Emerging Social Engineering Trends in 2024

Social engineering tactics are advancing at an alarming pace, with cybercriminals constantly refining their strategies to exploit human weaknesses. Historically, these tactics primarily involved simple methods like email phishing or deceptive phone calls, designed to trick individuals into revealing personal information or login credentials. However, with the increasing reliance on digital communication channels and the proliferation of personal information shared online, attackers have more resources at their disposal than ever before. Social media, email, and even SMS have become breeding grounds for new and creative attacks. The rise of AI and automation has further amplified the impact, enabling cybercriminals to deploy these attacks on a larger scale, with more precision, and at a lower cost.

A sophisticated social engineering trend on the rise for 2024 is angler phishing. This tactic thrives on the widespread use of social media platforms such as Twitter, Facebook, and Instagram. In these scams, attackers create fake customer service accounts to trick users into sharing sensitive information, pretending to be legitimate company representatives. By carefully mimicking the support profiles of real businesses, they manage to deceive unsuspecting individuals into handing over personal data, all under the pretense of resolving a problem.

Angler phishing is just one part of a much larger trend with other tactics like thread hijacking in Business Email Compromise (BEC), smishing (SMS phishing), and vishing (voice phishing) becoming more pervasive, exploiting trust across multiple communication channels. As these methods become more sophisticated, both organizations and individuals face growing risks, necessitating stronger defenses like multi-factor authentication (MFA), advanced email security tools, and heightened vigilance against potential scams.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.