



Dan Bougere

Embrace the Click: Five Effective Social Engineering Protections

Technical Track: Intermediate

If you ask an IT professional to name the one thing that keeps them up at night, social engineering scams would definitely be on that list! Your users continue to click on links and run malicious programs no matter what you do, and hackers continue to take advantage of them. Isn't it time to accept that behavior and build an effective defense around it rather than wishing it wasn't so? Shouldn't we be focusing on how to better train our users to recognize threats rather than shielding them from the harsh reality they face? Wouldn't it be great to approach these problems from a realistic expectation rather than unattainable perfection? Here are five methods that will build a stronger, more effective, and LESS expensive social engineering defense for your organization.

Biography

Dan Bougere is a Senior Security Consultant at Securicon, LLC, providing clients with customized security assessments that combine traditional vulnerability assessment with controlled penetration testing that take into account real world threats as well as the client's business processes. Dan has over 13 years of combined experience in both government and commercial sectors as a contractor for the Department of Defense in Afghanistan, a Global Network Exploitation and Vulnerability Analyst in the National Security Agency's TAO office, and other roles with intelligence community partners, business, and local governments.

Dan earned a Bachelor of Science degree in Software Engineering Technology from the University of Southern Mississippi, a Master of Science degree in Information Assurance from Capitol Technology University, and a Master of Science degree in Technology Studies (Offensive Security) from Eastern Michigan University. Dan is a Certified Information Systems Security Professional (CISSP) and holds multiple certifications from SANS, CompTIA, and Microsoft. He also teaches courses for SANS in the Washington, DC area in incident handling, intrusion analysis, network forensic analysis, and security essentials.