SUCCESSFUL STEPS TO STOP PHISHING SCEMES

MediaPRO
Cybersecurity & Privacy Education

WHY PHISHING MATTERS

Someday, maybe on a day just like today, your employees will get a phishing email.

Email clients are getting better and better at filtering them out, but they're not perfect.

Phishing is an attack vector that shows no sign of slowing down. If you're reading this to get some advice on running a simulated phishing program, you probably don't need this proven to you. Here are some stats anyway.

94%

of malware is delivered by email (CSO Online)

28%

of U.S. employees admitted struggling to identify a phishing email *(2020 State of Privacy and Security Awareness Report)*

Phishing remains one of the top access points for data breaches *(2020 Verizon Data Breach Investigations Report)*

1 PREP YOUR COMMUNICATIONS PLAN
2 DEFINE YOUR METRICS
3 INFORM LEADERSHIP
4 SEND YOUR BASELINE PHISH
5 ANNOUNCE THE PROGRAM
6 TELL OTHER DEPARTMENT HEADS
7 PROGRAM LAUNCH AND ESCALATION
8 SUPPORTING COMMUNICATIONS
9 DIGGING INTO THAT DATA
10 PROFIT

SIMULATED PHISHING DEFINED

Enter the simulated phishing program, an important way for employers to see how vulnerable their people are to this social engineering attack and train them to do the right thing with the real thing.

The goal of a phishing simulation program is to provide employees with a safe, simulated environment where they can learn about what real phishing attempts look like in the wild.

But what makes a good phishing simulation program? How many emails should you send and how often? How difficult to identify should they be? How do you track improvements?

We'll walk through the steps to take to establish a simulated phishing program, from developing a communications plan and sending your first baseline phishing test, to building an ongoing program integrated into a larger security training and awareness initiative.

A phishing simulation program shares a goal with your primary training program: to teach.

It shouldn't feel like a "gotcha" moment, or an attempt to make your employees feel stupid. The point is to make them feel like you're all working together toward keeping your organization's digital infrastructure and sensitive data safe.

Step 1: Prep Your Communications Plan

You should have a plan for how your simulated phishing program will flow squared away before you dive in. At the very least, this will make it easier to lay out your initiative for your executive team and specific department heads (more on that soon).

Points to cover in your communications plan should include:

- Frequency of simulated phishing email campaigns
- Supporting educational content you plan to include (articles on the company intranet, supporting graphics, etc.)
- Messaging for announcing the program companywide and employee-facing instructions for how to report a suspicious email

The best programs we've seen have common branding carried throughout their phishing educational content. Here we mean giving your program a catchy name; one that your people will see and instantly associate with it. We're fans of plays on words (something like "Phresh Phish of the Day), but the possibilities are wide open.

A catchy name teamed with consistent colors and even font choices for your phishing communications helps engage your employees and makes clear the importance your organization places on this threat and the educational content behind it.

Step 2: Define Your Metrics

The Big M; metrics will tell you and your company if your program is getting results.

Put simply, the most important thing to track is how often your phishing emails get reported: **the report rate**.

Click rates are often touted as the primary metric of simulated phishing success, but these can be too easily manipulated by tweaking the difficulty of phishing campaigns. If click rates are too low, then you're not sending tough enough phishing emails.

Report rates help demonstrate your ultimate goal: *engagement*. You want people to tell you if they think they received a phishing email; simulated or not. The more they report, the more engaged your employees are.

Long story short: click rates are useful, but report rates are vital.

Step 3: Inform Leadership

Your bosses need to know what you're doing and why. This is where you'll be thankful you worked out a communications plan.

If your leadership is still on the fence about initiating a simulated phishing program in the first place, use data to quantify just how big of a problem phishing is and what the risk is to your organization. This can come in the form of suspicious emails blocked by your email client or malicious downloads prevented (IT will be your good friends here, as they should always be).

Step 4: Send Your Baseline Phish

Before you launch your full program, you'll need to send a campaign without telling the company. Only your IT help desk should know.

Why all this secrecy? Keeping this first campaign under wraps is the best way to gauge your people's everyday susceptibility to phishing emails. They won't be expecting a test, meaning they'll be just as vigilant (or not) as they usually are.

Establishing initial reporting percentages and click through rates is important to show how your primary simulated phishing and training initiative has improved behaviors later on.

The first simulated phishing email should not be too easy, but not too hard either. Consider something like a phony package shipping confirmation or a new voicemail announcement. The link should lead to a simple 404 page.

Again, the point of this first campaign is to simply collect a baseline of clicks and reports.

Step 5: Announce the Program

Wait, didn't we just say the simulated phishing campaigns you're running should be secret?

Well, yes and no.

The baseline phishing email should not be public knowledge to glean as true an assessment as possible of your organization's susceptibility to phishing.

But after you get a baseline, your full, multi-month program should be formally announced to all employees. In fact, you should over-communicate about the problem to avoid an impression that the program is a test or that you're trying to trick anyone. Communicate that the program is educational — it's training.

This announcement should include some key elements:

- The simulated phishing program is part of the company's ongoing security training and awareness initiative
- Advice on what makes an email suspicious in the first place
- How to report phishing emails (many simulated phishing platforms have reporting buttons that can be integrated into business email clients)
- Where to find additional company resources on phishing (such as your company's intranet)

Step 6: Tell Other Department Heads (and Heads Only)

Inform other departments within your organization if you're planning to spoof emails from them (we'll talk more about using a variety of spoofed emails later).

Hackers are going to send your employees emails that appear to come from individuals in your organization, like a CEO looking for an urgent wire transfer, or departments, like HR, asking for a quick turnaround on personal information.

Give these teams a heads-up before the phishing simulation campaign, so you can make sure that you're not interrupting their normal work with a flood of worried emails from your employee population. This should include:

- A brief explanation about why you're running a simulated phishing program
- Instruction that if they get questions about suspected phishing emails from their own people to tell them to report the emails to IT

Step 7: Program Launch and Escalation

You've stated your intentions companywide, now it's time to launch your program.

We recommend no more than one campaign per month but at least once per quarter. Your baseline phish should be used to inform the sorts of emails you send out first.

Lots of people caught? Start easy and slowly turn the dial.

Impressive report rates? Praise the people who report, and then make the primary campaigns a little tougher, but keep thanking those who report.

Do a little digging to see if specific departments or locations did better or worse than the average. People like to see how they compare so you might eventually consider reporting on a department basis for department heads only.

Here are some ideas for types of phishing campaigns to run:

- Password reset requests
- Shipping notifications around the holidays
- Requests purporting to be from HR (again, inform your HR director before you do this) concerning W2s around tax time
- Spear phishing campaigns targeting specific departments or even positions (wait until at least you're three or four campaigns in, though, as spear phishing is a big jump in complexity)

Long story short: Get creative! You'll eventually want to "turn the dial" on your campaigns' complexity to make sure your employees are continually challenged. Most simulated phishing solution providers will include multiple phishing templates built in, sometimes even with the ability to build your own from scratch.

Important thing to remember: No matter the phishing emails you concoct, make sure you send your IT team screenshots beforehand so they know what's part of your program. This way if users forward simulated phish to them and ask what to do, they can tell them to report it with the report button (without giving away that it's a simulated phish).

Step 8: Supporting Communications

Call It reinforcement or awareness, no simulated phishing program is complete without supporting content outside of the emails themselves.

These can include everything from eye-catching infographics to short articles and videos posted on your company intranet. Occasional reminders to all employees about how to report phishing emails are also useful to send, interspersed with the simulated phishing emails themselves. Last but not least, specific web pages people who click simulated phish get sent to should be educational and supportive. Again, we're not going for "gotchas" or scolding.

This content should be tied into your larger training and awareness initiative whenever possible. Try to achieve a similar look and feel to help your people mentally connect the varied training content you've deployed.

Simulated phishing programs are useful, but you shouldn't rely on them alone to influence behavior change. Industry analysts at Gartner say as much in their report *Innovative Insight for Anti-Phishing Behavior Management:*

> "Anti-phishing behavior management solutions are not a tool for initiating cultural change. Assess your organizational culture first, and deploy anti-phishing as part of a comprehensive program of security behavior management and education."

(For some inspiration, we've got a toolkit of free resources all about the dangers of phishing.)

Step 9: Digging Into that Data

So your phishing program is up and running.

Now what? It's time to look at the data.

First of all, congratulate the people who reported! This can be as simple as a friendly "Thank You" pop-up connected to your email client's phishing report button.

Also consider providing rewards for those who consistently avoid phishing attempts, such as gift cards, security swag, or a lunch on the company. Everyone loves free food!

If you have a large organization, you can enter all the names of the people who reported phish into a drawing every month. You can also give kudos on your security portal or company newsletter to people who reported REAL phish.

If you have the resources, send them a personal thank you and cc their manager. A little positive recognition can go a long way. You just might find a future security ambassador in the process.

For the people who consistently fell for your spoofed emails, follow up with a short training course and track their completion. In MediaPRO's own Phishing Simulator, targets who click on phishing lures see a teachable moment on the landing page that's displayed to them. But you can also configure the campaign to automatically enroll them in a short training course. In the Learning Management System (LMS), set a due date for the training and automate the training reminder emails that are sent to employees until the training is completed. Remember to keep the tone of the reminder email upbeat and helpful.

While exploring the data, look for patterns. Try to find what signals the data might be sending. Are repeat clickers more common in a specific department? In a specific geographical region? Bosses or "rank-and-file?" This information can be used inform both additional phishing campaigns and training and awareness materials.

Seeing total clicks go down is a common indicator of improvement, but as we've said, user reporting is the most important metric in your program. It's an indicator of engagement, which is exactly what any training and awareness manager wants.

Step 10: Profit

Yeah, so we're referencing an internet meme that dates all the way back to 1998 (seriously look it up) as our last point. But if you made it this far, we figure you could use a laugh.

In all seriousness, though, a thoughtful simulated phishing program, tied to other security training and awareness elements, will pay dividends.

A program built with engagement in mind is a big step toward establishing a security culture in your organization.

An engaged employee will say something when they see something, will tell their coworkers about it. That's how culture spreads. And that sort of thing is priceless.

About MediaPRO

MediaPRO is nationally recognized for producing award-winning online training that reduces risk and improves end-user behaviors. Combine this training with our phishing, reinforcement, and assessment tools, and you've got an awareness program that meets your compliance requirements and safeguards business assets. MediaPRO's products are used by the most risk-aware companies in the world, have won more than 100 e-Learning awards, and have earned us a place as a Leader in Gartner's Magic Quadrant for Security Awareness Computer-Based Training.