TraceSmishing

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

The New Threat

The fact of the matter is, attackers just keep getting smarter. People are starting to wise up to the threat of phishing emails, and organizations all over the world provide training to their employees on how to recognize phishing attacks. So now attackers are turning to phishing through SMS text messages, or "smishing." While smishing is a threat to any mobile device, the biggest targets are corporate owned phone numbers.

Many companies provide mobile phones to their employees for business use, and these tend to house organizational information that attackers want to exploit. Attackers can easily target phone numbers with the same ease as email addresses, and your organization needs to be prepared.

Keep Company Phones Secure

TraceSmishing was designed to test your employees against a simulated real-world attack on their company mobile devices. Our platform includes multiple text message templates, distribution by groups or individuals, and syncs with TraceEDU to offer training as soon as an employee fails a smishing attempt.
You can use TraceSmishing to test your employees year-round and increase security awareness at your organization to prevent a breach from happening. You can segment the smishing however you'd like, based on department, time of year, or anything else you can think of.

Let Us Help!

You can handle your smishing program on your own, or have us manage the testing for you. With Managed TraceSmishing, we'll take care of the text message content based on the most up-to-date smishing techniques (with your input), scheduling of smishing texts, and lining up training for those that fail. After each round of testing, we'll provide you with a somprehensive report so you can track your employee retention to information security policies and see improvement over time. If you choose to handle the testing on your own, you'll be able to run your own reports right from the platform!

With TraceSmishing You Can Expect:

- **Simulated text message smishing campaigns sent to your employees**
- **Customized text message smishing templates**
- **Distributions scheduled to meet your security awareness needs**
- **Expert recommendations on best practices in simulated smishing engagements**

Frequently Asked Questions

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

What's the difference between getting the program and doing the smishing internally and having Trace manage our smishing efforts?
If you run smishing internally, you'll need to set up the distribution groups, choose the message(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 smishing distribution?
This is done automatically if you are using AD/LDAP sync, or manually by creating a user up uploading a CSV file.

Will Trace smish my employees continuously or only on set intervals?
This depends very much on the scope of the engagement. Smishing is typically done in intervals and the text messages are not all sent at once.

How customizable are the text messages? Can I customize them myself no matter which version of TraceSmishing I get?
Text messages are very customizable - all content can be modified to suit your needs. You can customize the text messages regardless of which version you get.

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

If an employee fails a smishing attempt, what happens?
Employees who fail smishing attempts are logged as such in our system and the details of the failure are reported to you. The details will include whether the smishing text was opened, whether the user clicked on the malicious link(s) included in the text, and exactly when the user failed the test (date and time). There is also 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 smishing 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 unlimited reports with detailed data in both PDF and CSV formats.

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

Are TraceEDU and TraceSmishing connected? Can I queue up training for those who have failed a smishing attempt?
Yes, users that fail smishing campaigns can be enrolled into TraceEDU education courses to increaes their awareness.

tracesecurity
Compliance, simplified.