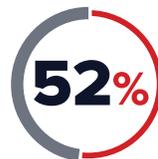**eSENTIRE**

DATA SHEET
Security Awareness Training

Knowledge to recognize, understand and avoid security risks.

Your employees are your business's greatest asset and greatest risk. Year after year, human error is one of the most prominent data breach causes. Adversaries are crafting increasingly sophisticated social engineering campaigns that can compromise your most cyber-savvy employees. Mitigate the risk of human error with insight from the world's leading Managed Detection and Response (MDR) service provider. Keep your employees up-to-date with the evolving threat landscape and the latest preventative measures with Security Awareness Training.

60% of breaches were caused by a negligent employee or contractor[1]

52% of small and medium-sized businesses reported phishing and social engineering attacks[1]

⭐ FEATURES

Tailored to your organization's needs
Every Security Awareness Training is scoped and tailored to your organization's knowledge gaps.

On-site or virtual
Training sessions can be performed on-site or virtually via video conference. Virtual sessions can be recorded for on-demand viewing.

Insight from the global MDR leader
The training features first-hand observations and expertise from the world's leading MDR provider.

Combine with phishing exercises
Validate and track your employees' progress by combining with phishing exercises.

🔖 BENEFITS

⊕ Hardens perimeter security posture

⊕ Meets compliance requirements

⊕ Helps develop your organization's security culture

⊕ Improves employee morale and team building

⊕ Decreases overall risk exposure

[1] *2018 State of Cybersecurity in Small & Medium Sized Businesses*

1 Build an understanding of the security landscape
- Data breach statistics
- High-impact data breaches

2 Discuss social engineering and how it relates to data breaches
- Social engineering principles
- Social engineering types
- Social engineering goals

4 Fill in knowledge gaps and misconceptions
- Website misconceptions
- Email misconceptions
- Ad misconceptions
- Wi-Fi misconceptions

5 Illustrate common attack methodologies
- Phishing
- Malicious scripting
- Network compromise
- Hardware attacks
- Exploit kits

6 Provide specific, actionable defenses
- Passwords
- Patching
- Proactive protection
- Pruning and patience
- Incident response

eSENTIRE.