MassCyberCenter
at the MassTech Collaborative

OMST
OFFICE OF MUNICIPAL & SCHOOL TECHNOLOGY

Cybersecurity: Staying Ahead of Threats Balancing People, Process and Technology

Minimum Baseline of Cybersecurity

John Petrozzelli, Director, *MassCyberCenter*
Susan Noyes, Director, *EOTSS Office of Municipal & School Technology*
Meg Speranza, Resiliency Program Manager, *MassCyberCenter*

October 15, 2025

Presented in Partnership with
MMA Massachusetts Municipal Association

Agenda

- Introductions
- Cybersecurity Threats to Municipalities
- What is Cybersecurity?
- The Minimum Baseline of Cybersecurity
- Resources to help municipalities with cybersecurity

Introductions

John Petrozzelli, Director
MassCyberCenter at the MassTech Collaborative
Petrozzelli@MassTech.org

Susan Noyes, Director
Office of Municipal and School Technology at the
MA Executive Office of Technology Services & Security
Susan.noyes@Mass.gov

Meg Speranza, Resiliency Program Manager
MassCyberCenter at the MassTech Collaborative
Speranza@MassTech.org

State and Regional Collaboration on Cybersecurity

MassCyberCenter and the Cyber Resilient Massachusetts Working Group

MassCyberCenter

Mission - Improve cybersecurity resiliency and create cybersecurity workforce development opportunities by building public awareness, creating cutting edge programs, organizing engaging events, and leading collaborative working groups.

Cyber Resilient Massachusetts Working Group

Mission – Bring together public and private sector leaders to identify ways the Commonwealth's innovative technology ecosystem can help Massachusetts organizations and critical institutions protect sensitive data, increase cybersecurity awareness, and respond to emerging threats.

- Improve cybersecurity resiliency in the Commonwealth through planning
  - Anticipate threats and seek intelligence
  - Promote cybersecurity best practices (CIS Top 18 Security Controls, NIST, and more)
- Collaboration through outreach and education
  - Working groups to build relationships on key issues and identify gaps to mitigate shortfalls
  - Leverage Massachusetts talent
  - Enhance cybersecurity awareness

The Working Group, led by the MassCyberCenter, has a rolling membership of approximately 120 members from 75+ organizations across the public and private sectors. Go to MassCyberCenter.org to find out more.

State and Regional Collaboration on Cybersecurity

Executive Office of Technology Services and Security

Office of Municipal & School Technology

The Office of Municipal and School Technology (OMST) supports local government (municipal) efforts to effectively serve their residents, students, and employees with the use of technology. It serves local government agencies, which include cities, towns, public school districts, public safety, municipal utility departments, counties, and planning commissions, across the Commonwealth.

- Guidance and technical assistance on technology initiatives, including implementation
- Promotion of state resources to improve local government operations, including
  - Municipal Cybersecurity Awareness Training programs
  - Community Compact Cabinet IT and Security Grant Opportunities
  - Municipal Local Cybersecurity Grant Program (SLCGP)
  - Health Check Program

For more information, go to
https://www.mass.gov/orgs/office-of-municipal-and-school-technology

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST OFFICE OF MUNICIPAL & SCHOOL TECHNOLOGY

POLL Question 1:

What types of cybersecurity incidents have you personally or professionally experienced?

Cybersecurity Threats to Municipalities

What makes local governments and schools attractive targets for cyber attacks?

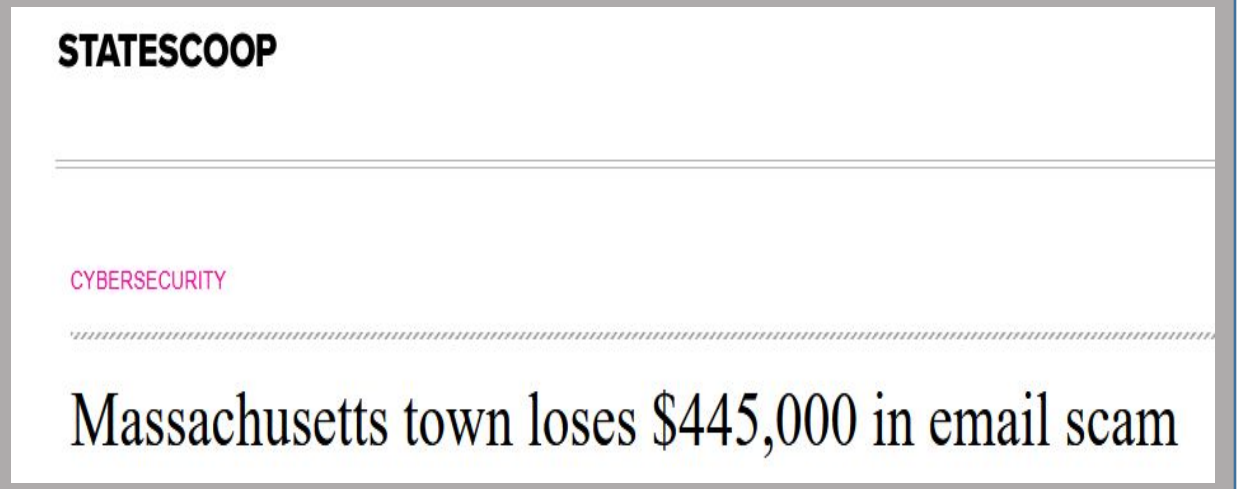
- They house private data
- Security often isn't a top (or well-funded) priority
- Attacks have been successful
- Attacks against local governments and schools are public-facing, providing a potent outlet and often resulting in a variety of disruptive, public consequences

Cybersecurity Threats to Municipalities

- Unintended disclosures by employees
- Hacking/Malware/Ransomware
- Insider Threats
- Zero Day Vulnerabilities
- Physical Loss
- Portable Device/ Removable Media
- Technology Intrusions
- Phishing/Spear-Phishing Schemes
- Man-in-the-Middle Attacks
- Wire Transfer Fraud
- Skimming Incidents
- Vendors/Subcontractors – Poor Security
- Protocols/Standards

Cybersecurity Threats to Municipalities

Attacks in the News



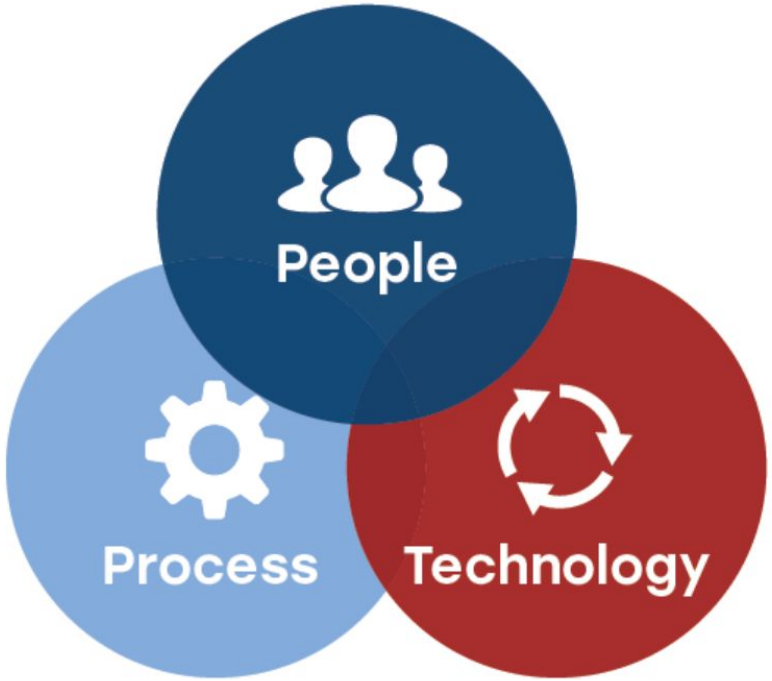
Schools Reopened Thursday After Ransomware Attack

– Local Newspaper, January 2023

What is Cybersecurity

- Leadership Talent/employment
- Training/education
- Citizens

- Cyber standards and procedures
- Incident response plans/ recovery
- Engagement



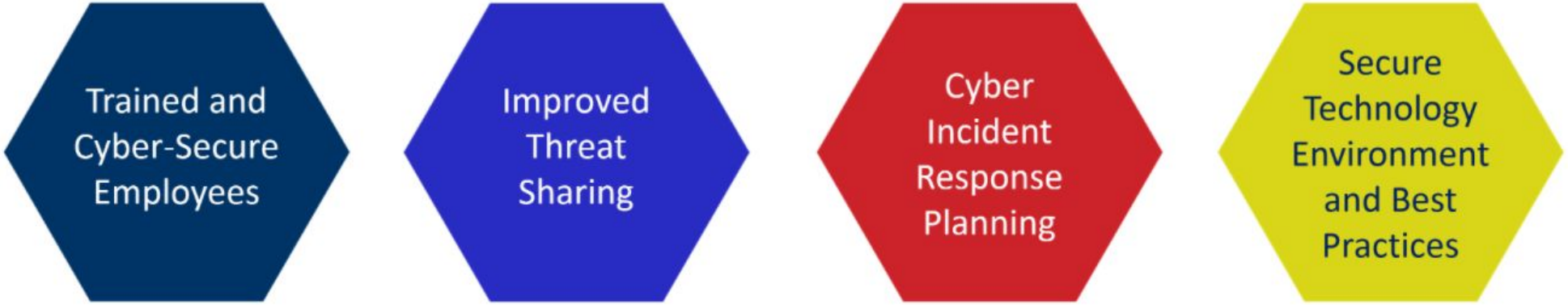
- Sensors
- Decision aids
- Defense tools

People, Process, and Technology work together to protect data confidentiality and integrity and provide data availability.

Minimum Baseline of Cybersecurity

A foundational-level of cybersecurity for Massachusetts organizations to improve their cybersecurity posture and protect their networks and data from cyberattacks using people, process, and technology.

There are 4 goals:



Each goal contains links to cybersecurity Resources.
For more information go to MassCyberCenter.org.

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

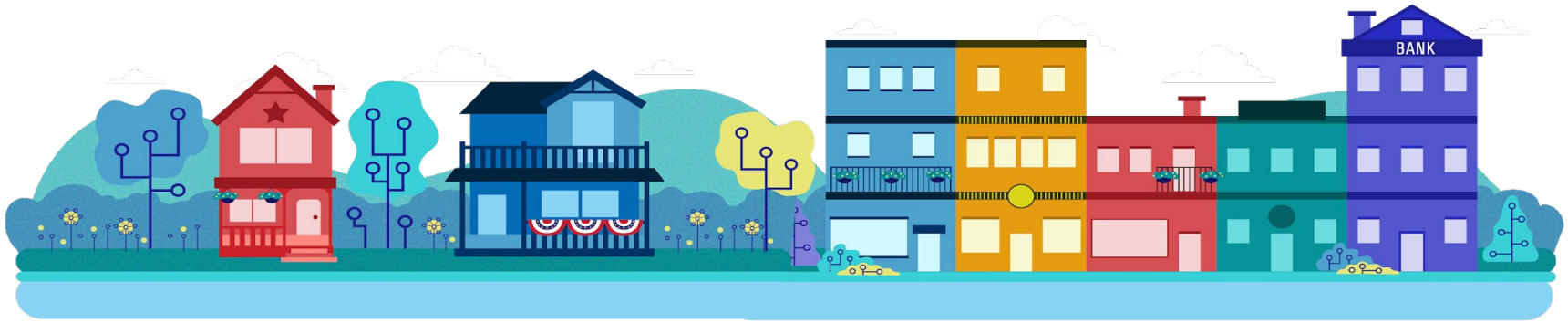
OMST Office of Municipal & School Technology

Minimum Baseline Overview Modules

A fun way to introduce the Minimum Baseline and goals.

Using a notional cyberattack occurring in the fictional town of Massboro as an example to explain the Minimum Baseline of Cybersecurity, the first module introduces the Minimum Baseline, and the other four modules explain each of the four goals.

Go to MassCyberCenter.org to experience the overview modules and learn more.



MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST OFFICE OF MUNICIPAL & SCHOOL TECHNOLOGY

Resources collated to help municipalities with cybersecurity
Commonwealth Cybersecurity Resources - A Cross-Agency Collaboration

EOTSS

Office of Municipal and School Technology (OMST)
Municipal Cybersecurity Awareness Grant Program
Cyber Health Checks

MassCyberCenter at the MassTech Collaborative

MassCyberCenter
Minimum Baseline of Cybersecurity
Cyber Incident Response Planning Materials

Community Compact Cabinet

Community Compact Program
Best Practices Program
IT Grant Program

EOPSS

Office of Grants & Research (OGR)
Homeland Security Grant Program (HSGP)
State and Local Cybersecurity Grant Program (SLCGP)

COMMONWEALTH FUSION CENTER
CFC

Massachusetts State Police – Commonwealth Fusion Center
Massachusetts Cybersecurity Program (MCP)

OSD
OPERATIONAL SERVICES DIVISION

Operational Services Division (OSD)
ITS78: Statewide Contract for Cybersecurity and Incident Response Services

MMA Massachusetts Municipal Association

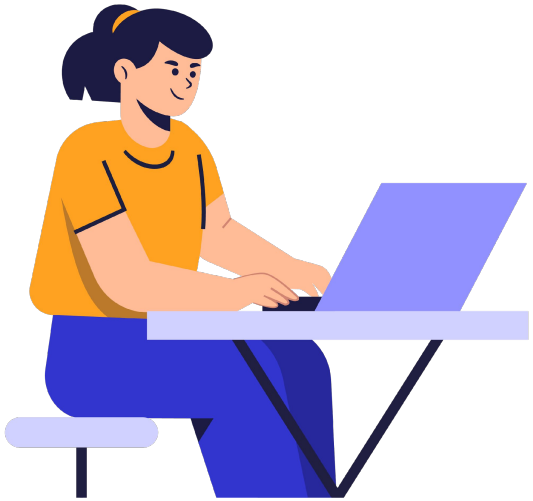
MassCyberCenter at the MassTech Collaborative

OMST OFFICE OF MUNICIPAL & SCHOOL TECHNOLOGY

POLL Question 2:

What types of cybersecurity training do you use today?

GOAL: Trained and Cyber-secure Employees



Benefits:

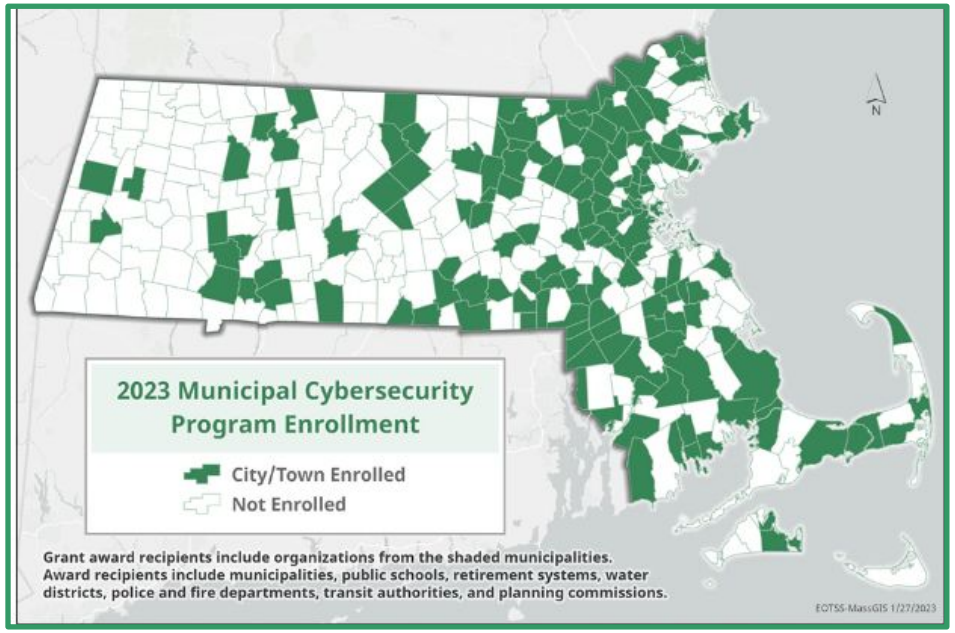
- Reduce the risk of cybersecurity incidents by improving the training and awareness of system users.

How to Achieve:

- Implement annual individual employee cybersecurity awareness training.
- Make it easy to do the training.
- Put incentives in place to get it done.

Municipal Cybersecurity Awareness Program (MCAP)

The Executive Office of Technology Services and Security's (EOTSS)
Office of Municipal and School Technology (OMST)
procures licenses and manages the Municipal Cybersecurity Awareness Program – **making the program FREE to participating organizations.**



https://www.mass.gov/info-details/cybersecurity-awareness-program

Municipal Cybersecurity Awareness Program (MCAP)

The Program Provides:

- Assessments
- Online modules
- Phishing campaigns
- Additional resources (posters, newsletters, webinars, etc.)
- Local Coordinator access to the training platform
- PDPs for those in Education (in alignment with the DESE PD requirements)

Learning Paths:

Traditional | Advanced | Comprehensive | Education

Who Can Take the Training?

Cities/towns
Libraries
Schools
Planning Commissions
Police & Fire Departments
Water Districts
Massachusetts Public Pension Systems (PERAC)
Municipally run utility departments, airports and housing authorities

**Town Leaders, Administration/Department Heads are encouraged to set the example for employees by completing the training.*

https://www.mass.gov/info-details/cybersecurity-awareness-program

GOAL: Improved Threat Sharing

Benefits:

- Respond faster to threats and improve regional awareness and resilience by sharing cyber threat information.

How to Achieve:

- Sign up for threat-sharing alerts from the Fusion Center, MS-ISAC, or CISA
- Come to the Bi-weekly Roundtable Calls through the MassCyberCenter or Monthly Calls from the Fusion Center.
- Get to know your neighboring cities and towns.
- Join a regional IT group through the EOTSS Office of Municipal and School Technology.

GOAL: Cyber Incident Response Planning

Have a Plan!

Benefits:

- Strengthen municipal defenses and minimize cyber incident impacts by creating an effective strategy for handling cyber incidents.

How to Achieve:

- Use the tools and resources at MassCyberCenter.org to create a plan to protect against and respond to a cyberattack.
- Test the plan using the *CyberSecureDeck Tabletop Exercise Card Game* or using a Cyber Range or attending *Cyber351*.

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST Office of Municipal & School Technology

Cybersecurity Considerations

Left of Boom (Pre-Incident)

Free State and Federal Resources:

- CISA
  - Cyber Hygiene (CyHy)
  - Web Application Scanning (WAS)
  - CISA Remote Penetration Testing
  - CISA Logging Made Easy
  - SCUBA Tool (Windows)
- Executive Office of Technology Services and Security (EOTSS)
  - Cybersecurity Health Check
  - Community Compact Cabinet Grants
  - EOTSS Cyber Awareness Training Grant
- Executive Office of Public Safety and Security (EOPSS)
  - Municipal Local Cybersecurity Grant Program – SLCGP (MFA funding and Awareness Training)
- MassCyberCenter
  - Cyber Resilient Mass Grant Program
- Windows Applocker (Free in Windows 10/11)
- MS-ISAC Malicious Domain Blocking and Reporting

Paid Services:

- Endpoint Managed Detection and Response
  - CyberTrust SOC (SentinelOne 24/7)
  - MS-ISAC SOC (Crowdstrike)

Right of Boom (Post-Incident)

Report an Incident:

Call the Commonwealth Watch Center at **508-820-2233**

Contact your Cyber Insurance Provider

MIIA Claims Contact:

David Dowd
Jillian McMartin
Phone: 800-526-6442
Email: MIIAclaims@MMA.org
Fax: 781-376-9907

Provide the following Details:

- Authorized Contact Name
- Any documents to support incident or claim
- Brief description of event

Important: All incidents and claims need to be reported immediately (within 24 hours) to MIIA.

Consider Contacting the following as well:

- Local Police Department
- EOTSS SOC (*Strongly Encouraged* under Executive Order 602)
- FBI - For BEC with financial loss – file www.IC3.gov report **AND** contact your financial institution immediately.

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST Office of Municipal & School Technology

GOAL: Secure Technology Environment and Best Practices

Benefits:

- Reduce the threat of cybersecurity incidents and minimize incident impacts by implementing some basic best practices to make your technology environment more secure.

How to Achieve:

- There are many best practices listed in the resources. Here are a few to get started:
  - Require strong passwords
  - Backup critical data and systems
  - Update and patch systems regularly
  - Do annual vulnerability assessments
  - Implement Multi-Factor Authentication (MFA)

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST Office of Municipal & School Technology

GOAL: Secure Technology Environment and Best Practices

IT Upgrade:

- Remove end of life hardware and software
- Change default passwords on network equipment
- Implement Least Privilege
- Implement Role Based Access Control

GOAL: Secure Technology Environment and Best Practices

Utilize Security Tools:

- EOTSS Health Check
- CISA Vulnerability Scanning
- CISA SCUBA tool
- CISA Web Application Scanning
- Endpoint Detection and Response
- Email Security
- Firewalls
- Zero Trust

MMA Massachusetts Municipal Association

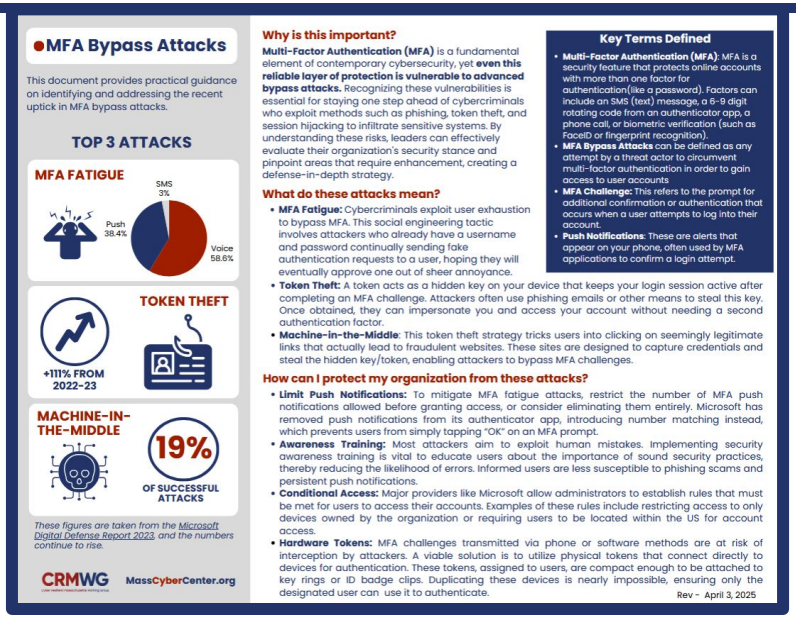
MassCyberCenter at the MassTech Collaborative

OMST Office of Municipal & School Technology

GOAL: Secure Technology Environment and Best Practices

CRMWG Products:

- MFA Bypass Attacks Guidance
- Municipal Attack Surface Guidance
- CyberSecureDeck



MFA Bypass Attacks

This document provides practical guidance on identifying and addressing the recent uptick in MFA bypass attacks.

TOP 3 ATTACKS

MFA FATIGUE

TOKEN THEFT

+111% FROM 2022-23

MACHINE-IN-THE-MIDDLE

19% OF SUCCESSFUL ATTACKS

These figures are taken from the Microsoft Digital Defense Report 2023, and the numbers continue to rise.

CRMWG MassCyberCenter.org

Why is this important?

Multi-Factor Authentication (MFA) is a fundamental element of contemporary cybersecurity, yet **even this reliable layer of protection is vulnerable to advanced bypass attacks.** Recognizing these vulnerabilities is essential for staying one step ahead of cybercriminals who exploit methods such as phishing, token theft, and session hijacking to infiltrate sensitive systems. By understanding these risks, leaders can effectively evaluate their organization's security stance and pinpoint areas that require enhancement, creating a defense-in-depth strategy.

What do these attacks mean?

- **MFA Fatigue:** Cybercriminals exploit user exhaustion to bypass MFA. This social engineering tactic involves attackers who already have a username and password continually sending fake authentication requests to a user, hoping they will eventually approve one out of sheer annoyance.
- **Token Theft:** A token acts as a hidden key on your device that keeps your login session active after completing an MFA challenge. Attackers often use phishing emails or other means to steal this key. Once obtained, they can impersonate you and access your account without needing a second authentication factor.
- **Machine-in-the-Middle**: This token theft strategy tricks users into clicking on seemingly legitimate links that actually lead to fraudulent websites. These sites are designed to capture credentials and steal the hidden key/token, enabling attackers to bypass MFA challenges.

Key Terms Defined

- **Multi-Factor Authentication (MFA)**: MFA is a security feature that protects online accounts with more than one factor for authentication(like a password). Factors can include an SMS (text) message, a 6-9 digit rotating code from an authenticator app, a phone call, or biometric verification (such as FaceID or fingerprint recognition).
- **MFA Bypass Attacks** can be defined as any attempt by a threat actor to circumvent multi-factor authentication in order to gain access to user accounts
- **MFA Challenge:** This refers to the prompt for additional confirmation or authentication that occurs when a user attempts to log into their account.
- **Push Notifications**: These are alerts that appear on your phone, often used by MFA applications to confirm a login attempt.

How can I protect my organization from these attacks?

- **Limit Push Notifications:** To mitigate MFA fatigue attacks, restrict the number of MFA push notifications allowed before granting access, or consider eliminating them entirely. Microsoft has removed push notifications from its authenticator app, introducing number matching instead, which prevents users from simply tapping "OK" on an MFA prompt.
- **Awareness Training:** Most attackers aim to exploit human mistakes. Implementing security awareness training is vital to educate users about the importance of sound security practices, thereby reducing the likelihood of errors. Informed users are less susceptible to phishing scams and persistent push notifications.
- **Conditional Access:** Major providers like Microsoft allow administrators to establish rules that must be met for users to access their accounts. Examples of these rules include restricting access to only devices owned by the organization or requiring users to be located within the US for account access.
- **Hardware Tokens:** MFA challenges transmitted via phone or software methods are at risk of interception by attackers. A viable solution is to utilize physical tokens that connect directly to devices for authentication. These tokens, assigned to users, are compact enough to be attached to key rings or ID badge clips. Duplicating these devices is nearly impossible, ensuring only the designated user can use it to authenticate.

Rev - April 3, 2025

Municipal Attack Surface

This document provides practical guidance for identifying and addressing the most common vulnerabilities discovered amongst municipalities in the Northeast Homeland Security Region of Massachusetts.

SSL Security Findings

48% SSL Not Available
27% SSL Expired
71% SSL Hostname Mismatch
21% Untrusted SSL Certificates

Email Security Configuration Findings

Quarterly Average Score of fixed vulnerabilities

Unnecessary Open Ports

The average score of the region improved most during Cybersecurity Month (October), indicating the collective efforts of cyber advocates throughout Massachusetts culminate in the fall.

CRMWG MassCyberCenter.org

Email Security (DMARC/SPF/DKIM)

Why is this important?

The simplest way for an attacker to compromise a municipality is to impersonate ("spoof") a trusted employee, vendor, or other external user via email. Without a DMARC policy (along with SPF and DKIM protocols), this is easy to do – there are even online services that will do it for you for about $25. Whether it is to trick users into downloading malware or, as has been seen more recently, into transferring large sums of money to fraudulent bank accounts, a missing or incorrectly configured DMARC policy puts your entire municipal organization at risk.

What do these vulnerabilities mean?

- **No DMARC Policy:** This is the simplest of the three, it simply means that there is no gatekeeper, and your organization is at risk for email compromise.
- **DMARC p=none:** A DMARC policy has three options for what to do with a message that fails the two checks – reject (return to sender), quarantine (put in spam), and nothing (aka "none"). The organization must define which option they want to use. In this case, the organization has a DMARC policy, but it is not doing anything.
- **SPF Not Enabled:** Your guest list is not enabled, and anyone is allowed in! Emails that look legitimate, but might have a non-obvious misspelling, or a foreign character inserted can easily come through to your users' inboxes.

Key Terms Defined

- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** is an email security policy that acts like a gatekeeper, checking whether incoming emails are really coming from the domain that is shown (e.g. @anytownma.gov). It checks incoming emails against two records, an SPF and DKIM, and one of the two must pass. If a message fails both, the policy dictates what should happen to the message.
- **Sender Policy Framework (SPF)** is an email security protocol that acts like a bouncer at a nightclub checking a guestlist. In this case, the guestlist is a list of IP addresses that are allowed to send emails to your domain (e.g., @anytownma.gov). If an email arrives at the "door" from an IP address not on the list, it is rejected.
- **Domain Keys Identified Mail (DKIM)** is an email security protocol that acts like a watermark on a check or currency, allowing the recipient to confirm its presence to ensure that an email message has not been tampered with in transit.

How can I fix them?

If you understand what DNS, DMARC, SPF, and DKIM are without any explainers like we have here, type "how to set up a DMARC policy" into your favorite search engine and follow the instructions. The journey to a fully implemented DMARC policy is not hard and does not have to cost you anything. However, it does take time and attention to ensure that you will not affect your email deliverability, so start today! There are also numerous vendors who can manage this journey for a fee if you need help. Reach out to your area IT Directors for recommendations.

If you do not understand these terms, reach out to your IT Director, or Managed IT Service provider today to ask whether you have a fully implemented DMARC policy. If the answer is no, find out what stands in the way, and begin the planning process to ensure that whatever resources are needed to complete this journey are available. The average cost of a business email compromise is $125,000 and can easily run much higher if internal IT systems are compromised.

Rev - April 3, 2025

MMA Massachusetts Municipal Association

Cyber Resilient Massachusetts Grant Program

Program Overview

Municipalities, small businesses, and non-profit organizations are eligible to receive grants of up to $25,000 to fund Managed Detection and Response (MDR) services from CyberTrust Massachusetts for up to 3 years.

Additional Information:

- Applications accepted on a rolling basis
- Applications must include a scope of work for MDR services from CyberTrust MA

Thank you!

MMA Massachusetts Municipal Association

MassCyberCenter at the MassTech Collaborative

OMST Office of Municipal & School Technology

ADDENDUM SLIDES

Helpful Massachusetts Websites and Links

- **MassCyberCenter.org**
- **Mass.gov | Cybersecurity and Enterprise Risk Management Program**

  https://www.mass.gov/orgs/cybersecurity-and-enterprise-risk-management
  Program that focuses on protecting citizen data, ensuring the availability of the Commonwealth's networks and systems, and maintaining the continuity of government operations and services.
- **Mass.gov | Report a cybersecurity incident**
  - Report to your local police department and request they notify the Commonwealth Fusion Center
  - Other resources for reporting incidents:
    https://www.mass.gov/info-details/report-a-cybersecurity-incident

Helpful Federal Websites and Links

- **Multi State Information Sharing and Analysis Center (MS-ISAC) and the Center for Internet Security**
  Alerts and Advisories sent from MS-ISAC on a regular basis about threats that may impact state, local, tribal, and territorial government, plus valuable tools, resources, and services. Membership is free for municipalities: https://www.cisecurity.org/ms-isac/
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  - Resources and guidance for State, Local, Tribal, and Territorial Governments: https://www.cisa.gov/
  - **CISA's Cyber Essentials**—a guide for leaders of small businesses and small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices: https://www.cisa.gov/cyber-essentials
  - **CISA STOP Ransomware:** https://www.cisa.gov/stopransomware
  - **CISA CYBERSECURITY AWARENESS PROGRAM** is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online: https://www.cisa.gov/cisa-cybersecurity-awareness-program
- **US-CERT Alerts** that you can subscribe to for up-to-date information on threats, hoaxes: https://www.us-cert.gov/ncas/tips
- **Federal Bureau of Investigation (FBI)**
  - **Internet Crime Complaint Center:** https://www.ic3.gov/
  - **FBI Incident Response Policy:** https://www.fbi.gov/file-repository/incident-response-policy.pdf/view
  - **FBI Fact Sheet** – When to report cyber incidents to the federal government, what and how to report, and types of federal incident response: https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

Additional Resources for Cybersecurity –
Frameworks, Best Practices, Training

- **National Institute of Standards and Technology (NIST)**
  https://www.nist.gov/
  In particular, the **Computer Security Resource Center (CSRC)** (http://csrc.nist.gov) holds a collection of papers that describe security best practices, called NIST Special Publications. They also create security assessment tools.
- **Cybrary**
  https://cybrary.it/
  Cybrary is possibly one of the best IT Security education sites on the internet. It contains full-length college course videos for everything from basic networking up to and including training for certifications, explanations of secure coding, penetration testing and everything else security related.

Additional Resources for Cybersecurity –
Blogs & Podcasts

- **Krebs on Security**
  https://krebsonsecurity.com/about/
  Brian Krebs, author of Spam Nation is also one of the better-known security bloggers in the world, having written over a thousand articles on security.
- **Security Nation Podcast**
  https://www.rapid7.com/blog/series/security-nation/security-nation-season-5/
  Security Nation is a podcast dedicated to celebrating the champions in the cybersecurity community who are advancing security in their own ways.
- **Security Now! Podcast**
  https://www.grc.com/securitynow.htm
  A weekly security-focused podcast that covers all topics from law, current events, to conference reviews and explanations of specific exploits as they are discovered in the world.