The Practice: Conducting Phishing Exercises

A particularly effective way of building agency, the "Yes, I can!" confidence that helps motivate us to take action, is having a chance to practice the new skill we're trying to learn. One of the best methods for strengthening Cybermindfulness muscles is through phishing simulation exercises. Consider adding a monthly phishing component to your organization's education efforts, if budget and time allows. This guide has some tips for getting a phishing practice program rolling at your organization.

✓ Pick a Phishing Simulation Tool

There are many tools, both paid and free, you can use to generate faux phishing messages for your organization to practice on. Infosec Resources has compiled a list of several low / no cost options to consider. We recommend checking out their article about top phishing simulators to help determine what might work best for you.

✓ Set the Stage with Your User Community

You'll hear a variety of opinions on this, but from our experience, it's best to let your colleagues know that your organization is adding phishing practice to its cybersecurity education program—you'll find a sample "kick-off" message on the next page.

✓ Keep Phishing Fun

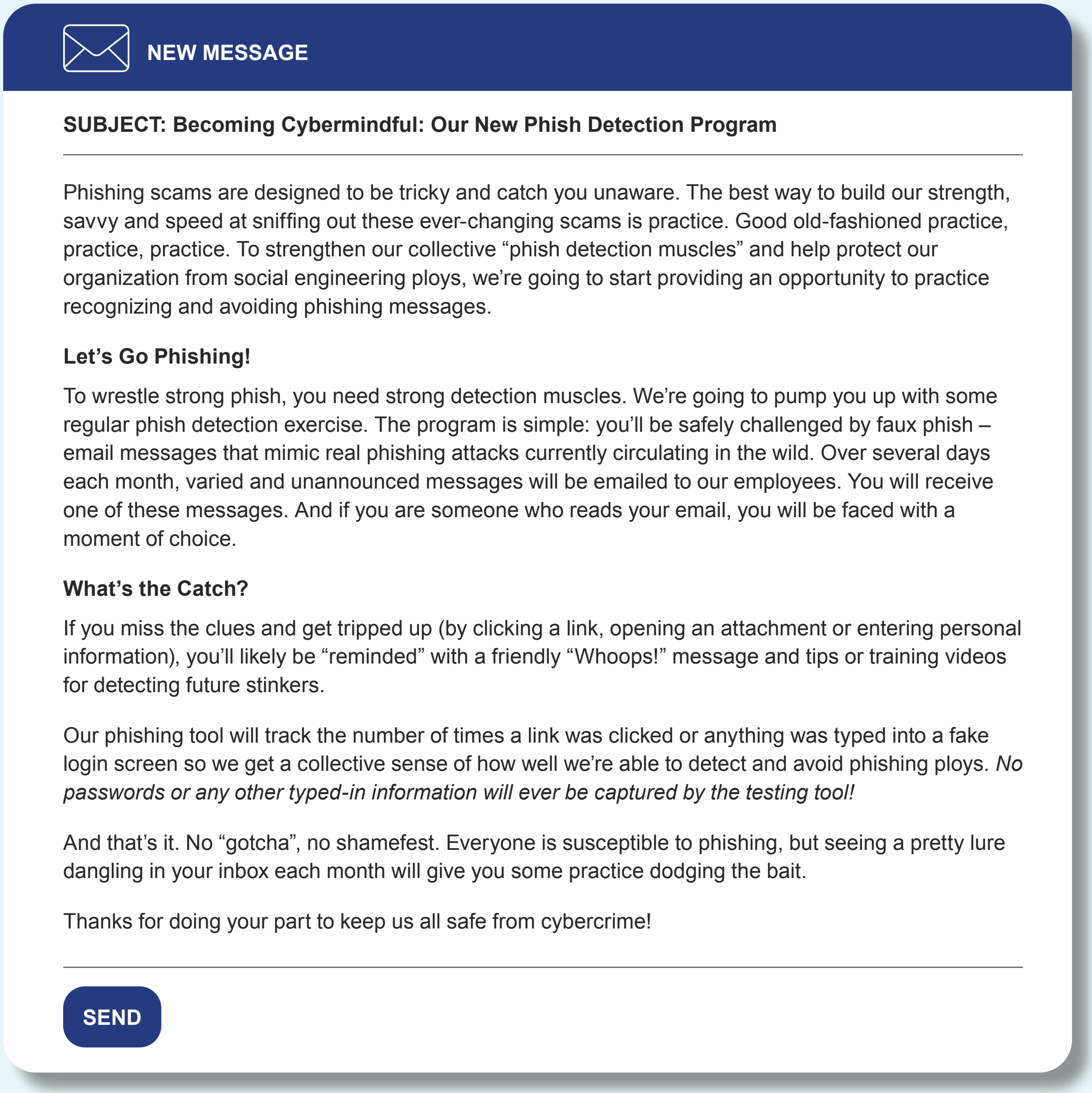
Nothing will kill enthusiasm for your phishing program quicker than fear of retribution or embarrassment. It's important to stay positive and friendly, regardless of how your colleagues perform in a given exercise. We're going to click from time to time, but our phishing exercises should arm us with information we can use to do better next time. Plus, seeing where we're most "phish prone" can help us target our educational outreach towards our most pressing pain points—that's great data to have! With all that in mind, here are a few tips:

- **Provide "just in time" feedback.** If your tool allows, provide your "phish clickers" with immediate feedback (like tips about red flags they may have missed) via a landing page or email.
- **Report results promptly.** Letting everyone know how your organization performed overall shortly after the conclusion of each exercise gives everyone a chance to celebrate progress or, if things went poorly, remember why we bother with cybermindfulness in the first place.

This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

- **Avoid shaming or "calling out" your clickers.** When reporting on the progress of your phishing exercise program, both to the organization as a whole and your leadership team, keep information about the performance of individuals confidential as much as possible. Repeat offenders might need additional training, but you shouldn't make them feel bad about it or cause them to worry their job or reputation is at risk.
- **Expect uneven performance.** If we're using our "phishical fitness program" correctly, we're bound to see our click rates go up and down a bit over time. Your goal should be to expose your organization to new or particularly relevant social engineering threats, not send the same "Your package has been delayed" message twenty times in a row until no one clicks on it anymore.

Sample Phishing Program Kick-Off Message



SUBJECT: Becoming Cybermindful: Our New Phish Detection Program

Phishing scams are designed to be tricky and catch you unaware. The best way to build our strength, savvy and speed at sniffing out these ever-changing scams is practice. Good old-fashioned practice, practice, practice. To strengthen our collective "phish detection muscles" and help protect our organization from social engineering ploys, we're going to start providing an opportunity to practice recognizing and avoiding phishing messages.

Let's Go Phishing!

To wrestle strong phish, you need strong detection muscles. We're going to pump you up with some regular phish detection exercise. The program is simple: you'll be safely challenged by faux phish – email messages that mimic real phishing attacks currently circulating in the wild. Over several days each month, varied and unannounced messages will be emailed to our employees. You will receive one of these messages. And if you are someone who reads your email, you will be faced with a moment of choice.

What's the Catch?

If you miss the clues and get tripped up (by clicking a link, opening an attachment or entering personal information), you'll likely be "reminded" with a friendly "Whoops!" message and tips or training videos for detecting future stinkers.

Our phishing tool will track the number of times a link was clicked or anything was typed into a fake login screen so we get a collective sense of how well we're able to detect and avoid phishing ploys. *No passwords or any other typed-in information will ever be captured by the testing tool!*

And that's it. No "gotcha", no shamefest. Everyone is susceptible to phishing, but seeing a pretty lure dangling in your inbox each month will give you some practice dodging the bait.

Thanks for doing your part to keep us all safe from cybercrime!