Secure Our World & Cybersecurity Awareness Month

Bob Nadeau, Partnerships Branch Chief
Laura Edwards, Section Chief, Awareness and Outreach

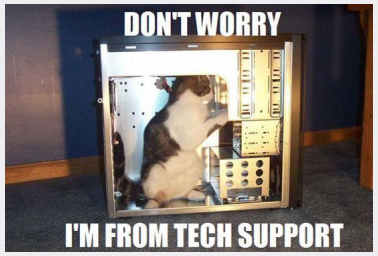
Small Business Cyber Threats

Your business is digitally connected—to employees, vendors & customers. Your systems store sensitive information. No business is too small to be an online crime target. Malicious actors have tools to conduct large-scale fraud schemes, hold our money & data for ransom, endanger our national security.

Top 3 Costliest Internet Crimes in 2023

$4.57 billion in '23: 38% annual increase

21,489 complaints $2.9B in reported losses



Tech Support Scams

SMALL & MEDIUM BUSINESS OWNERS

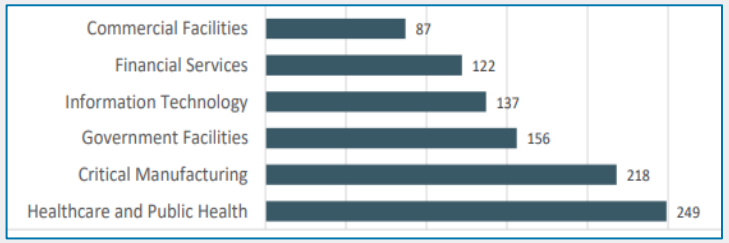
99.9% of all U.S. businesses & employing nearly half of the private workforce, a cyber threat to our small businesses is a threat to our overall economy.

Business E-mail Compromise Scams

Subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

60% of small companies that suffer a cyber attack are out of business within six months.
(NCA)

Ransomware Attacks



2023 FBI Internet Crime Center Report (IC3)

SECURE OUR WORLD

What to Do

Types of business email compromise scams

Email is the starting point for 91 percent of cyberattacks.[2] Learn about the most common types of compromised email.

Data theft

Sometimes scammers start by targeting the HR department and stealing company information like someone's schedule or personal phone number. Then it's easier to carry out one of the other BEC scams and make it seem more believable.

CEO fraud

Scammers either spoof or hack into a CEO's email account, then email employees instructions to make a purchase or send money via wire transfer. The scammer might even ask an employee to purchase gift cards, then request photos of serial numbers.

Account compromise

Scammers use phishing or malware to get access to a finance employee's email account, such as an accounts receivable manager. Then the scammer emails the company's suppliers fake invoices that request payment to a fraudulent bank account.

False invoice scheme

Posing as a legitimate vendor your company works with, the scammer emails a fake bill—often closely resembling a real one. The account number might only be one digit off. Or they may ask you to pay a different bank, claiming your bank is being audited.

Lawyer impersonation

In this scam, attackers gain unauthorized access to an email account at a law firm. Then they email clients an invoice or link to pay online. The email address is legitimate, but the bank account isn't.

SECURE OUR WORLD

What to Do

2023 CRIME TYPES continued

By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

Descriptors**			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

General

You can report various forms of cybercrime to the following agencies:
CISA: cisa.gov/report **FBI:** ic3.gov

Hacked Account

Report your hacked account to the respective platform's support team. Find direct links to popular platforms here: staysafeonline.org/online-safety-privacy-basics/hacked-accounts/

Ransomware

Contact local law enforcement, including:

- **CISA:** cisa.gov/forms/report
- **FBI:** fbi.gov/contact-us/field-offices
- **U.S. Secret Service:** secretservice.gov/contact/field-offices

Identity Theft

Report identity theft to:
FTC: identitytheft.gov

You can also report to:
ID Theft Resource Center:
idtheftcenter.org or call 888.400.5530

Tax-Related Cybercrime

Report tax-related phishing messages or calls to the IRS via email: phishing@irs.gov

More about tax fraud:
irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity

Credit Card Fraud

Report credit card fraud to your credit card company or use the FTC's fraud, scam and bad business reporting tool: reportfraud.ftc.gov

Elder Fraud

If you or someone you know has been the victim of elder fraud, contact the U.S. Department of Justice's National Elder Fraud Hotline 833.372.8311

Social Security Fraud

Notify the Social Security Administration if you suspect any fraudulent activities related to your social security number: ssa.gov/fraud or call: 800.269.0271

Business Email Compromise

Report spoofed business-related emails or scams to your organization's IT department and the FBI at: ic3.gov

Online Stalking

If you believe you are being stalked or are a victim of stalkerware, call, chat or text the National Domestic Violence Hotline:
Call: 800.799.7233
Chat: thehotline.org
Text: "Start" to 88788

Cyberbullying

Report cyberbullying to the platform where the bullying occurred or to your child's school.

Report to local law enforcement if there have been threats of violence, stalking or hate crimes at: stopbullying.gov/cyberbullying/how-to-report

Phishing

Report suspicious emails to your email platform and then delete it. Or you can also report to:

- **FTC:** reportfraud.ftc.gov
- **Anti-Phishing Working Group:** reportphishing@apwg.org
- **AARP Fraud Watch Network:** 877.908.3360

1. Establish a culture of cybersecurity
2. Select and support a "Security Program Manager."
3. Review and approve the Incident Response Plan (IRP)
4. Talk with your CISA regional office for resources
5. Talk with employees, vendors, customers & implement cyber safe actions
6. Demand Secure By Design principles from your software provider

SECURE OUR WORLD

2023 FBI Internet Crime Center Report (IC3) &
CISA Secure Our World

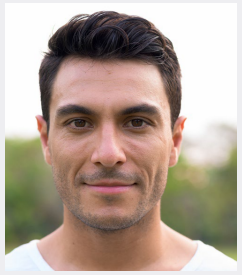
Launch 9/26/2023

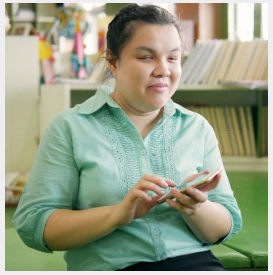
cisa.gov/SecureOurWorld

Audience & Messages

We are primarily targeting:

Adults—ages 26-57



Gen X and Millennials

SMB owners

SMALL & MEDIUM BUSINESS OWNERS

With messaging centralized around the four behaviors:

- Use MFA
- Manage passwords
- Recognize phishing
- Update software

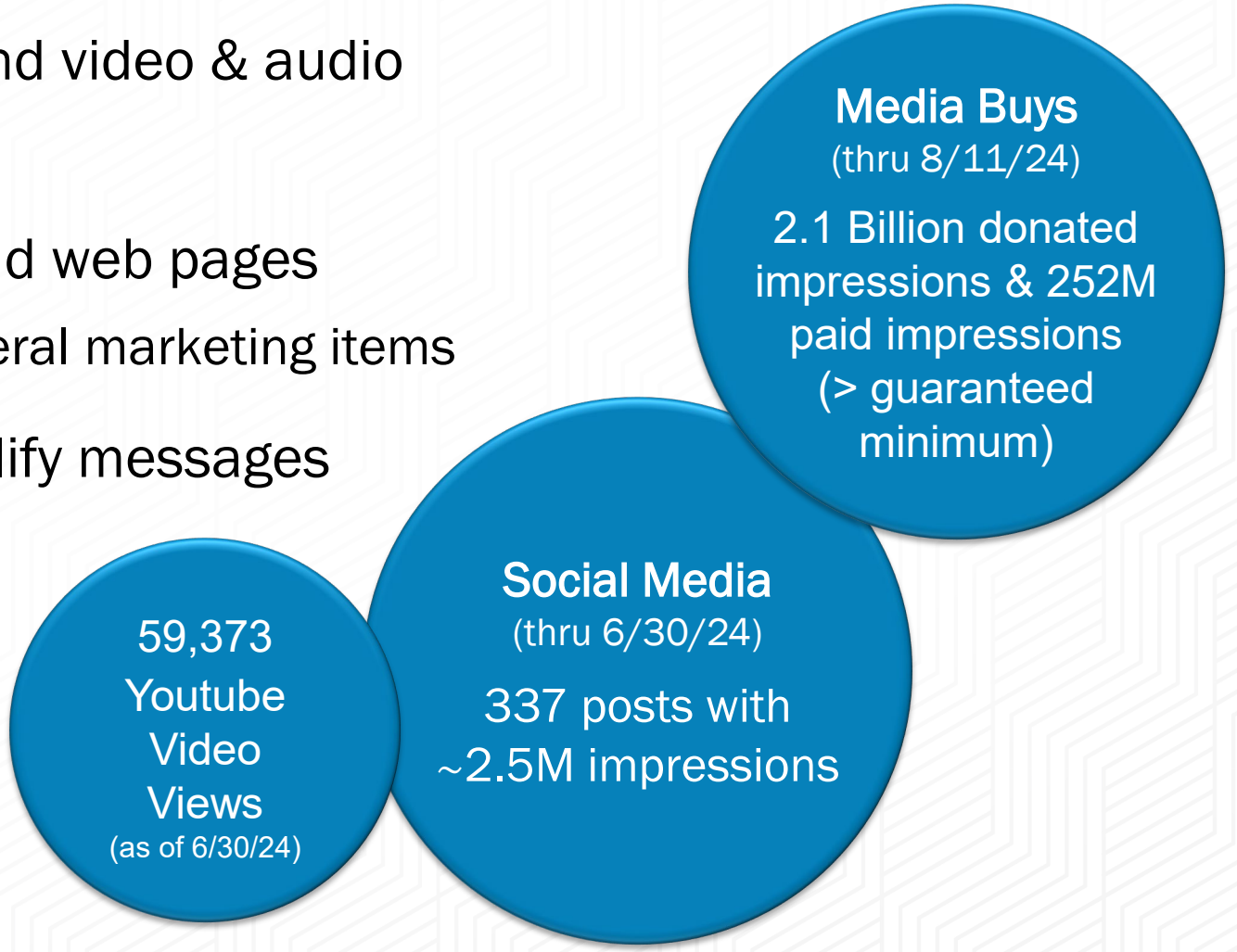
First PSA

Second PSA

SECURE OUR WORLD

Year 1 Wrap Up

- Secure Our World Year 1 had significant impact and reach with our target market
- Produced PSA #1 in 60/30/15 second video & audio
  - English & Spanish versions
- Developed tip sheets, animations, and web pages
  - Multiple ads, social media posts, several marketing items
- Priority on more partnerships to amplify messages
- PSA #2 launch in May
- Upcoming release of 4 new videos



SECURE OUR WORLD

Cybersecurity Awareness Month 2024

- **Theme**: Secure Our World
- **Key Messaging**:
  - Use strong passwords and password managers
  - Turn on MFA
  - Recognize and report phishing
  - Update software
- **Target Audiences**:
  - General public
  - Cybersecurity professionals, particularly those in security training and awareness
  - Small- and medium-sized business owners
  - Parents and teachers
  - The disabled community and their caretakers

- **Official Hashtags**: #CybersecurityAwarenessMonth and #Secure Our World
- **Free Resources:** The Cybersecurity Awareness Month 2024 Toolkit is available to download at cisa.gov/cybersecurity-awareness-month.
- **Save the Date**: Join CISA and NCA on October 2nd at 2pm ET as we kick-off the 21st Cybersecurity Awareness Month. To register visit staysafeonline.org.

SECURE OUR WORLD

To learn more, visit
cisa.gov/SecureOurWorld &
cisa.gov/cybersecurity-awareness-month

Contact us at
AwarenessCampaigns@mail.cisa.dhs.gov