Phishing Planning Document



# Executive Overview

The purpose of this document is to help you plan, maintain and measure an effective phishing assessment program as part of your security awareness program. It is based on the experiences and lessons learned from hundreds of security awareness officers. Below are a series of steps and questions. By going through each step, you will be ready to launch a high-impact and engaging phishing program. If you have any comments or suggestions on how to improve this document, please email us at [community@securingthehuman.org](mailto:community@securingthehuman.org).

# Goals

Define the goals of your phishing program first. Below are the most common goals we see. We recommend that you build all these goals into your program at some point.

1. **Measure Human Risk**: Your program is designed to measure how vulnerable your organization is to phishing attacks and what impact your organization’s awareness program is having on reducing that risk.
2. **Reduce Human Risk**: Your goal is to reduce the risk of people falling victim by reinforcing key phishing learning objectives. You do this by notifying people when they fall victim and potentially providing additional training.
3. **Measure Detection**: Your program is designed to measure your organization’s ability to detect and report phishing attacks.
4. **Increase Detection**: Your goal is to increase people’s awareness for the need to report phishing attacks and reinforce how to report such attacks. You are developing what is often called the Human Sensor.

For many organizations, it is common to have a failure rate of around 40% for their very first phishing assessment (depending on type of phish, culture of organization, current state of awareness, etc). Over time, it is possible to get that failure rate down to 5% or even less. Remember, it is impossible to eliminate risk, including human risk. But you can dramatically reduce it and measure that reduction. Finally, once you have a mature awareness program, the people that most commonly fail phishing assessments we tend to see are new hires.

# Planning

You need to identify the following key points to successfully plan your phishing program:

1. **Approval**: Has management approved the phishing program? If so, who approved it? Is it in writing?
2. **Project Manager**: Who is responsible for the phishing program? What departments does this person have to coordinate with before each phishing email is sent out? Examples include the information security team, the training department, help desk and Human Resources.
3. **Frequency and Timing**: How often are you going to run your phishing assessments? We recommend monthly for maximum impact. Be sure to randomize on what days you send your phishing emails, to include sending them mornings, evenings or even weekends and holidays.
4. **Target**: Whom will you target in your phishing program? Will different targets get different types of phishing emails based on their risk category? Will you identify targets by role, department, region or some other method?
5. **Language**: Will you need to support phishing in multiple languages?

# Key Points to Success

Most phishing assessment programs fail not because of technology issues but due to human or emotional issues. As you plan and execute your phishing program, keep these key points in mind:

1. **Emotion**: Phishing assessments are like any other assessment or penetration test in many ways. However, the biggest difference between assessing a computer and assessing people is that computers do not have feelings but people do. If you execute your phishing program without taking people’s feelings into consideration, you will quickly upset both employees and management, causing your phishing program to fail.
2. **Announce**: Announce and explain your phishing program to the entire organization ahead of time. Explain to them what you are going to do and why. Be sure to emphasize that you are not out to trick anyone; you are just replicating the same attacks the bad guys are launching. You can find an example of such an email in the appendix of this document.
3. **Start Simple**: Start your phishing program with a simple phishing email that everyone should be able to detect. Perhaps even tell them exactly when you will launch the very first one. No one should fail, but many people will. This way, people will not resent the program when you first launch it. A common mistake many organizations make is they start their phishing program by making their first phishing email as tricky as possible, which causes huge numbers to fail and generates widespread resentment. In addition, be careful of using lures that are too emotional or sensational; this may make employees feel betrayed or may be forwarded outside of the organization. Start slow and simple. Only start increasing the difficulty of your phishing emails after people are used to the program.
4. **Coordination**: For larger organizations, you may want to coordinate with other business units. For example, they may want to provide input on whom to target in their organization or what type of phishing emails they feel will be the most effective.
5. **Names**: Do not publicly reveal names of people who fall victim and do not create a wall of shame. In fact, we recommend that no one in management receive the names of people who fall victim. If they do, employees will learn to resent the program, as they will believe anytime they fall victim, it will negatively impact their careers. The only time an employee should be reported to anyone in management is if they are a repeat offender and represent a high risk.
6. **Detection**: Ensure there are 2-3 ways people can detect the phish when you send it. (No, analyzing IP headers does not count.).
7. **Europe / Unions**: If you are planning a phishing program in Europe or other regions with very strong privacy regulations, you may need to approach your program differently. First you will most likely need a Works Council (WC) approval, or something equivalent. Begin with educating your Works Council on the dangers of phishing and the impact to employees (remember that Work Councils are only concerned about the individual – not your organization). It is also important to not use terms such as ‘*testing*’ or ‘*assessment*’ but instead use terms such as ‘*training’*. Alerts go off if Work Councils believe employees will be tracked or punished for their actions. If you have a Human Resources or Learning Management team, coordinate with them to build message in a way that will work with your Works Council. In addition, you may have to modify how you collect information in your phishing program and/or what is done with that information. Remember, you can still run an effective phishing program even if you never know who fell victim.

# Results

What do you want to happen when someone falls victim? Specifically, what happens when a person clicks on a link or opens an attachment? Options are:

1. **Not Notified**: The victim is not notified they fell victim to the test. This approach is best used purely for metrics because there is no reinforcement. However, this is good for establishing a baseline or as an annual metric for measurement.
2. **Notified**: The victim is given immediate feedback that explains they just fell victim to a phishing assessment and how they could have detected it was a phish. In addition, follow-up training can be provided. This method is highly effective at reinforcing key behaviors, as this can be an emotional moment for the victim; they will remember the incident and, as a result, are more likely to change behavior.

Do not report someone to management if he or she has fallen victim for the first time. For repeat offenders that continually fall victim and represent a high risk, the following is one approach you can take. We recommend you modify this process to best fit your own organization’s culture / requirements.

1. **First violation:** Employee is notified they fell victim and given the option to take additional training. This can include online training or links to additional information.
2. **Second violation:** Employee is notified, their manager is copied and employee is required to take additional training.
3. **Third Violation**: Employee is notified and their manager is notified. In addition their manager is required to have a meeting with employee. The result of that meeting is then reported to the security team. Finally, employee has to take additional training.
4. **Fourth Violation**: Employee is notified, employee’s manager is notified and employee must report to Human Resources.

As part of the results, you need to decide if you are going to track how many people reported the phishing attack. Specifically, do you want to measure people’s detection capabilities (often called the Human Sensor)? If you want to track reporting of the phishing emails, you will need to define several points, to include:

1. **How**: Whom do people report a phishing attack to and how do they do it? This could be something as simple as an email alias, or perhaps something more sophisticated, such as a website submission form or a plugin built into the browser.
2. **Criteria**: What are the criteria for reporting? Do people report any scam or phishing email, regardless of how simple the attack is? Or do people report only sophisticated attacks or emails they are not sure about?

# Reporting Results

After each phishing test, consider how you will report the results. We recommend you have a process like the following:

1. **Employees**: After every phishing test, send a follow-up email to every individual that was targeted in the phishing test. The follow-up email should explain that a test was sent, how the phishing email could have been identified and how many people fell victim to it. In addition, you may want to include a screenshot of the email itself. The purpose here is to reinforce key learning objectives for those who may not have fallen victim or even noticed the phishing email. We recommend you send the follow-up email 24-48 hours after the assessment. You can find an example of such an email in the appendix.
2. **Management**: Have a process in place to update management on the results. We recommend you do so quarterly or bi-annually. That way, you are focusing more on strategic trends as opposed to individual phishing assessments. For example, you may want to look for patterns of behavior by business unit – some units may be more susceptible than others due to the nature of their jobs (e.g., call centers, HR, sales staff). You can also analyze what types of phishing emails appear to have the greatest impact on the organization or if your training has effectively changed behavior over time. Finally, depending on your organizations culture you can compare the results of different business units or departments, perhaps create a sense of competition on which group can get the best scores.

# Appendix A: Phishing Assessment Announcement

If you plan on having a phishing assessment program, we highly recommend you let people know about it ahead of time. Let them know what the ground rules, what they should and expect and why. Clear communications ahead of time are key for people accepting the program.

*Team,*

*As you know, we take information security extremely seriously. As part of our on going security awareness program at times we will be testing your understanding of this training, to include quizzes, awareness surveys and assessments.  Starting next month we will be kicking off phishing assessments. A phishing assessment is nothing more then 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 these emails will not harm you in any way, they are only designed to measure behaviors and 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, on a random day and time. Each month will be different.*
* *If you fall victim to one of these phishing emails you will be notified immediately. However, your name is not reported to management or anyone on the security team, 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]. She is overall responsible for our security awareness program and will be happy to hear from you.*

# Appendix B: Phishing Assessment Follow-up

Example of an email 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 very simple ways to determine that this was a scam.*

*1. The email was extremely generic in nature.  Notice how it does not have your name but uses the introduction "Dear Customer" instead. The attack is designed to work against anyone.  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 people can read and learn from it.