

## *Protecting Customer Data at Rest and in Motion*

Targeted phishing attacks, often referred to as "spear" phishing or whaling, are a significant threat to all organizations especially banks. As the conventional network perimeters of most organizations have gotten more secure due to the maturing of protective technologies such as firewalls, Virtual Private Networks, Intrusion Detection Systems, and Intrusion Prevention Systems, resourceful and determined attackers have shifted focus back to the human element, which is often the weakest link in protecting data at rest and in motion. This allows them to traverse the path of least resistance and get to the crown jewels - customer data.

Why spend days attempting a complex SQL injection attack against the bank's customer-facing online interface, when a few crafty emails targeted at a handful of employees can do the trick - this is the hacker mindset. Over the years we have seen phishing emails that target employees at banks get more sophisticated and virtually impossible for anti-phishing technologies to detect. These emails prey on human fear and greed to lure employees to behave in ways that are detrimental to the bank's security posture. Thus, we believe employee awareness and ongoing training are key to fighting this growing pandemic.

There is more to security than shrink-wrapped technology. Even with a whole array of state-of-the-art technologies in place, you cannot ignore the human element. Social engineering tactics were quite popular years ago, and are now making a strong comeback. The final defense against attacks by "hackers" is human intelligence and awareness. Teaching employees that don't view security as part of their job function, that they are a critical component of the bank's security posture isn't easy.

This is especially true when it comes to targeted phishing attacks that rely on human reaction to be successful. It has been proven that merely displaying posters and talking about security are not effective in improving employee awareness. The innovative approach of mock phishing exercises that emulate phishing attacks against employees and take advantage of the "teachable" moment when they fall prey, by presenting training materials, is the most effective way of raising awareness. This technique has been recommended by reputed bodies like SANS and researchers at Carnegie Mellon University.

Our web-based solution, PhishMe.com, allows you to easily set up and execute such mock phishing exercises in a matter of minutes. You can choose one of our built-in phishing themes or build your own to tailor the level of sophistication of the exercise based on the goal of the engagement, e.g. a basic assessment may entail a phishing email with a link to a phishing site, while an advanced one may include attaching specialized faux-malicious code that passes through email filters, and emulates an outbound network connection from the victim's machine to Intrepidus Group controlled resources. PhishMe also collects key metrics on user behavior in a manner that can be presented to senior management. Most importantly, our solution gives you the ability to use our training materials or your own to present to employees that are found to be susceptible. We recognize that every bank is different and thus, give you full control in tailoring your exercises - and accompanying security training.



**Rohyt Belani**  
CEO

**Rohyt Belani** is CEO and co-founder of the Intrepidus Group and Adjunct Professor at Carnegie Mellon University. Prior to starting the Intrepidus Group, Mr. Belani has held the positions of Managing Director at Mandiant, Principal Consultant at Foundstone and Researcher at the US-CERT. He is a contributing author for Osborne's Hack Notes – Network Security, as well as Addison Wesley's Extrusion Detection: Security Monitoring for Internal Intrusions. Mr. Belani is a regular speaker at various industry conferences including Black Hat, OWASP, ASIS, SecTOR, Hack in the Box, Infosec World, TechnoSecurity, CPM, ISSA meetings, and several forums catering to the FBI, US Secret Service, and US Military.

