Combating Social Engineering in 2024

Psychological manipulation through social engineering has become a pervasive threat to businesses and their employees in 2024.

Understanding the evolution of social engineering and its prevalence is the first step in combating it. But equally important is understanding how to face this growing challenge — and what your organization can do.

Phishing will continue to be the biggest threat to businesses, made even more harmful with Gen AI.

81% of businesses have seen an increase in phishing this past year.

Social engineering attacks have become more sophisticated via Gen AI adaptive content in emails to evade detection by security filters and through more direct targeting of individuals.

Cogntive dissonance is high when it comes to the efficacy of phishing training programs.

88% of respondents think their company's phishing testing program is effective.

However, only 85% of users report 75-100% of suspicious activity within their phishing testing program.

16% of businesses ultimately want to eliminate the use of these attacks altogether.

Organizations agree that the removal of passwords through passkeys will eventually help reduce the threat of social engineering.

Adapting to the evolving nature of social engineering attacks, particularly phishing, is to the integrity and safety of your business's data.

Ultimately, though, the elimination of passwords will be challenged against a type of attack that manipulates human behavior.

Want to learn more about combatting social engineering within your own organization?

Get the full book here.