Automated Security Awareness Program for Marmot Library Network Inc

April 12th, 2022

Welcome

Congratulations on becoming part of the KnowBe4 ASAP family. The following pages reflect your individual survey responses and contain recommendations for specific training modules, videos and supporting materials to help you catapult your training plans into a mature and multifaceted information security awareness program.

A successful information security awareness program is essential to ensure your employees are empowered with the knowledge they need to protect your organization. While employees are your most important asset, they are at the same time your weakest link and your last line of defense. One of the best ways to make sure your employees will not make costly errors regarding information security is to institute company-wide security awareness training initiatives.

Effective security awareness and training programs are multifaceted. For example, an effective program will include:

✔ Deployment of learning modules that cover topics critical to the organization, related to behavior, policy, or compliance expectations

✔ Simulated phishing and social engineering attacks so that employees are conditioned to look for red flags in any communication they receive

✔ Additional supportive messaging, information delivery methods, communication channels, and interactive activities so that your organization has the best chance to effectively develop a sustainable security mindset within each employee, job role, division, and region

✔ Knowledge and skills that are relevant and transferrable to an employee's personal life and overall security hygiene

KnowBe4
Human error. Conquered.

Task List

☐	1. Engage your stakeholders	about 2 hours | April 22nd, 2022
☐	2. Customize your KnowBe4 console	30 minutes | April 25th, 2022
☐	3. Whitelist KnowBe4's mail servers	Variable | May 4th, 2022
☐	4. Add users and create groups	about 4 hours | May 10th, 2022
☐	5. Create and complete a baseline phishing campaign	30 minutes | May 16th, 2022
☐	6. Review the results of your phishing test	30 minutes | May 17th, 2022
☐	7. Establish a procedure for users to report suspected phishing emails	Variable | May 19th, 2022
☐	8. Communicate with your users about your security awareness program	30 minutes | May 23rd, 2022
☐	9. Assess your users' security awareness knowledge	30 minutes | May 25th, 2022
☐	10. Develop a threat response and management process for reported phishing emails	Variable | May 27th, 2022
☐	11. Create a foundational training campaign	about 3 hours | June 2nd, 2022
☐	12. Create a training campaign for phishing test "clickers"	about 2 hours | June 8th, 2022
☐	13. Create an ongoing phishing campaign	about 3 hours | June 28th, 2022
☐	14. Create, upload, and distribute policies	about 2 hours | July 4th, 2022
☐	15. Create training campaigns for your compliance training modules	about 2 hours | July 8th, 2022
☐	16. Set up a Scam of the Week campaign	about 1 hour | July 11th, 2022
☐	17. Determine your security culture	30 minutes | July 13th, 2022

KnowBe4
Human error. Conquered.

Task List

- [ ] 18. Create training campaigns for your role-based training modules | Customer Service Team   about 3 hours | July 20th, 2022

- [ ] 19. Create training campaigns for your role-based training modules | Executives & Leaders   about 3 hours | July 27th, 2022

- [ ] 20. Create training campaigns for your role-based training modules | Finance Staff   about 3 hours | August 3rd, 2022

- [ ] 21. Create a security awareness training campaign | August   about 3 hours | August 1st, 2022

- [ ] 22. Create training campaigns for your role-based training modules | IT Staff   about 3 hours | August 10th, 2022

- [ ] 23. Create training campaigns for your role-based training modules | Payment Card Processors   about 3 hours | August 17th, 2022

- [ ] 24. Create training campaigns for your role-based training modules | Developers   about 3 hours | August 24th, 2022

- [ ] 25. Create training campaigns for your role-based training modules | Frequent Travelers   about 3 hours | August 31st, 2022

- [ ] 26. Identify high-risk groups so you can take action   about 1 hour | September 1st, 2022

- [ ] 27. Create a recurring, targeted, high-risk phishing campaign   about 1 hour | September 12th, 2022

- [ ] 28. Set up a Security Hints and Tips campaign   about 1 hour | September 13th, 2022

- [ ] 29. Review and select posters to display around your organization   30 minutes | September 14th, 2022

- [ ] 30. Review and select games for your training campaigns   about 2 hours | September 23rd, 2022

- [ ] 31. Review newsletters and security docs and plan delivery method   30 minutes | September 26th, 2022

- [ ] 32. Set up a vishing campaign   about 2 hours | October 5th, 2022

- [ ] 33. Set up a USB drive test campaign   30 minutes | October 7th, 2022

- [ ] 34. Check in on the effectiveness of your program   30 minutes | October 10th, 2022

Task List

35. Share user behavior improvements with your organization's leadership   about 1 hour | October 12th, 2022

36. Create a low-difficulty phishing campaign for high Phish-prone users   about 1 hour | October 14th, 2022

37. Create a high-difficulty phishing campaign for low Phish-prone users   about 1 hour | October 18th, 2022

38. Use targeted training to initiate a training campaign for high-risk users   about 2 hours | November 8th, 2022

39. Create a security awareness training campaign | November   about 3 hours | November 1st, 2022

40. Create a security awareness training campaign | February   about 3 hours | February 1st, 2023

KnowBe4
Human error. Conquered.