RSA Conference 2019

BETTER.

Peer2Peer

Speed Dating for Security: 200 Creative Engagement Ideas in 50 Minutes

P2P1-W10: Speed Dating for Security: 200 Creative Engagement Ideas in 50 Minutes

Bianca Wirth, Manager, Corporate Security Education & Awareness, Insurance Australia Group

Speed Dating for Security: 200 Creative Engagement Ideas in 50 Minutes

There is a growing understanding in cyber security that the people element of the traditional people-process-technology triangle is a critical aspect of ensuring your organisation achieves security in depth. Training people on two key aspects – how to recognise and how to report a cyber security issue or incident – is one of the key methods in distributing your cyber risk.

In this peer-to-peer session, the goal was to come up with as many creative security engagement, education and awareness ideas in the 50 minutes. The target was set – 200 ideas! With 30 participants that would be 6 ideas per person and with participants from a diverse range of skills, experience and company sizes in the room, I felt it would be achievable.

We started the session by having people face each other in groups of 3's and 4's with large pieces of paper and markers to write their ideas down.

I introduced the session by giving the teams some guidance on brainstorming their ideas. We started with risks as the basis of the issues they were trying to educate people on:

1. What are the top people-related cyber security **risks** to your business? *For example, people don't recognise and report phishing attempts.*
2. **Who** is associated with these risks? *For example, people working in payroll and accounts payable roles would have a high impact (e.g. financial loss) if they could not recognise and report phishing attempts.*
3. What should people **know** to help minimise these risks? *For example, we need people to recognise a phishing attempt and report it to our SOC.*

With these three basic questions as prompters, the brainstorming commenced. After 10 minutes, the participants on the inside tables moved to the left and engaged with a new team to start the brainstorming again with fresh perspectives.

The ideas that the teams came up with varied in depth – but here they are:

Positive ideas (using the carrot)

1. Classroom-based training for phishing
2. Tips for home use / personal use / personal cyber security to reach the audience
3. Create a security ambassador / advocate program
4. Create a 'state of the Cyber' organisational report to educate the C-suite
5. Have giveaways with security tips
6. Use social platforms / posts
7. Take your child to work day exercises
8. Remedial training for repeat offenders
9. Print your own posters
10. Posters that are digital including:
    a. Physical security
    b. Secure coding
    c. Seasonal scams

   d. Personally identifiable information (PII)
   e. Confidential definitions

11. Create infographics
12. Create a video series / campaign / content
13. Games and prizes / swag
14. Recognition programs
15. Awareness campaigns on monitors around the organisation
16. Cyber memes and funny pictures
17. Adult cyber colouring books
18. Gamification & competition
19. Bus wrap sticker for advertisements on buses
20. Choose your own adventure training
21. Cyber food truck event
22. Computer based simulations and training
23. Phishing awareness tests
24. Dumpster diving contest – dig through your organisation’s bins to show what sensitive information is being thrown into the trash
25. Stickers for laptops and other equipment
26. Periodic bite-sized training (videos and interactive <10 minutes in length)
27. Portable instructions on who to contact
28. Spear phishing and general phishing emails
29. Manual calling (vishing)
30. Positive reinforcement
31. Incentivisation
32. Characters / pets / personal
33. Catchy tag lines
34. Pop-ups
35. Crowd-source ideas
36. Internal apps
37. Monthly raffles
38. Reporting forms
39. Thank yous for reporting
40. Run a roadshow
41. Create a community
42. Create a safe email box and train people to forward email
43. Auto-direct phishing URLs to SOC and SOC reaches out
44. Peer review for secure coding
45. Educate on the top app security risks
46. Secure coding training

47. C-level engagement
48. “Report this” button
49. Quarantine spam
50. Points and/or badges for skill levels e.g. taking training, watching videos
51. Simulated phishing – make it look realistic and get more sophisticated over time
52. Security check tools e.g. Vericode, Rational Rose
53. Security awareness training (including testing) as precursor to creating a password, onboarding and setup
54. Safety/security warning at login screen (rotating messages)
55. Run an escape room
56. Run a virtual escape room
57. Game of Threats (in-person role playing e.g. PwC)
58. Personal digital profile (e.g. E&Y)
59. In-home assessments
60. Mock interviews – post-incident
61. Table-top exercise – crisis communications
62. Collectible cards
63. Board games
64. Capture the flag (CTF) / Virtual hackathon
65. Scripted shows / serials
66. External benchmark metrics for the Board and Executive presentations
67. Survey immediately after phishing test failure or incident
68. Personal follow-up or interview a focus group
69. Onboarding kit – welcome message, phishing simulation program welcome
70. New hire use agreement
71. Secure traveller program with ‘just in time’ messages
72. Mobile app with education resources (including for home/family)
73. Executive level dashboards
74. What’s in it for me (WIIFM)
75. Secure it at home
76. Public service awareness
77. External security ambassadors
78. Public engagement
79. Plain English messaging
80. Executive Assistant engagement
81. Run exercises with certifications
82. Scenario-based role playing
83. Security festival / fair
84. Collectible pins

85. Email newsletters e.g. explain technical fixes / blockers
86. Contests for completing patching
87. Contests for completing training
88. Internal phishing examples
89. Teaching employees to report
90. Password training
91. Host a security day
92. Lunch & learn style events
93. Theatrical performances
94. Zero trust data protection

Borderline (these might get you in trouble or may not have the desired effect)

95. Password cracking
96. Consequence model for risk violations e.g. compensation impacts, written warnings, terminations)

Negative ideas (using the stick)

97. Create a phishing "jail" for repeat offenders where all their external email goes to the junk folder
98. Take away pay increases for repeat offenders

Although we didn't make it to 200 ideas, there were several duplicates consolidated in the above list. There was also plenty of great discussion in the room and many participants wanted to stay longer to keep brainstorming.

Based on my experience, some of these initiatives will work better than others. For example, creating a 'phishing jail' can send the wrong message to employees and inhibits the business from operating. Your security education and awareness initiatives should never impact business operations.

The goal for education and awareness overall is to create **behavioural change** and this can be achieved by influencing people's motivations. Motivations can be both intrinsic (they do it because it makes them feel good) and extrinsic (they get something physical from it like a prize). Using the stick rarely influences people's motivations in a positive way.

About the Author:

Bianca Wirth is a specialist in the human side of Cyber Security. She developed and currently manages the corporate security education & awareness program at Insurance Australia Group. With over 20 years' experience in IT and security, she has consulted to over 100 Australian and New Zealand organisations from a diverse range of industries and government; worked for a large global software vendor; developed a successful consulting business. She is currently completing a Masters of Information Security, has several other technology and project management qualifications and sits on a university advisory board. In 2017 Bianca designed and delivered the course "Phishing Countermeasures" for an Australian University, with over 3600 participants, and guest lectured at other Unis on this topic.