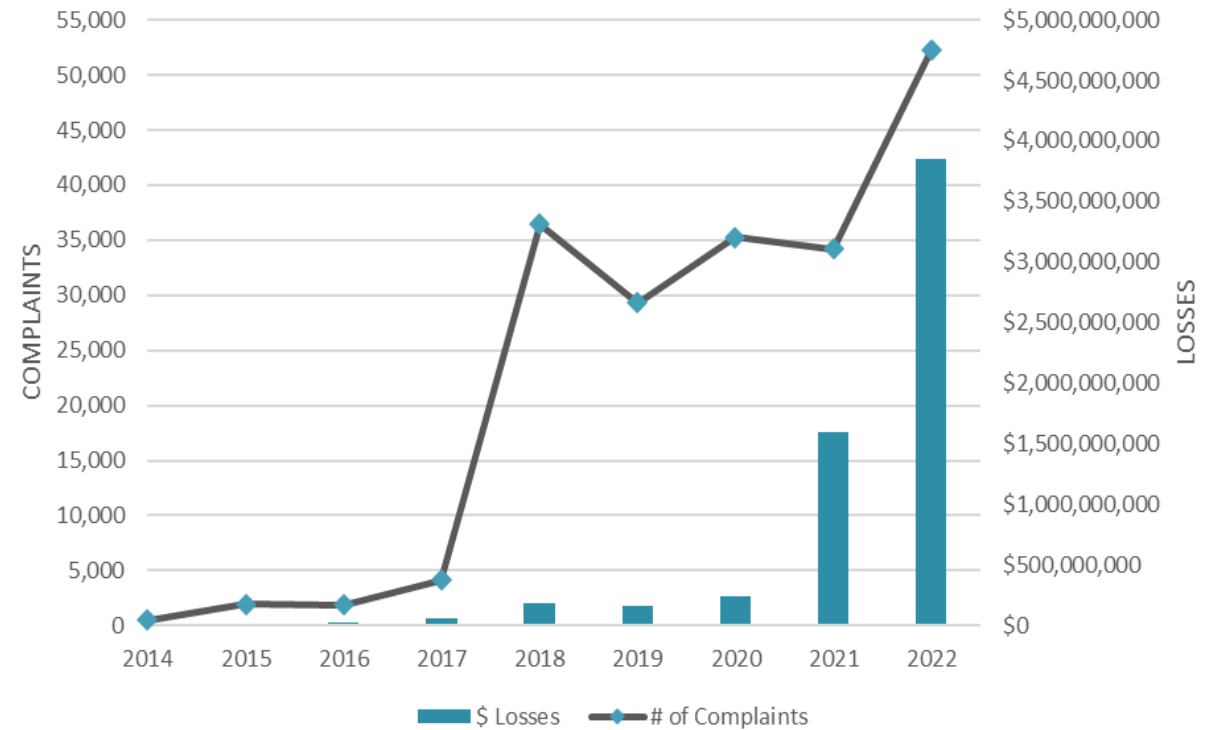
Losses

2022

Most
Reported
Fraud:
Investment

Most
affected:
30 - 39
Years Old

IC3 Complaints with Reference to Cryptocurrency



IC3 Support

Major Initiatives

Ransomware, Intrusions
Call Center Fraud
Crypto Investment
Elder Fraud
Kill Chain
Complaint Aggregation
Case Support
Trending

Outreach / Presentation

Presentations
Webinars
Podcasts
Media Inquiries
Interviews

Product Publications

Public Service
Announcements
Cyber Security Advisories
Annual Reports

SUPPORT	2023	2022
Case Enhancements	310	190
Search Requests	103	284
Data Disseminations	3,825	4,754
Guardians	5,347	4,023
Cases Opened	398	441

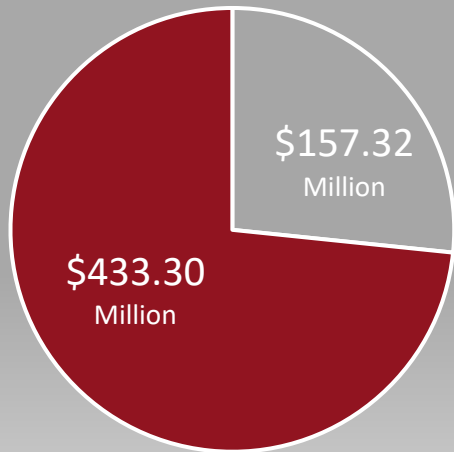


Recovery Asset Team (RAT)

Functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis

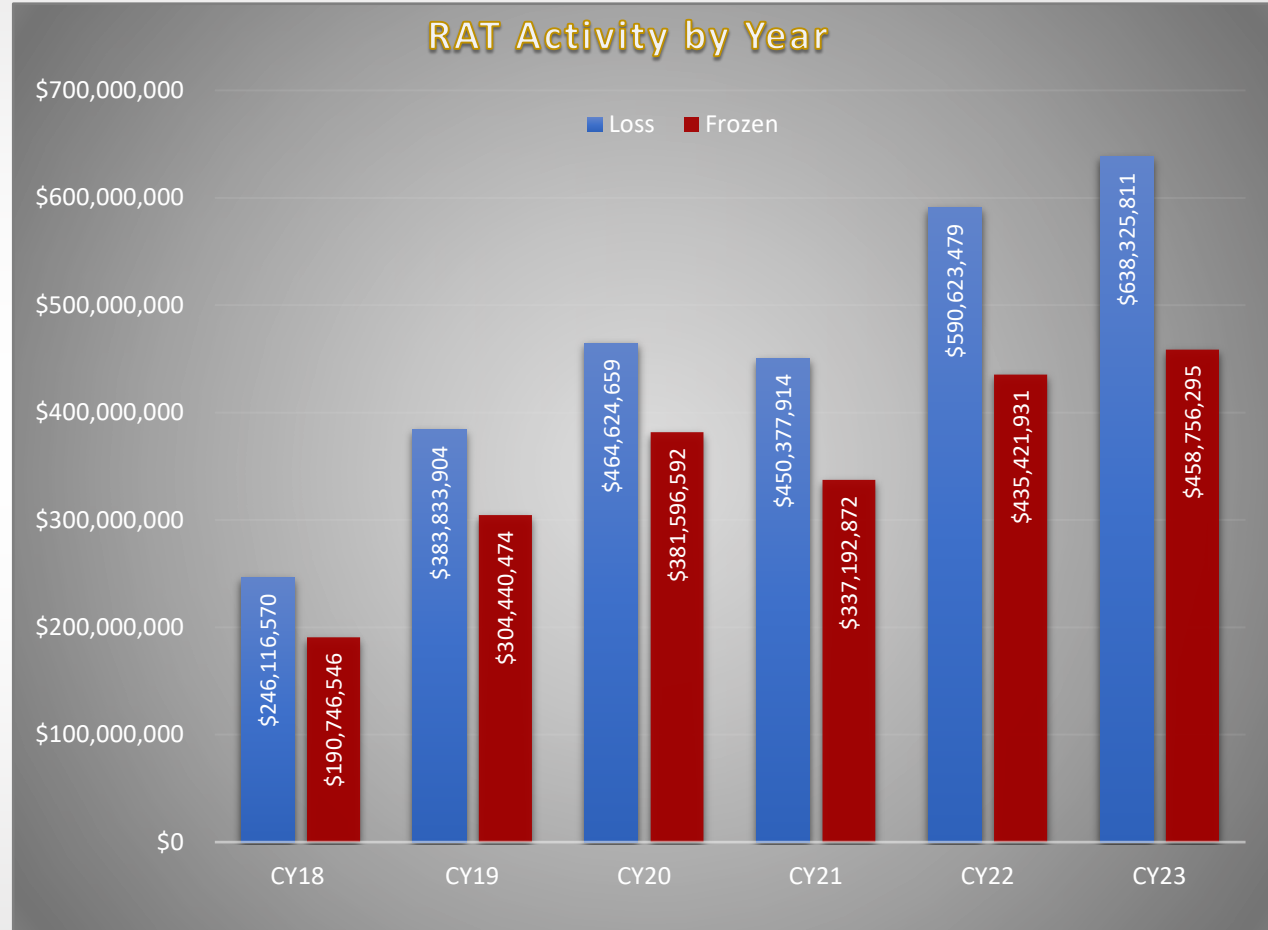
2022 Successes

- 73% Success Rate
- 2,838 Incidents
- \$590.62 Million Losses
- \$433.30 Million Frozen



□ Remaining Losses ■ Frozen Funds

RAT Activity by Year

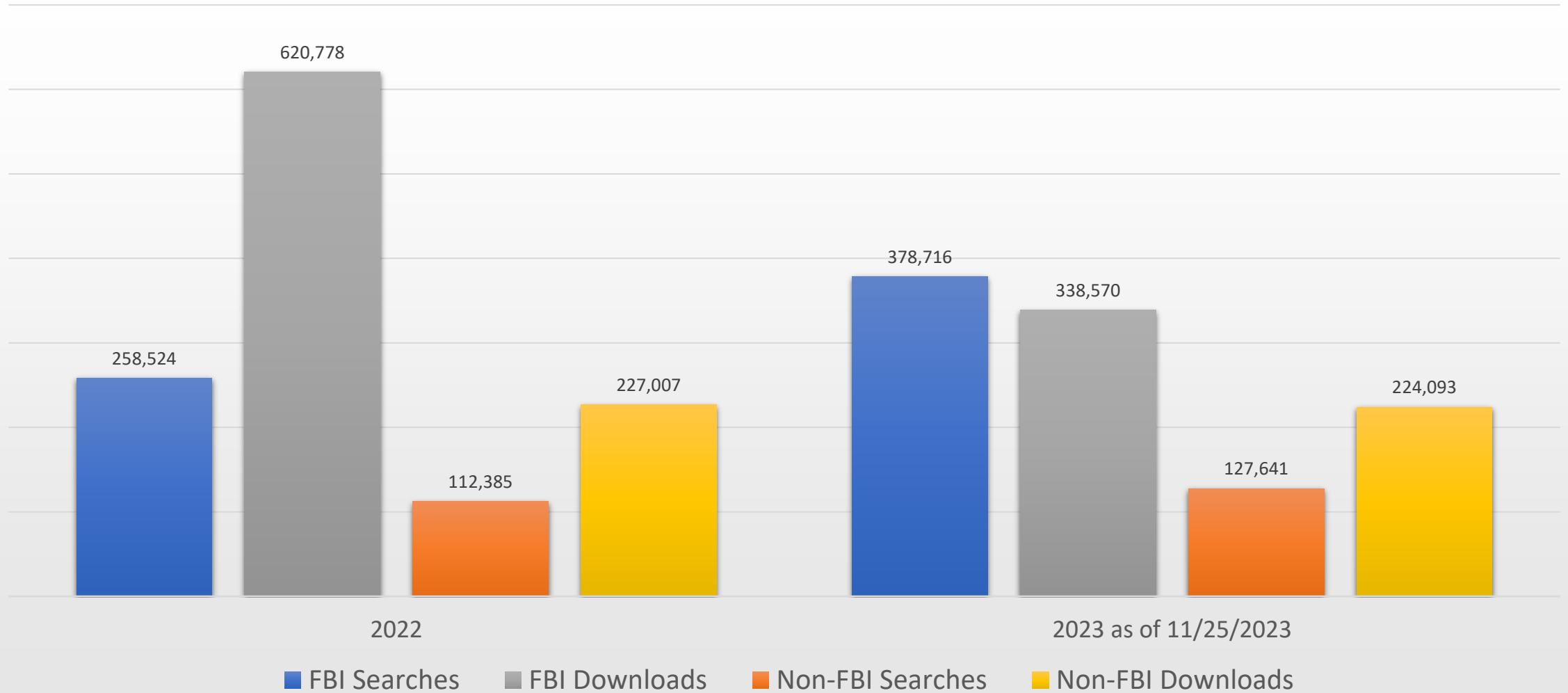


IC3 Remote Access

- Access to the IC3 database, via remote query, is automatically granted to sworn law enforcement and FBI employees
- All other LEEP users are evaluated on a case-by-case basis
- Email LE-SearchAssist@ic3.gov for search requests or with questions.



IC3 Remote Query



Our Partners



- 56 FBI Field Offices and 63 LEGATS
- Foreign Law Enforcement
 - GAEN, GASA, International Threat Group (NFIB, RCMP, CoLP, CAFC)
- Government Agencies
 - Secret Service, Homeland Security, Federal Trade Commission, State and Local Law Enforcement
- Private Sector
 - National Cyber-Forensics and Training Alliance
 - Financial Institutions, Cryptocurrency Exchanges

Success Stories

Case Support

- Tech Support (Knoxville): Five individuals, including one subject from India charged with being the Owner/Director of the call center in India. Three individuals in Iowa and one individual in Maryland are accused of facilitating payments on behalf of the Indian call center. ~15,000 victims; ~\$15 million losses.
- Call Center Fraud; FY23 - FBI enabled 26 arrests through 13 joint operations with Indian authorities.

FFKC

- Between January 2014 – December 2022, internationally over **\$731** million dollars frozen for possible recovery.
- Between February 2018 – December 2022, domestically over **\$1.6** billion dollars frozen for possible recovery.

Questions?

UC SSA L. Wes Quigley

LE-SearchAssist@IC3.gov



What's New, and What's Ahead, at the National Cybersecurity Alliance

Lisa Plaggemier

Executive Director
National Cybersecurity Alliance





**NATIONAL
CYBERSECURITY
ALLIANCE**

What's New, and What's Ahead, at the National Cybersecurity Alliance

Lisa Plaggemier
Executive Director, National Cybersecurity Alliance

February 14, 2024

About Us

We empower a more secure, interconnected world.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.

NATIONAL CYBERSECURITY ALLIANCE



**HBCU
Career
Program**



2023 Results



 COMMITTEE ON HOMELAND SECURITY

[Garbarino, Swalwell Introduce Bipartisan Resolution To Recognize Cybersecurity Awareness Month](#)

October 24, 2023 | [Press Release](#)

Congressman Andrew R. Garbarino (R-NY-02), Chairman of the Homeland Security Committee's Subcommittee on Cybersecurity and Infrastructure Protection, recently introduced a House Resolution to recognize October as National Cybersecurity Awareness Month.

SEPTEMBER 29, 2023

A Proclamation on Cybersecurity Awareness Month, 2023

 BRIEFING ROOM  PRESIDENTIAL ACTIONS

Digital technologies today touch nearly every aspect of American life – from our classrooms and communities, to our economy and national security. That is why – this Cybersecurity Awareness Month – my Administration renews our commitment to securing cyberspace and seizing the unlimited potential of our digital future.

- **4,080** Champions from 93 countries and all 50 states
- **765** people tuned into our 20th Cybersecurity Awareness Month Virtual Kick-off event
 - 40% increase from 2022's virtual events
- **43,274 individuals** posted about the campaign in **136,646 posts** across social media platforms
 - Resulted in 651,263 engagements and **1.8b** impressions

Cybersecurity Awareness Month

Speaking Engagements

- **9,500** individuals from **135** organizations attended an NCA talk or virtual game show in 2023
- <https://staysafeonline.org/programs/request-a-speaker/>

Secure Our World



Follow these top tips to stay safe online!

USE STRONG PASSWORDS...

Make your passwords:

Long: At least 16 characters

Complex: Use upper and lowercase letters, numbers and symbols

Unique: Use a different password for each account



...AND A PASSWORD MANAGER

Password managers can

- Store all your passwords
- Tell you when you have weak or re-used passwords
- Generate strong passwords for you
- Automatically fill logins into sites and apps

TURN ON MULTIFACTOR AUTHENTICATION



It provides **extra security** by confirming your identity when logging into accounts, like entering a code texted to a phone or generated by an authenticator app.

RECOGNIZE AND REPORT PHISHING

Common signs of a phish include:

- Urgent/alarming language
- Requests for personal or financial info
- Poor writing or misspellings
- Incorrect email addresses or links

Spot a phish? Report it, then delete it



UPDATE YOUR SOFTWARE

Software updates ensure your devices are protected against the latest threats. Turn on the **automatic updates** in your device's or app's security settings!



OUTSMART online outlaws

Avoid Phishing Scams with Three Simple Tips

Phishing scams are online messages designed to look like they're from a trusted source. We may open what we thought was a safe email, attachment or image only to find ourselves exposed to malware or a scammer looking for our personal data. The good news is we can take precautions to protect our important data. Learn to recognize the signs and report phishing to protect devices and data.

1

Recognize the common signs

- Urgent or emotionally appealing language
- Requests to send personal or financial information
- Unexpected attachments
- Untrusted shortened URLs
- Email addresses that do not match the supposed sender
- Poor writing/misspellings (less common)



2

Resist and report

PHISHING **SPAM**

Report suspicious messages by using the "report spam" feature. If the message is designed to resemble an organization you trust, report the message by alerting the organization using their contact information found on their webpage.

3

Delete

Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**

DELETE

Avoiding phishing is one way to **Secure Our World.**



We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

Twitter | Facebook | YouTube | Instagram | LinkedIn | RSS | Email | #SecureOurWorld

- Evergreen awareness campaign
- Tip sheets, infographics, social media posts & graphics, sample press release, virtual backgrounds
- PSAs

#SecureOurWorld this

CYBERSECURITY AWARENESS MONTH

CYBERSECURITY AWARENESS MONTH

2023 Partner Toolkit

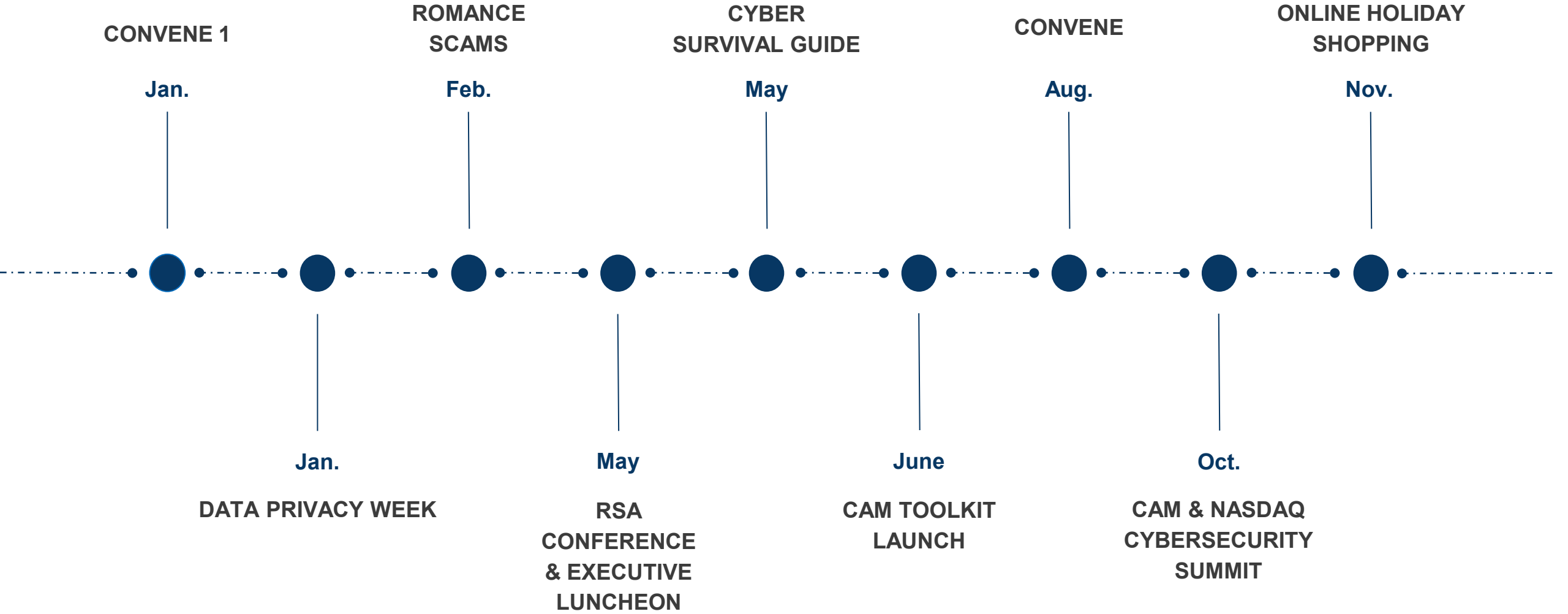
#CybersecurityAwarenessMonth
#SecureOurWorld

Presented By


Security Behaviors

1. Password hygiene: password creation, password management, etc
2. Using Multi-Factor Authentication (MFA)
3. Installing the latest updates
4. Checking emails for signs of phishing
5. Backing up data

2024 NCA Events & Campaigns Timeline



2021



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2021

2022



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2022

2023



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

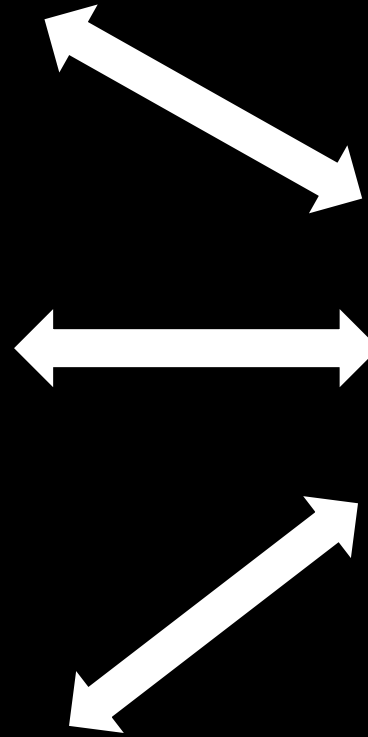
Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2023

Capability

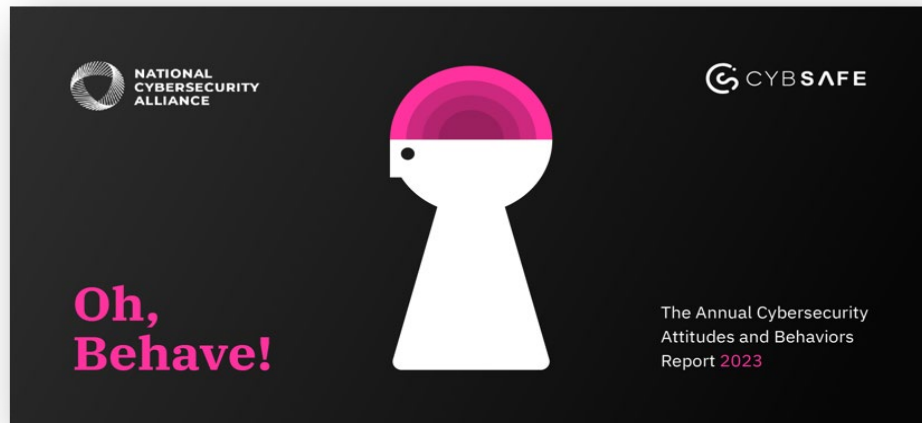
Motivation

Opportunity



Behavior

Oh Behave 2023



- Launched Oct 3, 2023
- 1,965 downloads to date
 - 65% increase compared to same period in 2022
- Coverage:
 - Fortune (UVM: 19M)
 - Beta News (UVM: 1M)
 - Dark Reading (UVM: 405K)
 - CyberWire (UVM: 32K)

Gen Z twice as likely to think cybersecurity isn't worth the effort



By **Ian Barker**

Published 1 week ago

[Follow @IanDBarker](#)

 [No Comments](#)

 [Share 3](#)

 [Share](#)

 [Tweet](#)



Q. What is your preferred method of remembering multiple passwords?

- a. I write them down in a notebook **31%**
- b. I write them down in a document on my computer **5%**
- c. I store them in my phone **11%**
- d. I store them in my email **5%**
- e. I just remember them (without writing them down) **24%**
- f. I save passwords in the browser **9%**
- g. I use a password manager application **12%**
- h. Reset at each log in **3%**

Oh Behave 2023 Results

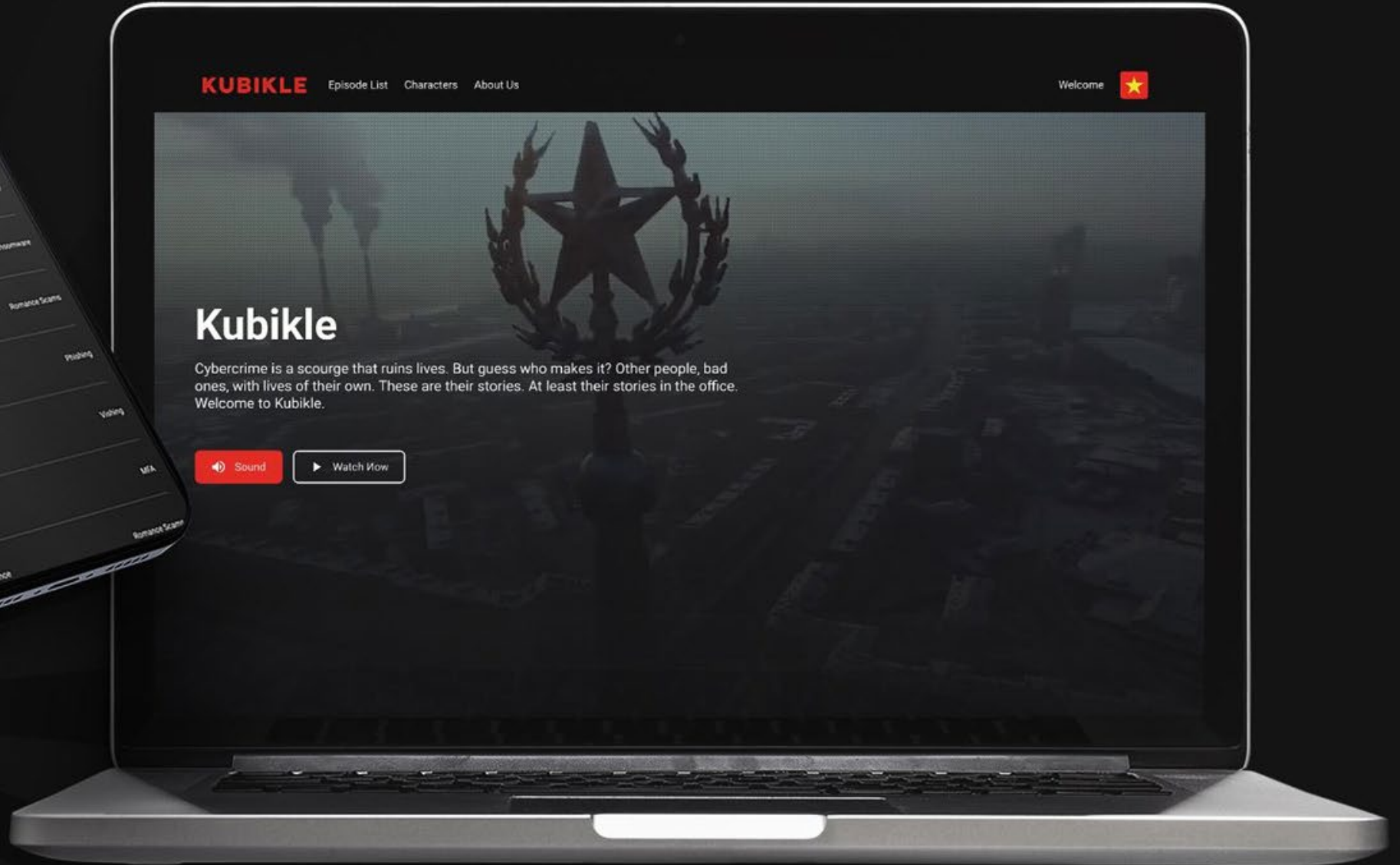
- 89% consider online safety a priority
 - 39% feel frustrated by work it takes
- 46% of Millennials say parents rely on them to stay safe online
- 83% of Baby Boomers feel that staying safe online is a priority
 - 52% of Gen Zers, 57% of Millennials agree
- 50% report they are better at spotting phishing attempts after cybersecurity training
 - 94% report adopting at least one new cybersecurity behavior

KUBIKLE

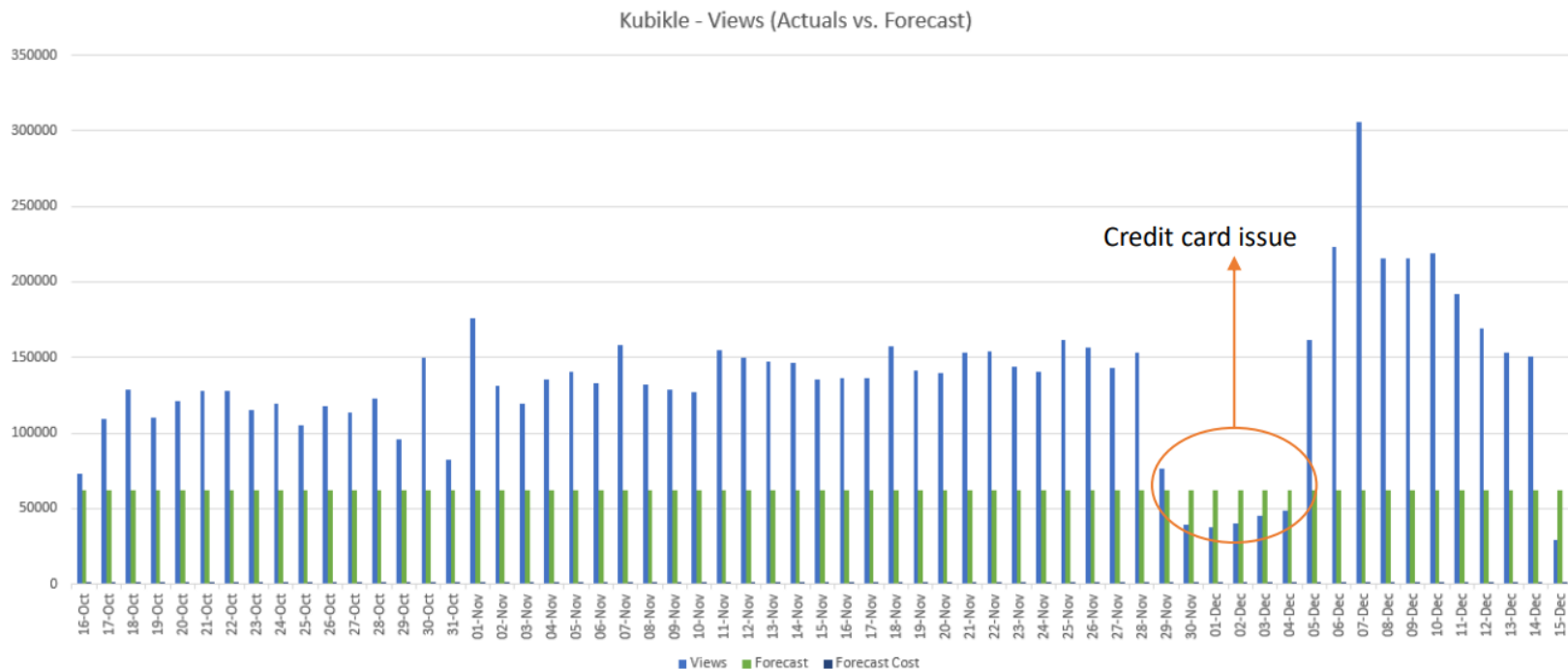
NATIONAL CYBERSECURITY ALLIANCE



<https://kubikleseries.com/>



NEXT TIME
ON
KUBIKLE



Total Campaign Targets	
Views	3,750,00
Budget	\$90,000
CPV	\$0.03

Performance	Actuals	Forecast	Index
Views	8,101,039	3,750,000	216
Cost	\$89,859	\$90,000	99
CPV	\$0.01	\$0.03	33

We ended at **~8.1MIL views**. We have more than doubled forecast at **215 index!**

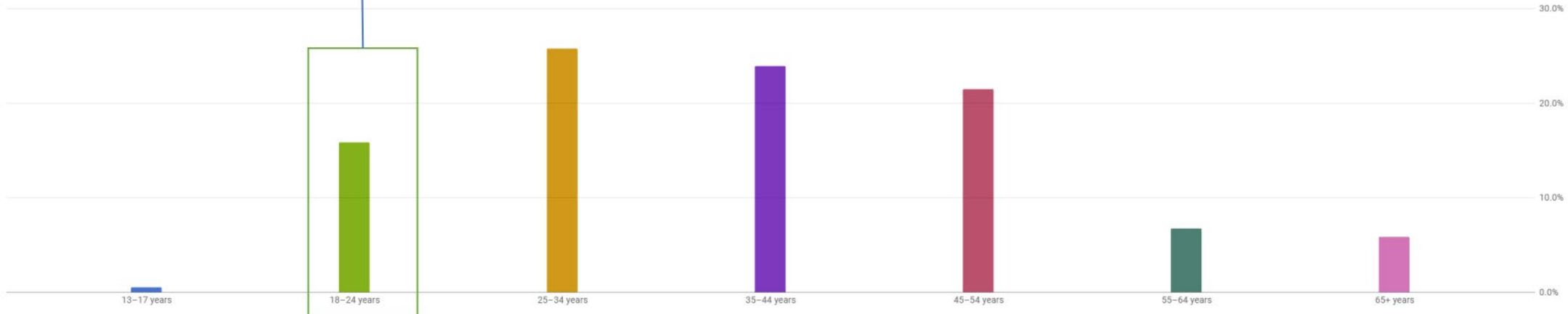
Cost-Per-View (CPV) at a third of forecast at **33 index!**

Campaign delivered **21M impressions** to a very targeted audience.

Other Metrics	
Impressions	21,113,041
Traffic Sessions	95696
Avg. View Time (US)	1:03s

Increase in 18–24-year-old engagement as per our last discussion. **15.8% up from 8%.**

Views by: Viewer age ▾



Viewer age ▾	Views	Average percentage viewed	Watch time (hours)
13–17 years	0.5%	89.4%	0.4%
18–24 years	15.8%	80.0%	15.2%
25–34 years	25.8%	73.4%	28.6%
35–44 years	23.9%	73.0%	25.0%
45–54 years	21.5%	71.9%	20.6%
55–64 years	6.7%	80.5%	5.7%
65+ years	5.8%	82.5%	4.6%

Audience segment

Audience segment	Campaign	Views
Cybersecurity Websites	Kubikle - Blended Audience - United States	749,319
Cybersecurity Websites	Kubikle - Blended Audience - Canada	599,015
Media & Entertainment › TV Lovers	Kubikle - Blended Audience - United States	575,787
Technology › Social Media Enthusiasts	Kubikle - Blended Audience - United States	392,466
Education	Kubikle - Blended Audience - United States	391,378
Software	Kubikle - Blended Audience - Canada	384,032
Media & Entertainment › Light TV Viewers	Kubikle - Blended Audience - United States	331,715
Software	Kubikle - Blended Audience - United States	325,949
Media & Entertainment › TV Lovers	Kubikle - Blended Audience - Canada	317,253
Technology › Technophiles	Kubikle - Blended Audience - United States	271,569
Education	Kubikle - Blended Audience - Canada	233,845
Media & Entertainment › Light TV Viewers	Kubikle - Blended Audience - Canada	190,685
Technology › Social Media Enthusiasts	Kubikle - Blended Audience - Canada	147,216
Technology › Technophiles	Kubikle - Blended Audience - Canada	141,561
Media & Entertainment › TV & Video Streaming Subscription Services	Kubikle - Blended Audience - United States	110,847
Media & Entertainment › TV & Video Streaming Subscription Services	Kubikle - Blended Audience - Canada	54,739
Business Services › Business Technology	Kubikle - Blended Audience - Canada	31,165
Business Services › Business Technology	Kubikle - Blended Audience - United States	25,413
Technology › Mobile Enthusiasts	Kubikle - Blended Audience - United States	25,192
Technology › Mobile Enthusiasts	Kubikle - Blended Audience - Canada	20,577
Media & Entertainment › DVDs & Videos	Kubikle - Blended Audience - United States	20,071
Media & Entertainment › DVDs & Videos	Kubikle - Blended Audience - Canada	12,575
Lifestyles & Hobbies › Business Professionals	Kubikle - Blended Audience - United States	11,681
People not in audiences	Nasdaq - Kubikle	8,952
Lifestyles & Hobbies › Business Professionals	Kubikle - Blended Audience - Canada	6,704
New Technology Products	Kubikle - Blended Audience - United States	1,858
Technology Industry	Kubikle - Blended Audience - United States	1,643
New Technology Products	Kubikle - Blended Audience - Canada	1,006
Technology Industry	Kubikle - Blended Audience - Canada	867
Media & Entertainment › Movie Lovers		701
Total		5,388,064

NATIONAL CYBERSECURITY ALLIANCE

Name	Impressions	Views
Information Technology	127,190 (19.64%)	73,619 (22.96%)
Marketing	90,526 (13.98%)	51,492 (16.06%)
Business Development	73,915 (11.41%)	41,363 (12.9%)
Engineering	71,922 (11.11%)	37,585 (11.72%)
Operations	56,282 (8.69%)	27,711 (8.64%)
Sales	53,452 (8.25%)	25,797 (8.04%)
Media and Communication	36,772 (5.68%)	20,049 (6.25%)
Program and Project Management	35,610 (5.5%)	18,842 (5.88%)
Arts and Design	29,879 (4.61%)	14,928 (4.65%)
Customer Success and Support	27,658 (4.27%)	14,179 (4.42%)
Consulting	22,147 (3.42%)	11,819 (3.69%)
Education	21,464 (3.31%)	9,991 (3.12%)
Community and Social Services	17,706 (2.73%)	8,507 (2.65%)
Product Management	14,121 (2.18%)	7,633 (2.38%)

YouTube views only. The data below excludes FB/IG, TW and LI.

New and Returning Viewers	Views ↓	Watch time (hours)
<input type="checkbox"/> Total	5,437,719	41,216.6
<input type="checkbox"/> New viewers	3,533,441 65.0%	28,381.1 68.9%
<input type="checkbox"/> Returning viewers	1,904,278 35.0%	12,835.5 31.1%

35% returning users, more than 1/3 of viewers are returning to view more content.

The content is engaging, and users are coming back for more.

Data point of interest.

TV as the #1 source for users viewing the content.

Device type	Views		Watch time (hours)	
<input type="checkbox"/> Total	5,437,719		41,216.6	
<input type="checkbox"/> Computer	247,331	4.6%	3,377.5	8.2%
<input type="checkbox"/> Mobile phone	334,426	6.2%	3,242.6	7.9%
<input type="checkbox"/> Tablet	69,983	1.3%	589.9	1.4%
<input type="checkbox"/> TV	4,785,613	88.0%	34,003.9	82.5%

88% of users, viewing the content from Smart TVs and/or also connecting their devices to one.

They are targeted by ads via desktop, mobile or tablet and the **TV ads are getting over 55% engagement rate. That is highly engaged behavior.**

This behavior indicate that users are coming back to view the episodes in the same manner as watching or binging on Netflix types of content. **83% of watch hours were done on TV.**



Vivian Cullipher • 3rd+
 Head of Content, Blancco Technology Group | Avid Writer | Compulsive Edi...
 Nicely done!

Like | Reply



Andrew Carson • 2nd
 Manager of Revenue Operations at Vendasta, Creator of The Conquer Loc...
[Dallas Bobryk Jason Coutu](#) lol

Like | Reply



Abdullah S. (He/Him) • 3rd+
 I love this show

Like | Reply



Joseph O. • 3rd+
 Cybersecurity Consultant, Intelligence Analyst, PCI Compliance Specialist
 Good watch

Like | Reply



Ben Alabaster - Cloud Adoption Strategist 2w ***
 (Rulebreaker/Rainmaker) • 2nd
 Cloud Adoption Strategist @ Resolutium Group | Simplifying Your Cloud J...
 This could become the next tech cult classic like hackers was in 1995 🤔

Like | Reply



@beckyhuss952 •
 I can't wait to see how this series plays out! Great way to promote Cyber Security!

REPLY 0 replies ▾ 👍 4 💬 ❤️ ⋮ 📺



@jehuty3 📺 • 2 weeks ago
 I have wanted this my entire adult life. Amazing.

REPLY 0 replies ▾ 👍 💬 ❤️ ⋮

Insights

Kubikle:

- Strong marketing + strong content = WIN.
- A well-planned campaign with focus on the right channel, the right audience, the right message outperforms ones that are too broad and less strategic.
- Testing and optimization is key.
- Insights can help build strategic priorities based on data for 2024.
- Build operating mechanisms to test out new initiatives based on learnings from this campaign.

KUBIKLE



**NATIONAL
CYBERSECURITY
ALLIANCE**

Stay safe online.



**NATIONAL
CYBERSECURITY
ALLIANCE**

Website

StaySafeOnline.org

Twitter

[@staysafeonline](https://twitter.com/staysafeonline)

Facebook

[/staysafeonline](https://facebook.com/staysafeonline)

LinkedIn

[/national-cyber-security-alliance](https://linkedin.com/company/national-cyber-security-alliance)

Email

info@staysafeonline.org

Q&A

Are There Any Questions?

Closing Remarks

Maureen Premo

Cyber Defense Education and Training (CDET)
Cybersecurity and Infrastructure Security Agency



Get Involved



Subscribe to the FISSEA Mailing List
FISSEAUUpdates@list.nist.gov



Volunteer for the Planning Committee
<https://www.nist.gov/itl/applied-cybersecurity/fissea/meet-fissea-planning-committee>



Serve on the Contest or Award Committees
Email fissea@list.nist.gov



Submit a presentation proposal for a future FISSEA Forum
<https://www.surveymonkey.com/r/fisseacallforpresentations>

SAVE THE DATE

**Federal Information Security Educators
(FISSEA) Conference**

May 14-15, 2024

Rockville, MD

#FISSEA | nist.gov/fissea

THANK YOU

We look forward to receiving your feedback via the post-event survey!

<https://www.surveymonkey.com/r/2024FISSEAWinterForum>

#FISSEA | nist.gov/fissea