

WHAT ARE YOU DOING TO MITIGATE THE RISKS TO YOUR BUSINESS

1. Are passwords required to access your company workstations?
2. How complex are the passwords required to access your company workstations?
3. Do you currently have anti-virus programs installed on your company workstations / network?
4. Do you take advantage of the patches and upgrades available from software providers?
5. What security measures are in place for the wireless devices used by your company / employees? (Have you ever heard of "[Smishing](#)"?)
6. Do you have segregation of daily duties? (e.g.: Are specific people granted access to the banking information? Are there specific duties assigned to specific employees?)
7. Do you perform background checks when hiring new employees?
8. What processes do you currently have in place to ensure the security of your business and related information? (e.g.: Do employees have access to the office after-hours? If so, how many and what is the deciding criteria to grant access?)
9. Who has access to download or install information on company workstations? (Are you only allowed to download or install programs if you are the administrator?)
10. If you have online banking for your business, do you monitor your accounts daily? Verifying balances and checking transactions?