

Email Compromise Checklist

- ___ Reset compromised email account password
- ___ Document and change password on other accounts that use same compromised password. Banking, personal email, social media accounts.
- ___ Consider Financial credit monitoring service. Credit freeze, Fraud Alert, Credit report alerts. Experian IdentityWorks, Credit Karma, myFICO, ID Watchdog
- ___ Monitor log in activity of affected account with geographic identifiers.
- ___ Implement Multi Factor Authentication (MFA) for all employees if not already implemented
- ___ Review and remove any suspicious forwarding rules or filters in email.
- ___ Check and review all sent email items.
- ___ Implement strong end point protection on all computers.
- ___ Verify all computers have end point protection enabled.
- ___ Monitor use of Administrator login throughout the company.
- ___ Communication to employees the importance of protecting passwords and log in information.
- ___ Change log in passwords to financial and confidential systems.
- ___ Initiate all employee password change.
- ___ Review password requirements and change timeline.
 - Suggest every 45-60 day change, do not reuse last 8 passwords.
 - Utilize long phrases: Combination of favorite song with band name, describe your childhood home and street name. BroadStreetHad3bedrooms
- ___ Define process for financial authorizations to banks, customers and vendors.
 - Look especially for requests for change of bank routing information.
 - Implement call and verify procedures with bank and vendors.