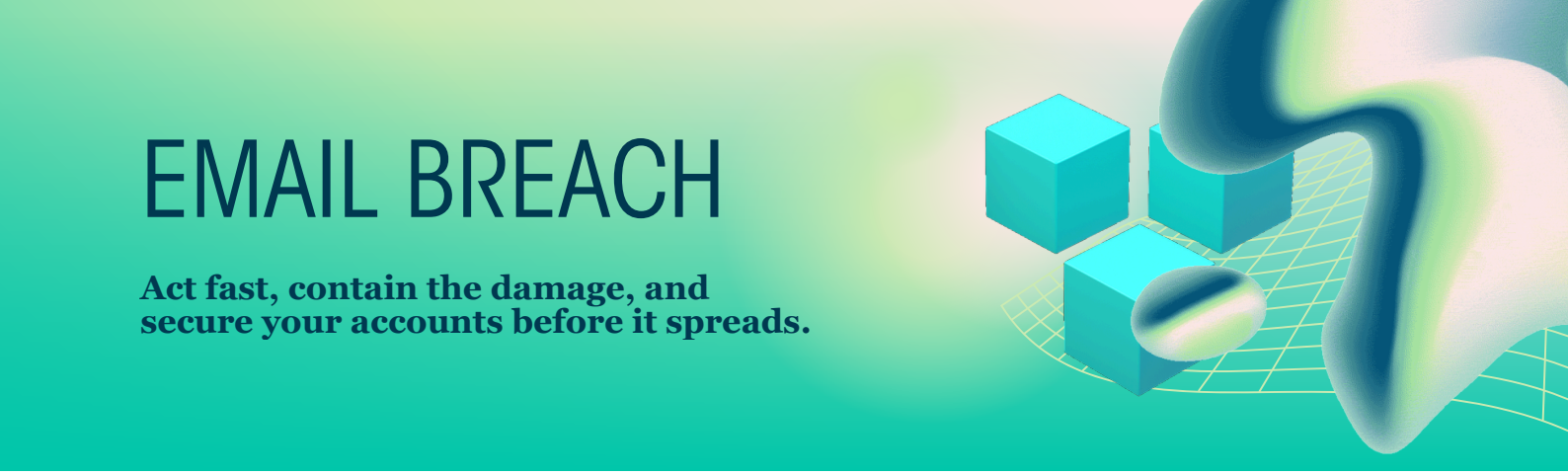

Email Breach Response Checklist for Small Businesses (2026 Edition)

Use this checklist to secure your accounts immediately and prevent further compromise.

Email Breach Response Checklist

1. Secure the Compromised Account Immediately

- ☐ Change the password to a new, unique password
- ☐ Do not reuse any previous passwords
- ☐ Use a password manager to generate and store credentials

Why this matters:
Attackers often maintain access until credentials are changed.

2. Enable Multi-Factor Authentication (MFA)

- ☐ MFA is enabled on the compromised account
- ☐ Authenticator apps or secure methods are used
- ☐ Backup authentication methods are secured

Why this matters:
MFA blocks unauthorized access, even if the password is compromised.

3. Identify and Secure Other Accounts at Risk

- ☐ All accounts using the same or similar password are updated
- ☐ Business-critical systems are prioritized (email, banking, CRM)

□ Password reuse is eliminated

Why this matters:
Attackers test stolen credentials across multiple platforms.

4. Remove Unauthorized Access and Sessions

□ Log out of all active sessions
□ Review connected apps and integrations
□ Remove unknown or suspicious access

Why this matters:
Attackers often maintain persistence through connected apps or sessions.

5. Check for Malicious Activity

□ Review sent emails for suspicious messages
□ Check inbox rules and forwarding settings
□ Look for unauthorized password resets or login alerts

Why this matters:
Email breaches are often used to send phishing emails or redirect communications.

6. Warn Internal Team and Key Contacts

□ Notify employees of the breach
□ Warn clients or partners if necessary
□ Advise contacts not to trust recent suspicious emails

Why this matters:
Stopping the spread reduces secondary attacks.

7. Watch for Phishing and Follow-Up Attacks

□ Be cautious of emails claiming to “fix” the issue
□ Verify all recovery-related communications
□ Avoid clicking unknown links or attachments

Why this matters:
Attackers often follow up with additional phishing attempts.

8. Monitor Financial and Sensitive Accounts

□ Review bank and payment accounts
□ Watch for unauthorized transactions
□ Consider fraud alerts or credit monitoring if needed

Why this matters:
Email breaches often lead to financial fraud attempts.

9. Evaluate Whether to Transition Critical Accounts

□ Consider creating a new secure email for high-risk accounts
□ Update login credentials for critical services
□ Limit reliance on the compromised account

Why this matters:
Severely compromised accounts may not be fully recoverable.

10. Keep the Original Account Secured During Recovery

□ Do not delete the account immediately
□ Use it temporarily for password resets
□ Protect it with MFA and strong credentials

Why this matters:
You may still need access to recover other accounts.

11. Reduce Your Long-Term Exposure

□ Remove unused or unnecessary accounts
□ Clean up old logins and services
□ Limit where your email is used

Why this matters:
Fewer accounts mean fewer future attack points.

12. Monitor for Future Breaches

□ Check breach monitoring tools regularly
□ Stay aware of new incidents involving your email
□ Act quickly if new exposure is detected

Why this matters:
Breaches often occur in waves, not just once.

What a Controlled Response Looks Like

Access is secured quickly
Unauthorized sessions are removed
Internal and external risks are contained

Future exposure is reduced

Quick Rule of Thumb

The longer an attacker has access, the more damage they cause.