Human Risk Management For Financial Services

As stewards of critical financial and personal data, financial service organizations and banks stand as prime targets for social engineering and phishing attacks. Safeguarding against these assaults is paramount, even as attackers devise new tactics to breach defenses. Protecting account credentials and assets is integral for doing business, maintaining customer trust and upholding your organization's brand.

Human Error Is The Primary Cause of Financial Cyberattacks

~70%

of **cyber breaches** within the financial services industry are **caused by human error**, according to various industry studies from IBM, Verizon and Deloitte

$6.08 million

Is the **average cost of a data breach** for financial service organizations globally, according to the IBM Cost of a Data Breach Report

219 days

On average, to **identify and contain a data breach** in the financial services industry, according to the IBM Cost of a Data Breach Report

A Social Engineering Assault

Here are 10 examples of social engineering attacks that financial service and banking organizations have suffered in recent years.

1. **Retail Banks:** Employees receive phishing emails impersonating a customer or a bank executive, leading to unauthorized access to banking systems.
2. **Credit Card Companies:** Call center representatives could be tricked by vishing (voice phishing) into divulging customer account information.
3. **Investment Firms:** Fraudulent requests for wire transfers generated through spear-phishing attacks specifically targeting high-level executives (whaling).
4. **Mortgage Lenders:** Smishing (SMS phishing) might be used to capture personal and financial data from individuals applying for mortgages.
5. **Insurance Companies:** Attackers may pose as insurance policyholders or agents to gain access to sensitive data.
6. **Payment Processors:** Social engineering may be used to install malware on systems handling payment card processing to skim card details.
7. **Online Brokerages:** Cybercriminals could use impersonation tactics to take over customer accounts or gain internal system access.
8. **Wealth Management Firms:** Phishing emails may be sent to clients with links to fake login pages designed to capture login credentials.
9. **Crypto Exchanges:** Users and employees might be targeted to provide access tokens or credentials related to cryptocurrency wallets.
10. **Peer-to-Peer Lending Platforms:** These services may suffer from social engineering where attackers impersonate borrowers or lenders to perform unauthorized transactions.

The Impact of Security Awareness Training on Financial Service Companies

Security awareness training (SAT) and simulated phishing is the foundation for driving vigilance, building a strong security culture and is the foundation for a human risk management (HRM) strategy.

KnowBe4's Global Phishing By Industry Benchmarking Report measures Phish-prone™ Percentage (PPP), or the number of employees likely to fall for social engineering and phishing scams. Here is the impact that KnowBe4's SAT platform had on financial service organizations of all sizes based on PPP.

	Small Businesses 1-249 Employees	**Medium Businesses** 250-999 Employees	**Large Businesses** 1000-10,000 Employees	**Enterprises** 10,000+ Employees
Baseline Phishing Security Test Results - No Training	23.1%	28.9%	38.4%	44.7%
After 90 Days of SAT	18.8%	18.8%	19.8%	16.8%
After One Year of SAT	3.1%	3.8%	4.8%	3.9%
Overall improvement of susceptibility to phishing attacks	**86%**	**87%**	**87%**	**91%**

KnowBe4's HRM+ Platform

The HRM+ platform is KnowBe4's innovative approach to human risk management. HRM+ transforms your largest attack surface — your workforce — into your biggest asset, actively protecting your organization against cybersecurity threats, strengthening your security culture and reducing human risk. It comprises:

Security Awareness Training

AI-powered security awareness training and simulated phishing that allows organizations to drive awareness and change user behavior. Build a stronger security culture by effectively managing the ongoing problem of social engineering.

Cloud Email Security

The only email security platform to continually assess human risk and dynamically adapt security controls, preparing customers to defend against advanced phishing threats, human error and data exfiltration.

Anti-Phishing

Security orchestration and proactive anti-phishing protection to allow your incident response and security orchestration teams to identify and stop phishing threats before they reach your users' inboxes.

Real-Time Security Coaching

The first ever real-time security coaching product that detects and responds to risky end user behavior to provide immediate feedback, improving overall security culture and reducing human risk.

Compliance Plus

Compliance training that delivers continuously updated, engaging, customizable content to users and allows your organization to take a comprehensive approach to security awareness and compliance training.

AI Defense Agents

AIDA is an advanced suite of AI-powered agents that elevates your human risk management strategy.

Learn More About HRM+

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

0449C1025