
Phishing Strategic Planning Document



Table of Contents

<u>EXECUTIVE OVERVIEW</u>	<u>3</u>
<u>GOALS</u>	<u>3</u>
<u>PLANNING.....</u>	<u>4</u>
<u>KEY TO SUCCESS.....</u>	<u>5</u>
<u>FIRST TIME OFFENDERS.....</u>	<u>7</u>
<u>REPEAT OFFENDERS.....</u>	<u>7</u>
<u>FOLLOWING-UP.....</u>	<u>10</u>
<u>PEOPLE REPORTING PHISHING ATTACKS.....</u>	<u>10</u>
<u>TIERED PHISHING TEMPLATES.....</u>	<u>11</u>
<u>METRICS AND MEASUREMENTS.....</u>	<u>12</u>
<u>APPENDIX A: PHISHING SIMULATION ANNOUNCEMENT</u>	<u>13</u>
<u>APPENDIX B: PHISHING SIMULATIONS FOLLOW-UP</u>	<u>14</u>
<u>APPENDIX C: CONTACTING REPEAT CLICKER.....</u>	<u>15</u>
<u>APPENDIX D: RESPONDING TO REPORTED PHISHING EMAILS.....</u>	<u>16</u>
<u>APPENDIX E: TIER 01 PHISHING SIMULATION EXAMPLE</u>	<u>17</u>
<u>APPENDIX F: TIER 02 PHISHING SIMULATION EXAMPLE</u>	<u>18</u>
<u>APPENDIX G: TIER 03 SIMULATION EXAMPLE.....</u>	<u>19</u>
<u>APPENDIX H – PHISHING FAQ (FREQUENTLY ASKED QUESTIONS)</u>	<u>20</u>

Executive Overview

The purpose of this document is to help you plan, maintain and measure an effective phishing simulation program as part of your security awareness program. The document is based on the experiences and lessons learned from hundreds of security awareness officers. There are two ways to leverage this document. If your phishing simulation program is new, or if you are new to the world of phishing then you should read this document from beginning to end. It will give you a comprehensive grasp of all the key challenges and approaches. If your phishing simulation program is mature and you are looking to solve a specific challenge, then refer to the Table of Contents and simply jump to the section you need help with. As Phishing Programs can be complex, you may want to consider creating a Program Charter to help document all the key points. Ask your Client Support Manager for an example if you would like one.

Goals

Start first with defining the goals of your phishing program, what is it you hope to achieve. Below are the two most common goals we see. Be sure to get data from your Security Operations Center (SOC) and Incident Response team on past phishing incidents to better understand what your top phishing risks are, as these can help you better clarify your goals. If you have a Threat Intel team they can provide insight on future, perceived threats.

1. **Reduce Phishing Risk:** Manage the human risk to your organization by reducing the probability of someone falling victim to a phishing attack. You may want to set as a goal a specific click rate, percentage of repeat clickers or a certain reduction of clickers over time. [Do not set a 0% click rate as your goal](#). As your phishing program matures you may adjust these goals or even develop different goals for different target groups, departments or locations.
2. **Increase Detection Capabilities:** Decrease the impact to your organization by improving people's ability to identify and report phishing attacks. You are developing what is often called the Human Sensor and is an extremely powerful resource, especially in detecting and stopping targeted attacks. If you are going to train your workforce to report phishing attacks ensure you have the resources and processes to consume, act on and respond to all submitted reports.

For many organizations, it is common to have a failure rate of around 30% 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 2% or even less. Remember, it is impossible to eliminate risk, including human risk. But you can dramatically reduce it and measure that reduction.

Planning

You need to take the following steps to successfully build your phishing simulation program:

1. **Approval:** Has leadership approved the phishing simulation program? If so, who approved it? Is it in writing? Consider any other necessary or anticipated approvals to include Legal, HR or Ethics. It may be beneficial to set the expectations before program execution.
2. **Project Manager:** Who is overall responsible for the phishing simulation program? What departments does this person have to coordinate with before each phishing simulation. For example, the Information Security team, Human Resources, Legal or the Help Desk?
3. **Frequency and Timing:** How often are you going to run your phishing simulations? We recommend monthly for maximum impact, with the test running for 2-5 business days, depending on the size of your organization. Be sure to randomize on what days you send your phishing emails, to include sending them mornings, evenings or even weekends and holidays. Consider any impacts to other functional teams. For example, many Help Desk teams are very busy on Mondays.
4. **Scope:** What regions or offices will you phish? Will you phish contractors, vendors, interns or other non full-time employees. If possible, we recommend phishing as many people as possible. Ensure that all executive leadership are also included in your scope. If you are not allowed to phish senior executives then we recommend you do not pursue your phishing program, this sets the wrong precedent and sends an undesirable message to your workforce.
5. **Target:** Will different target groups get different types or tiers of phishing emails based on their risk category? Will you identify targets by role, department, region or some other method? If you are just starting your phishing program we recommend you keep things simple and phish everyone with the same phishing email. Over time as your program matures you can change to different phishing simulations based on different target groups and risks levels. For more information on selecting different phishing templates based on target groups, refer to the Tiered Phishing Template section.
6. **Language:** Will you need to support phishing in multiple languages, if so which languages? This includes any anticipated training.

Key to Success

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

1. **Emotion:** Phishing simulations are in many ways like other security assessments or penetration tests. However, the biggest difference between assessing a computer and assessing people is that computers do not have feelings - 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. This is training to help them. 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 simulation that everyone should be able to detect. Perhaps even announce ahead of time 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 simulation as targeted as possible, to demonstrate just how vulnerable their organization is. This approach causes huge numbers of people 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. In fact, your very first phishing simulation is less about metrics and more about simply building cultural acceptance. Only start increasing the difficulty of your phishing emails after people are used to the program, say six to eighteen months later. For more about different tiers of phishing templates refer to the Tiered Phishing Templates section.
4. **Coordination:** For larger organizations, you may want to coordinate with other business units or departments. For example, the SOC, Incident Response, Help Desk and email teams will require notification and can also support and promote the program. Additionally, other stakeholders 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:** Never 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 anyone should be reported for clicking is if they are a repeat offender and represent a high risk (covered in more detail in the Repeat Clickers section).
6. **Detection:** Ensure there are at least two to three indicators that the simulation is a phish. Sending out a phishing simulation with no way for people to determine it is a phish will only create frustration and anger (No, analyzing IP headers does not count.).
7. **Privacy Laws / Unions / Work Councils / Represented Employees:** If you are planning a phishing program in Europe or other regions with very strong privacy regulations or union rules, 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*' or '*simulations*'. 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, such as only collecting the number of people who clicked, not their names or identities. Remember, you can still run an effective phishing program even if you never know who fell victim.

First Time Offenders

What do you want to happen when someone clicks for the first time? There are two general options.

1. **Not Notified:** The learner is not notified they fell victim to a simulation. This approach is best used purely for metrics as there is no reinforcement or learning opportunity. However, this approach is good for establishing a baseline or as an annual measurement. We recommend this approach once a year providing you have been periodically testing throughout the year.
2. **Notified:** The learner is given immediate feedback after clicking that explains they just fell victim to a phishing simulation and how they could have detected it was a phish. In addition, follow-up training can be provided, such as a micro-video. This method is highly effective at reinforcing key behaviors, as this can be an emotional moment for the learner. They will remember the incident and, as a result, are more likely to change behavior. More on this from the [BJ Fogg Behavior Model](#).

Do not report someone to management if they have fallen victim for the first time. That will quickly create resentment and the reporting has no value, as a first time click is an outstanding training event. Only report and act on an individual that is a repeat offender.

Repeat Offenders

For repeat offenders that continually fall victim (to both simulated and / or real phishing attacks) and represent a high risk, you will need to define some process on how to respond. This process is very different for every organization as is it driven by your organization's policies, culture and tolerance for risk. How a university handles a tenured professor that is a repeat clicker will be very different then how a defense organization developing the F-35 fighter handles a repeat clicker. However, before you define the process you have to first define what a repeat clicker is. We do not consider someone that opened a phishing email as 'a clicker'. People have to open emails to get work done and review the email. Our definition of 'clicking' is opening an attachment, clicking on a link or falling victim to the simulation in some way. Make sure you are working with your Human Resources as you define what a repeat clicker is and the steps you take as a result. As this could impact work status of your workforce, Human Resources should be involved in every step. Here are some options for defining a repeat clicker (there is no industry recognized definition of the term).

1. If you phish everyone in your organization with every phishing simulation, then you can define a repeat clicker as someone who clicks a certain number of times over a certain time period. For example, if you phish everyone every month you can define a repeat clicker as someone who clicks three times in a calendar year, clicks 50% of the time over a six month period, or falls victim three consecutive months in a row.
2. If you phish only a sampling of people every time, make sure previous clickers are always included. For example, let's say you are a very large organization (100,000 employees) and only phish 10,000 random people every month. What you could do is then automatically include everyone that clicked on the simulation from the previous month. So what you end up doing is every month you are phishing 10,000 random people PLUS everyone who clicked the previous month.

Once you have defined what a repeat clicker is, you can then build your processes. The first thing we recommend is interviewing repeat clickers (or at least a sampling of them) to better understand the issues involved. There may be an issue you are not aware of, such as perhaps they have a learning disability, dyslexia or a personal event that is negatively impacting them. Perhaps they are not actually being trained when you believe they are or you need to make changes in your training approach. Gather feedback on the phishing training program, you may be surprised at what you learn. Ultimately your goal is to determine if they are a repeat clicker due to motivation (they don't care) or ability (they can't determine if an email is legitimate or a phish). In the Appendix is an example email template you can use for reaching out to a repeat clicker. In addition, consider an escalation process especially if your organization has a low risk tolerance. An escalation process has increasing consequences after each repeated click. Below is one example.

1. **First violation:** Learner is notified they fell victim to a phishing simulation and given the option to take additional training. This can include online training, in person training or links to additional information. If you experience a high volume of first time offenders, a Just In Time training page can be presented to the clicker when opening the attachment or clicking on the link.
2. **Second violation:** Learner is notified they fell victim, their supervisor is copied and the learner is required to take additional training.
3. **Third Violation:** Learner is notified they fell victim, however their supervisor is sent the email and the Learner is copied. In addition, their supervisor is required to have a meeting with individual. This Learner/supervisor session is imperative since the fourth violation results in Human Resource involvement. The result of that meeting is then reported to the security team. Finally, learner has to take additional training.

4. **Fourth Violation:** Leaner is notified they fell victim; their supervisor is notified and they must report to Human Resources for further action.

One option for a repeat clicker is “re-set” them by sending repeat clickers the simplest phishing simulations possible (see Tiered Templates section) to help them build their confidence and their understanding of the fundamentals. If you have a large number of repeat clickers perhaps treat them as a separate or unique target group with each phishing simulation. Finally, here are some key questions to consider when rolling out a Repeat Clicker program

1. Document what a Repeat Clicker program is and why you want one.
2. Who is in charge of it?
3. What is your definition of repeat clicker?
4. What is the scope of the program, who falls under it? Employees, contractors, interns, volunteers?
5. Do you have any strategic goals or objectives you want to define?
6. Is your overall approach more punitive or nurturing?
7. Who is responsible for tracking repeat clickers and how will they do it?
8. Who is responsible for tracking the training repeat clickers complete?
9. Who is responsible for reporting repeat clickers to Business Units or supervisors? Who should have access to that information?
10. Who is responsible for communicating all of this to the company once agreed upon, who will answer employee questions?

NOTE: If your documented process for repeat offenders includes HR involvement or punitive actions, be certain you can support the metrics with absolute confidence. You will need to defend the statistics, chances are you will be challenged.

Following-Up

After every phishing simulation, send a follow-up email to every individual that was targeted. 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 closing of the assessment test. You can find an example of such an email in the appendix.

An option to also consider is gamify this process. After every phishing simulation, identify everyone who did NOT click and reported the email, and then enter them into a raffle. Select one person and then give that person a token reward, such as a \$15 gift card for lunch or the local coffee shop. Then, include that person's name as the winner of "Surviving the Phish" raffle in the monthly follow-ups. People love this as it recognizes those who do not click. People do not care so much about winning the \$15 gift card, what they care about is having their name in the follow-up email that everyone reads. Surprising powerful and yet simple motivator.

People Reporting Phishing Attacks

As part of your program, you need to decide if you are going to teach people to report phishing attacks, and if so how are you going to manage that reporting process? 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, a plugin built into the browser or an email client add-on.
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?

One suggestion. If you do have people reporting, encourage them to include how they detected the email was a phish. This way you can start tracking which indicators are the most effective to be teaching people, and which indicators are the least effective (and perhaps stop teaching them).

Tiered Phishing Templates

If your phishing program is new we recommend you start simple by sending the same phishing template to everyone. However, as your program (and organization) matures not only will your overall click rate go down but you will begin to identify higher risk roles, departments or target groups, such as accounts payable. At such a point you may want to consider using a tiered approach. A tiered approach enables you to create different categories of phishing simulations that become progressively more targeted and harder to detect. Then different target groups are assigned different Tiers based on your requirements. Here is one way you could approach Tiered phishing simulations.

- **Tier 01:** This tier is the simplest and represents the most common or generic type of mass phishing attacks and are the easiest to spot. These emails have misspellings, poor or little graphic design, and are often based on well-known scams. After someone has been exposed to Tier 01 phishing simulations over a period of time (perhaps 6-12 months) you can begin migrating them to Tier 02 phishing simulations. Another metric you can use is when the phishing click rate falls below 5-10%, consider moving to Tier 02. For an example of a Tier 01 phishing simulation refer to the Appendix.
- **Tier 02:** Tier 02 phishing simulations are designed for more experienced employees who have gone through multiple phishing simulations and who have the awareness and behaviors needed to repeatedly identify Tier 01 phishing simulations. These phishing simulations still represent large scale, mass phishing attacks but are more professional and /or more personalized, such as using the victim's name or the email references the company or industry they are working for. These simulations have no spelling or grammar mistakes and are more likely to be work related, personalized or have powerful emotional hooks. As a result, they are more difficult to spot. For an example of a Tier 02 phishing simulation refer to the Appendix.
- **Tier 03:** This tier represents targeted attacks, such as spear phishing, whaling or BEC / CEO Fraud. These phishing emails are highly customized and often used for smaller, high-risk target groups (Accounts Payable, senior executives, Human Resources) or highly trained staff. For ideas on Tier 02 or Tier 03 type phishing templates not only work with your phishing vendor but your Security Operations Center and Incident Response team. What are the most common phishing attacks they are seeing, especially customized or targeted attacks, and highly targeted employees i.e.CIOs. Use those real attacks as templates for your more targeted phishing simulations. For an example of a Tier 03 phishing simulation, and more background on targeted attacks, refer to the Appendix.

Metrics and Measurements

When it comes to metrics the first thing to remember is that you are not measuring a single value in a single point of time. For example, we do not recommend doing only one phishing simulation, then taking that click rate (say 18%) and then trying to decide if that is good or bad. The value of metrics is how you are doing over time. For example, track how the click rate has changed over the past 18 months (hopefully dramatically down). As your program matures you may identify different departments, regions or risks groups and track them individually. These are the most common metrics we see organizations track over time.

- **Overall Click Rate:** Overall percentage (or number) that fell for the simulation. This is the metrics most organizations start with.
- **Repeat Clickers:** Percentage or number of people that are repeat clickers. We tend to see this metric in more mature phishing simulation programs. To be honest, this is the one we feel you should be more concerned about in the long term.
- **Reporting:** Percentage or number of people that did not fall for the simulation and instead reported the phishing simulation.

If you are using different Tiered phishing simulations you may have to track your metrics by Tier, as people are more likely to fall victim to a Tier 03 simulation as opposed to a Tier 01 simulation. In addition, 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 your 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 Simulation Announcement

Before starting your phishing simulation program, we highly recommend you let people know about it. 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.

Folks,

As you know, we take information security extremely seriously. As part of our ongoing security awareness training we will be kicking off a phishing simulation program. A phishing simulation is nothing more than when we send out a phishing email pretending to be a cyber attacker. We will be simulating the very same email attacks that the bad guys are targeting with us today. These simulations will not harm you in any way, they are only designed to help you learn how to identify these scams and protect yourself at work and at home. A couple of key points:

- We will be sending out these emails periodically, on a random day and time.*
- If you fall victim to a phishing simulation you will be notified right away. Your name is not reported to management or anyone on the security team, no one will know and it will not impact you in anyway. This training is simply designed to help you learn. We are all in this together.*
- Twenty-four hours after the closure each assessment we will send an email out to everyone explaining the phishing simulation and how you could have identified 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.

NOTE: If you do have an escalation process for repeat clickers, you may want to add something about that to this notification email.

Appendix B: Phishing Simulations Follow-up

Example of an email used to follow-up after a phishing simulation.

Folks,

As some of you may have noticed we had our periodic phishing simulation this week. As always, the purpose of these simulations 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 simulation that went out. If this had been a real attack, simply clicking on the URL in the email 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 how the email creates a strong sense of urgency, trying to rush you into making a mistake.

3. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.

As for the simulation, only 8% 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. Finally, the simulation has concluded, if you still have the email in your inbox, please just delete the email or open to review the brief awareness hints.

Thanks!

NOTE: Be sure to include screenshot of the attack in the email so people can read and learn from it. Even better, highlight or circle in that screenshot the indicators of a phishing attack.

Appendix C: Contacting Repeat Clicker

Below is an example email template you can use for reaching out to a repeat clicker. Make sure whatever template you do use is first reviewed by Human Resources and/or Legal. Do not contact someone who has clicked for the first time. That is purely a training event, we do not want them to feel singled out for learning. The only time you reach out to someone is if they have repeatedly failed the simulations and represent a high risk to your organization. Also, try to use this as an opportunity to help and create an ambassador. You do not want to come in hard with repercussions, or security will quickly develop the reputation of being difficult to work with and to be avoided.

Dear [Name],

We noticed that you have fell for several of our phishing simulation trainings in the past months. These simulations replicate the very same attacks the bad guys are launching against both our company and you at home. If you have a moment, we would really appreciate 20 minutes of your time to ask you a few questions and better learn how we can help you identify and stop these attacks. People like you are key to protecting our data and reputation, we need your help. In addition, we want to be sure you can make the most of technology at home also. Could you let us know when we can stop by your office sometime this week or next?

Your dedicated (and appreciative) information security team.

Appendix D: Responding to Reported Phishing Emails

If you are training your workforce to report phishing attacks, you need to ensure you always respond to any reported email. Positive feedback like this ensures people will continue to report. If someone reports a suspected attack and receives no response, they are far less likely to report again. Keep in mind, when someone reports a phishing email they have no idea if the phish was part of your phishing simulation or a real attack. Do not clarify either way, simply recognize them for their efforts and the impact it has.

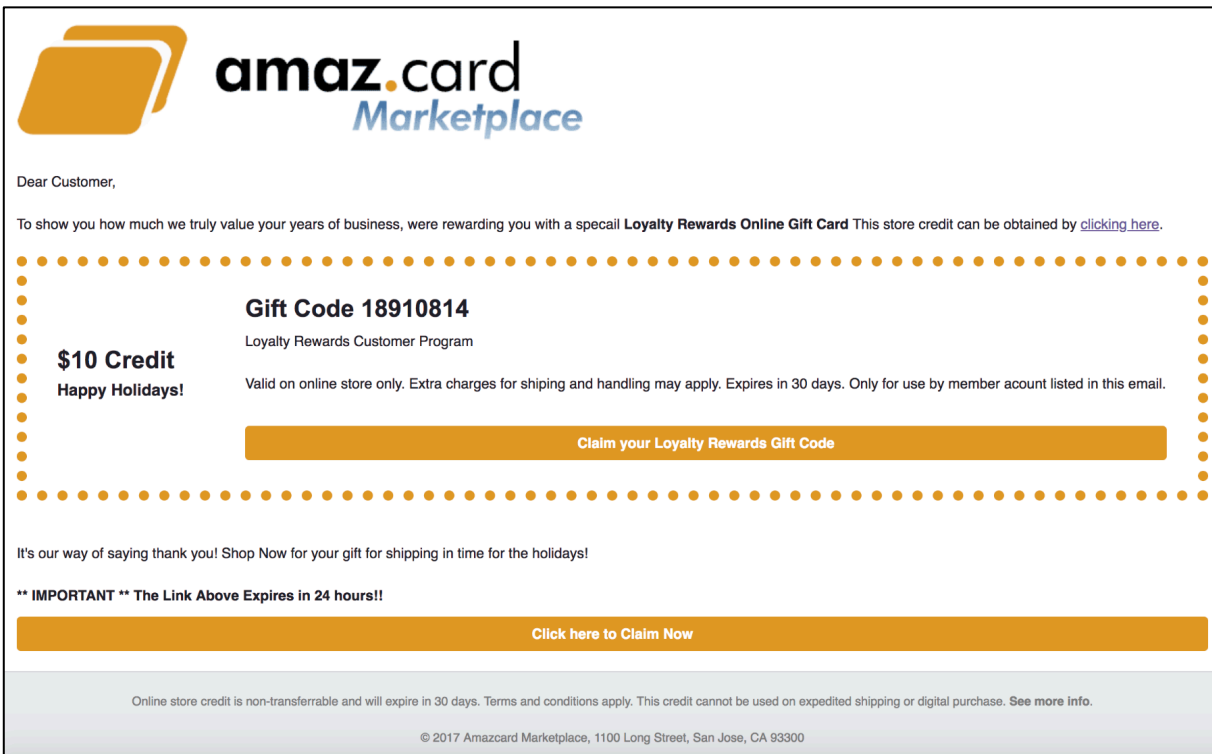
Dear [Name],

Thank you so much for your phishing submission, our security team greatly appreciates it. Our team will review the email and quickly act accordingly. We work extremely hard at and invest a tremendous number of resources in ensuring phishing attacks do not get through our networks, unfortunately we cannot identify or stop them all, especially customized targeted attacks. It's because of people like you we are far more secure. Keep up the amazing work, we greatly appreciate it!

Your dedicated (and appreciative) information security team.

Appendix E: Tier 01 Phishing Simulation Example

This is an example of a simple phishing simulation. It is generic "Dear Customer" and easy to detect as this organization does not really exist, so you could not possibly be a customer for it or belong to it's rewards program.



Appendix F: Tier 02 Phishing Simulation Example

This is a more targeted and personalized simulation. Personalization is becoming more and more common in mass scams or emailings due to [the vast amount of information cyber criminals can easily purchase on people](#). In this example below, we use the individual's name, which is very easy for a cyber criminal to obtain. Second, the simulation leverages both urgency and curiosity (two strong emotional triggers) in this email as it's tax related. Three, this email is work related which people are more likely to fall for while at work.

Dear {fname},

Our records indicate that your employer has enrolled in the Employee Self Service Paperless W2 Program. As a result, you do not receive a paper W2 for the tax season but instead receive an e-mail notification that your tax information is ready for viewing.

This notice is to remind you that your W2 is ready for viewing:

[Click here to view W2](#)

If you have trouble accessing your forms at the link above, please contact your Accounting or Payroll department for support.

To change your Employee Self Service Paperless W2 Program preferences or update your contact information, [access your profile information here](#).

- TaxPortal

Appendix G: Tier 03 Simulation Example

These simulations are the hardest to detect because of the customization and personalization. This is what people consider spear phishing, whaling or CEO Fraud / BEC type attacks. These simulations have no logo or branding as they usually emulate a simple email conversation. The attacker often pretends to be an individual that the target knows, such as their boss, a senior leader or a partner they are working with. They do this through email spoofing. Spoofing is nothing more than forging the FROM email address to make it appear it came from someone else, this is extremely simple and can be done multiple ways. For example, the attacker can create a domain name that looks like your company's. Or even more common now is the bad guys use a generic @gmail.com email address they control, but make sure the email has your boss's name. So for example, they send the email from "Your Boss's Name"<david37428@gmail.com>. Most people do not bother reviewing the email address, only the name. Attackers obtain this information using [through OSINT methods](#), such as researching the target organization on LinkedIn. Often targeted emails are very short with only several sentences, have a sense of urgency and a generic signature such to "Sent from my mobile device".

{fname}, We're scheduling a team meeting and want to know your availability. Please check the Team calendar and let us know if you have any conflicts with the suggested times. Thank you very much.

Calendar: [{hook_url}](#)

Sent from my iPhone

Appendix H – Phishing FAQ (Frequently Asked Questions)

Q: Why do we phish our own employees?

A: To help you. Phishing simulations help you recognize real phishing attacks, both at work and at home. They toughen you up for the below-the-belt sucker punch that a real hacker could deliver at any moment. They also help our security team focus and gauge the effectiveness of training efforts.

Q: Is everyone phished, or just some people?

A: Everyone in every department is phished, including executives, senior managers, and IT staff. We like to do this as an equal opportunity training program.

Q: Who can be tricked?

A: Anyone. Even IT pros have been fooled. But folks who are paying attention and know what to look for are very difficult to trick.

Q: I clicked the link. Am I a failure?

A: Absolutely not. Mistakes are a necessary part of learning any new skill, be it riding a bike or recognizing fake email. The key is learning from those mistakes. That is the entire purpose of these simulations, to provide you a safe environment to learn.

Q: Are supervisors or HR informed when an employee falls victim?

A: No. The goal is to improve skills. Naming victims doesn't aid learning.

Q: Are employees disciplined for failing simulations?

A: The only time there are consequences is if someone repeatedly falls victim, representing a high risk to our organization.

Q: Why does it matter if I fail a simulation?

A: If you are vulnerable to simulated attacks, then you are vulnerable to real attacks. Real attacks are all too common, and the consequences can be severe.

Q: What could happen if I fall victim to a real phish?

A: You, your co-workers, or the public could be harmed by a security breach. Nobody wants to be the negligent employee who carelessly opened the door and let criminals in to loot the shop.