Commonwealth of Massachusetts
EXECUTIVE OFFICE OF HOUSING & LIVABLE COMMUNITIES
Maura T. Healey, Governor ◆ Kimberley Driscoll, Lieutenant Governor ◆ Edward M. Augustus Jr., Secretary

Public Housing Notice 2024-12

To: Local Housing Authorities
Fr: Ben Stone, Undersecretary of Public Housing and Rental Assistance
Re: Cyber Security Alert: Protecting your LHA from Active Threat of Cyber Criminals
Date: July 31, 2024

What You Need to Know – Key Points

LHAs are increasingly vulnerable to cyber-attacks targeting the LHA's funds, impersonating the LHA for fraudulent purposes, or even holding the information in the LHAs computer systems for ransom. Large and small Massachusetts LHAs have been hit by multiple cyber attacks in recent weeks.

The best ways to implement cyber security are:
1.) to be vigilant and implement precautions like requiring strong passwords and multi-factor authentication.
2.) training LHAs employees about how to spot and prevent cyber fraud; and
3.) working with an IT vendor that will ensure the LHAs data is saved to a safe backup and protected against malicious codes, like viruses and malware.

LHAs are eligible to participate in a **free** Cybersecurity Health Check Program through the Commonwealth Executive Office of Technology Services and Security (EOTSS). This program will provide a cyber risk assessment and grant eligibility to fund identified protective measures.

Immediate Action Required

LHAs need to take immediate action to avoid cybersecurity threats. Start by reading this PHN carefully and sharing it with your staff and Board. EDs should go to the Mass Cyber Center Website and complete the Minimum Baseline of Cybersecurity for Municipalities training ASAP. LHAs should complete all five steps in the *What Steps Should your LHA Start With?* section below.

TABLE OF CONTENTS

What is the Danger of this Threat?

Local Housing Authorities (LHAs) are increasingly vulnerable to cyber-crime due to their reputation as easy targets with available funds and less advanced technology and security practices. In recent weeks, cybercriminals have successfully attacked several Massachusetts LHAs.

These cyber-attacks, which all occurred in May and June included:

- business email compromise leading to fraudulent emails with malicious links sent to an LHAs contacts directory;
- theft of over $100,000 in grant funds using a social engineering attack on a community preservation fund;
- false invoices being submitted for payment which resulted in misdirection of almost $200,000 of capital funds now not available to send to the actual vendor that did the work;
- ransomware attack which held an LHA's data for a $50,000 ransom which caused the LHA to lose data, staff time and incur high technical and legal expenses.

These are not isolated incidents. Organized cyber-criminal groups deliberately target LHAs across the country, so LHAs must maintain awareness of the threat and constant vigilance.

Cyber-criminals typically gain entry to LHA systems through "social engineering": identifying people within the organization and approaching them under false pretenses for nefarious purposes. Today's techniques are much more sophisticated than the scam emails you may have seen in the past, utilizing intricate psychological tactics and artificial intelligence technologies to exploit vulnerabilities within the LHA's systems and personnel. For example, someone may pressure you with a sense of urgency to click on a link that will install spyware on the user's computer. The emails and documents sent by these criminals may appear legitimate, so LHA users should note that small inconsistencies such as missing area codes, different letterhead, misspelling, unfamiliar emails, or new people signing the document are a "red flag" and should trigger a high level of scrutiny.

Cyber fraud can cause financial loss, loss of data, high costs and loss of employee time, stress, and reputational harm. Regulatory compliance issues related to data protection and privacy also can create burdensome and expensive legal fines and penalties, as well as notification requirements. Even more concerningly, Ransomware Attacks encrypt the victim organization's data and will provide a decoding key only when a financial demand is paid. These attacks will paralyze your data and disrupt your LHAs operations if it isn't able to recover the data quickly, whether by paying the ransom or setting up a new system from a back-up of uncompromised data.

LHAs should know that cyber-attacks don't just occur through computers; social engineering can also come through phone calls, text messages, and mail and even by someone visiting the LHA who has unauthorized access to computers and passwords. Given new cyber-crime trends, LHAs should be aware of and on watch for common real estate scams including wire transfer fraud, Deed fraud (such as the recent attempt to foreclose on Graceland mansion with a falsely recorded deed), and rental listing scams, where a fraudster may pretend to be the LHA.

How can the LHA protect itself?

Ransomware attacks and cyber-crime have only accelerated since the pandemic, as the widespread adoption of remote work has created more opportunity to hack into LHAs networks by using personnel's smart phones and computers as an entry point into the LHAs secure network. This danger is why LHAs need to have a strong computer use policy, segregated networks, and personal and work passwords should never be the same.

According to the non-profit National Cybersecurity Alliance the top four ways to stay safe online are:

1. Use strong passwords
2. Turn on multifactor authentication
3. Recognize and report phishing
4. Update software regularly

Strong Email Security and Passwords:
Email is usually the easiest way that cyber criminals can get into the LHA's data. Good practices and employee training are crucially important. Every LHA should have a secure email portal, and work toward migrating away from email names that include AOL, Hotmail and Yahoo. Business and personal email should not be intermingled. All personnel should have their own unique email, and system login and email passwords should not be shared. Nothing is more vulnerable than a weak password, so employees should use strong passwords which are changed regularly.

Multifactor Authentication:
Even stronger protection will come with the use of multi-factor authentication. An LHA should only allow system access to those employees who require it, and the list of system users who are authorized should be reviewed periodically. The LHA also must remove login credentials from employees no longer in your organization.

Beware of Phishing and Social Engineering Attacks:
Whether on email or when using the internet, an employee should always be alert and attentive to links before they click on them. Red flags include misspellings, the domain does not match the company, foreign domains, the brand name is in the URL but not part of the domain name. The user should hover over redirect links to ensure that they are from a trusted source and not a suspicious domain name.

Employees can be trained regarding suspicious emails and provided with a way to report phishing emails, and then double delete them. When a suspicious email, link or transaction request is received, LHA staff should take steps that may include elevation to a supervisor, checking in with a trusted contact number for the vendor, notifying the LHA's IT department if applicable, or doing more due diligence work.

Update Software Regularly:
Software updates are provided to ensure that loopholes and areas of security risk are made stronger. However, the user needs to update their operating software or other systems regularly to ensure that these problems are fixed. It is important to patch your software whenever there is an update, but you can automate this process by checking off automatic updates in your system settings. However, if your LHA is operating obsolete systems, it may be necessary to retire them if they cannot be made acceptably safe.

Technical Aspects:

- Data in the LHA's computer systems needs to be regularly backed up to a safe server; fortunately, this process is much easier now with the use of cloud-based data services.

- LHAs should maintain an inventory of their systems and closely monitor all device endpoints on their data network, including printers and remote connection devices. Cameras and digital speakers should have their default passwords changed and ideally operate on a separate network that does not access confidential LHA data.

- Mass data storage devices accessible through USB ports present serious risks, including malware and accidental data leaks, prompting many LHAs to restrict access to these devices. It's crucial to only trust USBs from reputable manufacturers and avoid using them on unknown devices to mitigate potential threats.

- Government agencies are encouraged to implement a "zero trust architecture" in their systems which will provide computer users with access only to the functions of the computer system which are necessary to perform their jobs, as well as implementation of redundant back-ups and systems that ensure that the damage is contained if one element of the system fails or is compromised.

Additional Protection Measures:

- ⓘ Financial employees should have procedures both for requesting and sending funds that allow the person they are doing a transaction with to know that it is legitimate. Any request for a change of name, contact information, or bank account numbers should be heavily scrutinized and confirmed so the LHA is sure the change is legitimate.

- ⓘ Electronic financial transactions, whether online banking or wire transfers, must be done with the utmost vigilance. Implementing positive pay systems with your LHAs banking partner will protect your LHAs accounts from being drained by counterfeit checks and also help with managing your cash flow.

- ⓘ Local Housing Authorities (LHAs) should monitor their digital footprint by regularly reviewing their websites and social media accounts to make sure they have not been spoofed and detect potential hacks. It's crucial to maintain strong passwords and update them regularly, particularly during staff changes.

- ⓘ Artificial Intelligence tools can also compromise security and confidentiality. LHAs should educate employees about the impact of their digital activities, including the use of Artificial Intelligence tools, which could lead to data breaches or the misuse of confidential information. Employees should avoid inputting sensitive data into tools like ChatGPT to prevent exposure to risks.

Free Expert Help is Available:
Reducing your LHA's vulnerability to a cyber-attack will require training, policies and attention to your computer systems, software and hardware. There is a resource that can assist with this work which is available to LHAs at no cost. The Commonwealth's Executive Office of Technology Support and Services has a program called the Cybersecurity Health Check Program which is offered through the Office for Municipal and School Technology. LHAs can apply for assistance with Policies & Procedures, Cybersecurity and other services to assess vulnerabilities, review remote access and resource allocation, vendor management review or a security report card and plan. This work will be done through vendors that are included in the ITS-78 Statewide Contract. Once an LHA has completed a risk assessment it will be eligible to apply for assistance through the Municipal Cybersecurity Awareness Grant Program. To learn more, you can watch this video or read this FAQ.

What should the LHA do if it Experiences a Data Breach?

If your LHA experiences a data breach you will need to take immediate action. The first steps that the LHA will need to take are to secure operations; fix system vulnerabilities and notify appropriate parties. While an LHA optimally should have its own plan to put into effect if it suffers a cyber-attack, a good guide to follow is the FTC's Data Breach Response: Guide for Business. Generally, the LHA will have to complete many steps which are briefly outlined below.

1) Secure your operations
   a) Hire experts including a data forensics team and an attorney with privacy and data security experience. (Category 4 in the ITS-78 Statewide Contract).
   b) Secure the LHA's physical and data assets. You will need to take all affected equipment offline but do not shut off or reboot your equipment until a forensic expert has evaluated the system.
   c) Review your digital footprint and financial accounts for fraud or intrusion.
   d) Do not forget to interview the people who discovered the breach and preserve evidence.

2) Fix Vulnerabilities
   a) Work with your experts to get your systems back up but also investigate how it can be made more secure, methods may include encryption, stronger password policies, network segmentation, and limiting access to system resources and data.

b) Train your employees with a focus on how to avoid similar incidents in the future.
c) Develop a communication and recovery plan.

3) Notify Appropriate Parties
   a) Notify EOHLC (both your HMS and Risk Manager (sarah.oleary@mass.gov)
   b) and other program partners
   c) Notify Law Enforcement including your local police, and if recommended by the local police the FBI or the US Secret Service. If mail fraud was involved the US Postal Inspection Service should also receive a report.
   d) Notify other affected businesses such as vendors and consultants whose financial information may have been compromised.
   e) Notify individuals including employees, tenants, applicants if confidential data was accessed.
   f) Contact your attorney and notify the Commonwealth of Massachusetts and other agencies who the data breach may have triggered notification requirements for.

What Steps Should your LHA Start With?

Because of the level of risk and potential damage to your LHA associated with the cybersecurity threat, EOHLC asks LHAs to take immediate action to help improve the security of your people, processes and technology. EOHLC recommends that all LHAs should take five actions as soon as possible to harden their defenses against cyber-crime.

1) **Discuss this PHN both with their employees and their Boards.** Note that LHA Boards can meet to discuss cyber prevention methods in closed sessions, using the Executive Session purpose to "discuss the deployment of security personnel or devices, or strategies with respect thereto." Together with this meeting employees should be provided with training information regarding the importance of password strength and integrity, safety on the internet and avoiding social engineering and phishing scams. We have created a packet of information that you can use for this purpose. Some free training links are included in the attachment to this PHN and many vendors offer excellent training services for a fair cost. This meeting will also be a good time to reinforce confidentiality laws and best practices with your staff.

2) **All Executive Directors should review all 5 modules of the Minimum Baseline of Cybersecurity for Municipalities on the Mass Cyber Center Website** (Introduction, Goal 1, Goal 2, Goal 3, and Goal 4). Completing all five modules will take less than two hours and give the ED a good level of mastery of the minimum baseline of cybersecurity for the LHA. After completing the training, the ED should decide how to train their employees to identify cyberthreats and implement best practices to secure the LHAs data.

3) **Ensure all personnel accessing LHA systems are using their own individual user ID and password** that passwords are strong and long and require regular updating and that computers will sleep and require a password to reactivate after a period of inactivity.

4) **Confer with your LHA's financial team,** including your banker and accountant, to ensure that all reasonable security measures for your organization are in place and determine what steps and policies should be added. If positive pay systems for check reconciliation are available your LHA should take advantage of them. Finance employees should set up procedures to prevent fraud in financial transactions.

5) **Evaluate if your LHA should participate** in the free Cyber Security Health Check Program described above.

EOHLC Technical Assistance
If you have any questions about this Public Housing Notice, have experienced a cyber security breach or need assistance connecting with resources, please call or email Risk Management Specialist, Sarah O'Leary, at sarah.oleary@mass.gov or (857)262-1170. Sarah can also help you assess whether your LHA would be eligible to obtain cyber-insurance coverage.

Cybersecurity PHN Attachment #1

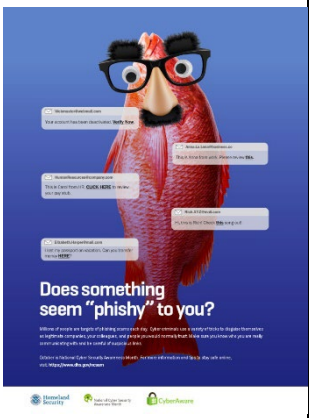
Information Security Training Resources for LHAs

EOHLC recognizes that LHAs have different staffing levels and technical capacities, and that training can be costly both in terms of the training material as well as the staff time dedicated to the training. We have identified some information security training resources which may be helpful to improve employee awareness and knowledge regarding cyber safety practices and work to offer LHAs additional training sessions on cybersecurity topics.

Given the inherent cyber threat and benefits to the LHA, EOHLC recommends that all LHA employes should be provided with training information regarding the importance of password strength and integrity, safety on the internet and avoiding social engineering and phishing scams. We recommend that the onboarding of new employees should include information regarding cyber training.

Your LHA can develop formal policies regarding cyber fraud and an emergency plan for response if your LHA becomes the unfortunate target of a cyber-attack. We strongly recommend that LHAs participate in the **free** Cyber Security Health Check Program which will qualify the LHA to apply for cyber security improvement grant funding.

Posters and Handouts



A PDF binder with the illustration and other selected posters and tip sheets accompanies the PHN.

EOTSS Protect Yourself Against Phishing Scams

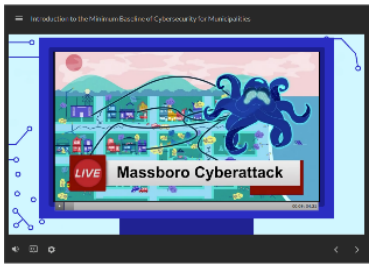
Massachusetts Comptroller, Fraud and Cybersecurity handout

CISA Protect Your Center from Ransomware customizable poster

CDSE Cybersecurity Posters

Information Security Training

EOTSS Training video on Anatomy of an Email – Spotting the Red Flags of Social Engineering (10 minutes)



MassCyberCenter 5 training modules of the Minimum Baseline of Cybersecurity for Municipalities (Introduction, Goal 1, Goal 2, Goal 3, and Goal 4). **This is highly recommended and will take less than 2 hours to provide EDs and other key LHA staff with a high degree of mastery.**

Cyber Defenders Interactive Training Game by HAI Group. In addition to this free training, LHAs with federal programs may have access to specialized cyber-awareness training modules through the HAI Group portal. https://resources.haigroup.com/cybersecurity-resources.

US Office of Inspector General Legal Services Corporation Cyber Security Resources Portal

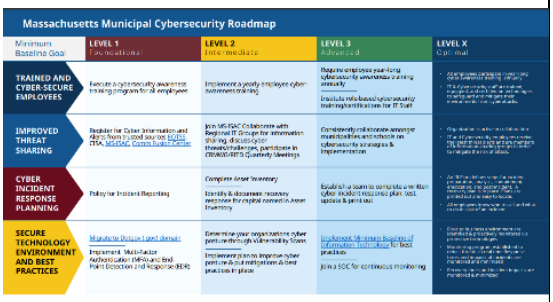
Government Technology Training video on Empowering Government with a Cyber-Aware Workforce with William Cole, Chief Technology Officer, EOTSS

Wizer Security Awareness Training: Free Security Awareness Training Playlist on YouTube.

Policies

EOTSS Policies, Standards and Guidelines

Massachusetts Municipal Cybersecurity Roadmap



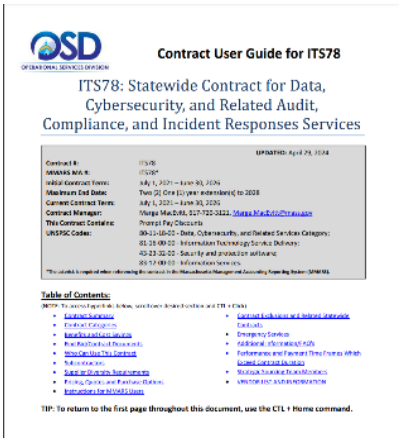
Office of Inspector General, Positive Pay Systems to prevent checking account fraud

Risk Assessment and Response Resources

EOTSS Office for Municipal and School Technology Cybersecurity Health Check Program

Federal Trade Commission Data Breach Response, A Guide for Business

CISA I've Been Hit by Ransomware Response Checklist



Commonwealth of Massachusetts, Statewide Contract for Data, Cybersecurity, and Related Audit, Compliance, and Incident Response Services. ITS78, Vendor list is PNH Attachment #2

National Cybersecurity Alliance Securing Smart Speakers and Digital Assistants

National Cybersecurity Alliance What to Do If Your Business Facebook is Hacked

The White House Executive Order on Improving the Nation's Cybersecurity

Cybersecurity PHN Attachment #2

Vendor List for Statewide Contract

June 2, 2021

Intent to Award Notification
Statewide Contract ITS78 for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services
COMMBUYS Bid # BD-21-1080-OSD03-SRC01-59288

The Strategic Sourcing Team (SST) for Statewide Contract ITS78 for Data, Cybersecurity, and Related Audit, Compliance, and Incident Responses Services extends their thanks to each Bidder for responding to the ITS78 Bid Solicitation. This is a Qualified List contract and as such, was not scored. Bidders having the required qualifications and meeting the RFR requirements and specifications for each applicable Category were selected for award in that Category.

Category 1: Full range of data, cybersecurity audits, compliance reviews and related consulting services

Company Name
7T LLC dba Arcas Risk Mgmt
JANUS Software, Inc., d/b/a JANUS Associates
Verizon Business Network Services LLC on behalf of MCI Communications Services LLC
Accenture LLP
Bulletproof Solutions, Inc.
CBTS
CDW Government LLC (CDW•G)
Lumen Technologies Group
CGI Technologies and Solutions Inc.
CitiusTech Inc.
Compass IT Compliance, LLC
CyberForce|Q, LLC
Data Ethics, LLC.
Deloitte & Touche, LLC
Digital Lantern, LLC
Eight Eleven Group
Ernst & Young U.S., LLP
Global Solutions Group, Inc.
Guidehouse LLP
Harbor Networks
HUB Technical Services, LLC.

Category 2: Risk assessments as they relate to internal and external (3rd party) components

Company Name
7T LLC dba Arcas Risk Mgmt
JANUS Software, Inc., d/b/a JANUS Associates
Verizon Business Network Services LLC on behalf of MCI Communications Services LLC
Accenture LLP
Bulletproof Solutions, Inc.
CBTS
CDW Government LLC (CDW•G)
Lumen Technologies Group
CGI Technologies and Solutions Inc.
CitiusTech Inc.
Compass IT Compliance, LLC
CyberForce|Q, LLC
Data Ethics, LLC.
Deloitte & Touche, LLC
Eight Eleven Group
Ernst & Young U.S., LLP
Global Solutions Group, Inc.
Guidehouse LLP
Harbor Networks
HUB Technical Services, LLC.
INNO4 LLC

INNO4 LLC
Kuma, LLC
KPMG, LLP
Netizen Corporation
NuHarbor Security
NWN Corporation
O'Connor & Drew, P.C., d/b/a OCD Tech
Presidio Networked Solutions LLC
Q.E.D., Inc. d/b/a QED National
MediTechSafe, Inc. (d.b.a. ResiliAnt)
RetroFit Technologies, Inc.
Rolta Advizex Technologies LLC
Spruce Technology, Inc.
Stealth-ISS Group® Inc.
Firstworld, Inc DBA Terminal Exchange
Tevora Business Solutions, LLC
Edward Davis, LLC d/b/a The Edward Davis Company
The Silicon BlackGroup, LLC
Toss Corporation
Windwalker Group, LLC

INTRASYSTEMS, INC.
Kuma, LLC
KPMG, LLP
Netizen Corporation
NuHarbor Security
NWN Corporation
O'Connor & Drew, P.C., d/b/a OCD Tech
Presidio Networked Solutions LLC
Q.E.D., Inc. d/b/a QED National
RetroFit Technologies, Inc.
Rolta Advizex Technologies LLC
Spruce Technology, Inc.
Stealth-ISS Group® Inc.
Firstworld, Inc DBA Terminal Exchange
Tevora Business Solutions, LLC
Edward Davis, LLC d/b/a The Edward Davis Company
The Silicon BlackGroup, LLC
Toss Corporation
Windwalker Group, LLC

Category 3: Cybersecurity testing and readiness services

Company Name
7T LLC dba Arcas Risk Mgmt
JANUS Software, Inc., d/b/a JANUS Associates
Verizon Business Network Services LLC on behalf of MCI Communications Services LLC
Accenture LLP
Blue Spruce Technologies, Inc
Bulletproof Solutions, Inc.
CBTS
CDW Government LLC (CDW•G)
Lumen Technologies Group
CGI Technologies and Solutions Inc.
CitiusTech Inc.
Compass IT Compliance, LLC
Custom Computer Specialists, Inc.
CyberForce|Q, LLC
Data Ethics, LLC.

Category 4: Information security and cybersecurity incident response services

Company Name
7T LLC dba Arcas Risk Mgmt
Verizon Business Network Services LLC on behalf of MCI Communications Services LLC
Accenture LLP
CDW Government LLC (CDW•G)
Lumen Technologies Group
CitiusTech Inc.
Custom Computer Specialists, Inc.
CyberForce|Q, LLC
Data Ethics, LLC.
Deloitte & Touche, LLC
Ernst & Young U.S., LLP
Global Solutions Group, Inc.
Harbor Networks
INTRASYSTEMS, INC.
KPMG, LLP

Deloitte & Touche, LLC
Eight Eleven Group
Ernst & Young U.S., LLP
Global Solutions Group, Inc.
Guidehouse LLP
Harbor Networks
HUB Technical Services, LLC.
INNO4 LLC
INTRASYSTEMS, INC.
KPMG, LLP
Netizen Corporation
NuHarbor Security
NWN Corporation
O'Connor & Drew, P.C., d/b/a OCD Tech
Presidio Networked Solutions LLC
Q.E.D., Inc. d/b/a QED National
RetroFit Technologies, Inc.
Rolta Advizex Technologies LLC
Spruce Technology, Inc.
Stealth-ISS Group® Inc.
Firstworld, Inc DBA Terminal Exchange
Tevora Business Solutions, LLC
Edward Davis, LLC d/b/a The Edward Davis Company
The Silicon BlackGroup, LLC
Toss Corporation
Windwalker Group, LLC

Netizen Corporation
NWN Corporation
Presidio Networked Solutions LLC
Rolta Advizex Technologies LLC
Spruce Technology, Inc.
Stealth-ISS Group® Inc.
Firstworld, Inc DBA Terminal Exchange
Tevora Business Solutions, LLC
Edward Davis, LLC d/b/a The Edward Davis Company
Toss Corporation