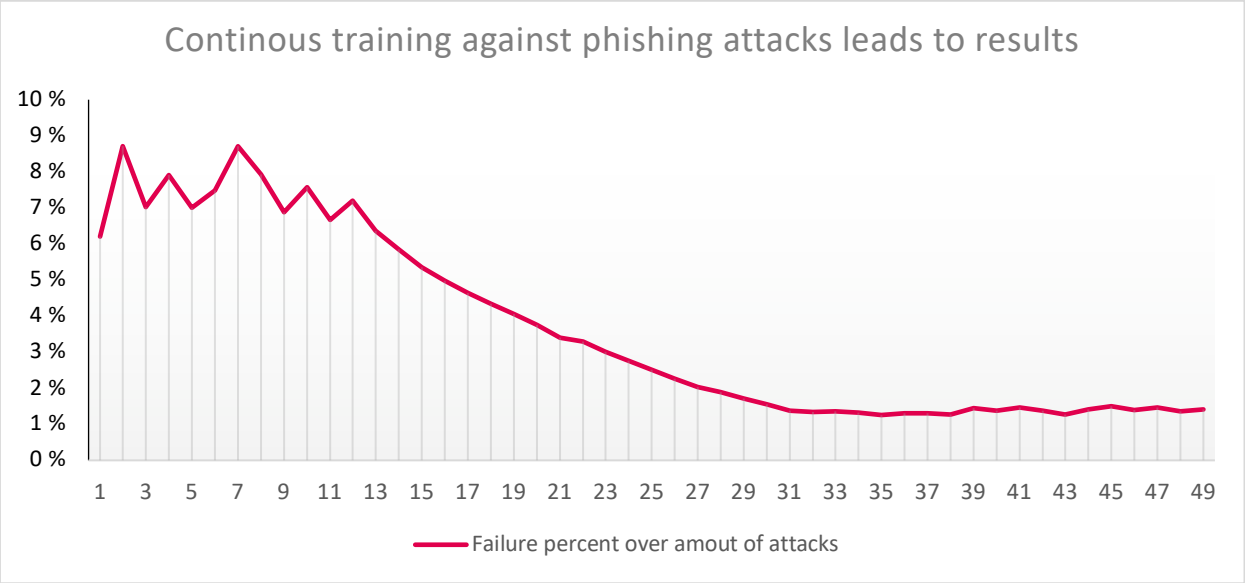
HOXHUNT

Security behavior change as a Service

WHEN SECURITY AWARENESS IS NOT ENOUGH



Problem:
Traditional cyber security training regarding email fails and penetration tests only give a single snapshot of the organizations performance. Employees are still clicking malicious email links and enabling macros. Many think that the fundamental problem is security awareness, however employees can be aware and still behave the wrong way when an attack is received. That is why organizations need to train people to respond to these attacks with the right behavior.

Solution:
HoxHunt trains employees to be social engineering and phishing resilient with AI. HoxHunt system acts as a virtual hacker that tries to invade your organization continuously with different types of phishing attacks – including CXO frauds, ransomware and credential phishing. Your employees' task is to identify and report these email-based attacks. The HoxHunt system rewards your employees for reporting both the simulated and real attacks, thus your employees get incentivized to recognize and report real attacks, enabling your IR team (or the HoxHunt IR module) to react to these anomalies.

Data:
With HoxHunt's gamified end-user first approach HoxHunt delivers measurable results on employee security behavior change. Rather than penetration testing and measuring employee's performance with a single attack in single point in time, HoxHunt Virtual Hacker trains your employees continuously with the latest attacks. Continuous simulation means that the right security behavior is sustained. Your employees start identifying the attacks (HoxHunt has the lowest click-through-rates 1,5% globally) and they start reporting them to your visibility (HoxHunt has the highest malicious email reporting rates 70% globally).

HoxHunt is trusted by Fortune 500 companies. References available upon request.

www.hoxhunt.com
contact: karri.kurunmaki@hoxhunt.com