TraceSmishing

DATASHEET

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.

Attackers have successfully used a number of smishing techniques, from shipping tracking information to bank account verifications. Some attacks have gotten so sophisticated as to start using speech synthesis, or a fake voice simulation of a trusted user.

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

TraceSecurity information security analysts will perform simulated smishing attacks on your company mobile devices. We provide multiple text message templates based on the most up-to-date smishing techniques that can be customized with your input.

We work with you to configure smishing tests to be sent based on your specific needs: regular interval testing throughout the year, specific groups or departments, or anything else you can think of. After each round of testing, we'll provide you with a comprehensive report so you can track your employee retention to information security policies and see improvement over time.

Frequently Asked Questions

Will you 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 sent all at once.

How customizable are the text messages?

Text messages are very customizable, but smishing campaign pricing will vary based on the complexity of the template content. Excessive or special characters are subject to additional charges per text message and data rates. We recommend that you keep smishing texts concise to best mimic real-world attacks.

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 user clicked on the malicious link(s) in the text and the date and time when the user failed the test. There is also an option to display a configurable webpage with a message to notify users of their failure with tips to improve security awareness.

What kind of reporting will I get and how often?

We will provide detailed reports outlining the results of each testing in PDF format. Reports are typically provided after each round of testing, but this can be customized to your needs.

How often are the text message templates updated?

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.

TraceSmishing Includes:

- Simulated text message smishing campaigns sent to your employees
- Customizable text message smishing templates
- Distributions scheduled to meet your security awareness needs
- Expert recommendations and best practices