# FIVE STEPS TO TAKE IF YOUR INFORMATION HAS BEEN COMPROMISED

February 2026

Cyberattacks can be highly disruptive, especially when personal or sensitive information has been compromised. While increasingly common, swift action can reduce harm. Here are five immediate actions to consider.

---

Consider private security firms that specialize in assisting with containment, recovery and investigation efforts as well as with engaging with local authorities.

---

## 1. Isolation & Containment

### Disconnect from Networks

- Disconnect compromised devices entirely from the network (Wi-Fi, Ethernet, wired-computer docks) including desktops, laptops, mobile phones and Internet of Things (smart home devices)
- Disable remote access for any compromised devices

### Secure All Accounts and Devices

- Start with most important accounts; prioritize email, financial and other sensitive data accounts
- Force all applications to logout, which can usually be done within "Settings," "Privacy" or "Account Options"
- Reset passphrase and enable multi-factor authentication (MFA) where available. Use an authentication application, email, phone, or SMS text
- Update all devices, software and applications

### Secure Identity

- Initiate credit freezes with the 3 major credit bureaus: Equifax (888-298-0045), Experian (888-397- 3742), and TransUnion (888-909-8872)
- Consider custodial freezes for any dependents, minors and adults

# 2. Notification & Reporting

## Engage Law Enforcement

- Contact local police and regional authorities such as Federal Bureau of Investigation (FBI's) Internet Crime Complaint Center (IC3) (202-514-2000) or through the portal at https://www.ic3.gov/ and visit IdentityTheft.gov if you suspect your identity has been stolen Disable remote access for any compromised devices

## Consider Hiring Third Party Assistance

- Engage a trusted cybersecurity firm to lead incident investigation, response, mitigation, recovery, continuous monitoring and mitigation
- Utilize personal information takedown services and dark web monitoring
- Consider public relations expertise to manage the narrative and minimize reputational harm

## Notify Relevant Parties

- Alert your financial institutions, set up fraud alerts and device notifications immediately and monitor for any suspicious activity
- Contact family and close individuals. Social engineering tactics and advances in generative artificial intelligence could allow the cybercriminal to impersonate you – decrease the risk of fraud by sharing with those close to you
- Notify personal cyber team, financial advisors, insurance, legal representatives and family office staff

# 3. Assessment & Risk Management

## Exposure and Damage Assessment

- Identify exposed or compromised systems, assets and information
- Verify financial damage and check for fraud such as unauthorized transactions and account changes, including access and communication settings

## Assess Reputational Risks

- Monitor for leaks of personal, sensitive or corporate information Utilize personal information takedown services and dark web monitoring

## Understand Legal and Regulatory Harm and Obligations

- Consult a legal advisor to better understand and manage legal and reputational harm as well as regulatory obligations

# 4. Recovery & Restoration

## Device and Network Cleanup

- Wipe compromised devices and network; conducting a factory reset / full wipe may not be enough depending on if or where the malware resides (e.g., kernel). Consult professional information technology services, if needed
- Rebuild networks and devices, restore from clean backups, and continue update

### Restore Financial and Personal Control

- Work with financial institutions to recover any stolen funds or correct fraudulent transactions
- Consider enrolling in or hiring third party monitoring services of financial accounts to help prevent identity theft or leaking of sensitive personal information

# 5. Continuous Monitoring & Resiliency

**If an incident response plan does not exist, now is a good time to make one. This should include isolation steps among the other steps mentioned here and framed with NIST framework.**

- Include call trees of both personal and professional contacts as well as third party vendors, where applicable.

**Continue to monitor accounts and keep notifications on to check for unauthorized activity or transactions.**

**Continue to monitor for identity theft, impersonation and private information on the dark web.**

**Regularly update your devices when new updates are available, including drivers.**

# Resources for Further Information and Assistance:

- U.S. National Institute of Standards and Technology (NIST) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: https://doi.org/10.6028/NIST.SP.800-61r3
- NIST Cybersecurity Framework 2.0: https://www.nist.gov/cyberframework
- U.S. Cybersecurity and Infrastructure Security Agency (CISA) No-Cost Cybersecurity Services & Tools: https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

---