

FBI John

The Voice of Cyber & Security

SPEAKER | AUTHOR | CONSULTANT

Cybersecurity

Active Shooter



March 19, 2024

John Iannarelli, ESQ, CSP®

P.O. Box 4524, Scottsdale, Arizona 85261

866-324-5646

John@FBIJohn.com

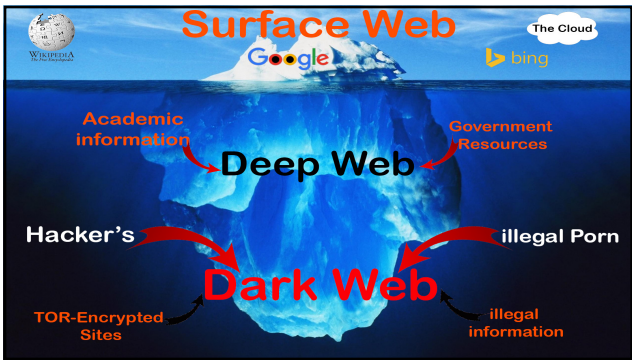
www.FBIJohn.com



1

Street Price Stolen Internet Items		
Item	Percentage	Price
Bank Account Number	23%	\$10 - \$1,000
Credit Card Number	13%	\$0.40 - \$2.00
Full Identity	9%	\$1 - \$15
Online Auction Account	7%	\$1 - \$8
Email Addresses	5%	\$0.83/MB - \$10/MB
Email Passwords	5%	\$4 - \$30

2



3

Cyber Threats to Transportation

“Transit Seeing More Cyber Threats”

- August 2023 news article

180% increase in ransomware attacks

Increase entry points for attacks

- onboard Wi-Fi
- autonomous vehicles
- contactless tickets
- vehicle location technology

FBIJohn

[illegible]

Cyber Threats to Transportation

“Advances in technology increases cyber concerns”

- Mineta Transportation Institute

IT not enough

- CISO
- Written policies
- Enterprise risk management strategy

FBI John

[illegible]

Cyber Threats to Transportation

Vendors

- Transportation must understand risks
 - current/future vulnerabilities
 - hardware/software
 - criminals taking control
- Vendor policies must align w/ cyber needs
 - Procurement should articulate

FBI John

[illegible]

Cyber Terrorism



Hactivist



Opportunist



Insider Threat



Third Party Threat



Nation States



Terrorists

FBIJohn

7

How Vulnerable Is Your Computer?

First time computer
connected to Internet,
how long before it is
compromised?

5 MINUTES

FBIJohn

8

Cost of Data Breach

Last year worst on record

15.1 billion records compromised

1,580 reported breaches

ID Theft Resource Center

U.S. Average - \$8 million

\$242 per record

Ponemon

Capital One Breach

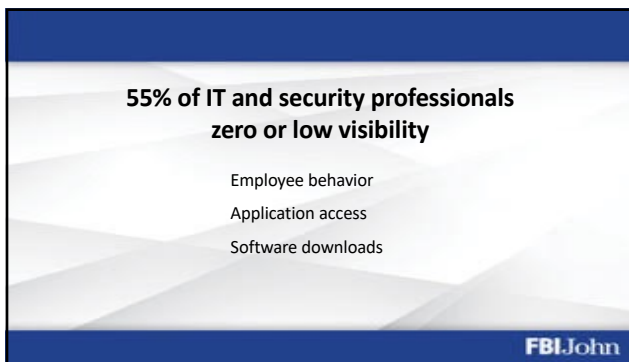
100 Million Records

FBIJohn

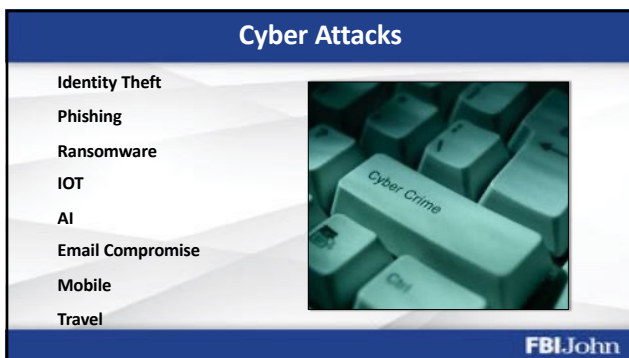
9



10



11



12

Identity Theft

Identity Theft Annual Loss \$52 Billion

By Rhyen Security Watch

According to the Federal Bureau of Investigation (FBI) estimates it is just as much as 60 million people in America that they are victims of some form of Identity Theft, resulting in an estimated "loss" exceeding \$50 Billion.

The recent report of the Federal Bureau of Investigation <https://www.fbi.gov/newsroom/press-releases/2017/07/2017-identity-theft-losses-exceed-50-billion> indicates that the federal government will spend \$100 Billion over the next ten years to fight against crime.

The use of personally identifiable information, such as an individual's name, identity number, name, and date of birth can result in various forms, including Identity Theft. Identity Theft is a serious crime that can result in millions of dollars of loss and can result in serious harm and information is used without authorization to commit fraud or other crimes. Identity Theft has been made gathering personally identifiable information in the public and private sector, also/when possible.

1 in 4 victims

FBI John

[illegible]

Crypto

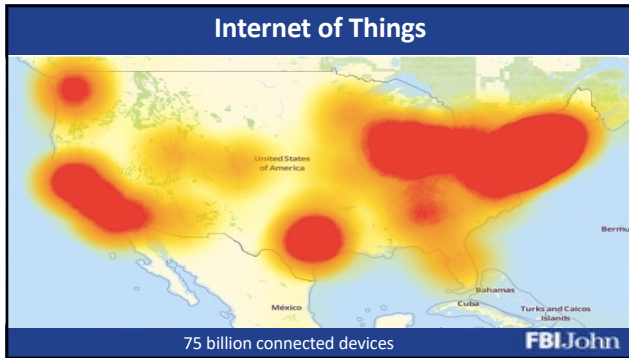
Locker

Spearware

Leakware

\$20 Billion in damages

FBI John



16

Artificial Intelligence

3 Types

- Narrow - chess
- General – human mind
- Super Intelligence – smarter than human brain

FBIJohn

The slide is titled 'Artificial Intelligence' and lists three types: Narrow (chess), General (human mind), and Super Intelligence (smarter than human brain). The FBIJohn logo is in the bottom right corner.

17

Business Email Compromise

FBI report for last year:

- 22,000 U.S. businesses victim
- \$2.4 billion
- 270% increase from prior year

Example: Spoofed Email

- John@FBIJohn.com
- John@FBIJohn.com

FBIJohn

The slide is titled 'Business Email Compromise' and provides statistics from an FBI report for the last year: 22,000 U.S. businesses victim, \$2.4 billion in losses, and a 270% increase from the prior year. It also includes an example of a spoofed email with two identical entries: John@FBIJohn.com. The FBIJohn logo is in the bottom right corner.

18

Mobile Devices

The Risks

- Contact list
- Infect desktop w/ malware
- Smishing
- Vishing
- Juice Jacking

FBIJohn

19

Travel Security

DURING

- Use RFID credit card holder
- Don't leave devices unattended
- Use privacy screen
- Avoid public Wi-Fi
- Hotel safe

AFTER

- Update devices
- Change passwords
- Backup data
- Remove apps
- Check credit card statements

FBIJohn

20

Cyber Safety

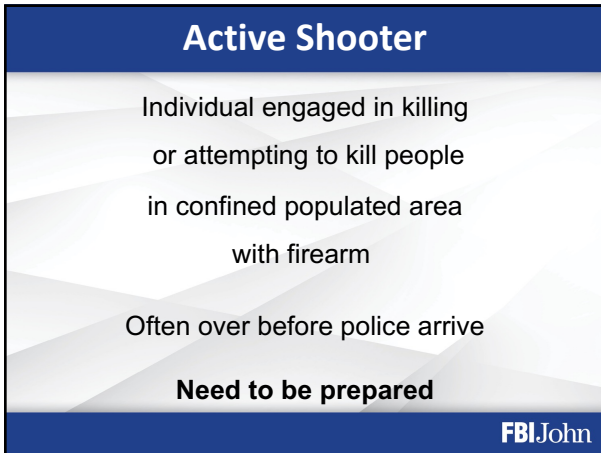
- Strong Passwords – Password Keeper
- 2 Factor Authentication
- Backup
- Cyber Insurance
- Fully Managed Recovery
- Outside Monitoring

FBIJohn

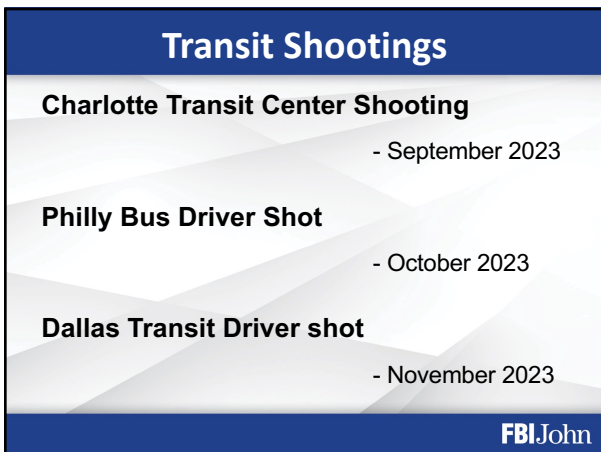
21



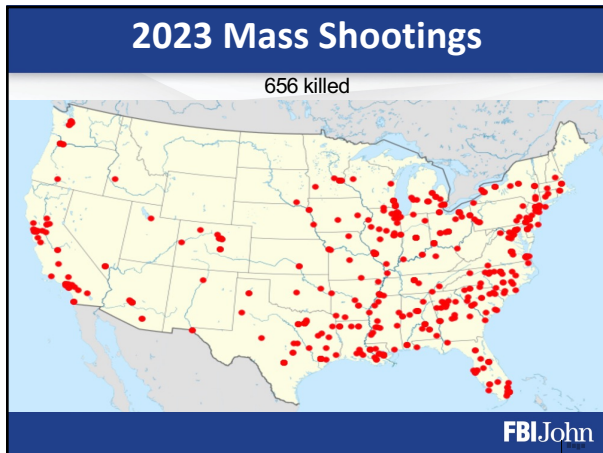
1



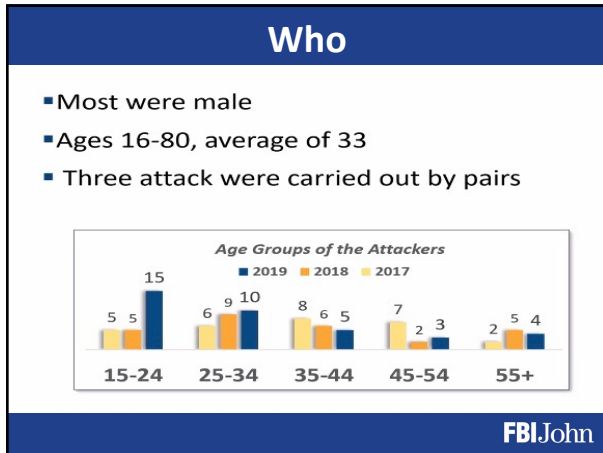
2



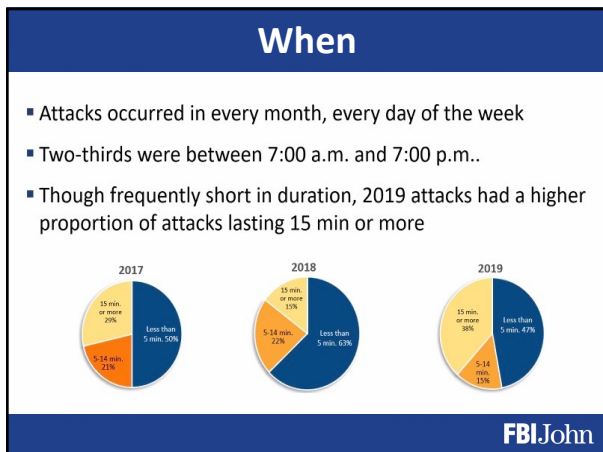
3



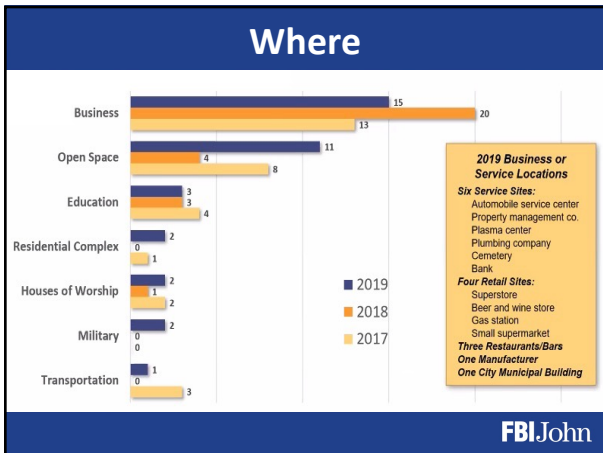
4



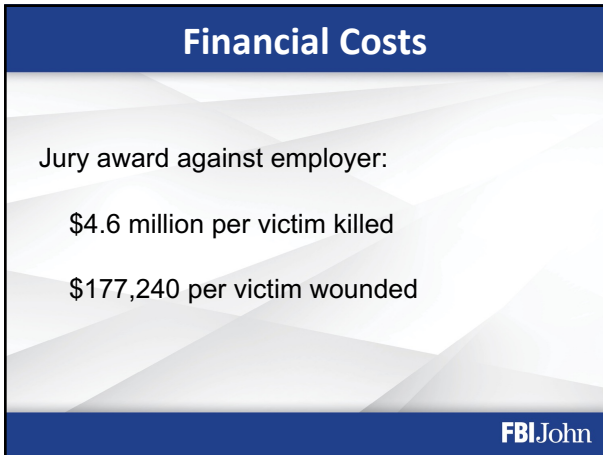
5



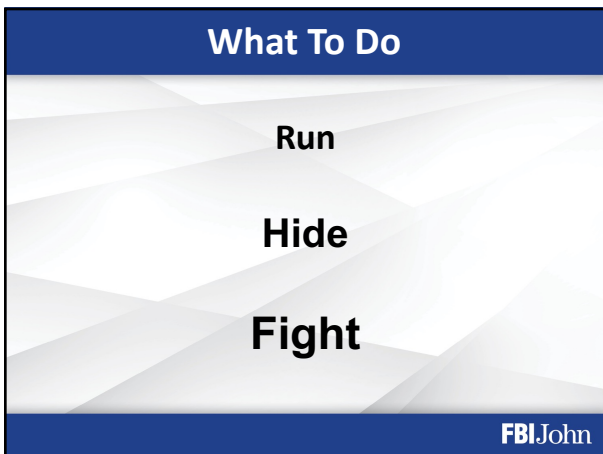
6



7



8



9

When Police Arrive

Remain calm

Raise hands

Follow orders

Do not stop and ask for help

Provide:

- location of shooter
- number of shooters
- physical description
- weapons
- number of victims

FBIJohn

10

Empowerment

Physical security assessment

Note two exits

- Know indicators
- Train personnel
- **Recognize sound of gunshots**

FBIJohn

11

Emergency Info

Emergency Services: 9-1-1

Local Emergency Information Line: _____

Local Police Department: _____

Local Fire Department: _____

Local Hospital: _____

Local FBI Field Office: _____

Facility Security: _____

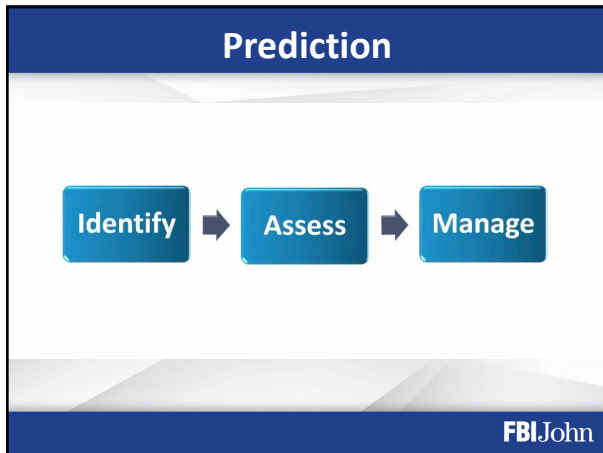
Facility Address: _____

Floor: _____ Suite/Room: _____

Office #: _____ Ext. _____

FBIJohn

12



13



14




15

Technical Assistance

Emergency Communication

- public address
- mass notification
- digital messaging

Two-Way Communication



Single Touch Launch



Quickly Capture Safe Status

FBI.John

16



17

Closing Thoughts

Average Shooting lasts 5 minutes or less

Average police response 8 minutes

Over before police arrive

Know how to protect yourself

FBI.John

18

FBI John

SPEAKER | AUTHOR | CONSULTANT

The Voice of Cyber & Security



John Iannarelli served 20 years as an FBI Special Agent. His investigative work included the Oklahoma City Bombing, 9/11 attack, shooting of Congresswoman Gabrielle Giffords, the Sony hack, and more. John also served as the FBI's national spokesperson and worked as the NFL Security Representative. He is the recipient of the FBI Director's Distinguished Service Award and holds an Honorary Doctorate of Computer Science.

Now, John is a national news on-air consultant and sought-after National Speakers Association Certified Speaking Professional®. He is an attorney and the author of 5 books, including Disorderly Conduct – Humorous stories from life inside the FBI and How to Spot A Terrorist Before It's Too Late.

John has presented to Fortune 500 companies, the UN, and the Vatican. As a speaker, consultant, and author, ***John's mission is to help people stay safe in both the cyber and physical worlds.***

SPEAKING TOPICS

- Cybersecurity for Business
- Active Shooter Prevention and Response
- Leadership & Ethics

SPEAKING ENGAGEMENTS

- Keynotes Conferences Breakouts
- Virtual Presentations

KEY AUDIENCE TAKEAWAYS

- Understanding their vulnerabilities
- Learning how to recognize threats
- Knowing how to avoid becoming a victim and what to do if they become one

WATCH KEYNOTE PRESENTATION EXAMPLE BY FBI JOHN:



AS FEATURED ON



Forbes

THE WALL STREET JOURNAL.



USA TODAY

The New York Times

Bloomberg



FBI John.com



John@FBIJohn.com



866-FBI-John (866-324-5646)



The Voice of Cyber & Security

Speaker | Author | Consultant

John Iannarelli, Esq.
FBI Special Agent (Ret.)

🌐 **FBIJohn.com**

🐦 **@FBIJohn**

✉ **john@FBIJohn.com**

☎ **866-324-5646 | 866-FBI-John**

IDENTITY THEFT MONITORING

<https://SmartIdentity-fbijohn.merchantsinfo.com>

The site has offers 2 packages:

Package 1:

- 3G Fully Managed Recovery
- 1 Bureau Credit Monitoring
- Score Tracker
- Dark Web Monitoring
- Lost Document Replacement
- Credential Vault
- VPN – 3 devices

Package 2:

- 3G Fully Managed Recovery
- 3 Bureau Credit Monitoring
- Score Tracker
- ID Protection Bundle which consists of:
 - Dark Web Monitoring
 - Criminal Records Monitoring
 - SSN Monitoring
 - Name and Address Monitoring
- Lost Document Replacement
- Credential Vault
- VPN – 3 devices

DIGITAL PROTECTION MONITORING

<https://blackcloak.io>

Home - Weekly penetration testing and regular scans of your home network to detect compromised networks, weak cybersecurity, BotNets and other security issues, and prevent decisions children and family make online from resulting in compromise.





Mobile Devices - Monitor, detect, prevent, and block threats to your devices, such as malware and ransomware, that occur when someone accidentally click on a malicious link or opens malware from a phishing scam. Black Cloak's U.S. based security operations team remediates any quantifiable attacks that are detected.

ACTIVE ASSAILANT/SHOOTER

TECHNICAL SOLUTIONS

CASTATUS

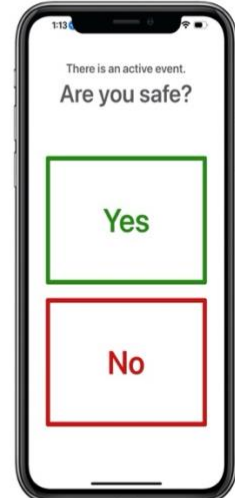
<https://castatus.com/FBIJohn>

	Sarah Garcia	3 minutes ago	Bobby is still in there.
	Jack Jones	2 minutes ago	I saw flames coming out of the third floor.
	Eric James	about a minute ago	Elevator is not working, but people are using the stairs.
	Bob Smith	2 minutes ago	No, I haven't seen him.

Two-Way Communication



Single Touch
Launch



Quickly Capture
Safe Status

PRESENTATIONS

Cybersecurity

Why rob a bank when a criminal can steal far more while sitting in front of a computer? Beyond just money, the sensitive personal information of both employees and customers is attractive to the cyber thief. Additionally, remote work technologies like mobile devices have provided cybercriminals with new ways to disrupt business and steal what is yours. Every year millions become victims because they did not know how to protect themselves from cybercrime. By using examples of actual FBI cases, John reveals the ways you are vulnerable to a cyberattack, the current threats and how you can protect yourself.

Key takeaways:

- (1) Understand the latest cyber vulnerabilities.
- (2) Learn how to avoid becoming a victim.
- (3) Understand what to do if a cybercriminal does attack.

This presentation references Iannarelli's books *Disorderly Conduct* and *WTF: Why Teens Fail and What to Fix*, a guide to keeping safe on the internet and elsewhere.

Active Shooter Prevention and Preparedness

Hear the behind the scenes stories of many of the most recent mass shootings, how they happened, how they were planned, how law enforcement responded, and important clues that could potentially prevent future such tragedies. The presenter has responded to two school shootings and the shooting of Congresswoman Gabriel Giffords. John was also present in Las Vegas when the Mandalay Bay shooting occurred, where he then served as an on-air Law Enforcement consultant for the Fox News Channel, CNN NBC, and other national news programs, giving him inside access to the crime scene. This access, in addition his having responded to numerous other critical incidents as an FBI Agent and police officer, gives John unique knowledge insights that he shares with his audience.

Key Takeaways:

- (1) Being able to protect yourself and family should an active shooter situation occur.
- (2) Warning indicators to identify those who plan such attacks.
- (3) Key steps to take during an attack to stay safe, and what to do afterward to recover.

This presentation references Iannarelli's book *How to Spot a Terrorist; Before It Is Too Late*.

Leadership & Ethics Lessons Learned Through the FBI

Through story telling of FBI investigations, the audience will hear the lessons learned that are applicable to today's business world. John shares inside stories from behind the scenes not otherwise shared with the public, detailing high profile cases, such as 9/11, the shooting of Congresswoman Gabby Giffords, the Enron collapse, and more. Likewise, the audience will also hear valuable insights from other

investigations never before discussed outside of the FBI. As is often the case with law enforcement situations, the audience will find this valuable presentation both informative and frequently entertaining.

Key Takeaways:

- (1) Identify the skills necessary for leadership and ethics.
- (2) Learn to how to lead by example.
- (3) Leverage and utilize the skills your employees so that everyone succeeds.

This presentation references John's just released new book, Disorderly Conduct.

How to Spot a Terrorist Before It's Too Late

How many times have we heard the phrase "If you see something, say something." However, when has anyone ever told us what we should be paying attention to see. John answers this question, sharing how you can help prevent the next terrorist attack by noticing a few simple indicators to identify someone who might be planning an act of terrorism. The audience will hear behind the scenes FBI stories, not otherwise discussed with the public, detailing some of the most infamous acts of terrorism that have impacted the United States, to include the Oklahoma City Bombing, 9/11 and the Orlando Airport shooting, just to name a few. Likewise, the audience will also learn of attempted attacks that were prevented that the public never knew happened.

Key Takeaways:

- (1) Be able to protect yourself and your family if you are amid a terrorist or active shooter event.
- (2) Being able to spot a terrorism planning event before it is too late.
- (3) Know how to respond to keep yourself safe.

This presentation references FBI John's book How to Spot a Terrorist; Before It Is Too Late.

Bank Robbery Prevention and Response

In the words of bank robber William Sutton when asked why he robs banks; "Because that where the money is." Banks have always been an attractive target for criminals and will continue to be for the foreseeable future. John shares the ways banks are commonly robbed, steps you can take to prevent and deter robberies, and how to best assist the responding law enforcement.

Key Takeaways:

- (1) Understand the various methods by which institutions are robbed.
- (2) Learn the warning signs that a robbery is imminent.
- (3) Know what to do both before and after a robbery to mitigate the risk.

This presentation references FBI John's books Disorderly Conduct and How to Spot a Terrorist; Before It Is Too Late.

