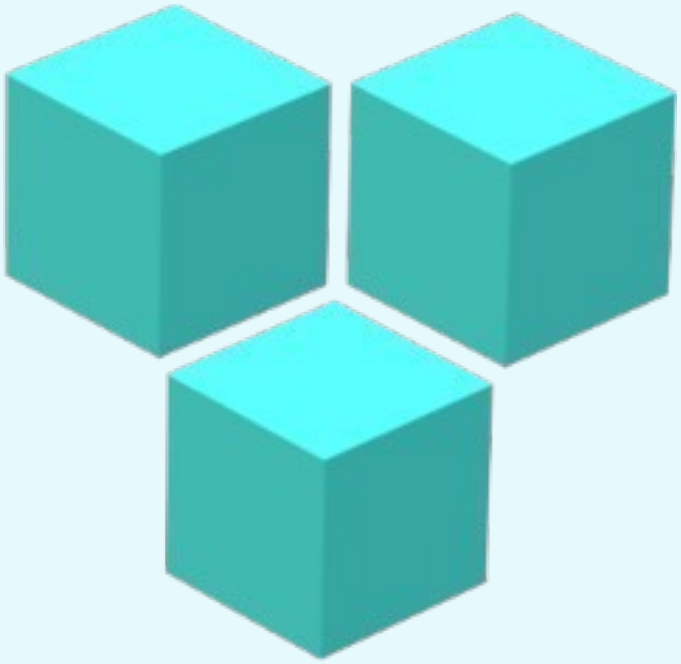


SofTouch Systems

Email Breach Response Guide

“Practical steps to recover your accounts and safeguard your digital identity.”

No-Surprise IT: Predictable. Proactive. Proven.

1. Change Your Password Immediately

Use a completely new password that you haven't used anywhere else. A strong password should be at least 12 characters long and include a mix of uppercase, lowercase, numbers, and symbols. We recommend using a password manager like 1Password to store and generate secure credentials.

2. Turn On Multi-Factor Authentication (MFA)

MFA adds a second verification step to your login. Even if someone steals your password, they can't access your account without the secondary authentication code sent to your device or app.

3. Check Where Else That Password Was Used

If you reused that same password elsewhere, change it on every other account. Hackers often test stolen passwords across multiple sites.

4. Review and Secure Connected Accounts

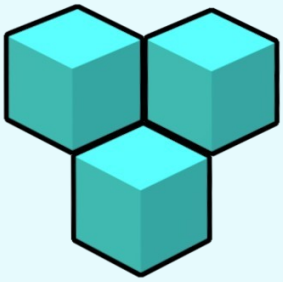
Log in to your email and review connected apps and devices. Remove any that look suspicious, and log out of all sessions before signing back in with your new password.

5. Watch for Phishing Emails

Be cautious of emails claiming to help you 'fix' your breach. These are often phishing attempts. Verify sender addresses before clicking links or downloading attachments.

6. Monitor Financial and Personal Information

If your personal or payment data was leaked, keep an eye on your financial accounts. Consider placing a credit freeze or fraud alert with major credit bureaus.



SofTouch Systems

Simplifying technology, maximizing results.

7. Create a New, Secure Email for Important Accounts

If your breached account becomes unmanageable due to spam, create a new address for critical accounts like banking and password recovery.

8. Don’t Delete the Old Email Yet

Keep your old email active for a few months so you can still receive password reset links. Protect it with a strong password and MFA, and use it only as a backup.

9. Clean Up Your Digital Footprint

Use tools like JustDelete.me or Firefox Monitor to find and delete unused old accounts. Reducing your exposure decreases your future breach risk.

10. Stay Informed and Recheck Regularly

Visit HaveIBeenPwned.com periodically to see if your email appears in new breaches. Regular monitoring helps you react quickly to new incidents.

✔ Tip: Prevention Beats Repair

Use unique passwords, enable MFA everywhere, and stay alert for phishing. Small habits today prevent big problems tomorrow.

Need help protecting multiple business accounts or domains? SofTouch Systems provides managed cybersecurity and email protection services for small businesses across Texas.

SofTouch Systems

Simplifying technology, maximizing results.