hfma
massachusetts-rhode island chapter

26th Annual Revenue Cycle Conference
From Kickoff to Cashflow: Building a Winning Revenue Cycle

COMMONWEALTH FUSION CENTER

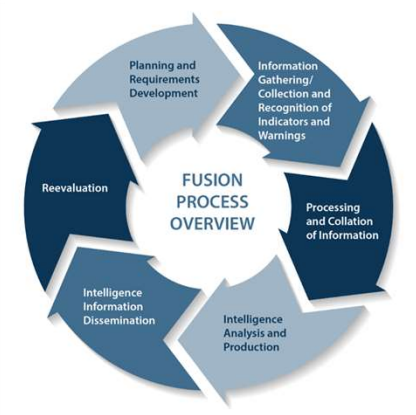
MASSACHUSETTS CYBERSECURITY PROGRAM

Lieutenant Edward Keefe
Massachusetts State Police
January 30, 2025

hfma
massachusetts-rhode island chapter

COMMONWEALTH FUSION CENTER MISSION

Unclassified//For Official Use Only



hfma massachusetts-rhode island chapter

MCP HISTORY

MASSACHUSETTS CYBERSECURITY PROGRAM

- Established in 2016 to address increasing cyber threats to Critical Infrastructure
- Information Sharing, Awareness Bulletins, Trainings, Pass-through Alerts, Threat Briefings
- MCP distro
- Partnerships

Commonwealth Fusion Center
Massachusetts

(U) Massachusetts State Police, Commonwealth Fusion Center
Malicious USB Attacks
4 March 2022

(U) Overview

(U) The FBI released an alert that cybercriminals are mailing malicious USB flash drives[1] through the US Postal Service. FIN7, a cybercrime threat group, has been conducting USB attacks by mailing USBs laced with malware to US organizations in US defense, transportation, and private sector entities. FIN7 has used two different schemes to trick victims into plugging in the malicious USBs. One scheme contains a package that appears to come from the US Department of Health and Human Services that reportedly contains information on current pandemic guidelines. The second lure comes as an Amazon gift box which contains a thank you letter, USB, and counterfeit gift card. According to the FBI, both packages contain USBs that when connected to a computer will send preconfigured commands that download malicious software, creating direct back door access for cybercriminals to deploy ransomware.

(U) Cybercriminals have also been known to plant malicious USBs in public areas hoping that unsuspecting victims will pick them up. "Lost and Found" USB attacks rely on victim's curiosity to see who the owner of the USB is or what type of files it contains. Cybercriminals may entice victims by labeling the USB as "finances, bonuses, payroll" or any title that may bait victims into plugging it into their computer.

(U) Never plug an unknown USB into your personal or work computer!

(U) Response Considerations

(U) Report incidents to your police department of jurisdiction.
(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, follow the link to the Internet Crime Complaint Center (IC3):
- Internet Crime Complaint Center - WWW.IC3.GOV

(U) Outlook

(U) The Massachusetts State Police, CFC is providing this information for situational awareness purposes only. Please report any suspicious activity to your police department of jurisdiction.

Sources:
(U) "FBI Warns FIN7 Campaign Delivers Ransomware via BadUSB," Dark Reading, 10 January 2022
(U) "FBI: Hackers use BadUSB to target defense firms with ransomware," Bleeping Computer, 7 January 2022
(U) "FIN7 Targets US Enterprises Via BadUSB," Bank Info Security, 11 January 2022
(U) "FBI warns cybercriminals have tried to hack US firms by mailing malicious USB drives," CSO, 7 January 2022

[1] USB Flash Drive – A removable data storage device that can plug into a computer's USB port.

Unclassified//FOUO
The information contained in this bulletin is unclassified.

hfma massachusetts-rhode island chapter

MASSACHUSETTS CYBERSECURITY PROGRAM

Vulnerability & threat intelligence project (VTIP)

FREE SERVICE

Established in 2019 to help mitigate common initial access vectors

COVID-19

Critical Infrastructure

Identify

Notify

Provide mitigation guidance & facilitate support

- ***Passive*** **Attack Surface Monitoring**
- **Public facing vulnerabilities, exposures misconfigurations**
  - **KEVs, Mass Exploitation Campaigns**
  - **Insecure remote access**
  - **Exposed OT/ICS/SCADA/IoT**
  - **Alerts & Proactive/Hunt**
- **Stolen/leaked credentials**
- **Typosquatted/lookalike domains**
- **FCC Covered List**

hfma massachusetts-rhode island chapter

REPORTING

MASSACHUSETTS CYBERSECURITY PROGRAM

- **You are our best source of Cyber Threat Intelligence!**
- Reporting entity **will not** be identified when sharing out information
  - *"a municipality in Massachusetts", "a K-12 organization in Massachusetts", "a public safety agency in Massachusetts"*
- **Shared information passed on to larger community for situational awareness and as actionable, timely, relevant CTI via MCP Distro**

hfma massachusetts-rhode island chapter

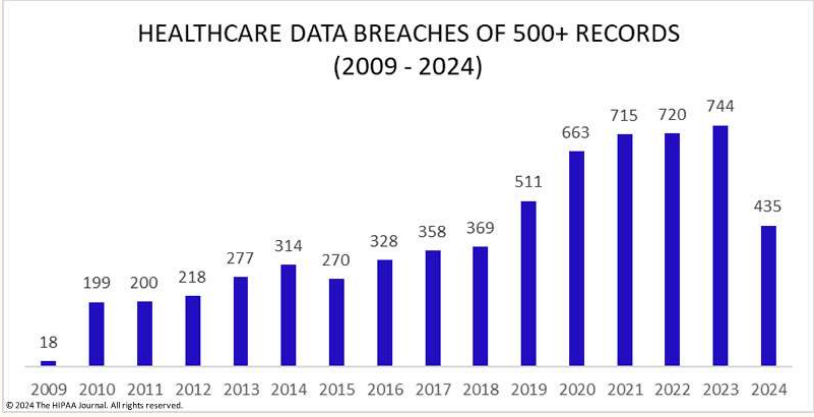
Homeland Security

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

FBI FEDERAL BUREAU OF INVESTIGATION

MS-ISAC® Multi-State Information Sharing & Analysis Center®

HEALTHCARE CYBER THREAT LANDSCAPE

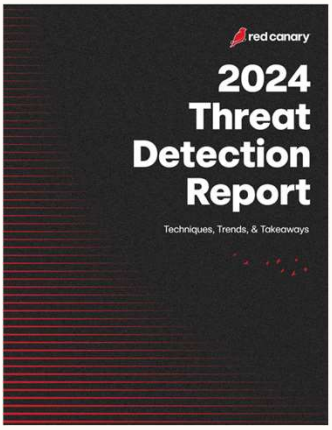


hfma
massachusetts-rhode island chapter

CURRENT THREAT LANDSCAPE

TRENDS

- Ransomware intrusions
  - Exploit public facing vulnerabilities
    - Servers & web-applications
    - Often unmonitored
  - Phishing help-desk employees
  - Phishing emails
    - SIM swaps

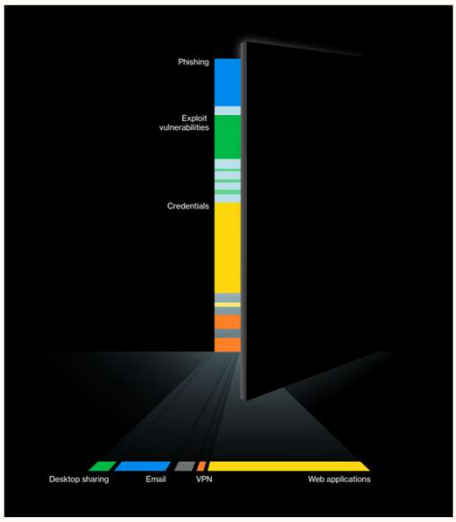


hfma massachusetts-rhode island chapter

CURRENT THREAT LANDSCAPE

TRENDS

- 2024 Verizon DBIR
  - 180% increase in attacks involving exploitation of vulnerabilities in 2023
  - 0-day & 1-day
  - Primarily leveraged by Ransomware operators
  - 10% breaches caused by misconfigurations



hfma massachusetts-rhode island chapter

CYBER THREAT ACTORS

- Cybercriminals
- Insider Threat
- Nation-State
- Advanced Persistent Threat (APT) Groups
- Hacktivists
- Terrorists

CYBER THREAT ACTORS

hfma massachusetts-rhode island chapter

SCATTERED SPIDER (FINANCIALLY MOTIVATED)

- Pre-texting and **Social Engineering** to obtain credentials to **privileged accounts** by tricking IT/helpdesk staff
- Send repeated MFA notification prompts to lead employees to press “accept”
  - MFA fatigue
- Perform **SIM swaps** for key personnel
- **Casino attacks – MGM & Caesars**

hfma massachusetts-rhode island chapter

UNNAMED HIGHER ED ORGANIZATION

hfma massachusetts-rhode island chapter

STAFF MEMBER ACCOUNT TAKEOVER

- **Social engineer of IT/Help Desk Staff**
  - **Reset password**
  - **Reset MFA**
- **Requested MCP Assistance**
  - **Shared call recording, TA's phone number, IP connectivity logs**
  - **Staff member is department lead & prominent researcher in subject area of interest to Nation States**

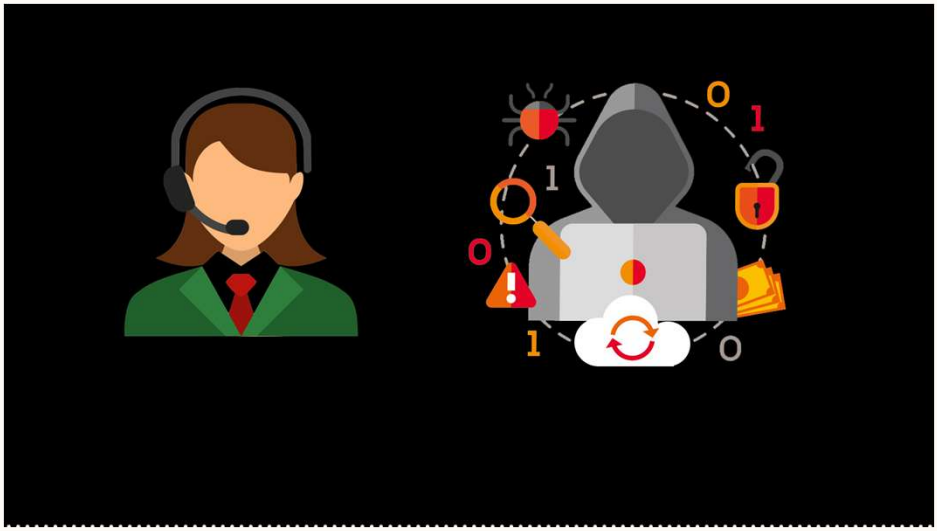

Bloomberg

Businessweek Technology

Hacking the Help Desk: How Attackers Talk Their Way Into Company Networks

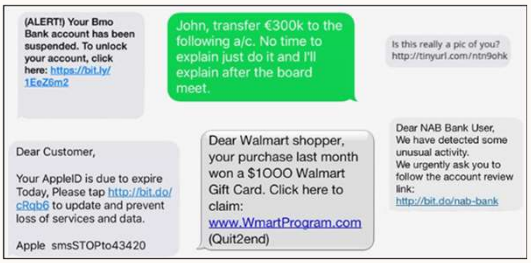
The group believed to be behind recent attacks on casinos excels at so-called social engineering, the term of art for tricking IT call center workers into unwittingly aiding them.

The MGM Grand hotel and casino in Las Vegas. *Photographer: Bridget Bennett/Bloomberg*



hfma massachusetts-rhode island chapter

TEXT OR SMS PHISHING AKA "SMISHING"



- Normally Urgent (BEFORE DEAL EXPIRES)
- Simply click to "claim reward"
- Account has been suspended, click now to fix

hfma massachusetts-rhode island chapter

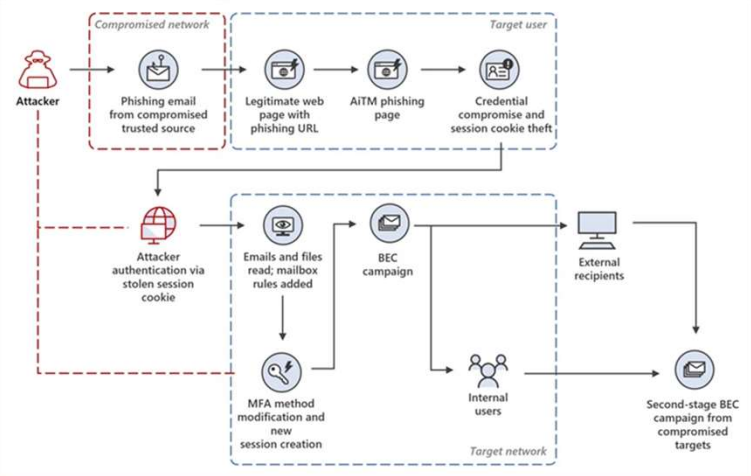
AITM ATTACKS - STORM 1167

Microsoft Threat Intelligence reporting

- Microsoft threat intelligence has identified this group as using the indirect proxy method to target systems in
- Once they gain persistence, they further their access by adding another MFA device to the account so they have access to the account
- Once they have gain access ,they will use the account address book to further their BEC compromise towards the organization, their partners, and customers

hfma massachusetts-rhode island chapter

AITM ATTACKS - STORM 1167



CYBER THREAT ACTORS

hfma massachusetts-rhode island chapter

VOLT TYPHOON (APT)

- Active since mid-2021
- Targeting US Critical Infrastructure Entities for purposes of **pre-staging in the event of geopolitical conflict**
- Use stealth, ***living-off-the-land*** techniques
- Exploit vulnerabilities in SOHO edge devices

hfma massachusetts-rhode island chapter

Black Basta Ransomware Group

- Russian speaking group know for executing double extortion attacks
- Not only known for affecting hospital systems such as laboratory and pharmaceutical services but also stealing patient data.
- The group focuses on English speaking countries.

hfma massachusetts-rhode island chapter

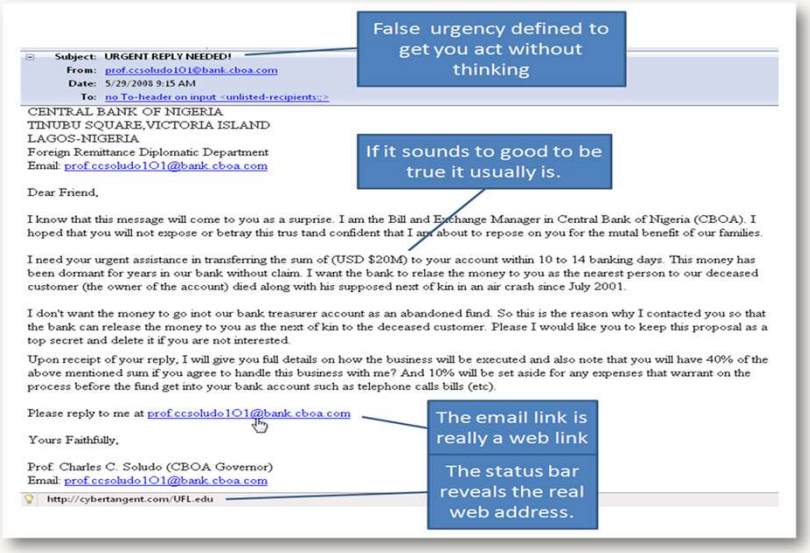
Black Basta Ransomware Group

Attack Techniques

From the Hacker News:

- Black Basta ransomware have been observed switching up their social engineering tactics, distributing a different set of payloads such as Zbot and DarkGate since early October 2024.
- Attackers make initial contact with prospective targets on Microsoft Teams, pretending to be support personnel or IT staff of the organization. In some instances, they have also been observed impersonating IT staff members within the targeted organization.
- Rapid 7 reports - send a malicious QR code to the victim user via the chats to likely steal their credentials under the pretext of adding a trusted mobile device.

hfma massachusetts-rhode island chapter



REAL WORLD AND PHYSICAL IMPLICATIONS OF CYBER ATTACKS

hfma massachusetts-rhode island chapter

- Adjusting room or equipment temperature levels
- Shutdown phone lines and other communications
- Modify settings to cause system or machine failure
- Opening/Closing critical infrastructure equipment (valves, pipes, vents, etc)
- Turn off warning alarms or notifications to prevent victims of active problem.

hfma
massachusetts-rhode island chapter

TLP:CLEAR

Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

MS-ISAC Multi-State Information Sharing & Analysis Center | Communications Security Establishment Canadian Centre for Cyber Security | Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité | National Cyber Security Centre

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), United States Department of Agriculture (USDA), Food and Drug Administration (FDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Canadian Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK)—hereafter referred to as "the authoring organizations"—are disseminating this fact sheet to highlight and safeguard against the continued malicious cyber activity conducted by pro-Russia hacktivists against operational technology (OT) devices in North America and Europe.

Actions to take today:

- Immediately change all default passwords of OT devices (including PLCs and HMIs), and use strong, unique passwords.
- Limit exposure of OT systems to the internet.
- Implement multifactor authentication for all access to the OT network.

The authoring organizations are aware of pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European Water and Wastewater Systems (WWS), Dams, Energy, and Food and Agriculture Sectors. These hacktivists seek to compromise modular, internet-exposed industrial control systems (ICS) through their software components, such as human machine interfaces (HMIs), by exploiting virtual network computing (VNC) remote access software and default passwords.

The authoring organizations are releasing this fact sheet to share information and mitigations associated with this malicious activity, which has been observed since 2022 and as recently as April 2024. The authoring organizations encourage OT operators in critical infrastructure sectors—including WWS, Dams, Energy, and Food and Agriculture—to apply the recommendations listed in the Mitigations section of this fact sheet to defend against this activity.

Overview of Threat Actor Activity

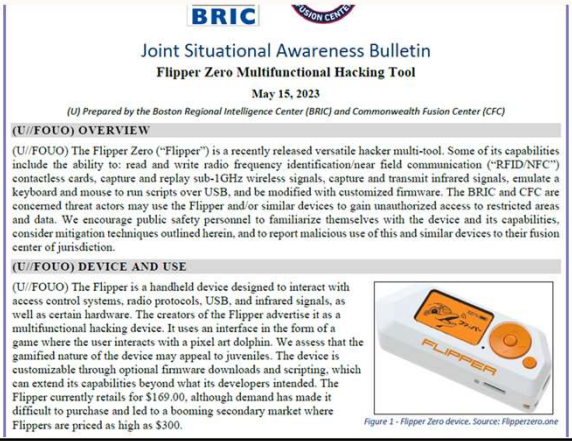
Pro-Russia hacktivist activity against these sectors appears mostly limited to unsophisticated techniques that manipulate ICS equipment to create nuisance effects. However, investigations have identified that these actors are capable of techniques that pose physical threats against insecure and misconfigured OT environments. Pro-Russia hacktivists have been observed gaining remote access via a combination of exploiting publicly exposed internet-facing connections and outdated VNC software, as well as using the HMIs' factory default passwords and weak passwords without multifactor authentication.

TLP:CLEAR

cisa.gov | central@cisa.dhs.gov | @CISAgov | @CISACyber | @cisagov | As of May 1, 2024

hfma
massachusetts-rhode island chapter

DEVICES THAT AFFECT CYBER AND PHYSICAL SPACES



BRIC | FUSION CENTER

Joint Situational Awareness Bulletin

Flipper Zero Multifunctional Hacking Tool

May 15, 2023

(U) Prepared by the Boston Regional Intelligence Center (BRIC) and Commonwealth Fusion Center (CFC)

(U//FOUO) OVERVIEW

(U//FOUO) The Flipper Zero ("Flipper") is a recently released versatile hacker multi-tool. Some of its capabilities include the ability to: read and write radio frequency identification/near field communication ("RFID/NFC") contactless cards, capture and replay sub-1GHz wireless signals, capture and transmit infrared signals, emulate a keyboard and mouse to run scripts over USB, and be modified with customized firmware. The BRIC and CFC are concerned threat actors may use the Flipper and/or similar devices to gain unauthorized access to restricted areas and data. We encourage public safety personnel to familiarize themselves with the device and its capabilities, consider mitigation techniques outlined herein, and to report malicious use of this and similar devices to their fusion center of jurisdiction.

(U//FOUO) DEVICE AND USE

(U//FOUO) The Flipper is a handheld device designed to interact with access control systems, radio protocols, USB, and infrared signals, as well as certain hardware. The creators of the Flipper advertise it as a multifunctional hacking device. It uses an interface in the form of a game where the user interacts with a pixel art dolphin. We assess that the gamified nature of the device may appeal to juveniles. The device is customizable through optional firmware downloads and scripting, which can extend its capabilities beyond what its developers intended. The Flipper currently retails for $169.00, although demand has made it difficult to purchase and led to a booming secondary market where Flippers are priced as high as $300.

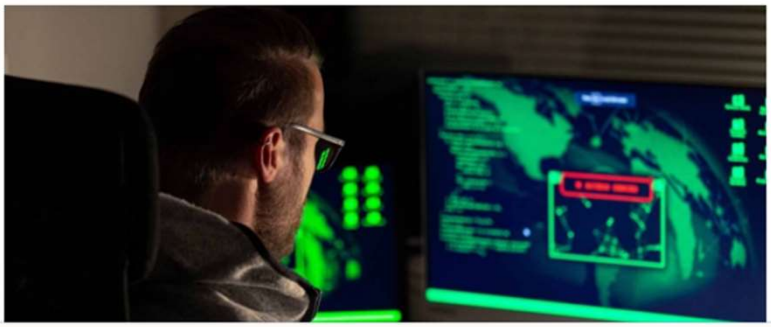
Figure 1 - Flipper Zero device. Source: Flipperzero.one

hfma massachusetts-rhode island chapter

Healthcare cyberattacks are costing an average of $11 million per breach

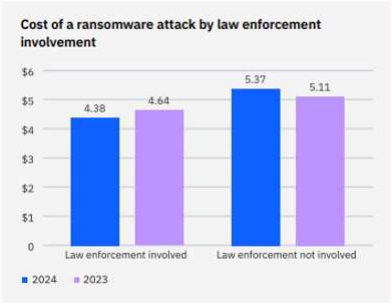
Ransomware attacks have dominated, accounting for over 70% of healthcare cyberattacks in the past two years.

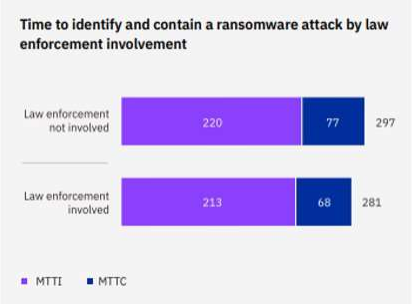
Nathan Eddy



hfma massachusetts-rhode island chapter

IBM COST OF A DATA BREACH REPORT 2024





$1M USD
or approximately 20% cost savings when law enforcement is involved in ransomware attacks

Law Enforcement involvement also sped up the time it took to identify and contain a breach (9% reduction in combined Mean Time to Identify & Mean Time to Resolve)

REPORTING TO LAW ENFORCEMENT – WHEN?

- A cyber incident is an event that could risk the confidentiality, integrity, or the availability of information systems. Cyber-incidents could lead to a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Victims are encouraged to report cyber incidents that may:
- Indicate unauthorized access to, or malicious software present on system and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, public health or safety, or any combination of those matters.
- Result in a significant loss of data, system availability, or control of systems.
- Impact a large number of victims.
- There are no minimum monetary loss thresholds for reporting.

REPORTING TO LAW ENFORCEMENT – HOW?

- Report the incident to your local police department of jurisdiction in accordance with your organization's existing notification policies, and request they notify the Commonwealth Fusion Center by telephone or email. It is important to establish a working relationship and protocols with these law enforcement points of contact and incorporate them into your incident response plan well in advance of a crisis.
- If you do not have an existing notification process that includes your local police department, you may contact the Commonwealth Fusion Center directly via telephone at **508-820-2233**.
- Once notified, someone from the Commonwealth Fusion Center will contact your organization's designated point of contact.
- Report the incident to other regulatory entities and Federal Law Enforcement in accordance with your organization's policies. Reporting a Cyber Incident to Law Enforcement **does not** fulfill regulatory data breach reporting requirements.

REPORTING TO LAW ENFORCEMENT – WHAT TO EXPECT?

hfma
massachusetts-rhode island chapter

- **We will NOT:**
- Contact the media or issue public statements.
- Notify regulatory agencies about a potential data breach.
- Perform services an incident response firm would provide such as the removal of malware or mitigation of the infection from your systems or network(s).
- Provide complete mitigation and remediation support.

- **We will:**
- ✓ Work discretely and confidentially with your organization's Incident Response Team, Legal Department, and/or a third-party incident response firm to identify and collect potential evidence.
- ✓ Work with federal and local law enforcement partners and prosecutors to coordinate the investigation to identify, locate, apprehend, and ultimately prosecute the threat actor(s).
- ✓ Facilitate communications with other organizations that could help mitigate the incident.
- ✓ Compare Indicators of Compromise and Tactics, Techniques, and Procedures in your incident with other similar incidents.
- ✓ Remain in contact with your organization throughout the investigation.
- ✓ Work with you to determine if you are amenable to pertinent threat intelligence being shared in a non-attributable manner to protect others who may be affected by the same type of attack.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MCP
Massachusetts Cybersecurity Program

No portion of the presentation should be video or audio recorded, copied, or photographed.

TLP GREEN

hfma
massachusetts-rhode island chapter

THANK YOU!

MCP
Massachusetts
Cybersecurity Program

General Inquiries: mcppol.state.ma.us

Report an Incident: 508-820-2233