LUCY ONBOARDING CHECKLIST

According to statistics, phishing simulations conducted in real time have two significant benefits, namely, doubling employee awareness retention rates and bringing about a near 40% ROI, compared to more traditional cybersecurity training methods. Other 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.

You should keep in mind, however, that employees – your organization's weakest cybersecurity link – cannot be trained overnight, so this endeavor will require careful planning. 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. Naturally, it's much easier to go through this process if you have a list of tips that can guide you through a simulation. In this article are the points you should consider.

General Planning

Name	Description	Questions	Link(s)
Get approval	Similar to approaching any important project, the first step in running a successful internal phishing training campaign is to make sure all concerned parties are notified and ready to comply. This includes executives, board of directors, IT and HR team, and your legal department. This step is usually accomplished fast and easy as it requires only a mild investment in phishing education in exchange of employee knowledge that can protect your company data from hacker attacks. Don't forget to consult your HR department to ensure your simulations comply with current company policies. It's also wise to reach out to your IT and Helpdesk Departments and discuss the planned activities with them.	•Did you get approval from the relevant departments (legal, risk, HR, support etc.)? •Has anyone voiced concerns you didn't consider?	No links

Name	Description	Questions	Link(s)
Define goals	Always make sure to state the goals of each activity, including information on what you want to be tested. Usually, phishing engagements are concerned with testing people and their reactions to phishing emails. The points of concern are: Will a user click on a suspicious link, fill in their credentials in a web form, install unknown software, or otherwise interact with the email contents? In many cases, however, phishing simulations test non-human defenses as well. These typically come in the form of spam and phishing filters that protect the company's mail server. Knowing that your network defenses work is great, but it's imperative that the phishing simulation reaches your employees. Additionally, make sure you warn your testers about any flooding protections set up on your mail server. Remember, running a phishing test has one main purpose: to educate your employees so they are aware of the hackers' tactics and of the ways to avoid becoming their victim. In no way should you try to catch your employees in a mistake without prior training or warn them about the scenarios beforehand as that wouldn't help either. The security of your company is your main goal, and your employees should be aware of that. 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.	•Did you 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?	No links
Past Education	Don't forget to consider prior simulations and trainings that you've conducted on the topic of phishing and scam detection. If your employees have already been trained to spot scams, you should probably consider more sophisticated attack simulations that will be more difficult to recognize.	• Have you already trained all users on phishing & social engineering? • Do you keep the results from past trainings to compare with future attack simulations? • How do trainings currently look like (length, interactivity, video, exam, design etc.)?	No links

Name	Description	Questions	Link(s)
Current exposure	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. Any publicly available information about your company can be used by attackers to create convincing phishing messages aimed at your employees. Your website and social media pages often offer all the data scammers need to run an attack, so keep an eye on any information that your partners share online about your organization. LUCY offers an employee online footprint analysis service for the price of USD 500. Its aim is to help you understand which of your sensitive employee information can be viewed on the Internet as well as the kind of data your employees tend to share publicly via their company e-mail address. Once you have a better idea of your data exposure on public channels, you’ll be equipped to help your staff understand how sharing their personal information can affect them and your organization. You can use this to develop a clear digital footprint policy for all users. Of course, you should not expect your employees to remove all traces of themselves from the Internet. What you can do instead is help them to better manage their digital footprint, so they share information in a way that protects them and the organization.	• Do you request of your employees to not use business email addresses for private services? • Do you want to perform an employee footprint analysis (the results can be used at a later point for specific eLearning)?	No links
Current Filter	It’s common for organizations to keep a sophisticated multi-tier system of defenses on their servers so phishing attacks would not reach their employees. Therefore, in order to successfully run a phishing simulation, you will need to whitelist the addresses from which the ‘threats’ will be sent. This whitelisting will need to take effect at email gateways, anti-virus software and web proxies.	•Is it possible to whitelist LUCY's IP and sender domain from the campaign scenario on the SPAM filter? • Is it possible to whitelist LUCY's 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)?	Avoid Spam Limit sending rate

Name	Description	Questions	Link(s)
Current protection	Do you know which types of malware can get past your defenses? What kind of security do you use against spoofing, malware, etc.? You can never plan a successful phishing simulation until you know and understand all the technical information involved. For instance: Employees who are allowed to run executable files should be tested for awareness toward downloads with executable content. LUCY features a handy built-in functionality called “mail- and web-filter test.” It provides the answer to one of the most important questions in securing Internet and mail traffic: Which file types can an employee download from the Web, and which e-mail attachments are filtered out or not? The tool is part of the LUCY framework and can be used for free. An analysis performed by our consultants is offered at USD 500.	•Do you know what file types can be attached to an email or downloaded and executed from the internet from a standard Windows client?	Filter Test

Technical Planning

Name	Description	Questions	Link(s)
Setup location	You can run the attack simulation from a cloud server or on-premise. Reasons for installing on an external server in the internet are: ■ Public IP address outside your network range: Prevents your infrastructure from being blacklisted. ■ Direct access: The server will not be blocked by any security products already in place within your own infrastructure. ■ Less possible conflicts with integration: A LUCY server placed directly in the internet will be setup very fast as it does not require a complex integration process with your mail, DNS and firewall infrastructure ■ Smaller attack surface: As the LUCY server requires a web based access for end users from the internet (e.g. accessing their mails from mobile devices), you might need to punch a hole in your firewall and allow inbound access to a LUCY server. If you place LUCY in the intranet (see this chapter), your might violate your zone concept. Reasons for installing LUCY on premises are: ■ Legal: Some laws might not allow you to store sensitive data on an external server outside your network or outside your country. Especially with the new data protection law in Europe (GDPR) you need to make sure any personalized or sensitive data is secured. ■ Integration with certain features: LUCY comes with different API's such as the LDAP API, the REST API etc. which are common for backend applications that are usually not exposed to the internet. ■ Security: LUCY might store sensitive data like windows login, user names, emails etc. within the database. Integrating the LUCY server in the internal protection layers (IDS, FW etc.) will minimize the risks of successful attacks.	• Do you plan to integrate LUCY with your internal systems (LDAP, LMS etc.)? If yes: you might probably want to consider an on-premise installation or a VPC (virtual private cloud)	Setup Guide
Prepare Hardware	Please make sure you have the hardware ready with sufficient disk space (>100 GB) and memory (>4 GB).	-	Hardware Specs

Installation

Name	Description	Questions	Link(s)
Download Software	If you have decided to do an on premise installation you will first need to download LUCY from our webpage. Please choose one of our installers or images: ■ Virtual Box: http://download.phishing-server.com/dl/lucy-latest/virtualbox.zip ■ Linux Installer: http://download.phishing-server.com/dl/lucy-latest/install.sh ■ ESX/ESXi: http://download.phishing-server.com/dl/lucy-latest/esxi.ova ■ Vmware Image: http://download.phishing-server.com/dl/lucy-latest/vmware.zip ■ Amazon: http://www.lucysecurity.com/PS/doc/dokuwiki/doku.php?id=installing_lucy_in_amazon If you require a different format (e.g. ovf), search for the according converter (e.g. search for “convert ova to ovf”). All downloads are automatically treated as a community edition.	-	-
Installation	Installation Once downloaded, please install LUCY according to the download type: ■ Installing LUCY on LINUX ■ Installing LUCY in Virtualbox ■ Installing LUCY in Vmware ■ Installing LUCY in Amazon ■ Installing LUCY on Windows ■ Converting LUCY from VMware ESX to Hyper-V As soon as the installation is finished, the automatic setup script should start.	-	Setup Script
Permit Access	Make sure that the necessary ports from and to LUCY are opened. If the server is placed within a DMZ or intranet and you have external mobile users that need to access LUCY, you probably need to enable port forwarding (http/https) on your firewall.	-	necessary ports

Post Installation Setup

Name	Description	Questions	Link(s)
Login	Login to LUCY with the Webbrowser using the IP address of your server. Continue the setup in the browser using the credentials provided in the setup script. As an alternative you can also use a domain name for the administration. If you want to use a domain for your administration UI, Connect to your LUCY instance with the root or phishing account. If you connect as root, please execute the command python /opt/phishing/current/tools/setup/setup.py (if you have a docker based installation, execute: docker exec -it lucy /bin/bash and then press enter and execute "python /opt/phishing/current/tools/setup/setup.py)". Within the setup script menu please choose menu item "domain configuration" and set the domain for your admin UI	• Did you think of reserving a domain for the administration frontend of LUCY?	Domain configuration
Download License	Please send us the workstation ID	-	LUCY Pricing

Name	Description	Questions	Link(s)
Update	Please make sure that LUCY can connect to the internet via http/https to our update server (162.55.130.83 - update.phishing-server.com). If you are using a proxy, please go to “advanced settings” and define your proxy first. • Please test the disk space before updating all templates. Show a warning, if disk space is not sufficient. Always install with “install + replace” • System update: show this button greyed out while templates are downloaded. If all templates are downloaded, allow the user to check for updates. Display an error if the http connection cannot be established.	-	Update LUCY
Mail Settings	Define your **default mail delivery method** in LUCY. If you plan a phishing siluation together with a training, you might want to consider using a different domain or een mail server for the awareness training. In case you use the build in mail server: set the hostname for the mail server.	• Do you want to perform a phishing simulation bundled with awareness training?	-

Name	Description	Questions	Link(s)
Domain Setup	You will need two domain types in LUCY: **Attack simulation domains** This is the domain you could use for your phishing website in your attack simulation. We recommend reserving first a generic domain like "cloud-services625.com". If you create a wildcard A-record for that domain, you can then use a matching subdomain. Let’s say you prepare a phishing simulation with some web-based email service. Using the subdomain "webmail" would give you the domain "webmail.cloud-services625.com" for the landing page. If you ask the user to download a file, you could use "download.cloud-services625.com" etc. If you want to do more sophisticated attacks you can reserve a typo squatted version of your own domain name. Typo squatting is a technique of registering domain names which look similar to some legitimate domain name. For instance, given google.com, one example of typo squatting domain might be g00gle.com. You can use the domain from your landing page also for the email sender (like sender@cloud-services625.com). But as the sender email domain is a free text field that can be used with any domain name, it is not required to reserve a domain for just sending emails. There are some rules though when it comes to sending on behalf of other domain names: a) You can only use domain names that really exist b) You can only use domain names that are not SPF protected (unless you white list them on your mail server) c) You can only use domains that also have an MX record That means, you cannot use "@apple.com" as there is an SPF entry for this domain. You also cannot use "@this-does-not-exist.com". But you could use "@example.com" - a domain that exists, but is not protected. The website MX Toolbox helps you verifying if a MX or SPF record exists. **Awareness Website Domain** Try to avoid using the same domain for attack simulations as for the awareness training. If possible, point a trusted domain record to LUCY like "training.your-domain.com" and send awareness emails using your own mail server as a relay in LUCY. If you don't have a domain registered yet, you can use the integrated LUCY Domain Registration Wizard. This feature is only available for commercial licenses, allowing you to reserve all the available domain names for an affordable price. Commercial clients have a built-in budget for using the domain API and are also able to later add credits for the domain reservation.	-	-

Name	Description	Questions	Link(s)
SSL Setup	If you want to generate a trusted certificate for the admin access you have two options: • Upload your own certificate • Create a trusted certificate using Lets Encrypt **SSL for your awareness training or attack simulation landing pages** Each campaign scenario can be configured with a custom landing page and SSL certificate. Please start the campaign setup wizard to setup SSL for your campaign after you finished the system setup.	-	SSL Setup
White-Label	The application can be visually adapted to corporate branding (custom copyright, software name, admin path, custom error page etc.)	-	custom branding
Client Setup	A client can be your own organization or the company who asked you to perform a phishing test. Each campaign has to be associated with a client. You can then create also "view-only accounts" for selected campaigns from specific clients or view/filter data based on the client name.	-	Client Setup
LDAP - SSO	In case you want to import your recipients via LDAP or allow them authenticate via SSO, you can configure this is LUCY in the according menus.	-	LDAP
Advanced Settings	Set the time zone, proxy and other advanced settings	-	advanced settings
Hardening	Consider going through the different hardening options LUCY offers	-	Security hardening
User Management	LUCY offers a role-based access control (RBAC) for the administration, restricting system access to authorized users. The permissions to perform certain operations are assigned to specific roles within the user settings. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular LUCY functions.	-	User Roles

Create your campaign

Name	Description	Questions	Link(s)
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 warn your employees about the upcoming campaign so they feel included in this plan toward protecting company sensitive data and digital infrastructure. You can also use this notification as a reminder about the importance of recognizing suspicious emails which can cause security breaches and loss of data. For instance, the ransomware attacks that keep developing have the potential to damage your company's reputation, lose customer trust and revenue, and even result in fines. Thus, it's even better if your CEO is involved, so your employees can understand that cybersecurity awareness is everyone's responsibility. Here is a sample first email taken from SANS Security Awareness Program: 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.	•Do you plan to communicate to your employees that you will perform phishing simulations?	No links
Allow users to report emails	If your employees notice suspicious emails, but notify no one, the threat remains. Make sure your users feel encouraged to seek help in situations that raise their awareness. A good report system can provide clues about the types of phishing attacks targeting your company, and thus help improve your defenses. A well-working report system where users can freely share their suspicions about potential attacks can also provide information about emails mistaken for phishing, and how that impacts your organization. Make sure you set up a general report email such as: report-phishing@yourorganization.com which employees can use when an email they receive looks suspicious. Educate them about the steps they need to take in case of a perceived threat and provide them with the tools to report it in an easy way, such as a plug-in report button embedded in their inbox. LUCY offers a phishing reporter plugin for various mail service platforms where employees can report suspicious emails with just one click. Note that this ease of reporting usually doubles the report rate of suspected emails, so it would be a good idea to provide your security team with the right tools and resources to handle and analyze the influx of emails. LUCY has a handy solution that applies machine learning to spot real attacks.	•Do you plan to give users the option to report emails via a plugin? • What type of email clients do you have in your environment and which ones should be supported? • Where should emails get reported? • Do you have any specifications in terms of icon design (report button) and text that is displayed, when a user reports a suspicious email?	Mail Plugin

Name	Description	Questions	Link(s)
Training first?	Before you initialize a phishing simulation assessment in your organization, your current employees should to go through an introductory training scheme. This same training will later be provided for new employees upon hiring (preferably before they get access to their company email accounts). Please list 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? •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 do you require department-specific training content? •Is the training “success” going to be monitored? And if yes: do you want it monitored on a personalized level? •Are there any penalties for users who refuse to participate in trainings? •What is the desired training frequency for the different training methods? How often do you plan to update the training content? •Are there already existing trainings, which should be incorporated into our training courses? •Do you also want to test the training know-how (e.g., via exams)? •Do you wish to include training gamification elements? •Should users get a certificate when they pass the training exams? •In which languages does the training need to be delivered? •Do training videos need to have close captions? •Do you want the training videos to have your own logo at the start and end? •What are the 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: in which minimal screen resolution? •What is the default browser and screen resolution for a standard user? •Are there any technological restrictions for the training courses (e.g., Java scripts blocked)? •Can we include links and sources (e.g., videos) from external servers or does all the training content need to run locally? •Current policies: Which security guidelines are to be incorporated into the training (e.g., training password security: minimum number of characters; internet usage guidelines, etc.)? •Training length: what is the desired length for the different courses (note: the same course could be presented as a 1-minute micro training module and an extended version)? •Training library: do you wish to have all training modules accessible through a central training library? •Do you wish to be able to edit all training content yourself? •Should the training run only on our platform or would you rather we create an export (e.g., SCORM) of all trainings for you? The LUCY database contains more than 250 interactive, web-based training modules (videos, tests, quizzes, games, and more) on various security topics. These can be given to employees based on the results of attack simulations, or independently. All trainings can be customized.	-	Training Settings

Name	Description	Questions	Link(s)
Frequency	Before you run a phishing simulation test, you need to plan for it. If you send the test emails too often, most employees will get used to recognizing them. And if you send them on occasion, you will not have enough statistics to analyze.The best approach is to create each phishing test as a series of simulations, e.g., a campaign, that runs for roughly 3 to 4 months. This strategy will give you a clear-cut way to understand the level of your employee-based security. It's important to set up your campaign with progressive difficulty. In other words, the first simulation email should be easy to recognize, then you can build the following ones up by exploring different angles and tiers of subtlety. Do not run more than 4 attack simulations per user/per year. 2 attack simulations per user/year are perceived as optimal.	•How many phishing simulations do you plan per year? •How many phishing emails should a user get per year (minimum/maximum)?	No links
Choose the groups	Sending a phishing simulation campaign out to the whole company at once might cause suspicion. Instead, choose a group of employees you'd like to test, and only target them with a specific simulation. You could also pick a dozen scenarios which you can then split among your employees for better analysis. Keep in mind that not all employees should be targeted in the same way. For instance, customer support may be at higher risk of receiving unsolicited emails, while your IT, financial, and data administration departments may be the target of more sophisticated types of phishing. You would do wisely to train your risk-group staff about all possible threats and provide additional support for them. User coverage and simulation frequency should be determined based on the perceived risk (Example: Finance & Payments – 2 themes / X months, senior leadership – 1 theme / X months). High risk functions / department / individuals handling important role in the organization should be covered more frequently as part of the simulation.	-	Creating groups
Data pivacy	All employee performance data you gather via phishing simulations should be treated as personal data. Don't overlook the potential implications if this data is made accessible to your company's public space. Treat your employees with respect and don't cause reputational or career stress. If your phishing simulation requests user data, you could use encryption. Another alternative is to purposefully use a site without encryption to create additional learning experience, teaching the user to never input sensitive data on an unencrypted site.	•How long will gathered data be kept? •What will be done with it? •How securely will it be kept? •Do you want to store the users' input data? •Do you want to submit the users' input data? •Encryption: Should the landing page for the attack simulation be accessed over an encrypted channel and does it require a trusted certificate?	Anonymous settings
Attack type selection	Phishing attacks don't always come in email form. Many scams come through social media and even phone calls, so you will do good to train your employees to recognize possible threats. Your training should encompass different phishing methods, so your employees will be well equipped for various attack types. It's advisable that your first phishing template is more basic and easier to recognize, but make sure each iteration of your campaign becomes more sophisticated. Utilize tactics such as smishing, file-based attacks, social engineering, etc. that your employees will encounter in the real world.	•What attack types do you want to use in your phishing simulation (you can choose between hyperlink, data entry, download, execution or mixed)? •Do you want to use email as the only delivery option or will you incorporate alternative methods as well (SMS, USB etc.)?	Attack Types

Name	Description	Questions	Link(s)
Scenario selection	When deciding whether to run one or more scenarios in your organization, you should always consider the downsides. For instance, a single scenario received by all employees at the same time is bound to raise suspicion. So, after a short while, you won't be able to measure the level of security awareness as the clicks will quickly wean down. A better strategy is to use multiple scenarios when you want to test employees in the same office space. If you do want to run a single template, you should make sure the content is general enough to be relevant to everyone in the company. Specific templates, such as "package delivery notification" and "online booking confirmation" will not be of interest to most of your employees. A template like "employee survey about [some generic topic]" or "required employee registration" would garner the interest of your target group. Think carefully about possible template limitations. There may be none, but sometimes clients don't want specific institutions or people to be impersonated. Another good idea is to keep in mind planned company activities and not jeopardize project trust unreasonably. For instance, 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. Once you have all of these figured out, you can start planning your phishing email scenarios. Look up current phishing strategies and refer to scam emails you have received. Think like a scammer and use the knowledge you have of your employees to create a campaign that is likely to get them curious. This may not come natural to you, but it's important to get shrewd and tricky. Use email templates typically sent out for company events, such as a course/seminar/team building sign-up form, or with an attached downloadable file containing information about a policy change. Devise your scenario by job specification and target that group of employees to whom it will be relevant. Use email templates they usually receive, then tweak them to make them sound believable. For instance, you could impersonate the Head of Finance and ask targeted employees for their invoice/ERP software credentials. Phishing emails that contain offers for "free" stuff are bound to get most clicks, so make sure you test them too. Your employees should have enough common sense to know that nothing comes for free and should be suspicious upon seeing such offers. They can be taught to check the underlying links by hovering over them, but make sure you instruct them to never click any suspicious links because they often are malicious. Remember, every phishing campaign must be thoroughly planned as scammers are getting more sophisticated and creative, sending out very convincing emails. Therefore, you should make sure your templates target the right group of people in a way that is subtle and intriguing for them. That's the only way you can test your employees' awareness, so you get realistic results of your cybersecurity.	•Do you plan to start with only 1 attack template or multiple templates? •If multiple templates: how many scenarios should be prepared in total?	No links

Name	Description	Questions	Link(s)
Real or not?	It's best to begin your phishing training with the basics. This way you can glean an idea of your employees' initial level of awareness. To do this, use typos, poor language, bad formatting, etc. in the templates you send. Easy examples include fake package shipments and incredible lottery wins, so start your campaign there. With training progression, you will notice higher report rates and lower click rates as your employees learn to spot the scams. Then you can up the level of complexity, and so on. It's good to know that emails which look as if sent from internal servers are more difficult to spot. Inherently, employees are likely to trust their colleagues or higher tier personnel. Spear phishing attacks, which use fully customized templates, are usually very effective. However, you shouldn't go all out with the first simulation round. Find the golden middle between spoofing the company logo or a manager's email and use a predefined template. Once this scenario runs its course and your employees are better prepared, you can get more creative. 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. So, don't set up fake bank account verification requests to be sent from your IT staff, for instance. Also, don't forget to keep the spoofed party in the loop before you begin the campaign. Adapt the same strategies when sending spoofed external emails, and make sure you use your common sense. If you want to send out fake emails concerning income taxes, do it in tax season, and the holidays are best for using package delivery notification templates. And make sure you spoof real companies (FedEx, UPS, Amazon, etc.); this is a great way to measure employee awareness for actual phishing attacks. Whatever strategy you decide to use, make the phishing attempts look as realistic as possible. This is the only way you can glean your employees' awareness for real-world scams. Finally, make sure you do not meddle with the copyrighted and trademarked logos of any private company or government agency. Those institutions will most certainly not welcome the usage of their logos even if it's for fake phishing emails.	-	Clone a Webpage
Which Email Sender?	An important part of your phishing attempt is choosing the best mail sender domain from which the emails will be sent out. If you have spam filters in place, choose a domain that will normally pass through them. Only use this strategy if you want to allow an external third-party mail sender to spoof your own domain or the domain of a frequently used vendor. There isn't much sense in using domains that would normally get filtered out via SPF protection – these will never make it to your employees' inbox anyway and will be met with little cooperation from staff. Spoof a known domain/your own domain? Use our spoofing check first to verify the technical possibility. If you spoof a known external brand, use a legal disclaimer and make sure the user is redirected to the awareness directly after the phishing.	• Do you also want to spoof your own company mail domain or spoof a domain from an external third-party vendor?	Spoofing
Catch email replies?	For better statistics, catch all possible reply types, including "out-of-office" messages and "no-delivery reports." Get feedback about the actual attack simulations to better analyze the results.	•Do you plan to catch email replies?	Mail Manager Response detection
Setup 404 Pages	Every phishing simulation you run will have a couple users who choose to type in the domain in the browser (sans the random identifier) instead of clicking the spoofed link. This may bring them to the software admin interface or show a random 404 error page. Make sure you know where they get redirected and adjust the page accordingly. Create custom "homepage": To prevent error messages from appearing or the end user from even coming to the login area of the admin console, you can create generic "homepages" within LUCY for the domains used in the phishing simulation.	•What should happen if the recipient is checking the domain in the browser behind the random URL?	404 Pages

Name	Description	Questions	Link(s)
When to send training?	You can opt in to send your phishing training immediately after a user fails the attack simulation. They could be instantly redirected to the training if they clicked a spoofed link, submitted some credentials, or attempted to download a file. This approach will gain the user's full attention, though they might warn their colleagues about the simulation. Another option is to delay the training, but make sure you send it from a trustworthy email that is different from the one used in the phishing simulation.	•Do you want to include a training for users who fall for the attack simulation? •Should the eLearning be delayed? •What is the content/length/type of the desired follow up training?	No links
Follow up training?	In every test you plan and run, there will be low performers, that is, users who fail to recognize the phishing emails. Part of your post-simulation job is to help those employees learn to recognize the threats and respond accordingly. A good way to continue with those people is to follow up with additional courses in real-time scenarios where you can track their results, as well as onsite trainings. Make sure you treat each employee with respect when discussing their low performance on a phishing test. If you patronize them, that will jeopardize their future communication with you, and you need them to trust you so they will come to you if they spot something fishy in their inbox. If this is the employee's first test fail, you can simply send them an e-mail noting their poor phishing test result. Make sure you mention how important cybersecurity is for the entire organization and offer additional materials to help them improve their awareness. Gently let them know that more phishing tests will follow, so they will have many more opportunities to show they are not a weak link in the system. Mention the "report phishing" button, if you have implemented it, or the report-phishing@yourcompany.com email that you set up for the purposes of scam reporting. Sometimes there may be people, even a handful of them or more, who continuously fail to recognize a phishing threat. Don't leave the matter unaddressed, but instead discuss it proactively. Give those users a tutorial explaining what phishing threats are and why they are dangerous for your company. Run some widely known examples from real life situations that have caused organizations tons of trouble and losses. It's imperative that each of your employees recognizes the legitimacy of cyber threats and that they are very likely to be attacked at some point.	•Do you plan to provide additional training for low performers outside of LUCY?	No links

Run your campaign

Name	Description	Questions	Link(s)
Test Run	For the time being of the test run, make sure all email addresses and page domains that you use in the simulated phishing email templates are whitelisted. Don't forget to also adjust any internal company settings so that all simulation tests end up in your users' inboxes. An important step you should not miss is testing the test on a few select emails, before sending it out to your employees. If you're not using a cloud-based spam filter, you would do best to simply whitelist the LUCY IP addresses and hostnames in your mail server. If this isn't the case, whitelisting should be done by email header in your mail server and by IP address or hostname in your spam filter. Products and services, you use in your mail or web environment should also be adjusted to prevent issues with deliverability. Note that our support team will be available should you need assistance. Most company mail servers and filters have rate limiting set up. This means that emails sent in bulk may be delivered slowly or get blocked altogether. Ensure your mail server and filter are set up so that the rate limiting rules are adjusted for the time you send out the phishing test emails. As an alternate scenario that isn't recommended, you can turn off the limiting rate of your server and filter to ensure all users receive the phishing test email. But you have to turn it right back on.	••Do you have an email account that can be used for testing purposes?	No links
Send all at once?	A great option to consider when sending out phishing simulation emails is scheduling. A scheduler allows you to plan test email delivery in a time frame of your choosing. Best practices include scheduling around weekends and vacations, not at night-time or Friday afternoon.	•Do you want to use a scheduler and if yes: what are the required rules?	Scheduler
Monitor	When you run your simulation, make sure you can and do monitor it in real time in case something goes awry. Having this kind of understanding of your campaign will allow you to catch replies, out-of-office messages and NDR, and to track any issues that may arise.The LUCY platform allows you to set up view-only users, where real-time statistics can be monitored without access to configuration pages.	-	Create Campaign reports Create Exports Monitor

Name	Description	Questions	Link(s)
Follow up communication	After you run your campaign, make sure you send out explanatory emails a few days to a week later. The emails should contain information about the importance of the used scenario as well as the clues you expected your employees to notice. Remember that positive feedback and consequence are the best ways to learn good behavior. So, set up a reward system for those employees who are able to spot the phishing clues and follow up by reporting the scams. Encouraging your staff will create trust in case of future threats – fake and real. For those who fail the test, and there will always be such individuals, follow up with training and additional courses until the employees in question learn to recognize the threats and report them. Your company needs to be immune to cyber threats, and this involves all of your users.	•Do you plan to do a follow up communication?	No links
Next Steps	Running a phishing simulation campaign has one main purpose: raising employee awareness to cyber threats. So, the first test is just the beginning. Build a baseline, reward high-performers, educate low-performers, and start planning your next scenario!	-	-
Rewards	If any of your employees achieve outstanding results, reward them. Congratulate their success in an email, noting everything they did right (no click-throughs or data leaks, timely reporting, etc.) to keep the company safe from cyber threats. You can stimulate an entire department if their cumulative results rated best in the organization. To bring things further, you can create a contest among departments to determine which one was the safest in a given period of time. As stimulation you could sponsor a lunch or dinner for the team with highest test and report results.	-	-

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=lucy_onboarding_checklist

Last update: **2021/09/29 10:28**