

How to Train Your AP Team on Ransomware

In the ever-evolving landscape of cybersecurity threats, finance professionals must be vigilant against the human element, which accounts for a staggering 74% of breaches (Verizon, 2023). With the average cost of a ransomware breach at \$5.13 million (IBM), investing in targeted training is paramount.



► Why Ransomware Training Matters:

- Employees are both the weakest link and the first line of defense.
- Building a security culture relies on recognizing the crucial role of individuals.
- Educated users help avoid financial, legal, and reputational costs of attacks.

Key Components of Ransomware Training

1

Understanding Ransomware Basics

Define ransomware and emphasize employee roles in prevention, detection, and mitigation.

2

Types of Attacks and Attack Vectors

Cover various ransomware types and attack vectors (e.g., social engineering, RDP, software vulnerabilities).

3

Recognizing Signs of Infection

Train employees to identify warning signs (e.g., phishing emails, unusual device behavior).

4

Response Protocol

Instruct on immediate actions, including disconnecting devices, reporting to IT, and not negotiating with attackers.

5

Prevention Best Practices

Educate on end-user practices (phishing awareness, URL caution, data backups, strong passwords), and implement enterprise-level measures

6

Regular Training and Simulations

Include phishing and ransomware simulations for real-world preparedness.