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
FISSEAUpsdates@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
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
How does the FTC collect data about romance scams?
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?
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.

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 $10,000.4

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

<table>
<thead>
<tr>
<th>FRAUD LOSS REPORTS PER 100,000 POPULATION</th>
<th>MEDIAN REPORTED DOLLAR LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>20-29</td>
<td>$480</td>
</tr>
<tr>
<td>30-39</td>
<td>$460</td>
</tr>
<tr>
<td>40-49</td>
<td>$450</td>
</tr>
<tr>
<td>50-59</td>
<td>$470</td>
</tr>
<tr>
<td>60-69</td>
<td>$500</td>
</tr>
<tr>
<td>70-79</td>
<td>$803</td>
</tr>
<tr>
<td>80+</td>
<td>$1,450</td>
</tr>
</tbody>
</table>
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

- Cryptocurrency: 19%
- Bank Wire Transfer: 14%
- Gift Card: 24%
- App: 15%
- Other: 27%

2022: Payment methods for romance scams by dollar loss amount

- Cryptocurrency: 34%
- Bank Wire Transfer: 27%
- Gift Card: 7%
- App: 3%
- Other: 28%
What does the 2023 Data Book tell us about romance scams?
## Comparing Romance Scam Data

<table>
<thead>
<tr>
<th></th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Fraud Reports</strong></td>
<td>39,875</td>
<td>54,213</td>
<td>79,696</td>
<td>69,583</td>
<td>64,003</td>
</tr>
<tr>
<td><strong>Number of Reports with Dollar Losses</strong></td>
<td>28,399</td>
<td>35,900</td>
<td>48,495</td>
<td>42,115</td>
<td>39,680</td>
</tr>
<tr>
<td><strong>Median Dollar Losses</strong></td>
<td>$959</td>
<td>$1,300</td>
<td>$1,870</td>
<td>$2,000</td>
<td>$2,000</td>
</tr>
<tr>
<td><strong>Total Dollar Losses in Millions</strong></td>
<td>$483M</td>
<td>$722M</td>
<td>$1,294M</td>
<td>$1,339M</td>
<td>$1,140M</td>
</tr>
</tbody>
</table>
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
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
Report to help fight fraud!

Report Now →

Protect your community by reporting fraud, scams, and bad business practices.
Empower through education
## Multimedia Education

<table>
<thead>
<tr>
<th>Articles on consumer.ftc.gov</th>
<th>Videos on ftc.gov, YouTube, and other platforms</th>
<th>Articles and blog posts directed to consumers and businesspeople</th>
<th>Strategic partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social media content with sharable graphics</td>
<td>Articles for specific audiences (college students, military, older consumers)</td>
<td>Data spotlights for news media and others</td>
<td>“Carpe podium!”</td>
</tr>
</tbody>
</table>
I'm not a photographer, but I can picture me and you together 😘❤️❤️❤️
Bad Romance: Top “Love Game” lies told by romance scammers


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
<table>
<thead>
<tr>
<th></th>
<th>THE MESSAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LET FAMILY &amp; FRIENDS KNOW YOU’RE LOOKING ONLINE AND PAIR UP WITH A PEER TO COMPARE NOTES.</td>
</tr>
<tr>
<td>2</td>
<td>DO REVERSE IMAGE SEARCHES FOR PHOTOS AND LOOK FOR TEXT ON SEARCH ENGINES.</td>
</tr>
<tr>
<td>3</td>
<td>A REQUEST FOR MONEY IS A NO.</td>
</tr>
<tr>
<td>4</td>
<td>AN “INVESTMENT OFFER” IS A NO.</td>
</tr>
<tr>
<td>5</td>
<td>A REQUEST FOR EXPLICIT PHOTOS IS A NO.</td>
</tr>
<tr>
<td>6</td>
<td>HELP OTHERS BY REPORTING SCAMS TO THE FTC AND TO THE PLATFORMS.</td>
</tr>
</tbody>
</table>
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

Mission: Keeping South Dakota a Safe Place to Live, Work, Visit and Raise a Family
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 of 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

- 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)

<table>
<thead>
<tr>
<th>Advanced Search String Examples</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taylor Swift</td>
<td>The words “Taylor” AND “Swift”</td>
</tr>
<tr>
<td>“Taylor Swift”</td>
<td>The exact phrase “Taylor Swift”</td>
</tr>
<tr>
<td>“Taylor Swift” –music</td>
<td>The phrase “Taylor Swift” but NOT the word “music”</td>
</tr>
<tr>
<td>site:[URL]</td>
<td>Restrict search to one website or domain</td>
</tr>
</tbody>
</table>

Visit googleguide.com for more search techniques
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:
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...

<table>
<thead>
<tr>
<th>Username</th>
<th>Display Name</th>
<th>Birthday</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections</td>
<td>Images/Video</td>
<td>Phone Numbers</td>
</tr>
<tr>
<td>Email</td>
<td>Employment</td>
<td>Schools Attended</td>
</tr>
</tbody>
</table>

Visibility of accounts is often dependent on privacy settings

Facebook       Tik Tok
Twitter/X      Telegram
Instagram      CashApp
LinkedIn        Venmo
SnapChat       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

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>True People Search (truepeoplesearch.com)</td>
<td>Results include current and previous addresses, telephone numbers (including mobile), email addresses, relatives, spouses, and associates</td>
</tr>
<tr>
<td>Fast People Search (fastpeoplesearch.com)</td>
<td>Similar to True People Search, but may produce results if a person removed their information from True People Search</td>
</tr>
<tr>
<td>Nuwber (nuwber.com)</td>
<td>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</td>
</tr>
<tr>
<td>Family Tree Now (familytreenow.com)</td>
<td>Targeting for those conducting family history research and specializes in connecting people to their relatives</td>
</tr>
<tr>
<td>That’s Them (thatthem.com)</td>
<td>Displays information not publicly available elsewhere</td>
</tr>
<tr>
<td>Yasni (yasni.com)</td>
<td>Similar to other search engines, but also provides news articles, websites, and social networks related to the person</td>
</tr>
<tr>
<td>How Many of Me (howmanyofme.com)</td>
<td>Tells how many people exist with a specific name (may help determine the effectiveness of targeted searches)</td>
</tr>
</tbody>
</table>

*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
- Craigslist may post phone numbers

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

Can search for similar to phone searches

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

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
Vulnerability Searches

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

SIGN UP NOW
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

#FISSEA
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
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*

<table>
<thead>
<tr>
<th>Year</th>
<th>Complaints</th>
<th>Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>351,937</td>
<td>$2.7 Billion</td>
</tr>
<tr>
<td>2019</td>
<td>467,361</td>
<td>$3.5 Billion</td>
</tr>
<tr>
<td>2020</td>
<td>791,790</td>
<td>$4.2 Billion</td>
</tr>
<tr>
<td>2021</td>
<td>847,376</td>
<td>$6.9 Billion</td>
</tr>
<tr>
<td>2022</td>
<td>800,944</td>
<td>$10.3 Billion</td>
</tr>
</tbody>
</table>
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

- $0 - $5,000,000,000
- 0 - 55,000 complaints

Bar chart showing the increase in complaints and losses from 2014 to 2022.
IC3 Support

<table>
<thead>
<tr>
<th>Major Initiatives</th>
<th>Outreach / Presentation</th>
<th>Product Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware, Intrusions</td>
<td>Presentations</td>
<td>Public Service</td>
</tr>
<tr>
<td>Call Center Fraud</td>
<td>Webinars</td>
<td>Announcements</td>
</tr>
<tr>
<td>Crypto Investment</td>
<td>Podcasts</td>
<td>Cyber Security Advisories</td>
</tr>
<tr>
<td>Elder Fraud</td>
<td>Media Inquiries</td>
<td>Annual Reports</td>
</tr>
<tr>
<td>Kill Chain</td>
<td>Interviews</td>
<td></td>
</tr>
<tr>
<td>Complaint Aggregation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trending</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUPPORT</th>
<th>2023</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case Enhancements</td>
<td>310</td>
<td>190</td>
</tr>
<tr>
<td>Search Requests</td>
<td>103</td>
<td>284</td>
</tr>
<tr>
<td>Data Disseminations</td>
<td>3,825</td>
<td>4,754</td>
</tr>
<tr>
<td>Guardians</td>
<td>5,347</td>
<td>4,023</td>
</tr>
<tr>
<td>Cases Opened</td>
<td>398</td>
<td>441</td>
</tr>
</tbody>
</table>
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

$157.32 Million
$433.30 Million

RAT Activity by Year

Loss Frozen

<table>
<thead>
<tr>
<th>Year</th>
<th>Loss</th>
<th>Frozen</th>
</tr>
</thead>
<tbody>
<tr>
<td>CY18</td>
<td>$246,118,570</td>
<td>$170,745,546</td>
</tr>
<tr>
<td>CY19</td>
<td>$304,440,474</td>
<td>$385,415,592</td>
</tr>
<tr>
<td>CY20</td>
<td>$450,377,914</td>
<td>$435,421,931</td>
</tr>
<tr>
<td>CY21</td>
<td>$331,192,872</td>
<td>$337,192,872</td>
</tr>
<tr>
<td>CY22</td>
<td>$638,325,811</td>
<td>$590,323,129</td>
</tr>
<tr>
<td>CY23</td>
<td>$590,623,479</td>
<td>$246,118,570</td>
</tr>
</tbody>
</table>
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.
Our Partners

- 56 FBI Field Offices and 63 LEGATS
- Foreign Law Enforcement
  - GAEN, GASA, International Threat Group (NFIB, RCMP, CoLP, CAFC)
- Government Agencies
- 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
What’s New, and What’s Ahead, at the National Cybersecurity Alliance

Lisa Plaggemier
Executive Director, National Cybersecurity Alliance

February 14, 2024
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.
2023 Results

- 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 1.8 billion 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 and complex.
- Use a mix of uppercase letters, numbers, and symbols.
- Use a different password for each account.

**AND A PASSWORD MANAGER**
- Password managers can:
  - Store all your passwords securely.
  - Generate strong passwords for you.
  - Automatically fill in your login information.

**TURN ON MULTIFACTOR AUTHENTICATION**
It provides extra security by confirming your identity when logging into accounts, like when setting up a new account.

**RECOGNIZE AND REPORT PHISHING**
Common signs of a phish include:
- Changes in your email address.
- Requests for personal or financial info.
- Poorly written or suspicious links.
- Changes in email addresses or links.

**UPDATE YOUR SOFTWARE**
Software updates ensure your devices are protected against the latest threats. Turn on automatic updates or set reminders for security settings.

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

#SecureOurWorld this CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY ALLIANCE
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
2021

Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2021

2022

Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2022

2023

Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2023
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
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
Kubikle

Cybercrime is an scourge that ruins lives. But guess who makes it? Other people. Bad ones, with lives of their own. These are their stories. At least their stories in the office Welcome to Kubikle

Next time on Kubikle
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.
Increase in 18–24-year-old engagement as per our last discussion. 15.8% up from 8%.
<table>
<thead>
<tr>
<th>Audience segment</th>
<th>Campaign</th>
<th>Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Websites</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>749,319</td>
</tr>
<tr>
<td>Cybersecurity Websites</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>540,015</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV Lovers</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>575,787</td>
</tr>
<tr>
<td>Technology - Social Media Enthusiasts</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>352,466</td>
</tr>
<tr>
<td>Education</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>391,378</td>
</tr>
<tr>
<td>Software</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>384,032</td>
</tr>
<tr>
<td>Media &amp; Entertainment - Light TV Viewers</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>331,715</td>
</tr>
<tr>
<td>Software</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>315,649</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV Lovers</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>317,233</td>
</tr>
<tr>
<td>Education</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>233,845</td>
</tr>
<tr>
<td>Media &amp; Entertainment - Light TV Viewers</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>190,685</td>
</tr>
<tr>
<td>Technology - Social Media Enthusiasts</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>147,216</td>
</tr>
<tr>
<td>Technology - Technologies</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>141,561</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV &amp; Video Streaming Subscription Services</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>110,847</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV &amp; Video Streaming Subscription Services</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>54,739</td>
</tr>
<tr>
<td>Business Services - Business Technology</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>25,413</td>
</tr>
<tr>
<td>Technology - Mobile Enthusiasts</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>28,192</td>
</tr>
<tr>
<td>Technology</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>20,577</td>
</tr>
<tr>
<td>Mobile Enthusiasts</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>20,071</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV &amp; Video Streaming Subscription Services</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>12,975</td>
</tr>
<tr>
<td>Media &amp; Entertainment - TV &amp; Video Streaming Subscription Services</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>11,681</td>
</tr>
<tr>
<td>Lifestyle &amp; Politics</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>8,922</td>
</tr>
<tr>
<td>People not in audiences</td>
<td>Kubrick - United States</td>
<td>8,922</td>
</tr>
<tr>
<td>Lifestyle &amp; Politics - Business Professionals</td>
<td>Kubrick - United States</td>
<td>6,704</td>
</tr>
<tr>
<td>New Technology Products</td>
<td>Kubrick - United States</td>
<td>1,858</td>
</tr>
<tr>
<td>Technology Industry</td>
<td>Kubrick - B2B Audiences - United States</td>
<td>1,643</td>
</tr>
<tr>
<td>New Technology Products</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>1,006</td>
</tr>
<tr>
<td>Technology Industry</td>
<td>Kubrick - B2B Audiences - Canada</td>
<td>967</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Impressions (% of Total)</th>
<th>Views (% of Total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology</td>
<td>127,190 (19.64%)</td>
<td>73,619 (22.96%)</td>
</tr>
<tr>
<td>Marketing</td>
<td>90,526 (13.98%)</td>
<td>51,492 (16.06%)</td>
</tr>
<tr>
<td>Business Development</td>
<td>73,915 (11.41%)</td>
<td>41,363 (12.9%)</td>
</tr>
<tr>
<td>Engineering</td>
<td>71,922 (11.11%)</td>
<td>37,585 (11.72%)</td>
</tr>
<tr>
<td>Operations</td>
<td>56,282 (8.69%)</td>
<td>27,711 (8.64%)</td>
</tr>
<tr>
<td>Sales</td>
<td>53,452 (8.25%)</td>
<td>25,797 (8.04%)</td>
</tr>
<tr>
<td>Media and Communication</td>
<td>36,772 (5.63%)</td>
<td>20,049 (6.25%)</td>
</tr>
<tr>
<td>Program and Project Management</td>
<td>35,610 (5.5%)</td>
<td>10,862 (3.5%)</td>
</tr>
<tr>
<td>Arts and Design</td>
<td>29,879 (4.61%)</td>
<td>14,920 (4.84%)</td>
</tr>
<tr>
<td>Customer Success and Support</td>
<td>27,658 (4.27%)</td>
<td>14,179 (4.42%)</td>
</tr>
<tr>
<td>Consulting</td>
<td>22,147 (3.42%)</td>
<td>11,819 (3.69%)</td>
</tr>
<tr>
<td>Education</td>
<td>21,464 (3.31%)</td>
<td>9,991 (3.12%)</td>
</tr>
<tr>
<td>Community and Social Services</td>
<td>17,706 (2.73%)</td>
<td>6,507 (2.05%)</td>
</tr>
<tr>
<td>Product Management</td>
<td>14,121 (2.18%)</td>
<td>7,633 (2.38%)</td>
</tr>
</tbody>
</table>
**YouTube** views only. The data below excludes FB/IG, TW and LI.

<table>
<thead>
<tr>
<th></th>
<th>Views</th>
<th>Watch time (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
<td>5,437,719</td>
<td>41,216.6</td>
</tr>
<tr>
<td><strong>New viewers</strong></td>
<td>3,533,441</td>
<td>28,381.1</td>
</tr>
<tr>
<td><strong>Returning viewers</strong></td>
<td>1,904,278</td>
<td>12,835.5</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Device type</th>
<th>Views</th>
<th>Watch time (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>5,437,719</td>
<td>41,216.6</td>
</tr>
<tr>
<td>Computer</td>
<td>247,331</td>
<td>3,377.5</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>334,426</td>
<td>3,242.6</td>
</tr>
<tr>
<td>Tablet</td>
<td>69,983</td>
<td>580.9</td>
</tr>
<tr>
<td>TV</td>
<td>4,785,613</td>
<td>34,003.9</td>
</tr>
</tbody>
</table>

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, Blanco Technology Group | Avid Writer | Compulsive Edi...
Nicely done!

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

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

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

Ben Alabaster - Cloud Adoption Strategist
(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

@beckyhusss952 •
I can't wait to see how this series plays out! Great way to promote Cyber Security!

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