SecurityAwareness.guru

34 STEPS TO THE PERFECT PHISHING SIMULATION

IT-SA OCT-26TH-2022

Palo Stacho

Palo Stacho - securityawareness.guru

- Cyber Security Awareness Campaign and Program
  - Manager
  - Engineer
  - Consultant

- Since 2015 fully dedicated to Cybersecurity Awareness
- Dozens of awareness projects D / A / CH and UAE among others also for banks, Lufthansa Group, Bosch, FRoSTA, Swisscom or Mobiliar Insurance

- Former Security Awareness Enthusiast @ ThriveDX

- Co-Founder LUCY Security Lucy

- Study Director Global Awareness Studies 2020 & 2022

- Business Angel & Startup Coach

FULL DISCLOSURE!

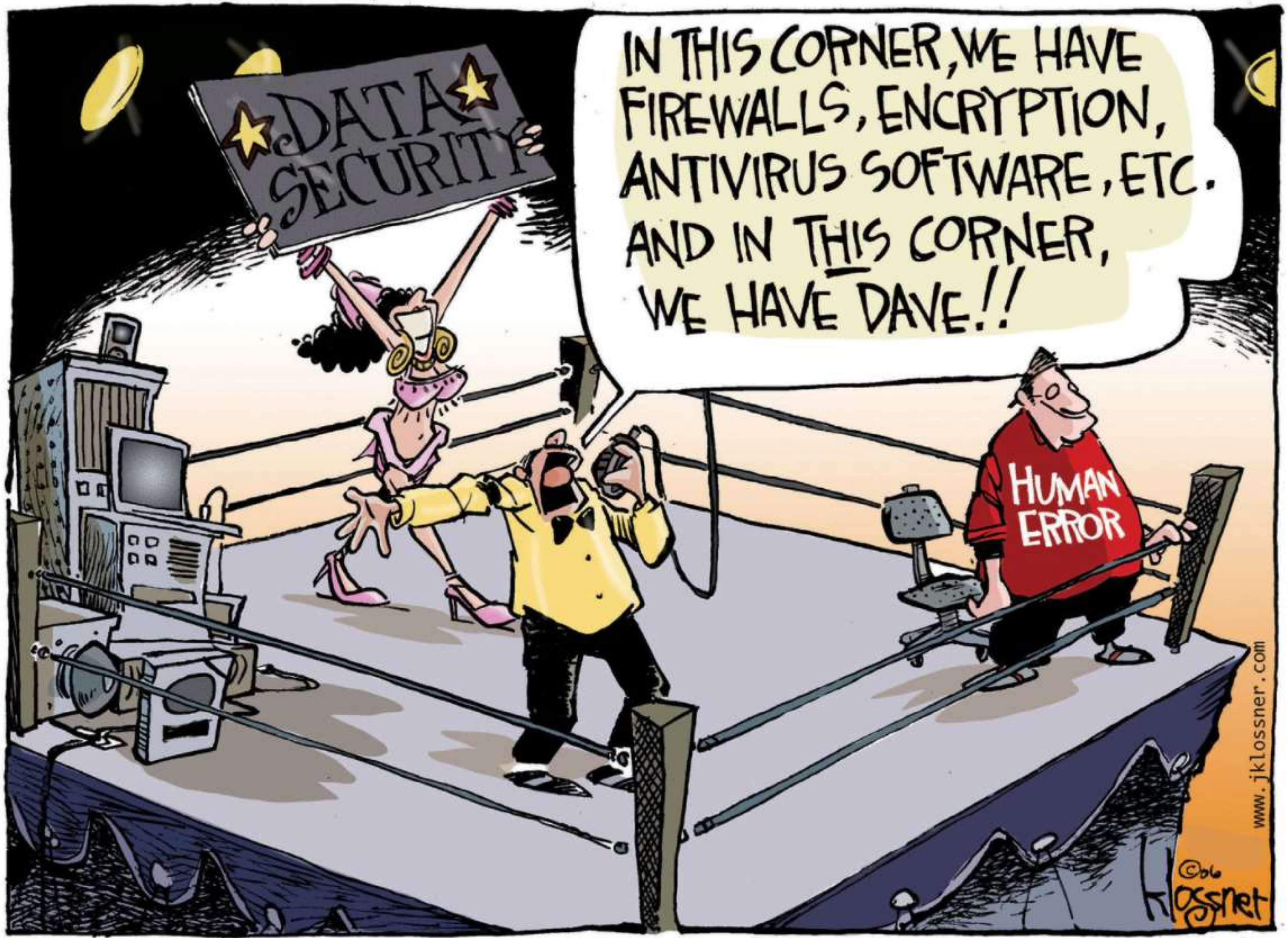
THIS IS AN OVERLOADED NERDY TOPICAL PRESENTATION

Scan the QR Code for the entire and detailed content at the end of the preso!

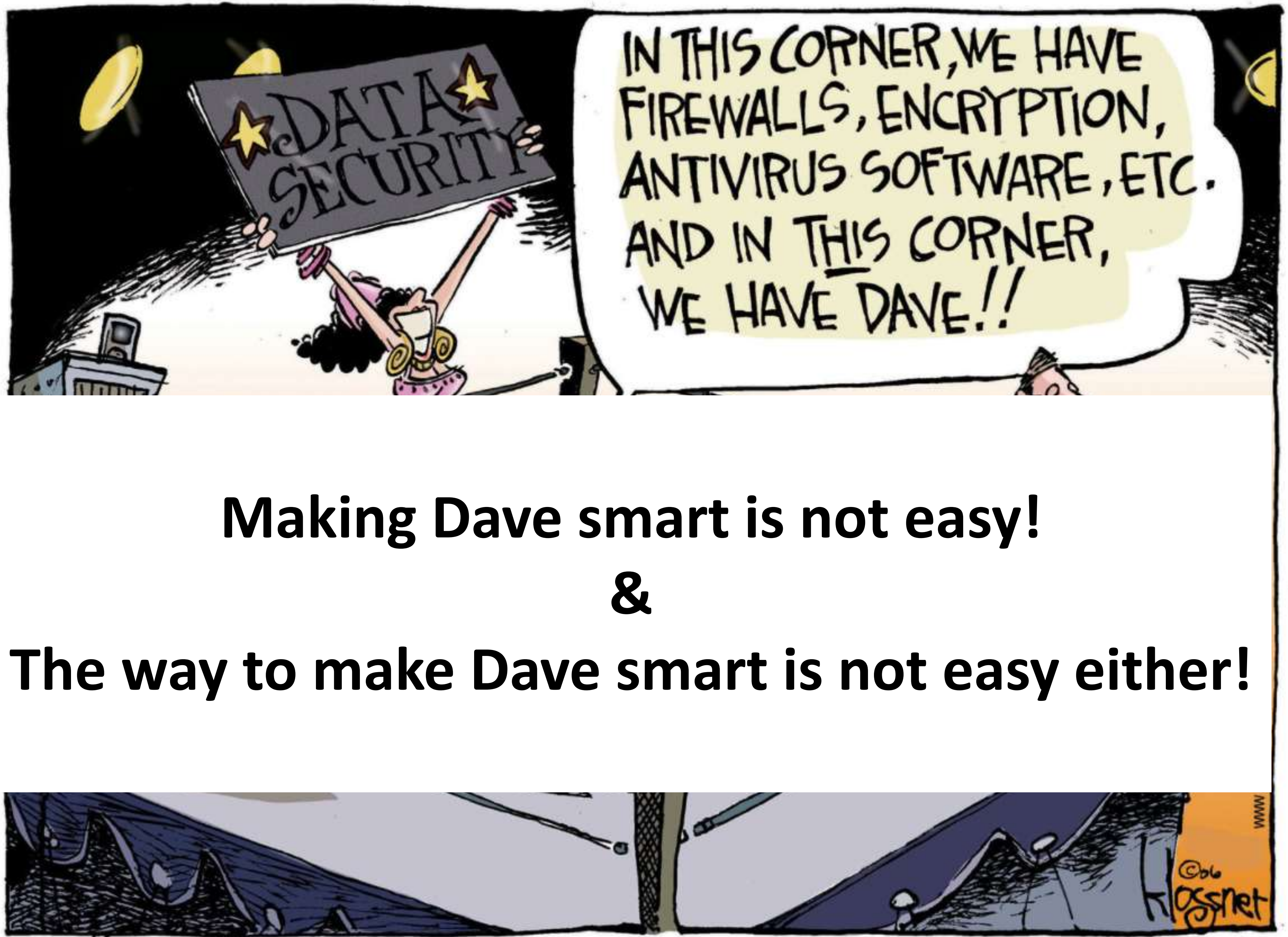
Cyber Security Awareness….

…is not Rocket Science.

But….


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

copyright 2006 John Klossner www.jklossner.com


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
©06 Klossner
www

Making Dave smart is not easy!

&

The way to make Dave smart is not easy either!

copyright 2006 John Klossner www.jklossner.com

So, train your staff with ongoing Awareness Campaigns

What do you need in order to create a perfect Phishing Simulation?

1. Get approval
2. Set Goals
3. Understand past education
4. Analyse and understand current exposure of employees in the Internet
5. Understand the infrastructure
6. Decide upon where you want to host the simulation(s)
7. Understand the technical parts from the user perspective
8. Initial communication
9. Allow users to identify and report suspective emails
10. Run the training first?
11. Selecting the right quantity and frequency
12. Choose the right people
13. Have data privacy in mind
14. Elaborate technical requirements for the web content
15. Know the limits of a given attack or training scenario
16. Selecting the right scenario type and becoming a little bit evil
17. Make it look real or not?
18. Add your own context to the scenario
19. Choose the right email sender domain
20. Decide what should happen if the users respond to attack simulations
21. Decide what should happen if the user is accessing the phishing domain directly
22. Select the right attack type
23. Decide on the usage of 3rd-party brands in a attack
24. If and when invite to an elearning in the case of a attack success
25. Subsequent follow up trainings
26. Define the disciplinary measures for the repeated occurrence
27. Test run(s)
28. Define scheduling rules.
29. Launch and monitor the campaign
30. Report the results
31. Follow up Communication
32. Create rewards
33. Define the next steps
34. Start over

Awareness Trainings and Tests are NOT Easy!

What do you need in order to create a perfect phishing simulation?

1. Get approval
2. Set Goals
3. Understand past education
4. Analyse and understand current exposure of employees in the Internet
5. Understand the infrastructure
6. Decide upon where you want to host the simulation(s)
7. Understand the technical parts from the user perspective
8. Initial communication
9. Allow users to identify and report suspective emails
10. Run the training first?
11. Selecting the right quantity and frequency
12. Choose the right people
13. Have data privacy in mind
14. Elaborate technical requirements for the web content
15. Know the limits of a given attack or training scenario
16. Selecting the right scenario type and becoming a little bit evil
17. Make it look real or not?

What do you need in order to create a perfect Phishing Simulation?

18. Add your own context to the scenario
19. Choose the right email sender domain
20. Decide what should happen if the users respond to attack simulations
21. Decide what should happen if the user is accessing the phishing domain directly
22. Select the right attack type
23. Decide on the usage of 3rd-party brands in a attack
24. If and when invite to an elearning in the case of a attack success
25. Subsequent follow up trainings
26. Define the disciplinary measures for the repeated occurrence
27. Test run(s)
28. Define scheduling rules.
29. Launch and monitor the campaign
30. Report the results
31. Follow up Communication
32. Create rewards
33. Define the next steps
34. Start over

1. Get approval

Buy-In activity!

- Did I get approval from the relevant departments (legal, risk, HR, support etc.)?
- Has anyone voiced concerns I didn’t consider?

2. Set Goals

- Measure the behaviors: A common issue with many training programs and phishing simulations is that their behavior remains unchanged throughout the course of the test. Identify the goals that your phishing simulation should meet, then design a path that evaluates if, and to what extent, each goal is accomplished. Ask yourself:
- KPIs - Did we already perform phishing simulations in the past and if yes: what were the average click/data submit rates?
- What is the expected click/data submit rate for the planed phishing simulation?
- What is the desired click and data submit rate after the simulation / training; after 1 year of simulation/training?

3. Understand past education

- Have I already trained all users on phishing & social engineering?
- Did my organization keep the results from past trainings to compare with future attack simulations?
- How do trainings currently look like (length, interactivity, video, exam, design etc.)?

4. Analyse and understand current exposure of employees in the Internet

Get abetter idea of your data exposure on public channels

One main tactic attackers use is ‘spoofing’, that is, creating emails that closely resemble those of trusted organizations.

They can then use those spoofed emails to attack your customers or employees.

Awareness Trainings and Tests are NOT Easy!

5. Understand the infrastructure

- Is it possible to whitelist the IP and sender domain from the campaign scenario on the SPAM filter?
- Is it possible to whitelist the IP and sender domain from the campaign scenario on the web proxy?
- Are there any limitations set on sending emails (for example a maximum number of emails in a specific time range)?
- Can I make sure that I set a scheduler to limit amount of emails in a given time frame?
- How to I make sure that my campaign mails do not get filtered?

6. Decide upon where you want to host the solution

Should I run the attack simulation from a cloud server or on-premise? Reasons for an on-premise installation are:

1. Legal
2. Integration
3. Security

- Do I plan to integrate the Awareness Solution with other internal systems (LDAP, LMS etc.)?

7. Understand the technical parts from the user perspective

- Do you know which types of malware can get past your defenses?
- What kind of security do you use against spoofing, malware, etc.?
- Do I know what file types can be attached

You can not plan a successful phishing simulation without knowing and understanding all the technical information involved.

8. Initial communication

The purpose of your phishing simulation is not to set a trap up for your employees to fall into.

On the contrary, it is to provide a safe environment where they can learn what phishing attempts look like in reality.

Therefore, it’s a good strategy to inform the employees prior to the upcoming campaign so they feel included.

9. Allow users to identify and report suspective emails

- What type of email clients do we use in our company and which ones should be supported?
- Where should emails get reported?
- Do we have any specifications in terms of icon design (Phish button) and text that is displayed, when a user reports a suspicious email?
- Do we have already a general report email such as: phishreporting@yourcompany.com
- Did we educate our users about the steps they need to take in case of a perceived threat?

10. Run the training first? - 1

Basically yes!

- Do I have a list of all the desired training topics to be covered?
- Through which medium (flyer, newsletter, on-site teaching, screensaver, poster, web-based teaching, etc.) should the security content be delivered to the employees?
- Are all or some parts of the training mandatory?

10. Run the training first? - 2

- Is there an optimal structure for training courses (e.g., start with theoretical part, then run a video, followed by a game, with the test at the end)?
- Do all employees in the organization get the same training or does my organization require department-specific training content?
- Is the training "success" going to be monitored? And if yes: Do I need it monitored on a personalized level?
- Shall I introduce any penalties and or other disicplinary actions for users who refuse to participate in trainings?

10. Run the training first? - 3

- What is the desired training frequency for the different training methods? How often do we plan to update the training content?
- Are there already existing trainings, which should be incorporated into our training courses?
- Do I also want to test the training effectiveness (e.g., via exams)?
- Shall I also include training gamification elements?
- Should users get a diploma or an course certificate when they pass the training exams?

10. Run the training first? - 4

- Which Languages? Shall I deliver training videos with close captions?
- Do I want the training videos to have our own logo at the start and end?
- Do I need to consider any requirements in terms of corporate design towards the training (font type, size, logo, etc.)?
- Does all training content need to work also on mobile devices? If yes: What's the minimal screen resolution?
- What is our default browser and screen resolution for

11. Selecting the right quantity and frequency

- How many phishing simulation campaigns shall I run per year?
- How many phishing emails in total should a user get per year (minimum/maximum)?

Best practice and scientific studies show that you should run MORE than four (4) attack emails per user/per year.

12. Choose the right people

Sending out a phishing simulation to the whole work force is reasonable in most cases.

On top of that, choose a group of employees you’d like to test, and only target them with a specific simulation.

That makes especially sense when you have user groups with a high(er) risk exposure.

Not all employees should be targeted in the same way.

Awareness Trainings and Tests are NOT easy!

13. Have data privacy in mind

- Anonymous Phishing Simulations?
- Un-anonymous Training Courses?
- How long do I need to keep the data collected?
- What is done with the data?
- At what level of security I need to store the data?
- Do I want to submit and store the users' input data (f.e. passwords on input forms)?
- Encryption: Should the landing page for the attack simulation be accessed over an encrypted channel and does it require a trusted certificate?

14. Elaborate technical requirements for the web

Mobile friendly?

- Do my attack & training templates need to be responsive and displayed correctly on certain minimal resolutions?

15. Know the limits of a given attack or training scenario

Examples:

If you’re planning to migrate from one security software to another (say, McAfee to Norton), you wouldn’t want to use a Norton phishing template.

Or if you are planning to run Microsoft migration or update, avoid to use such simulation attack templates.

16. Selecting the right scenario type and becoming a little bit evil

REALISTIC!
CONTEXT!

Remember, every phishing campaign must be thoroughly planned as scammers are getting more sophisticated and creative, sending out very convincing emails.

17. Make it look real or not?

Start with generic scenarios

Become more and more sophisticated

Use simple scenarios all the time (add them to the sophisticated ones)

18. Add your own context to the scenario

Always strive to create believable content. If your campaign includes a spoofed email from your financial department, make sure to use appropriate language, terminology, names, etc. Also, don’t forget to keep the spoofed party in the loop before you begin the campaign.

Think about the usage of 3rd party brands

19. Choose the right email sender domain

An important part of your phishing simulation is choosing an appropriate mail sender domain from which the emails will be sent out.

- Do the processes exist for me to whitelist the sender domains used for awareness campaigns?
- Do I also want to spoof my own company mail domain or spoof a domain from an external third-party vendor?

20. Decide what should happen if the users respond to attack simulations

For better statistics and recognizeability:

- Do I want to catch email replies?
- Do I want to “hide” the link in the message template?

21. Decide what should happen if the user is accessing the phishing domain directly

- What should happen if the recipient becomes suspicious and is checking the domain in the browser behind the random URL?

22. Select the right attack type

- What attack types do I want to use in my phishing simulation?
- Do I want to use email as the only delivery option or shall I incorporate alternative methods as well (SMS, USB , VISHING etc.)?

23. Decide on the usage of 3rd-party brands in a attack

- Does it make sense to use third party brands for phishing simulation? And if so, in which case?
- Does it make sense to use my own brand for phishing simulations and if so, do I also build a spoofed homepage of my brand for this purpose?

24. If and when invite to an elearning in the case of a attack success

- Do I want to include a training for users who fall for the attack simulation?
- Should the eLearning sent immediately or should it be delayed?
- What is the content/length/type of the desired follow up training?

25. Subsequent follow up trainings

- Should I provide additional training for low performers outside of my awareness platform?
- Shall I provide on-site tranings for my employees, especially for the low performers?

26. Define the disciplinary measures for the repeated occurrence

People make mistakes. This fact should be taken into account when considering whether and which disciplinary measures should be introduced in the organization. On the other hand, employees also bear responsibility for their work, and this should also be taken into account.

- What disciplinary action do I take for repeat offenders?
- With whom in the organization do I discuss such possible measures?
- Where do I document repeated occurences

AWARENESS TRAININGS AND TESTS ARE NOT EASY!

27. Test run(s)

- Do I have an email account or a list of pilot email recipients that can be used for testing purposes?

28. Define scheduling rules.

- Send out during working hours?
- What about the weekend?
- So, do I want to use a scheduler and if yes: what are the required rules?

29. Launch and monitor the campaign

- Do I need to monitor a campaign when it is launched?
- Do I want to have view access for dedicated users?

30. Report the results

- Do I want the reports in word, pdf, or raw format (CSV)?
- What are the grouping characteristics in reporting (department, language, country, function, scenario, etc.)?
- Should the reporting be integrated in the monitoring (SIEM, CSIRT, SOC..) may be even via API (depending on the tool used)?
- What type of reports does my organization expect (example: short management summary vs long report)?
- How should reports be delivered to me and my peers and in what frequency?

31. Follow up Communication

Remember that testimonials and positive feedback are the best ways to trigger good behavior.

Transparent reporting and communication (even anonymous) will create trust within your workforce

AWARENESS TRAININGS AND TESTS ARE NOT EASY!

32. Create rewards

Make it fun!

Reward engaged employees

Make it playful

33. Define the next steps

- What is my next campaign?
- Shall I set up and maintain an ongoing Cybersecurity Awareness Programme?

34. Start over

One simulation is no simulation

Safe behaviour is the goal

It’s a long run

Keep it funny and entertaining!

Get the Full Content

Scan the QR Code for the entire and detailed Content