apalala

Human Security Testing:
Code of ethics v1.02

September 2019

1. Introduction

Scams, phishing and more recently smishing are currently the most common forms of deception using electronic communication. Phishing, particularly, is a major threat for enterprises as 13% of data breaches involve social engineering attacks (Verizon Data Breach Incident Report 2018) taking mostly the form of spear phishing.

Phishing and spear phishing are attacks using emails as a vector to lure the recipients to click on a weblink (or, more recently, to search for information leading the recipients) to a malicious website on which they will be lead to enter their username and passwords for the website that is mimicked by the malicious website or to install, willingly or unwillingly, a malware that can be used later to take the control of the recipients' computer.

To mitigate the risks linked to social engineering, security team may send regularly phishing emails to a random sample of its staff to train them and keep them aware of the risks.

This document describes what can be done, what is prohibited, what kind of data will be collected, how they will be processed and for what purpose.

1.1. Scope

This document applies to all phishing campaigns managed by the organization and its subsidiaries.

1.2. Objectives

Clearly define what can be done and what will be forbidden within the campaigns and with the data related to the phishing tests.

2. Purpose of the phishing campaigns

The phishing campaigns have multiple goals:

1. to estimate the likelihood of a successful exploitation of phishing techniques on our personnel and regularly monitor the progresses of our mitigation attempt;
2. to raise awareness of the issue amongst our personnel and change the attitude towards emails to increase the likelihood of detecting such email;
3. to increase the level of phishing detection skills of the personnel who are abused by such kind of email by providing specific trainings;
4. Increase the number of people reporting phishing attempts to the security response team;
5. Improve our knowledge of the mechanism involved in phishing detection to better focus our effort on the right control, being a training, a better user interface or any initiative that could lead to a reduction of the likelihood of a user being abused by a social engineering technique.

3. Boundaries

Real life social engineering attempts have no boundaries. Criminals will use all the tricks in the book to reach their goal. As they are often criminal organization with huge means or sometimes even sponsored by states, their only limits are their knowledge of the human cognition and their creativity.

Beliefs that advanced attacks only exist in movies may prevent people to detect it. Consequently, we must be able to subject our staff to the more realistic scenarios in order to train them efficiently. However, it doesn't mean we shouldn't set some boundaries or some ground rules.

3.1. Impersonation

An email sender can be spoofed, making the email looking like it can come from a legit or well-known and trusted source. Even if some technical controls can make it harder to use someone else's domain, it is still difficult to verify the first name and last name of the sender.

Consequently, it is realistic to use the name of people belonging to the organization or close to it. However, such impersonation must be done with the prior written approval of the person that will be impersonated. This impersonation must be limited in time and to a well-defined scope that must be clearly explained to the person that will be impersonated.

Impersonating another company's services or personnel is illegal and might have a considerable impact on their services (increase of call to their support, complaints, start of an investigation). It cannot be done without the prior approval of an executive of the said company. The same prohibition applies to the impersonation of any individual.

Also, some people can be put in copy of a phishing email or mentioned in the body of the phishing email. In such case too, the persons whose name has been used must be informed and give their authorization prior to the sending of the phishing email to the targets.

3.2. Threats

Some phishing techniques can use threats to achieve their goal. Life threats, blackmail, or any attempt to use fear as a driver **is strictly prohibited**.

On top of being unethical and dangerous for the psychological and physical health of the recipients, it won't serve an educational purpose as real threats won't be less effective due to previous exposure. However, managers should create an environment that allows staff and contractors to report threats and blackmail to them.

3.3. Active corruption and bribing

A realistic scenario can involve offering a material gain to the recipient. It could even be a form of bribery. Such scenarios could be tested but it would be illegal to act against this person. This kind of exercise must only aim at measuring a global exposure to the risk without getting down to an individual. Personal data must be anonymized to prevent identification of an individual.

3.4. Use of sensitive personal data

While criminals wouldn't hesitate to use any knowledge about a target's religion, political tendencies, criminal history, sexual orientation or ethnicity, such kind of information must not be used in an ethical phishing campaign.

4. Data Handling

4.1. What do we measure?

We measure the following parameters for each email sent (when relevant):

- Images have been accessed: (Yes/No) + Time,
- Link in email has been clicked: (Yes/No) + Time,

- Attachment in email has been open: (Yes/No) + Time,
- Scripts in the document's viewer have been enabled: (Yes/No) + Time,
- Information has been provided on the web site: (Yes/No) + Time,
- Email has been reported to the security team: (Yes/No) + Time;

We also use

- Email address of the target (Hashed with a Salt for long time storage),
- Time and date of the email delivery,
- Language of the recipient,
- Language of the message sent,
- Recipient's department,
- Recipient's country and location,
- Recipient's seniority,
- Recipient's age range,
- Recipients previous results to the tests,
- Has the recipient been previously trained for phishing and when.

4.2. Why do we need these parameters?

The first measures (image accessed, link clicked, information provided, and phishing reported) are used to measure the behaviour of the recipient and estimate its/her level of skills to detect phishing emails.

Time and date of the email delivery and the click matter as studies show that the time of the day and the day seems to have an impact on the click rate.

Language matter as the use of a secondary language might have an impact on the click rate.

Department, country and location are relevant as some departments can receive more (external) emails than others and it might have an impact on the results. Also, it will give use a way to measure the impact of the cultural relevance of some scenarios (Xmas gifts) and help us further tailor the trainings.

The recipient starting date will help us estimate the impact of our trainings and exercises on the click rate. During the first months, newcomers are less likely to have been trained on phishing detection. The age range is used to separate an effect due to the age from the seniority and absence of training.

4.3. Processing of the results

Public email addresses from employees and contractors will be uploaded to a third party that is used to send the phishing emails and measure their effects (see 4.1 for details on what is measured). The platform and the data are only accessible by the human security officers in charge of managing the phishing campaigns (2 or 3 persons maximum). As soon the scenario will be completed, data will be exported from the third-party platform and personal data will be anonymized and stored on a restricted access system. Original data on the third party will then be erased.

5. Document control

Author:	Emmanuel Nicaise
Owner:	Apalala sprl
Confidentiality:	Public
Last update:	03/09/2019
Version:	1.2
Creation date:	20/08/2018

Version	Date	Author	Change description
1.0	20/08/18	E. Nicaise	First draft
1.1	07/07/19	E. Nicaise	Split data handling and code of ethics
1.2	03/09/19	E. Nicaise	Minor changes and new design