IMPORTANT STEPS IN PLANNING & EXECUTING YOUR FIRST CAMPAIGN

Does it make sense to really test employees?

Yes. The benefits of a simulated attack training are:

- It increases specific awareness of the phishing and Malware threats. When employees fall for a simulated attack, they become more aware of the real threat and more receptive to the messages from IT security.
- It improves the general awareness of security. Simulated attack programs help to open the lines of communication between employees and security staff which in turn helps to improve the efficiency of general security awareness training.
- It provides security training metrics. Simulated attacks allow you to track the effectiveness of your security training over time and to target the areas or people that most need additional training.

What is needed for a successful awareness campaign?

For security awareness to be successful, it needs to be ingrained into the culture of your organization. The phishing test is just a small part of the whole awareness campaign. Without the appropriate context, the security messages from posters or presentations are lost. A blame-free culture should be created so that your employees can alert you if they feel that a mistake has been made. Education and awareness of security, successfully adopted throughout your organization, can have a measurably positive impact.

What are the best practices to ensure that you get the most out of your training program?

- Get internal buy-in to the approach from executives in all departments. Get executives from all departments on board.
- Conduct Anti-Phishing training before starting your assessments. Assess the existing level of user awareness prior to starting a new simulated attack methodology. This gives you a baseline for judging the effectiveness of this methodology and to plan future campaigns.
- Alert all your end users/employees before you start the assessment program so no one feels that they have been “tricked.”
- Start out with easy to detect emails and then gradually make them more difficult.
- Targeted spear-phishing emails should not be deployed until the end of the first year of your program, unless these are a pressing concern.
- Use variations of a category of phishing scenarios to gauge learning.
- Conduct assessments no more than monthly or quarterly.
- Keep the names of those who fall victim (fail) confidential. If there are circumstances under which you would report the information to management, such as five-time or greater repeat-offenders, explain that to end users upfront.
- Send out the results of the assessment as soon as possible after you deploy it, preferably within 48 hours of sending out the phishing email. Explain what was suspicious about the email and remind end users that it is a training exercise and that the names of those who fell for the

simulation are not reported to management.

What other preparations need to be done?

- 1.Please alert your IT or Helpdesk Department.
- 2.For the duration of the test, whitelisting the email address or addresses from the simulated phishing email templates you have chosen for simulated phishing emails.
- 3.Whitelist the domain name of the chosen landing page.
- 4.Adjusting any other settings, as necessary, to ensure the simulated phishing emails make it to end user inboxes.
- 5.Always do a test run with a few sample emails before sending them out to recipients.
- 6.Use LUCY's SPAM/Performance Test to make sure that the server can handle all requests and that emails don't get filtered.

E-MAIL COMMUNICATION AHEAD OF THE CAMPAIGN

If you plan on conducting a phishing test, we recommend that you let people know about it ahead of time. Let them know what they should expect and why. Clear communication ahead of time is key for people to accept the program.

Phishing Assessment Announcement

Here is a sample email taken from SANS Security Awareness Program:

Team,

As you know, we take information security extremely seriously. As part of our on going security awareness program, at different times, we will be testing your understanding of this training, including quizzes, awareness surveys and assessments. Starting next month, we will be kicking off phishing assessments. A phishing assessment is nothing more than when we send out an email pretending to be a hacker. These are the very same email attacks that the bad guys are sending. The only difference is that these emails will not harm you in any way. They are only designed to track how many people fall victim to them and to help you learn how to identify these scams and protect yourself.

A couple of key points.

• We will be sending out these emails once a month randomly. Each month will be different. • If you fall victim to one of these phishing emails you will be notified immediately. • If you fall victim your name will not be reported to management. It will not impact you in anyway. This training is designed to help you learn. • Twenty-four hours after each assessment, we will send an email out to everyone explaining the attack and how you could have figured out the email was a scam or attack.

If you have any questions about this program or suggestions on how to improve it, please contact [Your Contact Information Here]. They are responsible for our security awareness program and will be happy to hear from you.

Phishing Assessment Follow-up Here is an example of an email taken from SANS Security Awareness Program used to follow-up after a phishing assessment.

Team,

As some of you may have noticed, we had our monthly phishing assessment this week. As always, the purpose of these assessments is to help you identify and protect yourself against common email based attacks. I've attached, at the bottom of this email, a screenshot of the scam that went out. If this had been a real attack, simply clicking on the attachment could have infected your computer. There were some simple ways to determine that this was a scam.

1. The email was extremely generic in nature. Notice how it does not use your name but uses the introduction "Dear Customer" instead. The attack is designed to work against everyone. If your bank had sent you an email it would have used your name. 2. Notice the poor grammar and misspellings. This is another indicator the email is an attack. 3. Notice how the email comes from a @hotmail.com account. Your bank would never use such an email address.

As for the assessment, only 13 people fell victim. Great job folks. Finally, be sure to download this month's security awareness newsletter "Social Engineering" from our internal company portal. As always, if you have any questions (or suggestions) about security please contact the help desk.

Thanks!

NOTE: Be sure to include screenshot of the attack in the email so that people can read and learn from it.

Checklist: what you may ask your client prior to a phishing campaign

Topic	Details
SPAM Whitelist	Is it possible to whitelist LUCY's IP on the SPAM filter and FW?
Recipients	How many users shall be tested? Is it possible to get a list of users including email, name and additional info (like department, location etc.)?
Recipients Allocation	Shall all recipients get the same scenario simulation or a simulation preferred, where user groups get different attack scenarios?
Test Mail	What is the mail address that can be used for testing the campaign?
Distribution method	Should the phishing simulation only be send via mail or also include SMS, USB or any other form of a portable media?
Scenario Type	Should the scenario type be hyperlink only or include a landing page? Does it need a malware simulation as well?
Data Extraction	If a malware component shall be used: what should it extract (e.g. system info)? What format is desired (Word Macro vs. Executable)?
Template	Does it need a fully customized template for the mail- and landing page or is it possible to use and adjust one of LUCY predefined templates?
Domain Details	Does it require to reserve one or multiple domains? Should the domain be similar to the clients domain name or completely different?
Encryption	Should the landing page be accessed over an encrypted channel and does it require a trusted certificate?
Privacy	Is it possible to store usernames and passwords from the attack on the system (partially, full or none)?
eLearning	Should the campaign include also eLearning content? If yes: does it need to be customized? It is required that individual eLearning statistics are also logged?

Topic	Details
Running the campaign	Should all mails be send simultaneously or is it better to send the mails over a longer time period using the scheduler?
Organizational	When can the test start, until when does it has to be finished?
View Only Access	Does the client wish to get a view only access on LUCY to monitor the campaign statistics?
Log & Success Level	What is considered a successful attack (link click, data submit etc.)? Should LUCY also trigger opened mails? Can advanced client side scripts (BeEF) be executed to gather more detailed information about the user?
Login Restrictions	If a landing page with a login is created: is it necessary to let the user submit the password or shall LUCY redirect the user to a different page before the full password is entered? Is it necessary to implement regular expressions on the login fields in order to avoid false positives?
Server Location	Should LUCY run in the cloud or on the client's premises?