FORTRA

DATASHEET

Human Risk Management Datasheet

Break the Chain of Social Engineering Attacks

Fortra Human Risk Management (HRM) cultivates user behaviors that disrupt the attack chain while enabling organizations to identify and mitigate human risk effectively. Fortra's team of offensive and defensive security experts understands the risky behaviors threat actors exploit and the positive actions that prevent compromises. Leveraging this insight, HRM delivers engaging, high-impact training and simulations grounded in real-world social engineering scenarios.

Moreover, HRM empowers administrators to effectively pinpoint areas of high risk using powerful analytics and a customized training curriculum based on user risk profiles. With Managed HRM and HRM Advisory Services available, organizations can quickly partner with Fortra experts to elevate their security awareness programs and strengthen their human firewall.

Instill Secure Behaviors

HRM effectively instills user behaviors that break the chain of social engineering attacks. The training content is developed by Fortra's offensive and defensive security experts, who possess deep insights into how attackers exploit user vulnerabilities. By providing ongoing training and simulations that respond to emerging threats, HRM ensures users remain one step ahead of attackers. Additionally, comprehensive curriculums focused on the highest-risk threats cover advanced protective behaviors, empowering users to safeguard themselves and the organization against sophisticated attacks.

Minimize Human Risk

Fortra empowers administrators to deliver impactful training that aligns closely with the real human risk present across their organization. Leveraging analytics at the individual user level, HRM pinpoints specific areas of risk to enable targeted interventions.

Engaging and high-impact content ensures that users effectively learn and retain key security behaviors during training. Furthermore, training customization based on user roles and risk profiles guarantees that the material remains relevant and tailored to everyone's unique needs, maximizing the overall effectiveness of the program.

KEY FEATURES

- In-depth training curriculums focusing on the high-risk threats
- Training and simulations for responding to emerging threats
- Engaging, high-impact training in a variety of easy-to-consume formats
- Comprehensive analytics with visibility down to individual users
- Customization based on user roles and risk profiles
- Integrated phishing reporting, triage, and response
- Optional program management by HRM professionals **(Managed HRM)**
- Customized program plans and expert guidance **(HRM Advisory Services)**

Improve HRM Maturity

Administrators can rapidly advance their security awareness training programs by providing the expertise, tools, and support needed at any stage of maturity. With a range of packages and pre-built training plans tailored to every maturity level, admins can quickly implement improvements and accelerate program growth without starting from scratch. This streamlined approach ensures that organizations can efficiently enhance their security posture regardless of their current capabilities.

For added flexibility, Fortra offers optional program management through Managed HRM services, allowing administrators to focus more on strategic leadership and less on day-to-day operations. Additionally, HRM Advisory Services provide expert guidance and program plan customization, ensuring that training initiatives are precisely aligned with organizational goals and evolving security challenges. Together, these options empower admins to build robust, effective programs with confidence and ease.

HRM Training Catalog

HRM enhances cybersecurity awareness through engaging and accessible content, and supports behavior change initiatives with diverse training formats tailored to varied learning needs.

Core Components

Training Formats

- **Courses & Quizzes:** Interactive modules with quizzes to reinforce and test knowledge.
- **Microlearning:** Concise modules targeting specific risks for better retention.
- **Nanolearning & Nanovideos:** Just-in-time, short-format training for specific threats like phishing and ransomware.
- **Role-Based Training:** Custom content for roles including executives, finance, HR, IT, and managers.

Specialized Content Areas

- **General Knowledge:** Covers essentials like phishing, data protection, device security, and incident reporting.
- **Cyber Games:** Gamified learning with real-world scenarios through Serious Games and Cyber Challenges.
- **Risk-Based Modules:** Tailored content focusing on high-risk behaviors and attack vectors, including phishing, malware, ransomware, social engineering, password hygiene, mobile and remote work security, identity theft, data privacy, and regulatory compliance.
- **Compliance & Privacy:** Training for laws and regulations (e.g., GDPR, CCPA, HIPAA, PCI DSS, NIS2, DORA).

Engagement & Reinforcement Tools

Communication Assets: Newsletters, posters, web banners, infographics, and short explainer videos.

Cyberpedia: A comprehensive resource for in-depth explanations for cybersecurity topics.

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.