How To Protect Against Business Email Compromise Threats

PONDURANCE

Business email compromise (BEC) is a common attack vector used by some of the top cybercriminals. We share our top tips to protect your organization's assets from this type of threat.

Recommendations for All Mail Servers

- ☐ **Enable multifactor authentication for all users**
  - We recommend that multifactor authentication is enabled for all users.
- ☐ **Disable legacy authentication and protocols**
  - Legacy authentication and protocols are easy for cybercriminals to manipulate. We recommend using an official application like IMAP/SMTP/POP3.
- ☐ **Set up and review alerts**
  - When reviewing and alerting on user role and group membership changes, you should be looking for risky logins, risky users, and rule changes.
- ☐ **Tag activity outside the organization**
  - Tagging email messages and/or subject lines originating from outside the organization can help you stay on top of suspicious activity.
- ☐ **Monitor for breach data**
  - You can stay up to date on breach data associated with your organization by registering at haveibeenpwnd.com. More information on the best practices for utilizing the data at haveibeenpwnd.com is shared in detail in our blog.
- ☐ **Conduct user security awareness training**
  - The end user is your first line of defense and should be armed with the knowledge to practice safe browsing habits and identify phishing emails. We put together a handy employee checklist that we recommend sharing with your staff.

Recommendations for Office 365 (O365)

- ☐ **Consider implementing conditional access, risk-based conditional access, and continuous access evaluation for O365**
  - These access tools available in Azure Active Directory allow your organization to implement if-then rules to empower users to be productive but also protect assets. Learn more about these options and how to implement these tools here.
- ☐ **Customize smart lockout features in O365**
  - This tool is a great defense against brute force attacks as it locks out those who guess a user's password or attempt to log in unsuccessfully too many times. You can learn more about how to implement this tool here.
- ☐ **Restrict bad passwords in O365**
  - Many create common passwords that are easy for bad actors to guess. Within Azure Active Directory, you can enable custom banned passwords, add entries to the banned passwords list, and test password changes with a bad password. Learn how to implement this tool here.
- ☐ **Use priority accounts in O365**
  - This tool allows you to specifically monitor accounts that are important like IT, executives, finance, etc. for phishing or other cyberattacks. Learn more about this feature here.

Things To Consider

- ☐ **Consider implementing password managers like LastPass or 1Password**
- ☐ **Disable email forwarding**
- ☐ **Consider modifying settings for application contents**

Business email compromise is part of the playbook used by a successful international cybercriminal organization conducting cyber financial fraud. Watch an on-demand webinar with our Manager of Incident Response, Max Henderson, where he dives into a case study on this cybercriminal activity including their motivations and target victims, their unique scheme to access data, and our recommendations to reduce the cybercriminal group's success rate.



REGISTER HERE

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204

Copyright © 2022 Pondurance