TracePhishing

The Email Problem

You've seen the headlines and news reports: "Big company breached." Many of these breaches were because of an employee clicking a phishing email. This seems to be pretty common for enterprise level organizations, but small and medium businesses may believe that they are too small to be phished and are 'out of the water.' However, the water has begun to rise with more hooks in it than ever before.

One of the largest issues facing organizations today are phishing emails, simply because of the ease at which an attacker can send them. These emails are sent out daily, and while spam filters may catch some, it requires employees who are properly aware of these threats to stop them all.

Recognize The Hooks

Picture this for a moment: you are a fish swimming along, and you see a nice worm dangling in front of you just ready to eat. You're excited at first, but instead of immediately biting, you decide to inspect it, as you've heard stories from other fish. You then notice the silver hook – and move on your way – deleting the email from your inbox and notifying your IT department.

TracePhishing is a lot like that. It trains your employees to hesitate before clicking links and really examine the email they are about to interact with. By sending out fake phishing emails, your employees get better at recognizing the real ones.

Create Your Own No Phishing Zone

TracePhishing is the perfect solution to establishing a phishing program in your organization and includes multiple email templates, distribution by groups or individuals, and syncs with TraceEDU to offer training as soon as an employee fails. The best part is that we will manage TracePhishing for you, crafting emails based on the most up to date phishing techniques (so your employees are being tested on what the bad guys are actually doing), sending out emails that are targeted to specific departments or across the whole organization, and supplying you with a comprehensive report so you can track exactly how much progress you've made. This is all done by our experts in cybersecurity, without you needing to commit more time or resources from your IT department.

An excellent piece of the Security Awareness puzzle, TracePhishing has the unique position of both educating your employees and assessing whether they are getting better at identifying threats. Combined with our other Security Awareness solutions, TracePhishing helps to ensure that your organization is a 'no-phishing' zone.

With TracePhishing You Can Expect:

- **Simulated email phishing campaigns sent to your employees**
- **Customized email phishing templates**
- **Distributions scheduled to meet your awareness needs**
- **Expert recommendations on best practices in simulated phishing engagements**

Frequently Asked Questions

How long does TracePhishing take to set up?
If Trace is performing a remote social engineering engagement for you, then there's virtually no software set up. If you're using TracePhishing to conduct your own phishing campaigns, set up is quick and easy and only requires a few minutes to begin phishing tests.

What's the difference between getting the program and doing the phishing internally and having Trace manage our phishing efforts?
If you run phishing internally, you'll need to set up the distribution groups, choose the email(s) that each will receive, and schedule their delivery each time you want to run a test. With Trace managing, you don't need to worry about making sure to set these up and run them on a periodic basis - you'll just get the results and report.

How do I add people to the program for phishing distribution?
This is done automatically if you're using AD/LDAP sync, or can be done by uploading a CSV or manually creating a user.

Will Trace phish my employees continuously or only on set intervals?
This depends on the scope of the engagement. Phishing is typically done in intervals and the emails are not all sent at once.

How customizable are the emails? Can I customize them myself no matter which version of TracePhishing I get?
Emails are very customizable – all content, images, etc. can be modified. You can customize the emails regardless of which version you get.

Can I set phishing emails to go out on a schedule? Can I add email variations to that schedule over time or do I need to create a new distribution?
Yes, phishing emails can be delivered on a schedule. Additional email addresses can be added to the schedule over time so that new users are included in active distributions.

If an employee fails a phishing attempt, what happens?
Employees who fail phishing attempts are logged as such in our system and the details of the failure are reported to you. The details will include whether the phishing email was opened, whether the user clicked on the malicious link(s) included in the email, and exactly when the user failed the test (date and time). Additionally, there is an option to display a configurable web page with a message to notify the users of their failure with tips to improve security awareness.

What kind of reporting will I get and how often?
If Trace performs phishing as a part of the service, a detailed report outlining the results will be provided in PDF format. There is also a reporting module that allows users to generate reports with detailed data in both PDF and CSV formats.

How often is TracePhishing updated? How often can I expect new phishing templates?
While there is no defined schedule for releasing new phishing templates, our team is continually searching for innovative methods for conducting phishing tests and will periodically release new templates. Additionally, our software provides the ability to create custom phishing templates which allow users to define their own content.

Are TraceEDU and TracePhishing connected? Can I queue up training for those who have failed a phishing attempt?
Yes, users can select training courses to be sent to users that fail phishing attempts when creating a phishing campaign.