TD Bank

Risk to Resilience: Cybersecurity Defense and Fraud Prevention Controls

NHLTA
May Conference 2026

FRAUD AWARENESS & PREVENTION

KATHERINE HECK
VICE PRESIDENT GOVERNMENT BANKING
TD BANK

Myths About Fraud

1. It has never happened here so our systems must **be adequately protected.**

2. **It only happens someplace else.**

3. **The loss is always covered by insurance.**

4. **There are sufficient controls in place.**

Your Bank Will Never...

- Call to ask for personal information
- Ask you to keep a secret or be dishonest
- Threaten to cancel your services
- Try to rush you into doing something
- Ask you to transfer money as part of an investigation
- Deposit money in your accounts without your knowledge
- Call or email to request remote access to your computer

Don’ts

- Do not access non-work related internet sites
- Do not use pop or flash drives
- Do not allow software downloads
- Do not click on hyperlinks
- Do not allow employees to add hardware or software
- Do not open an email from an unknown sender
- Do not use auto login features
- Do not share passwords and User Id’s
- Do not leave sensitive material out

Do's

Best Practices

- ✓ Talk to your bankers
- ✓ Timely bank reconciliations
- ✓ Secure check stock, signature stamps, statements
- ✓ Shred documents
- ✓ Educate - Update and review controls with employees
- ✓ Run random audits
- ✓ Use positive pay
- ✓ Use ACH debit block & filters
- ✓ Review insurance coverage

Online Best Practices

- ✓ Use dual controls
- ✓ Use dedicated treasury computer
- ✓ limit online access (site access)
- ✓ Limit authorities
- ✓ Change passwords often
- ✓ Sign off when done
- ✓ Update & Scan with anti-virus software
- ✓ Use a firewall

Use basic cybersecurity training. This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.

Identify available cybersecurity training resources. Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.

Stay current on cybersecurity events and incidents. This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.

Encourage employees to make good choices online and **learn about risks** like phishing and business email compromise.

Build a Strong Cybersecurity Culture

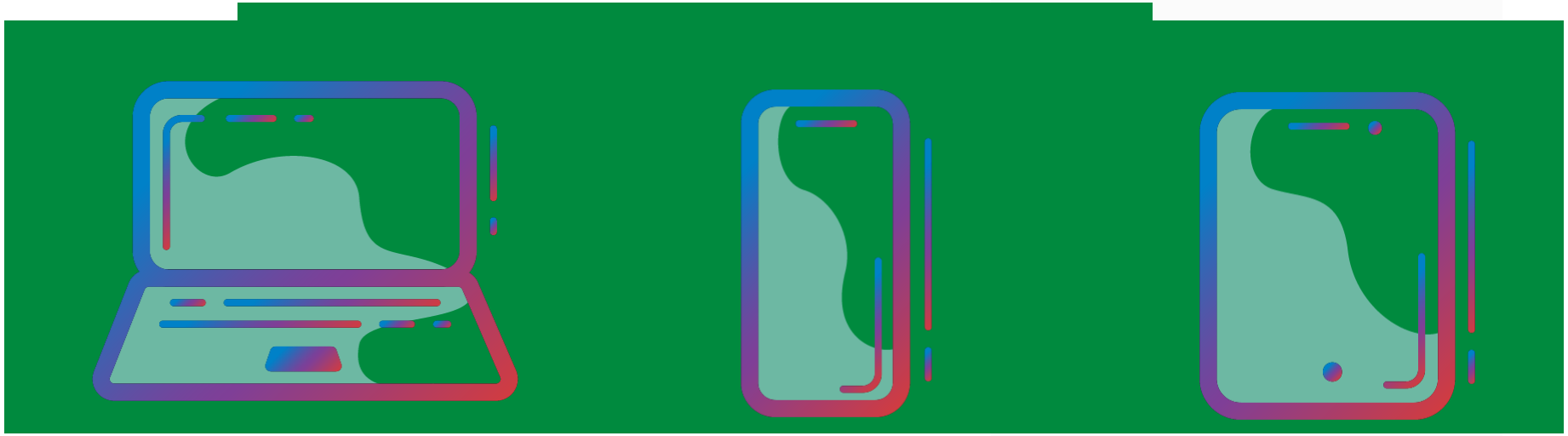
4 Easy Ways to Stay Safe Online

Use Strong Passwords and a Password Manager

Turn on Multifactor Authentication

Recognize and Report Phishing Attacks

Update Your Software



PAYMENT FRAUD LANDSCAPE

Protective Actions

Education:

- ✓ Train all staff, especially those with access to company assets and bank accounts

Prevention:

- ✓ Dual authentication
- ✓ Access and admin controls
- ✓ IT Security

Detection:

- ✓ Automation
- ✓ Reconciliation

TRUST | ADVICE | SECURITY

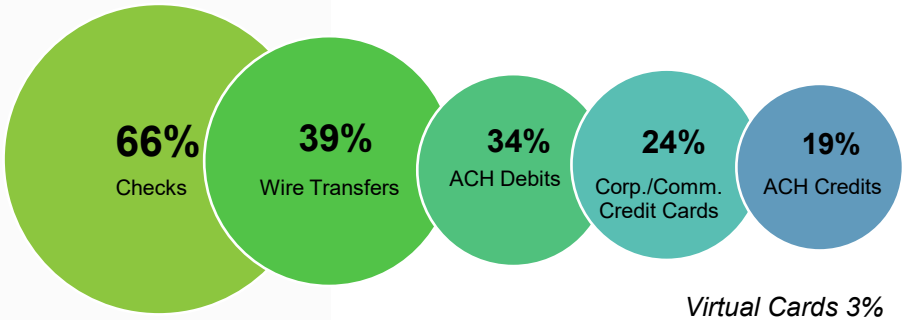
Targeting:

- 80% of governments targeted
- Susceptible regardless of size

Sources of Fraud:

- Business Email Compromise (61%)
- Outside Individual – forged check or stolen card (58%)
- Related Third Party - vendor or service provider (26%)

Payment Methods Targeted for Fraud:



Virtual Cards 3%
Faster & 3rd Party Pay 3%
eWallets, Crypto 2%

Source:
AFP 2021 Payments Fraud & Control Survey

Protective Actions:

- ✓ Refer to Ransomware Guide at CISA.gov
- ✓ Research and track groups, attacks, and new developments
- ✓ Review ransomware and attack stages provide by the Multi-State Information Sharing and Analysis Center (MS-ISAC)

Targets:

- Major organizations
- Third-parties
- Government Agencies
- Healthcare Practices

Ransomware Payments in 2023 surpassed $1B USD, the highest number ever observed

Extortionist Tactics:

- Search networks and steal data before they encrypt the system
- Select information is shared on "name and shame" sites

Fraud and cyber threats facing public libraries are escalating in frequency, sophistication, and financial impact.

The Library Threat Landscape

80% of U.S. public libraries faced some form of cybersecurity incident

73% surge in ransomware attacks on libraries in 2023 vs. prior year

$76K median loss per occupational fraud case in nonprofit organizations

10% of all occupational fraud cases occur in nonprofit organizations

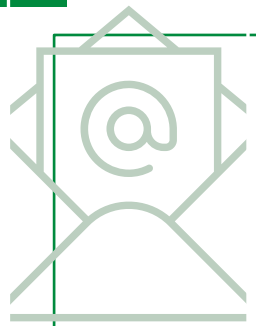
Sources: ACFE 2024 Report to the Nations · ALA Data · Cybersecurity in U.S. Public Libraries Survey (2020)

The Fraudsters are recruiting you!

When the fraudsters realize they cannot access your accounts by the old methods, by issuing Checks & debiting your account via ACH, in order to perpetuate fraud… they need you to participate.

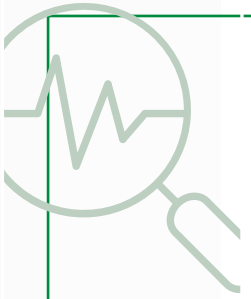
Every library — regardless of size — is a **target**.
Proactive controls and vigilance are your strongest defense.

Cyber Threats



Phishing:

- This involves sending fraudulent emails, often containing links to fake websites, to trick users into entering their credentials or personal information.

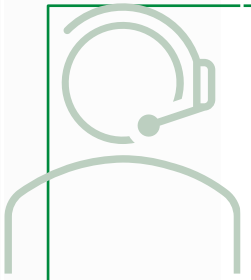


Spear-phishing attacksr:

refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. These types of attacks are aptly called “spear” phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

Smishing:

- This is a form of phishing that uses text messages (SMS) to lure victims into clicking on malicious links or providing information.



Vishing:

- This involves voice calls or voicemails to manipulate victims into divulging confidential information, often impersonating legitimate organizations.

Phishing & Ransomware Attacks

The two dominant cyber threats targeting public libraries today

Phishing

ENTRY POINT

- The **#1 delivery vector** for ransomware and credential theft attacks on libraries
- Common lures: fake overdue notices, spoofed vendor invoices, and fraudulent eBook login pages
- Staff targeted via emails impersonating ILS vendors, OCLC, or state library agencies
- **99%** of public libraries offer internet access — massively expanding the attack surface

#1 Attack Vector

VS

Ransomware

PAYLOAD

- Attacks on libraries **surged 73%** in 2023 versus the prior year
- 2024 incidents: Solano County — Apr Seattle Public — May Delaware Libraries — May
- Disables catalogs, circulation, patron records, email, and public websites simultaneously
- Recovery takes **days to weeks** and can cost hundreds of thousands in remediation

73% Surge in 2023

Phishing email arrives → Staff clicks → malicious link → Ransomware deploys → Systems locked

CYBER THREAT PROFILE

Business Email Compromise (BEC)

Payment Redirect Schemes

Fraudsters impersonate legitimate vendors and request bank account changes for payments, diverting funds to criminal accounts.

Director/Trustee/Other Person of Authority Impersonation

Attackers spoof library director or town manager emails to authorize emergency wire transfers or purchases — leveraging urgency and authority.

Cleveland Public Library Case

2024

Nearly **$400,000** redirected to a fictitious vendor after a spoofed email changed payment routing. Ohio Auditor found **no internal controls** to detect fictitious vendors. Full amount recovered via insurance and bank clawback.

Red Flags to Watch For

- ⚠ Urgent tone
- ⚠ Unusual payment changes
- ⚠ Email address variations
- ⚠ Bypass normal approvals

Sources: FBI IC3 Reports · Ohio State Auditor · ACFE 2024 Report to the Nations

KNOWLEDGE IS POWER

*"In a time of turbulence and change, it is more true now than ever that **knowledge is power**."*

-John F. Kennedy

Business Email Compromise is driven by the interception, and subsequent weaponization of contemporaneous and privileged information

BUSINESS EMAIL COMPROMISE (BEC)

DEFINITION OF BUSINESS E-MAIL COMPROMISE

- A Business e-mail compromise (BEC) is when a scammer **impersonates** a company employee or other trusted party, and tries to trick an employee into sending money, providing confidential information, etc.

- Emails are generally sent to the victims from **fake or compromised email accounts.**

- BEC attacks rely on impersonation and other **social engineering** techniques to trick people into interacting on the attacker's behalf.

- **Social Engineering -** The use of deception to manipulate people into performing actions or divulging information; usually through the exploitation of human error and taking advantage of trust in digital communications.

BUSINESS EMAIL COMPROMISE (BEC)

HOW BUSINESS E-MAIL COMPROMISE WORKS

- A BEC scam starts with **research**. An attacker will sift through publicly available information about your company from your website, press releases, and even social media posts. He/she might look for the names and official titles of company executives, your corporate hierarchy, and even travel plans from email auto-replies.
- Attackers often gain access to a company email account through **phishing**.
- Attempt to gain access to accounts belonging to the executives, HR, finance, accounting department, etc.
- To remain undetected, he/she might use **inbox rules** or change the reply-to address so that when the scam is executed, the actual user will not be alerted.
- The **attacker can monitor emails** in the company and wait until an opportune time to inject themselves and their scam into the conversation.

2023 FBI Internet Crime Complaint Center (IC3) Report

By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	$4,570,275,683	Extortion	
BEC	$2,946,830,270	Employment	
Tech Support	$924,512,658	Ransomware*	
Personal Data Breach	$744,219,879	SIM Swap	
Confidence/Romance	$652,544,805	Overpayment	
Data Breach	$534,397,222	Botnet	
Government Impersonation	$394,050,518	Phishing/Spoofing	
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	
Other	$240,053,059	Harassment/Stalking	
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	
Real Estate	$145,243,348	Crimes Against Children	
Advanced Fee	$134,516,577	Malware	
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

*Descriptors***			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1

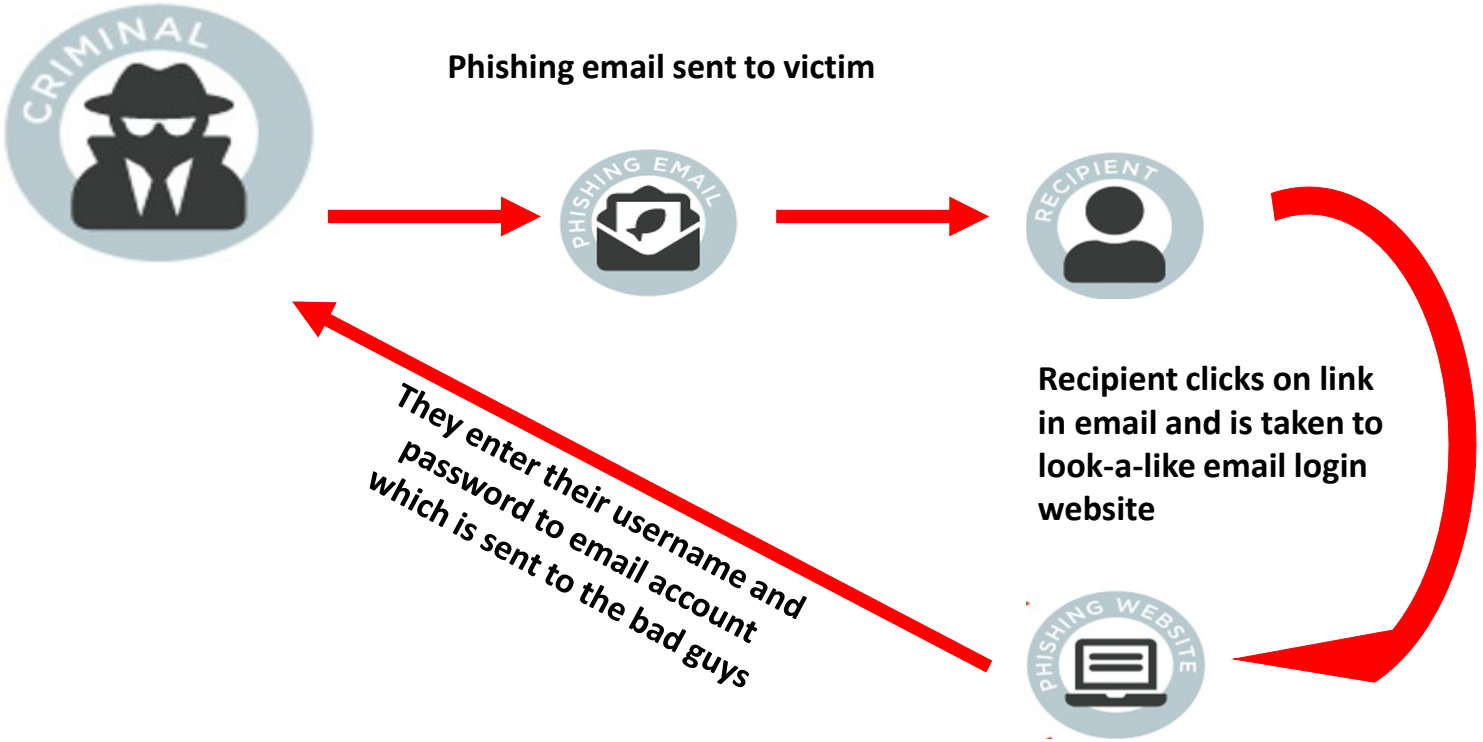
By Complaint Count

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		

*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

2023 FBI IC3 Report - https://www.ic3.gov

BEC IN ACTION



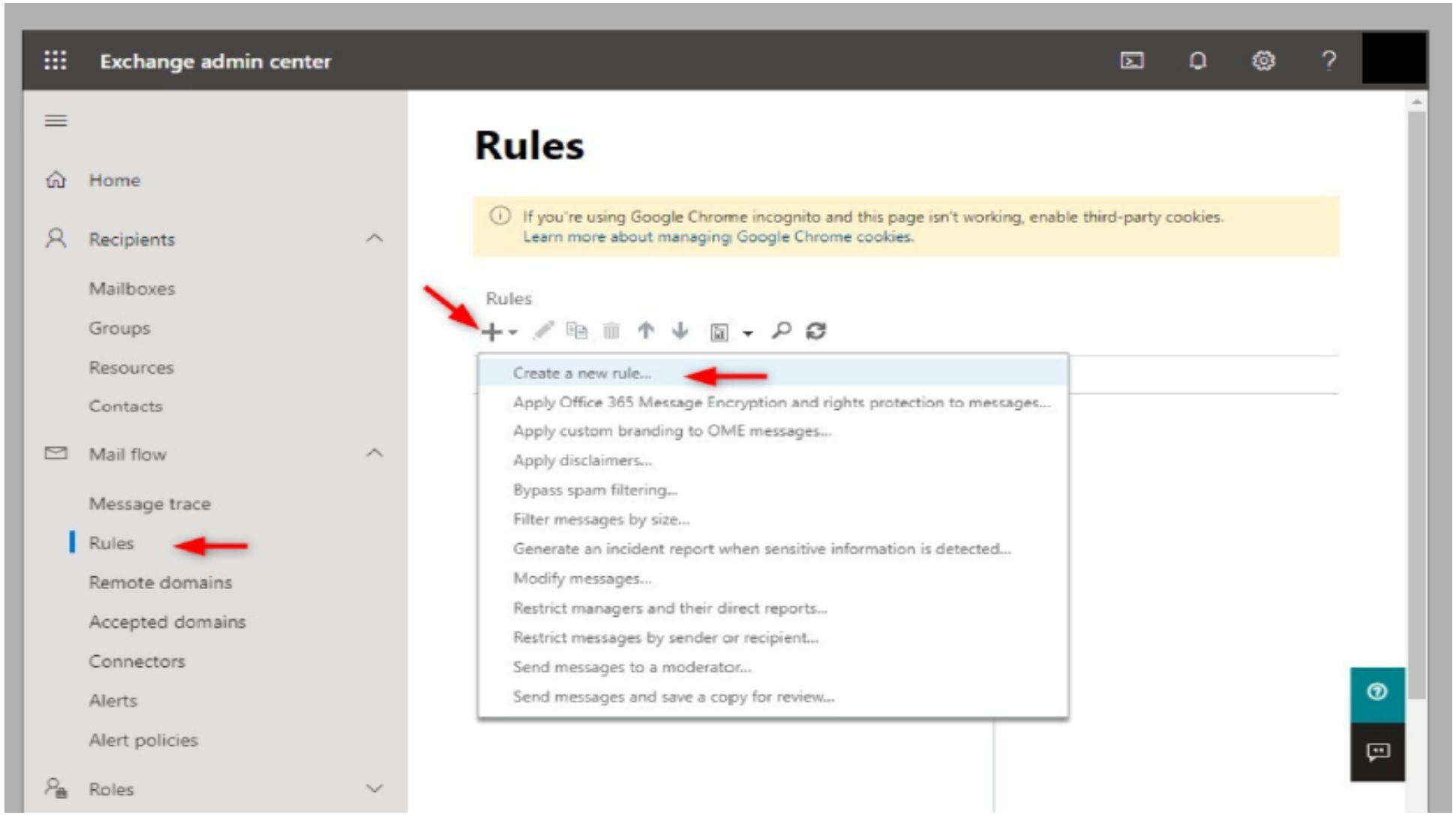
OPERATIONAL TACTIC – EMAIL RULES

Once the criminal actors gain access to email accounts, the most common form of surveillance is to set up email rules in the account settings to auto-forward, then delete the auto-forwarded emails to avoid detection.

Other than the email rule, **no evidence of the surveillance is visible**. This allows the actor to remotely monitor the account **even if the password is changed**

If the password or access method remains the same, the criminal actor will manipulate the victim's inbox to prevent detection or to further facilitate the fraudulent transactions

Intrusion Successful - Rules added



Spoofed Email Addresses

- Another common tactic is to create an e-mail with a spoofed look-a-like domain. For example, instead of john.smith@realcompany.com, the attacker might use:

john.smith@realc**0**mpany.com
john.smith@rea**1**company.com
john.smith@realco**rn**pany.com
john.smith@realcompany**s**.com
john.smith@real**l**company.com
john.smith@**gmail**.com

- If you do not pay close attention, it is easy to get fooled by these slight differences!

- Can cost the attacker less than $10 to create these (and that $10 is usually stolen)

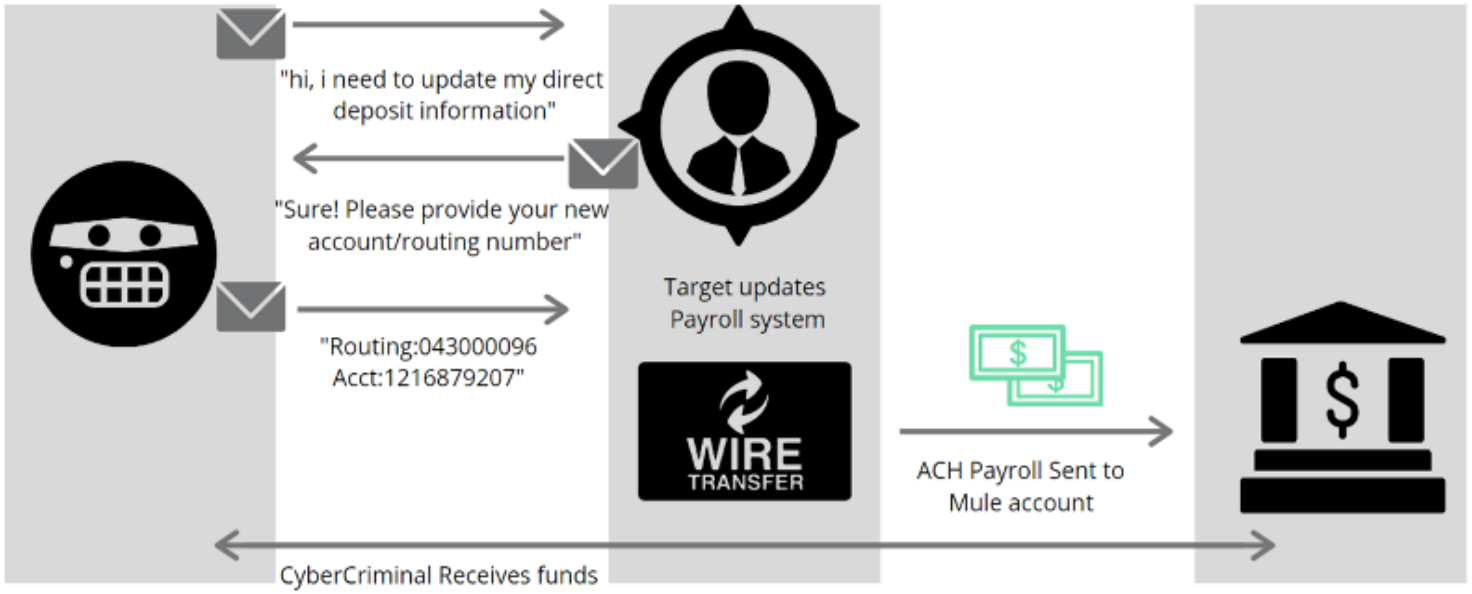
BEC in Action

PAYROLL DIVERSION / DIRECT DEPOSIT FRAUD

- Cyber criminals try to **redirect an employee's paycheck** to an unauthorized bank account under their control.

- Payroll diversion fraud often starts with **phishing emails.**

- **Focused on their targeting**. To succeed, these scams must correctly identify someone in the **HR or payroll department** to make changes to an employee's direct deposit information.



https://www.proofpoint.com/

Payroll Deposit Scam Mitigation

- Remove ACH Direct Deposit forms from publicly available websites.
- Consider removing accounts payable and HR personnel email addresses from publicly available websites.
- Communicate any payroll changes in person or through a secure, official channels. Don't accept payroll change requests from personal email addresses.
- **Be wary of requests to utilize financial institutions that have prepaid debit card services.**
- Multiple parties, including the payroll administrator, should verify and approve any request to change direct deposit information. This multi-step approval process can prevent unauthorized changes.
- Set up internal alerts for any changes in bank account details. Make sure payroll system end users are trained to monitor for changes to direct deposit information.

BEC Incident Mitigation Road Map

- Trusted devices
- Multi-Factor Authentication (MFA)
- Trusted IP addresses – “Whitelist IP”
  - Geofence to local region
  - Block known anonymizer IPs
  - Block certain ISPs
- Ensure that logs are being retained for at least 30 days
  - Often bad actors can be monitoring accounts for months prior to the attack so the longer the data is preserved the better
- Verbally verify payment changes using a previously known/**verified phone number**
- Training – Tabletop Exercises
- Purchase/maintain similar domain names

HAVE A PLAN

Vendor Fraud & Procurement Schemes

Common patterns exploiting weak purchasing controls in public libraries

Ghost Vendors

Fictitious companies created by insiders to bill for services never rendered. Libraries with small purchasing departments are especially vulnerable.

INSIDER THREAT

Kickback Schemes

Staff accept gifts, gifts in kind, bribes from vendors in exchange for awarding contracts without competitive bidding. Common where a single employee controls procurement.

NO-BID CONTRACTS

Billing Fraud

Vendors overbill for supplies, subscriptions, or services. 31% of small nonprofit fraud cases involve billing fraud.

31% — ACFE 2024

Duplicate Payments

Weaknesses in accounts payable allow duplicate invoices to be paid without detection. Automated controls and independent review are essential.

REQUIRES AUTOMATION

Source: ACFE 2024 Report to the Nations — Occupational Fraud in Nonprofit Organizations

Internal

Examples

A timeline of major theft cases targeting library with real financial impact

1990S–2017

Carnegie Library of Pittsburgh

Archivist **Gregory Priore** and dealer **John Schulman** stole **300+ rare items** worth **$8 million** over 25 years — including Newton's *Principia Mathematica*, 276 hand-colored Blaeu Atlas maps (1644), and incunabula. Both pled guilty in 2020.

$8M in losses

25 years undetected

2004–2011

Saugus Public Library, MA

Employee **Linda Duffy** diverted **$965,742** in donations, fines, and GE Foundation matching funds. Forged **90 checks** with a supervisor's signature. Sentenced to **5 years in federal prison**.

$965,742 stolen

90 forged checks

Insider Access Risk

Trusted employees with **key access**, knowledge of security gaps, and ability to **manipulate inventory records** pose the greatest risk to special collections. **Defense in depth** — multiple overlapping security measures — is essential.

Physical Controls

Regular Inventories

Multi-Person Access

Massachusetts — Cases & Response

Saugus Public Library Embezzlement (2004–2011)

Employee Linda Duffy stole **$965,742** over 7 years — diverting charitable donations and fines to a decoy bank account, forging **90 checks**, and defrauding the GE Foundation of **$400K+** in fake matching donations. Sentenced to **5 years federal prison** plus full restitution (FBI/DOJ).

Boston Public Library Ransomware (August 2021)

A cyberattack caused a **system-wide outage** affecting online services, public computers, and printing across **25+ branches** for a full week. No evidence of data theft, but demonstrated the vulnerability of large urban library systems to ransomware.

MBLC Cybersecurity Initiative

Massachusetts Board of Library Commissioners awarded **$181,093** in state cybersecurity grants to **eight library networks** — funding VPN, MFA, backup infrastructure, and recovery strategies to improve resilience statewide.

State Auditor Performance Audit (2023)

Performance audit of MBLC covering **2020–2022** reviewed internal controls, compliance, and financial management of state library grant programs — reinforcing oversight standards for Massachusetts public libraries.

Sources: FBI/DOJ Case Records • ALA Cybersecurity Reports • MBLC Grant Records • Massachusetts State Auditor

Connecticut & Rhode Island

State-level audit findings and systemic cyber risk across interconnected library networks

Connecticut

STATE LIBRARY AUDIT FINDINGS

⚠ **$215M in assets not properly accounted for**

23 items with missing or incorrect locations (**$94,245**)

5 items not physically tagged (**$9,764**)

8 museum objects not accessioned into inventory

Donated assets **not assigned acquisition values**

State Auditors issued **5 findings** with **4 repeat findings** (FY 2023–2024)

⚠ Critical lesson: Inventory control failures create conditions for undetected theft — repeat findings signal systemic weakness.

Rhode Island

CONCENTRATED CYBER RISK

Small, interconnected library networks — a single breach could cascade across consortium systems

Libraries must align with **state cybersecurity frameworks** for unified defense

Vendor contracts should include **security requirements** and incident response provisions

Consortium-shared systems amplify the blast radius of any compromise

SHARED REGIONAL CHALLENGES

Aging IT infrastructure across all six states

Limited cybersecurity budgets

Dependence on shared systems that **amplify breach impact**

All New England states share systemic vulnerabilities — aging infrastructure, lean staffing, and consortium dependencies mean a breach in one library can threaten an entire regional network.

Across the state, *Friends of the Library* groups make an extraordinary impact- contributing both dedicated volunteers and critical financial support to their local library.

Friends Group Vulnerabilities

Volunteer-Led Operations

Friends groups often rely on volunteers **with limited financial training and cyber/fraud training** creating opportunities for fraudsters.

Cash-Intensive Fundraising

Book sales, bake sales, and event proceeds handled in cash with— require additional checks and balances- **keep cash secure at all times!** (See 2/2026 West Lebanon Girl Scout Cookie cash box theft at Walmart)

Lack of Segregation of Duties

Often a single treasurer handles receiving, recording, depositing, and reconciling funds — the **#1 fraud risk factor** identified by the ACFE. See 4/30 /26 Union Leader Cover Page Article

Common Schemes

Check tampering, skimming from book sale proceeds, unauthorized credit card use, fictitious reimbursements. **74% of nonprofit fraud stems from management/officer positions.**

Internal

Resources

Free Resources

Assessments, Workshops, Exercises
https://www.cisa.gov/how-we-can-help-region-resources

State & Local Cybersecurity Grant Program
https://www.doit.nh.gov/cybersecurity/state-and-local-cybersecurity-grant-program

Training, Incident Response Plan Development
https://nhprimex.org/explore-training/category/online/

Printed Materials, Training, Exercises
www.theatomgroup.com/mcdp

ADDITIONAL RESOURCES AT YOUR FINGERTIPS

Protect yourself.

Stay up to date on common fraud and scams.

- Understand what to watch out for.
- Know how to respond.
- Access tools and resources to help along the way.

Scan the QR code below to get started.

Or visit: td.com/fraudprevention

TD Bank
Fraud Control
TD Commercial Banking Security Center

American Bankers Association (ABA)
banksneveraskthat.com

Association for Financial Professionals (AFP)
2024 AFP Payments Fraud and Control Survey Report

Cybersecurity & Infrastructure Security Agency
CISA Insights
CISA Cyber Hygiene Services

National Council of Information Sharing & Analysis Center (ISAC)
National ISACs

National Institute of Standards and Technology
NIST Cyber Framework

SAFE-guarding Your Library- The Security Guide

The Human Firewall | What You Can Do

Takeaways | Actionable Tips & Calls to Action

Online Security

- ❑ Never divulge your user credentials to anyone
- ❑ Bookmark banking sites – don't rely on search
- ❑ Avoid public wi-fi, unsecure e-mail, and unsolicited links
- ❑ Verify website security - click padlock for SSL certificate

Defend & Protect

- ❑ Activate bank-offered security services to mitigate fraud
- ❑ Report scams urgently
- ❑ Verify payment instructions verbally with a trusted source

Establish & Enforce

- ❑ Make cyber hygiene a priority for all points of access
  - Use unique passwords across platforms and accounts
- ❑ Back up data often and install security patches promptly
- ❑ Review and adhere to cyber insurance policy requirements

Prepare & Test

- ❑ Complete payment security training and attest annually
- ❑ Plan for an incident – steps to take, numbers to call
- ❑ Test data back-ups regularly

Mitigation Strategies: Layers of Defense

- **Company-Driven Strategy & Tactics**
  - Physical & Network Security
  - AP Change Management Policies
  - Security Culture / Risk Management Mindset
  - Train Employees & Contractors Adapt Behaviors & Habits
- **Bank-Offered Services**
  - Check Block
  - ACH Block
  - Check Positive Pay with Payee Verification
  - ACH Positive Pay with Debit Blocks/Filters
- **Company & Bank Dual Approach**
  - Ancillary Training & Education
  - Daily Reconcilement (Info Rptg)
  - Separation of Duties Access Controls & MFA
  - Secure Validation and Storage of Vendor Information

Best Practices: Protect, Detect, Recover

	People	Process	Technology
Prepare & Protect	▪ **Staff training** ▪ Separation of duties ▪ Identity & role-based access management ▪ Establish audit reporting and accountability measures	▪ Identify critical assets/data ▪ Conduct risk assessments ▪ Incident Response Plan (IRP) ▪ **Robust vendor management protocols** ▪ Establish communication channels/back-up channels	**Engage security professionals***: ▪ Device/software controls ▪ Perimeter/network security ▪ Secure/authorized connectivity ▪ Rapid patching & response ▪ Apps & Systems Recovery *Internal CIO/CISO or third-party Security as a Service (SECaaS) to address internal gaps
Detect	▪ Information/knowledge sharing ▪ **Staff/vendor background checks for sensitive data handling** ▪ Build skill set with finance staff to identify a breach	▪ End-to-end process controls ▪ Security vulnerability/phishing disclosure (e.g., phishing@td.com) ▪ Security Incident Management ▪ **Regularly perform account reconcilement to detect anomalies**	▪ Network & endpoint* monitoring ▪ **Further automate detection by exploring new tech (AI tools?)** ▪ Regular gap analysis of capabilities *Endpoints are devices that connect to a network
Respond & Recover	▪ **Overcommunicate to rebuild trust and instill confidence** ▪ External/Internal Comms Plan (if primary phone/email breach) ▪ 1st, 2nd and 3rd delegates for all key participants (especially if the effects of a breach are protracted)	▪ Activate the **I**ncident **R**esponse **P**lan and engage IRP team ▪ Corrective security controls ▪ Re-examine investigation results ▪ **Incorporate new intel & practices from post-event review** (e.g., mock breach exercises)	▪ **Triage impacted systems for restoration and recovery** ▪ Resume regular system(s) testing ▪ Contact federal law enforcement re: available decryptors for encryption algorithms that have been broken previously by security researchers

Industry Resources | Incident Reporting

Protect yourself.

Stay up to date on common fraud and scams.

- Understand what to watch out for.
- Know how to respond.
- Access tools and resources to help along the way.

Scan the QR code below to get started.

Or visit: td.com/fraudprevention

Report a fraud or cyber crime incident
Call your bank immediately | Notify the FBI at IC3.gov | File a fraud report via FTC.gov

TD Bank
TD Fraud Control
TD Commercial Banking Security Center

American Bankers Association (ABA)
banksneveraskthat.com

Cybersecurity & Infrastructure Security Agency
CISA Cyber Hygiene Services
CISA: Secure Our World

National Cybersecurity Alliance
staysafeonline.org

Cybersecurity Consultation

Top Ten Cybersecurity Recommendations

PRIMEX³ RISK MANAGEMENT BULLETIN

With cyber attacks becoming more frequent and severe, we need to continually adapt through education and information-sharing efforts. There are numerous recommendations on how local government entities can limit this risk. These are our recommendations:

1. **USE .GOV DOMAIN:** These domains are now managed by the Federal Government's Cybersecurity and Infrastructure Security Agency (CISA) and are free to local government entities. This domain will provide comfort to your citizens and those you communicate with that you are in fact a government organization and not a spoofed email or website. The .gov domain also provides you with additional email protections not available through publicly available domains.

2. **LEARN YOUR BASELINE:** Whether free through CISA, or paid through a trusted private cybersecurity company, obtaining a cybersecurity assessment will help you find your baseline. This is the starting point for improving your organizational cybersecurity stance. Look for an assessment that provides a network scan, employee interviews, uses penetration testing, and provides results via executive-level reports that are easy to understand.

3. **EMPLOYEE TRAINING:** The threat landscape we face today is one that frequently targets employees. These attacks are constantly evolving and increasingly sophisticated, so cyber security awareness training should be a regular part of employee onboarding and development.

4. **STOP AND VERIFY:** Phishing emails are wide-net attacks, designed to trick users into providing login credentials or to click on a malicious link or attachment. While there are numerous recommendations on how to handle these types of emails, the most important thing you can do is **STOP AND VERIFY** the email source and purpose. Remember, don't forward suspicious emails. Take a screenshot of anything that looks suspicious (without clicking on it), or simply request assistance from your IT staff or Managed Service Provider.

5. **USE PASSPHRASES:** Increasing the complexity of your passwords will improve organizational security. Passphrases should be between 11-25 characters and can include spaces. It only takes password-cracking software approximately seven minutes to decipher the average eight-character password, but it would take 34 years to decipher a complex 11-character passphrase. Coordinate this process with your IT staff or Managed Service Provider.

Primex
NH Public Risk Management Exchange
Trust. Excellence. Service.
46 Donovan Street, Concord, NH 03301 800-698-2364 www.nprimex.org

Top Ten Cybersecurity Recommendations

PRIMEX³ RISK MANAGEMENT BULLETIN

6. **USE MULTI-FACTOR AUTHENTICATION:** With phishing emails becoming the norm, you need a strong defense. Employees can be tricked into providing username and password information to cyber criminals, and this may result in future cyber attacks. Without the individualized pin produced from a hardware token or phone app to authenticate the account to the intended user, attackers will not be able to access your network to further their efforts.

Primex³ Cybersecurity Portal Access

The Primex³ Cybersecurity Portal provides members with one-stop access to custom-tailored information about cybersecurity and privacy. Visit the cybersecurity portal on your dashboard for up-to-date information about the latest cyber threat alerts. Improve your cybersecurity knowledge through best practice tips and tools and self-assessment questionnaires.

7. **BACK UP YOUR SYSTEMS NIGHTLY:** Meet regularly with your IT Director, Staff, and/or Managed Service Provider and make sure off-site backups are saved nightly, with verification of their existence weekly. Backups can be disabled or encrypted during a ransomware attack, and without this verification you will likely never know until you attempt to restore your systems.

8. **CREATE INCIDENT RESPONSE AND CONTINUITY OF OPERATIONS PLANS:** If your organization becomes the victim of a cyber attack, you can rely on these plans to help you act and obtain professional assistance more quickly and potentially mitigate the impact of the incident. Be sure to regularly update and practice these plans. Additionally, you will have greater peace of mind knowing you are well prepared.

REMEMBER:

In order to ensure best practices while working from home, always use a Virtual Private Network (VPN). This is simply an encrypted connection over the internet from a device to a network, protecting your work from a potential attacker.

9. **DEVELOP BUSINESS POLICIES AND PROCESSES:** Business Email Compromise attacks trick employees into believing a request is legitimate. Having systems in place will take pressure off employees by requiring secondary approvals for change-of-information requests or high-dollar transactions. Don't make ACH change request forms publicly available on your website. Ask vendors and employees to make these changes in person so you can verify authenticity.

10. **CALL YOUR RISK MANAGEMENT CONSULTANT:** Primex³ has a consultant who is eager to assist you with your cybersecurity questions and needs. Call before you're in the midst of a cyber emergency.

For more information, please contact your Primex³ Risk Management Consultant at 800-698-2364 or email *RiskManagement@nhprimex.org*.

Primex
NH Public Risk Management Exchange
Trust. Excellence. Service.
46 Donovan Street, Concord, NH 03301 800-698-2364 www.nprimex.org

Internal

Micro-Trainings

Webinars

PRE-RECORDED WEBINAR

Available 24/7

Finding Your Organization's Cybersecurity Baseline

Read more

Register

PRE-RECORDED WEBINAR

Available 24/7

Cybersecurity Basics Webinar

Read more

Register

PRE-RECORDED WEBINAR

Available 24/7

Cybersecurity for Emergency Dispatch Supervisors

Read more

Register

PRE-RECORDED WEBINAR

Available 24/7

Peterborough: Lessons Learned From a Business Email Compromise

Read more

Proceed to training

PRE-RECORDED WEBINAR

Available 24/7

CIS Control 07: Continuous Vulnerability Management

Read more

PRE-RECORDED WEBINAR

Available 24/7

CIS Control 08: Audit Log Management

Read more

PRE-RECORDED WEBINAR

Available 24/7

Pre-recorded Webinar: Cybersecurity Consultation Program Overview

SERIES

Jan. 12, 2028

Cybersecurity Micro Training Videos (Full Series)

Read more

Internal

Contact Information

New Hampshire Contact Information		Free Resources
Rick Rossi **Cybersecurity Advisor**	**richard.rossi@cisa.dhs.gov** **+1 202-770-8991**	**Assessments, Workshops, Exercises** **https://www.cisa.gov/how-we-can-help-region-resources**
Cori Casey **Risk Management Consultant**	**ccasey@nhprimex.org** **+1 603-759-6884**	**Training, Incident Response Plan Development** **https://nhprimex.org/explore-training/category/online/**
Jason Sgro **Senior Partner**	**jason@theatomgroup.com** **+1 603-501-0003 #104**	**Printed Materials, Training, Exercises** **www.theatomgroup.com/mcdp**
Katherine Heck **VP, Government Banking** **Christina Duane** **VP, Government Banking**	**katherine.heck@td.com** **Cell:603-933-9997** **christina.duane@td.com** **Cell: 603-770-3572**	**TD Bank** **Fraud Control** **TD Commercial Banking Security Center**

Best Practices for Detecting & Detecting Fraud