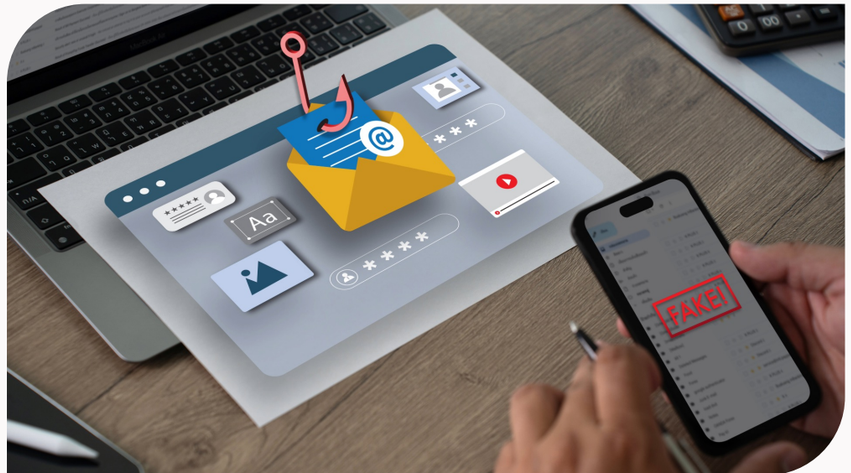


Corporate Account Takeover (CATO)

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

Corporate Account Takeover (CATO)

Understanding the threat, recognizing the signs, and protecting your business from one of today's most dangerous forms of electronic financial crime.

1. What is CATO?
2. How Attacks Work
3. Recognizing Compromise
4. How to Respond
5. How to Protect Your Business

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

What is Corporate Account Takeover?

CATO is the business equivalent of identity theft, an evolving electronic crime that exploits businesses of all sizes. It specifically targets companies with limited or no computer safeguards and minimal controls for fund disbursement through online banking accounts.

Who Is at Risk?

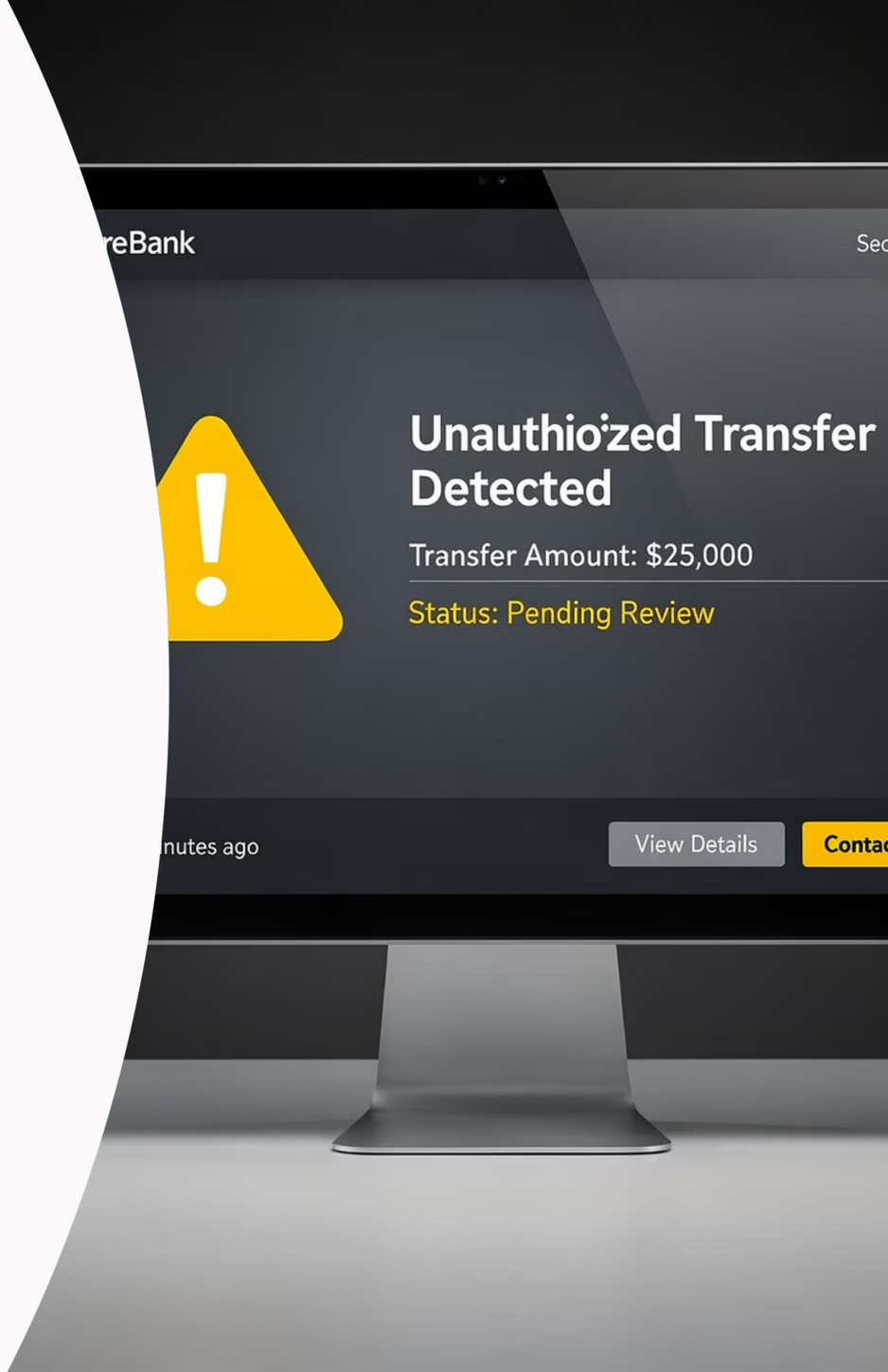
Any business with online banking access, especially those lacking strong internal controls or IT security infrastructure.

What Do Criminals Want?

Access to your online banking credentials so they can redirect or remove funds, often before you even notice.

Why Is It Dangerous?

Funds transferred by criminals are often unrecoverable once the attack is complete.



MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

Attack Vectors: How CATO Strikes

Phishing & BEC

Fake financial or payroll websites steal login credentials. SEO poisoning promotes fake sites above legitimate ones. Business Email Compromise impersonates trusted contacts.

Malware

Infected email links or websites install malware. Criminals silently monitor victims for weeks or months, waiting for the right moment — holidays, after hours, or after a token is used.

Social Engineering

Criminals impersonate banks, support staff, or law enforcement via fake texts, calls, or emails — tricking victims into sharing credentials, MFA codes, or OTPs.

Other Vectors

Session-hijacking, malicious social network sites, person-to-person downloads, and infected ads on popular websites all serve as entry points.

⚠ **Remember: The bank will never ask for your login credentials or One-Time Passcode (OTP) over the phone.**

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

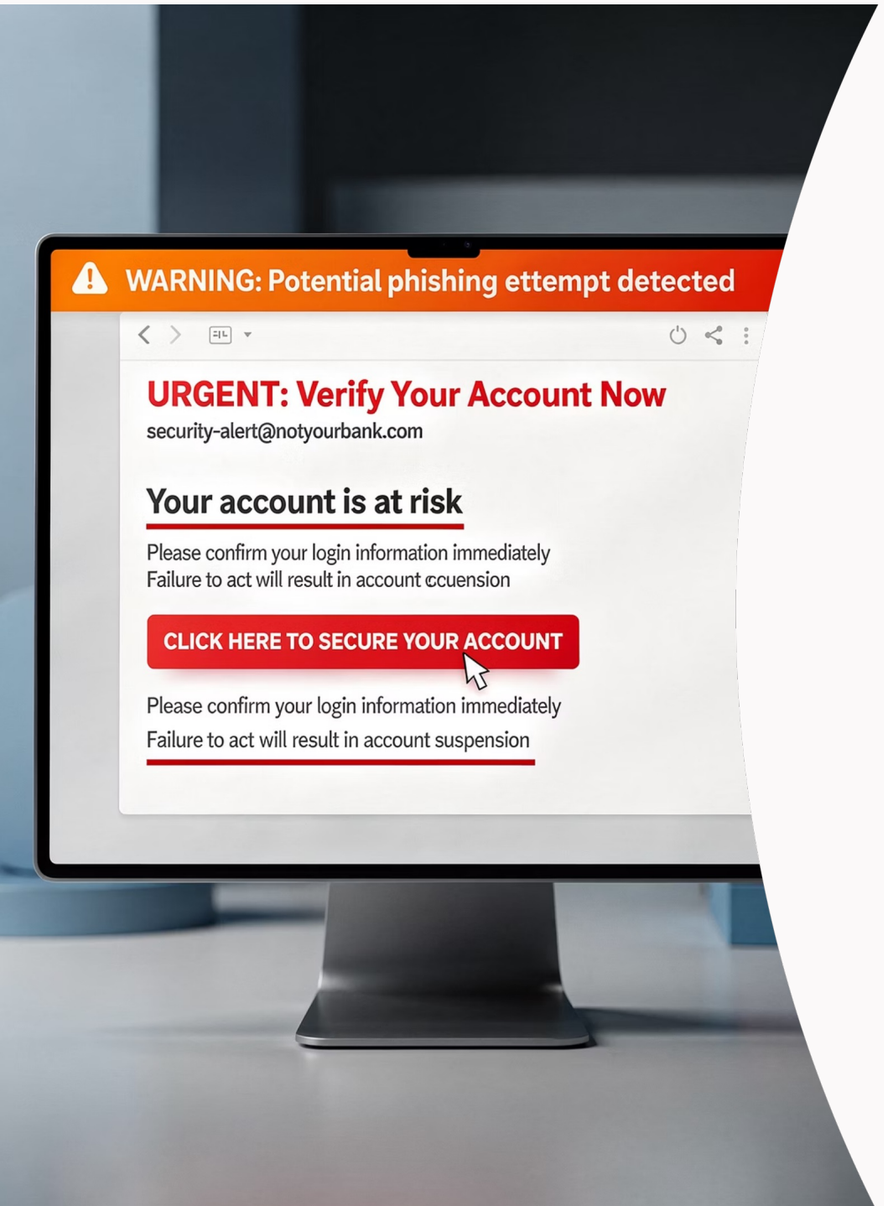
Where Do Attacks Come From?

According to the FBI's Internet Crime Complaint Center (IC3) 2025 Annual Report, cybercrime complaints and financial losses continue to rise year over year, with Business Email Compromise and fraud schemes among the costliest attack types reported.

Report cybercrime incidents to the FBI at ic3.gov — the Internet Crime Complaint Center tracks and investigates these attacks nationally.

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF



Spam & Social Engineering Examples

Attackers combine spoofing, social engineering, and phishing into convincing messages. Here's what to watch for in a suspicious email:

Mismatched Sender Identity

The “from" name says your company's HR or Talent Management, but the actual email address belongs to an unrelated domain.

Inconsistent Content

The subject line says "Strategic People Management Update" but the body assigns a punch item, the action doesn't match the subject.

Incorrect Company Name

Your company name is misspelled, hyphenated incorrectly, or lacks proper capitalization, a telltale sign of a spoofed message.

Wrong Recipient Logic

The email is addressed to billing@yourcompany.com but was sent directly to you, a mismatch that signals a mass phishing attempt.

MARTHA'S VINEYARD BANK

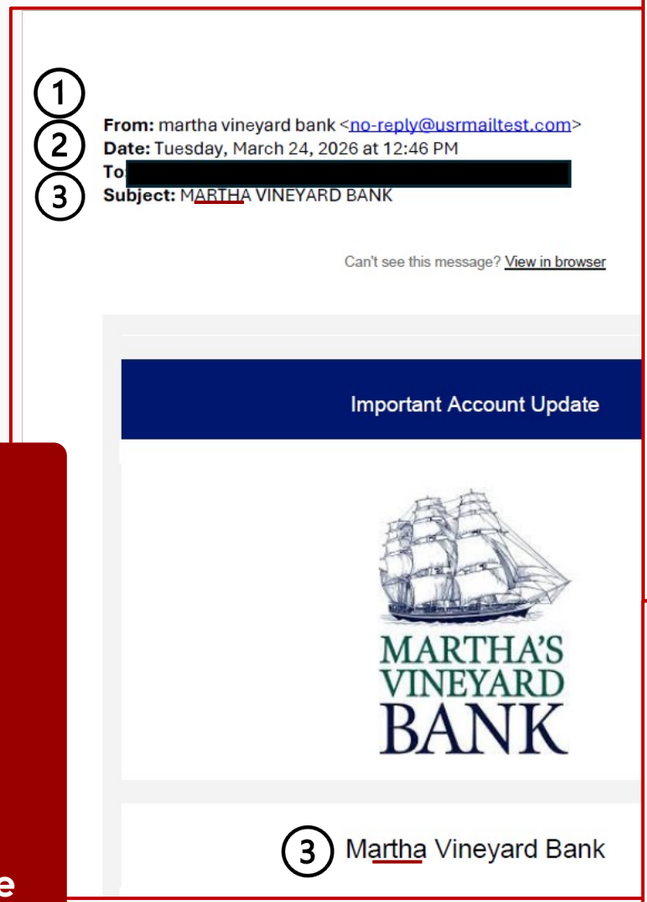
Member FDIC | Member DIF

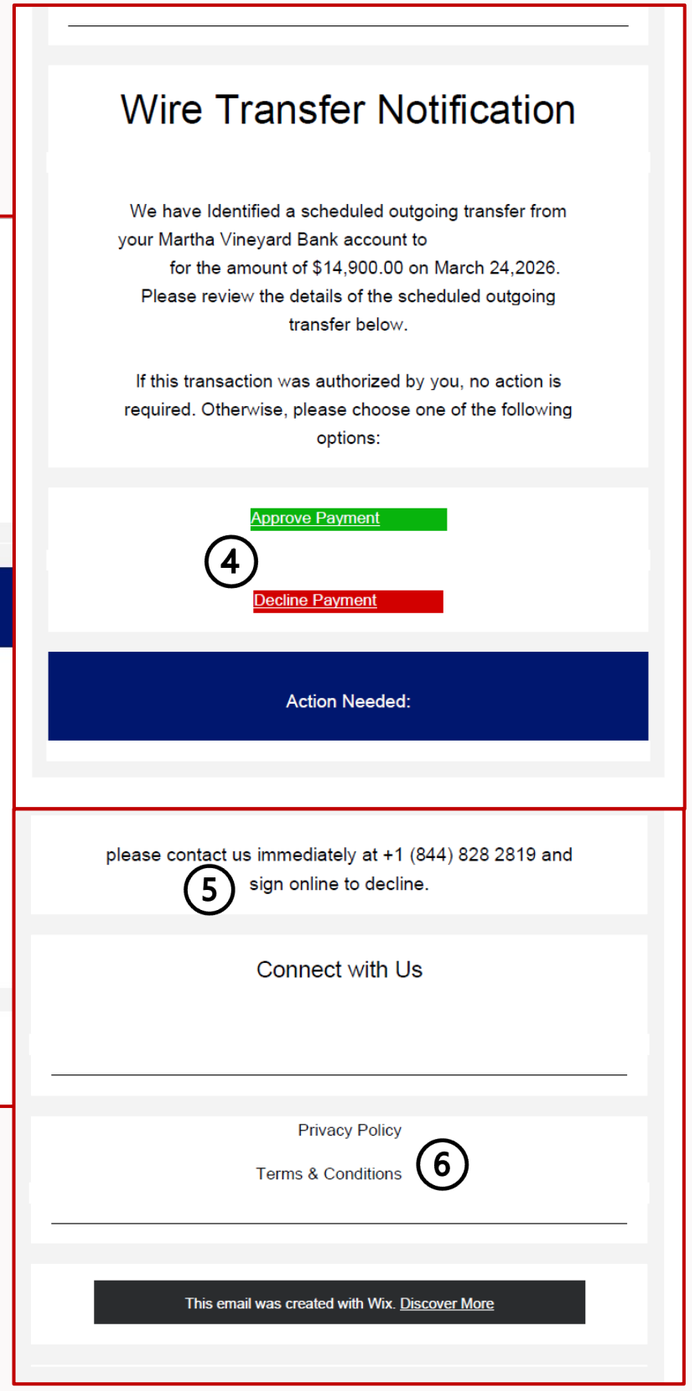
Recognizing Phishing Emails

Phishing emails are designed to look legitimate, but red flags are always present if you know what to look for.

Key Warning Signs

1. **Sender's email address doesn't match the organization**
2. **Email directed to a generic address but sent to you personally**
3. **Misspellings, incorrect grammar, or wrong company name**
4. **Action in the email doesn't match the subject line**
5. **False urgency, short deadlines to pressure a response**
6. **Navigation links (Home, Contact Us) that lead nowhere**





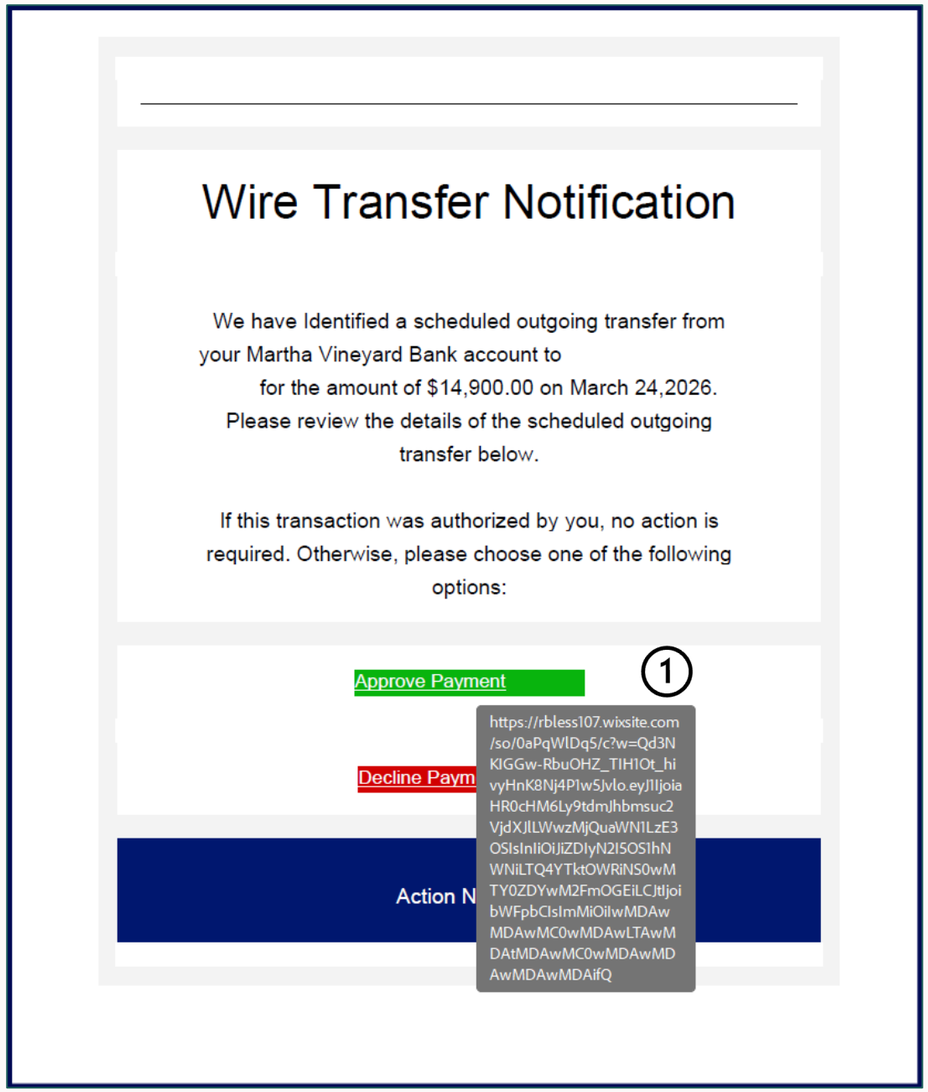
MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

Recognizing Phishing Emails

What To Do

1. **Hover over links to reveal the actual destination URL before clicking**
2. **Look up contact information independently, don't use what's in the email**
3. **Check that logos, bank names, and branding are exactly correct**
4. **When in doubt, call the institution directly using a known number**



MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

Is Your Computer Compromised?

Criminals often operate silently for days or weeks. Knowing the warning signs can help you act before funds are lost.

Visual & Performance Changes

New toolbars, unexpected icons, a different login page, sudden loss of speed, or inability to shut down or restart.

Unexpected System Behavior

Computer locks up, reboots unexpectedly, or displays unusual pop-ups — especially messages claiming the bank system is "unavailable" mid-session.

Banking Access Issues

Inability to log into online banking may mean criminals are blocking your access while they control your funds.

Unexpected OTP Requests

A one-time passcode request mid-session, or a caller asking for your OTP over the phone. **The Bank will never ask for this.**

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

How to Respond to an Attack

Initiate Response
Contact your Financial Institution immediately

Secure Systems
Change passwords and disconnect compromised devices

Notify Law Enforcement
Contact local cyber crime unit and request transaction hold

Report to FBI
File via IC3 and notify state agencies as needed

Speed is critical!

Every minute counts when funds are in motion.

Have your bank's key contact list prepared in advance.

Secondary Steps:

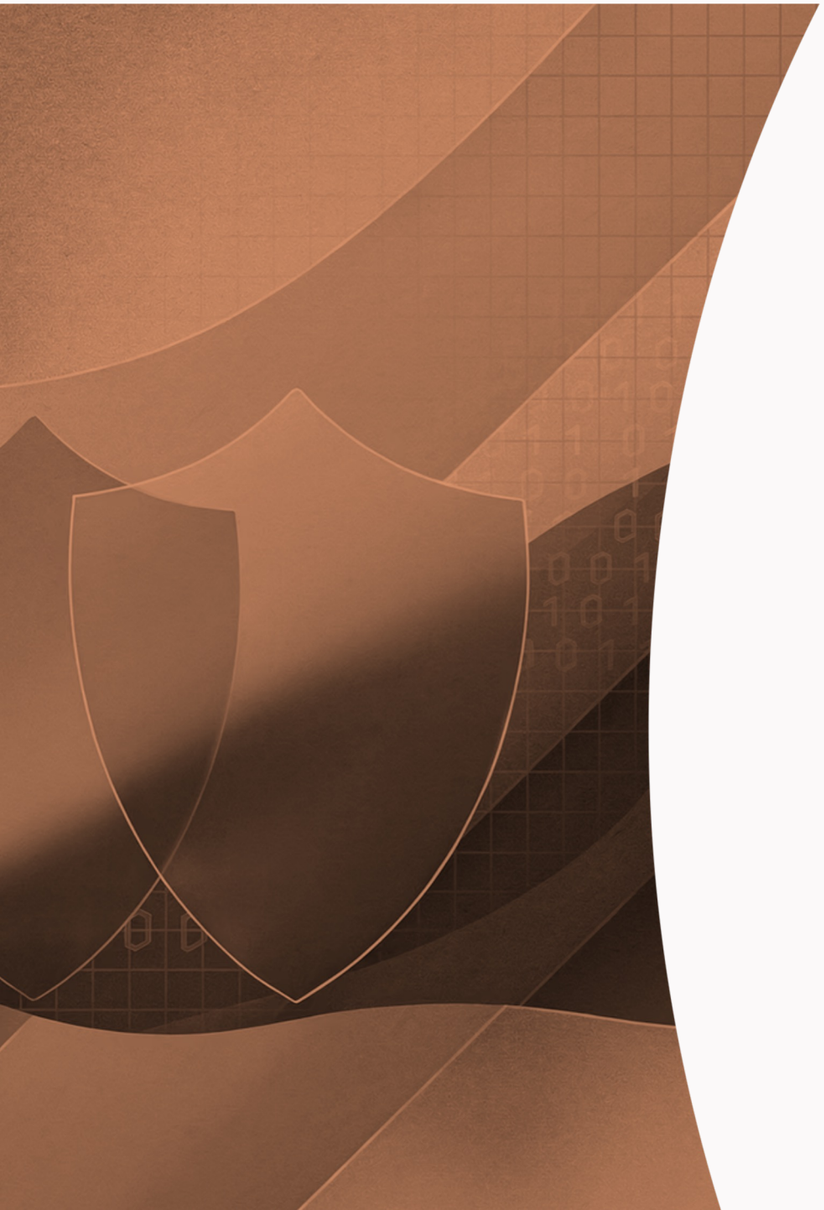
- Contact your insurance carrier
- Engage legal counsel
- Hire a third-party forensic IT company

Incident Response Plan Must Include:

- A leadership team with authority to act on bank accounts
- Pre-established contacts: FI, law enforcement, legal, IT support
- Log all events and preserve evidence (chain-of-custody)

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF



How to Protect Your Business

Education & Vigilance

- Educate employees on phishing and social engineering
- Never open attachments or click links in suspicious emails
- Reconcile accounts daily and react immediately to suspicious activity

Online Banking Security

- Use Positive Pay (Sound Pay) for check fraud prevention
- Require Dual Control for ACH or Wire Transfers
- Keep daily limits low and enroll in account alerts

Technical Prevention

- Engage an IT professional; limit administrative rights
- Deploy firewalls, intrusion detection, and data-loss prevention systems
- Use anti-virus/malware protection and enable spam filters
- Keep all devices updated — allow security patches (Adobe, Java, etc.)

Insurance & Liability

- Discuss Cyber or Fraud Liability Insurance with your agent

MARTHA'S VINEYARD BANK

Member FDIC | Member DIF

Final Thoughts & Helpful Resources

Stay Educated

Keep up with the latest cybersecurity best practices. Educate your team regularly awareness is your first line of defense.

Invest in Security

Cyber threats evolve constantly. Invest in IT professionals, updated software, and cyber liability insurance to stay protected.

Ask Questions

Be cautious of unknown senders and pop-ups. When something feels off, verify independently before acting.

Helpful Links

FBI Internet Crime Complaint Center

ic3.gov — Report cybercrime incidents directly to federal investigators.

Massachusetts Attorney General

mass.gov/how-to/file-a-consumer-complaint — Consumer complaint filing (note: more consumer-focused than business).