



Commonwealth of Massachusetts
**EXECUTIVE OFFICE OF HOUSING &
LIVABLE COMMUNITIES**

Maura T. Healey, Governor ♦ Kimberley Driscoll, Lieutenant Governor ♦ Juana Matias, Secretary

Public Housing Notice 2026-12

To: LHA Boards and Staff, Fee Accountants
From: Fatima Razzaq, Assistant Undersecretary of Public Housing and Rental Assistance
Date: October 14, 2026
Re: PHN 2026-12: Cybersecurity Alert: Protecting LHA Funds and Financial Accounts

What You Need To Know

- LHAs should be aware of cyber-security measures, ensure staff have cybersecurity awareness training, disable inactive employee accounts; implement password updating and complexity requirements, as well as multi-factor authentication.
- Personal Financial Transactions and LHA financial transactions should not occur on the same device.
- Conduct LHA financial business only on LHA-owned or LHA-managed devices; keep personal shopping and financial activity off LHA devices; and don't access LHA financial accounts on personal devices.
- Use systems and policy to protect your LHA, enroll if your bank offers positive pay services; all requests to change payment information should be independently verified from original contract documents, and require secondary approval from another person;
- Immediately report suspected fraud to your financial institution, law enforcement, and EOHL.

October is Massachusetts Cybersecurity Awareness Month

October is Cybersecurity Awareness Month and EOHL wants to remind LHA Board members and staff that LHAs are vulnerable targets of cyber criminals and that everyone needs to play their part to protect public funds and data. Cybercriminals increasingly rely on ordinary human activity - clicking a link, downloading an application, responding to an urgent message, or using a compromised device - to gain access to organizational systems and financial accounts.

A recent "[malvertising](#)" cyber-attack at an LHA began when an LHA employee clicked a shopping link on Facebook, inadvertently downloading malware on an LHA employee's phone. The malware compromised the employee's log-in credentials for the LHA's payroll account. **Within just two days, criminals changed the LHAs log-in and bank account information, and diverted more than \$30,000 through multiple unauthorized transactions.**

This October, EOHL recommends that every LHA review its cybersecurity practices with staff and its Board. [Mass Cyber Center provides this excellent free training resource](#). LHAs are advised to promptly revoke email and network access upon separation from employment and suspend or restrict access during periods of inactivity or when the employee cannot connect through an approved, secure method. LHAs should also confirm that appropriate safeguards are in place for financial transactions, and remind employees to stop and verify before clicking, downloading, or changing payment information. More detailed Cybersecurity information can be found at [EOHL Cybersecurity PHN 2024-12](#).

Think Before You Click!

Cybercriminals do not need to compromise an entire LHA network to steal public funds. They go “Phishing” using fraudulent emails, links, attachments, and even text messages to gain access to your technology. A compromised phone, computer, password, email account, or authenticated session may provide an opportunity to access financial systems or redirect legitimate payments. Malware can be introduced through malicious advertisements, links, attachments, downloads, or applications that appear legitimate. Always think before you click, hover over links before clicking to ensure that it is going to a known website. If you think you may have entered a compromised website notify your computer vendor immediately.

This risk applies to ordinary LHA transactions, including payroll, utilities, credit cards, vendor invoices, banking, and other electronic payments. **Remember, any suspected compromise involving LHA funds, financial systems, credentials, or payment information should be reported to EOHLC immediately.**

Keep LHA Business and Personal Activity Separate

LHA financial transactions and other sensitive LHA business should only be conducted on LHA-owned or LHA-managed devices. Personal shopping and financial transactions should never be conducted on LHA devices which are also used for LHA financial transactions.

- **Do not use personal devices for LHA financial business.** Do not access or authorize LHA payroll, banking, credit card, utility, accounting, vendor-payment, or other financial systems from a personal phone, tablet, or computer.
- **Do not shop on LHA devices.** Do not use an LHA laptop, desktop, phone, or tablet for personal online shopping, banking, payment applications, promotional offers, coupons, or similar personal transactions.
- **Keep credentials separate.** Do not use personal email or personal accounts for LHA business, and don’t repeat personal passwords on LHA accounts, or vice versa.
- **Be careful with offers and downloads.** Limited-time offers, advertisements, QR codes, links, attachments, and downloads can be used to install malware or steal credentials.

EOHLC recognizes that carrying separate work and personal devices may be inconvenient. However, the risk of combining the two environments is greater: a compromised personal activity can expose a device used to access LHA systems. See [FBI Business Email Compromise](#) for further information.

Verify Before You Pay Or Make A Change

Never rely solely on an email, text message, or electronic request to change where LHA money will be sent.

- **Use fraud-control systems offered by your bank to safeguard LHA accounts.** Work with your financial institutions to set up protections such as [positive pay for checks issued by the LHA, this prevents counterfeit checks, and ACH Positive Pay and ACH filters or blocks](#), that will prevent misappropriation of electronic transfers such as payroll, utilities, credit cards, and vendor payments.
- **Independently verify changes.** Make it a policy to confirm any request to change a vendor bank account, payroll information, direct deposit instructions, mailing address, payment destination, or other financial information using contact information already known to the LHA - not the contact information in the request.
- **Two separate sources should confirm the change of information.** Changes to vendor or other payment destinations should be approved by a second authorized LHA employee or official before funds are released.
- **Use strong authentication.** Maintain individual user credentials, strong unique passwords, and multifactor authentication wherever available.

Report Suspected Fraud Or Cybercrime Immediately

Early reporting may improve the ability to stop or recover a fraudulent transfer and to contain the damage to a compromised account or device. Immediately contact the LHA’s bank or financial institution and, if funds have been transferred, request a recall or reversal and ask the bank to contact the receiving institution. Contact the LHA’s IT provider and preserve relevant emails, messages, transaction records, devices, and other evidence; do not delete or alter potential evidence. **Notify EOHLC straight-away** by informing your Housing Management Specialist and EOHLC Risk Management when the incident is discovered—not months later—so EOHLC can assist with response, recovery, insurance, legal, and other available resources. Also contact local law enforcement and report the incident to the FBI’s [Internet Crime Complaint Center \(IC3\)](#).