

Cybersecurity Training for Financial Teams

Purpose:

This training aims to raise awareness about the importance of cybersecurity in financial operations, as well as to provide practical guidance on safeguarding sensitive data, preventing financial fraud, and adhering to regulatory compliance standards.

Audience:

Individuals working within financial teams, including but not limited to:

- Staff responsible for managing financial transactions
- Financial officers or treasurers overseeing school or municipal finances
- Staff involved in purchasing or procurement processes
- Municipal or school board members who make financial decisions
- Any other personnel who have access to financial data or systems within the school or municipal administration

Outline of the Training:

- 1. General Cybersecurity for Financial Workers:** A comprehensive overview of cybersecurity practices tailored to the specific needs and responsibilities of financial professionals.
- 2. Common Forms of ACH Fraud:** Identification and mitigation strategies for prevalent forms of fraudulent Automated Clearing House (ACH) transactions in financial operations.
- 3. Business Email Compromises:** Understanding and preventing unauthorized access to financial data and transactions through compromised email accounts and communication channels.
- 4. Building Secure Human Controls:** Establishing robust procedures and protocols to minimize human error and enhance the security posture of financial operations.
- 5. Advanced Phishing Training:** Advanced techniques and strategies for recognizing and mitigating sophisticated phishing attacks targeting financial personnel and systems
- 6. Limiting the Documents You Provide Online:** Best practices for minimizing the risk of identity theft and fraud by restricting the amount of personal and financial information shared online.
- 7. Maintaining Payroll and Key Functions:** Cyber crimes may last weeks, how will you maintain key functions during multi-week cybersecurity outages.
- 8. Understanding IT and Finance Cooperation** for data protection
- 9. Supporting Remote work** for Financial Workers
- 10. Q&A Session**



NH Municipal Cyber Defense Program

The New Hampshire Municipal Cyber Defense Program (MCDP), managed by The ATOM Group, is a key initiative for enhancing New Hampshire's Cybersecurity Defense Services. Funded by the NH Department of Information Technology and the State and Local Cybersecurity Grant Program, it aims to protect public trust in technology by providing comprehensive Cybersecurity training.

The MCDP is critical to New Hampshire as it enhances cybersecurity readiness across municipal and public sector entities. This program stands out because it is customized based on the municipality's type, job description, and organization's existing cybersecurity readiness.

For more information, please contact:

Emily McGovern

Cyber Operations Specialist
NH Municipal Cyber Defense Program (MCDP)

Email:

emily@theatomgroup.com

Phone:

603.501.0003 x107

Website:

theatomgroup.com/mcdp



New Hampshire

DoIT

