



Scott Greaux

Human Defenders: How the “Weakest Link” Can Become Your Organization’s Greatest Strength

Are your users more likely to cause – or prevent – your next data breach? With the majority of state-sponsored attacks targeting humans rather than computers, a user-base that is resilient to common attack methods is an important element of your security posture. An immersive training program can teach employees to not only recognize those attack methods, but also to report suspicious activity and provide valuable threat intelligence to the IR team. In this presentation, Rohyt will offer insights into the tactics adversaries use to target your users, and discuss innovative training methods proven to improve user behavior and security posture.

Biography

Scott Gréaux has over 15 years of diverse information technology experience spending most of the past decade developing solutions to address complex information security problems. Most recently Scott served as General Electric’s Deputy Chief Information Security Officer where he led key global initiatives such as Policy and Policy Frameworks, Security Awareness, Advanced Threat initiative coordination and Information Security metric reporting.

During his tenure at GE he was uniquely positioned to see the threat of advanced phishing techniques and developed a multi-faceted program to address the phishing risk in a large enterprise.

Scott brings his extensive experience and unique blend of business management and creative marketing practice to PhishMe where he works with customers to develop robust anti-phishing programs. Greaux also oversees PhishMe’s managed service offering, support operations and leads PhishMe’s Customer Advisory Board where he works with customers and industry thought leaders to align PhishMe features with the ever changing threat landscape.