Email or Network Breach Response Guide

A compromised email account or network breach can jeopardize client confidentiality, trust account security, and your ethical obligations. This guide outlines key steps to consider when responding to an email or network breach. Circumstances may vary, so be sure to consult with a qualified IT consultant or cybersecurity specialist for guidance specific to your situation.

1. **Change Passwords & Lock Down the Account**
   - Change the password on the compromised email immediately.
   - Sign out of all devices and sessions.
   - Enable multi-factor authentication (MFA) if it is not already active.

2. **Scan Devices for Malware**
   - Ensure the latest security updates are installed, run a full anti-virus and anti-malware scan, and update your operating system and applications.
   - **Disconnect Your Devices, if Necessary:**
     - If multiple systems appear impacted, temporarily disconnect the device from Wi-Fi or the network to stop further access.

3. **Check for Tampering**
   Look for:
   - Unauthorized forwarding email rules
   - Changed recovery email or phone number
   - New inbox filters
   - Suspicious logins

4. **Reach Out to an IT Consultant**
   This is the next key step after initial self-containment. An IT consultant can do sections 2 and 3 more thoroughly and start the full investigation.

   Contact an IT/security consultant to:
   - Confirm the source of the breach
   - Review logs
   - Help secure systems
   - Determine whether data was accessed
   - Determine which clients' information may have been exposed
   - Determine whether attachments or contacts were accessed
   - Determine whether the hacker sent emails from your account

5. **Notify Your Cyber Insurance Carrier (if applicable)**
   They may provide:
   - Legal counsel
   - IT support
   - Client notification assistance
   - Coverage for costs related to the breach

6. **Document Everything and Preserve Evidence – this protects you if questions arise later**

   Keep a simple log:
   - What happened
   - When you discovered it
   - Steps you took
   - Who you contacted

   Save:
   - Suspicious emails
   - Error messages/screenshots
   - Logs (if available)
   - Copies of altered settings

   ❖ Do not wipe devices unless advised by your IT consultant!

7. **Notify Your Bank**
   - Verify Trust Account safety
   - Review account activity
   - Confirm daily balances
   - Enable Positive Pay

8. **If you discover trust account fraud, suspicious activity, or believe your firm (or you) are victims of identity theft, call The Florida Bar's Attorney Consumer Assistance Program (ACAP) at 1-866-352-0707**

   Call ACAP immediately if:
   - There is any unauthorized trust account transaction(s)
   - Your bank reports suspicious activity
   - Someone impersonates your firm (fake emails, fraudulent checks, spoofed communications)
   - Client funds may be at risk
   - You suspect identity theft affecting your practice

9. **Notify Affected Clients (if their data was at risk) if:**
   - Their information was accessed
   - Their matter was exposed
   - Their funds may be at risk

   When contacting affected clients, keep it simple and focus on:
   - What happened
   - What you have done
   - What they should watch for
   - Your plan moving forward

   ❖ If the hacker sent emails from your account, notify your contacts so they don't click malicious links!

10. Comply With Florida Breach-Notification Laws

If personal information (SSN, financial information, etc.) was exposed, Florida law may require notice to affected individuals and sometimes the Attorney General. *See Florida Statue 501.171 Security of confidential personal information*

- Consult breach counsel if unsure.
- Additional Resource: LegalFuel Data Breach Notification Checklist

11. Notify Credit Bureaus, or Law Enforcement (as needed)

Especially if:

- Financial information was exposed
- Fraudulent wire transfers were attempted
  - FBI Internet Crime Complaint Center (IC3)
- Trust account or operating accounts were targeted

12. Prevention Going Forward

Use Strong Security Basics:

- MFA for all accounts
- Consider using a password management application (e.g., Dashlane, 1Password, etc.), which securely stores and generates complex passwords, making it a much safer alternative to writing them down. Please note: These are examples only. You should conduct your own research to determine the best password management solution for your needs.
- Conduct automatic software updates
- Implement encrypted email or secure client portal
- Apply spam filtering and phishing protection

13. Complete an Annual Review of Systems with Staff

Once a year, review:

- Your passwords
- Devices
- Cloud accounts
- Backup systems
- Who you would call if something happened

14. Create a 1-Page Emergency Plan

List:

- IT contact(s)
- Cyber insurance contact
- Breach-experienced attorney
- Florida Bar ACAP Department (1-866-352-0707)
- Your bank's fraud department
- Law Enforcement Contacts