

Reinforcing Email Security: Defending Against Soft Threats



Protecting Your Inbox from Soft Threats

1. Introduction:

Email communication is a lifeline for billions of people worldwide, but it's also a playground for cyber threats. One in three businesses has faced a phishing attack, with victims losing over \$52 million in 2022 alone. - Soft threats are a common email security risk that can compromise sensitive information.



Global Email Use: Email is used by an estimated 5 billion people worldwide.

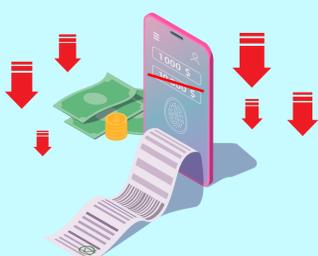
Rising Threats: With widespread email use, threats have escalated.



Business Impact: 1 in 3 businesses have experienced a phishing attack.



Financial Loss: Victims lost over \$52 million to phishing scams in 2022.



2. Understanding Soft Threats:

Soft threats are deceptive attacks, including phishing, malware, and social engineering, designed to trick email users. They exploit human vulnerabilities and often go undetected, highlighting the need for stronger security strategies.



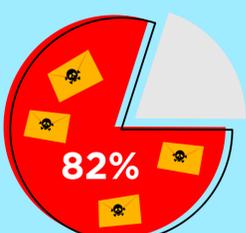
Types of Soft Threats: Soft threats include phishing, malware, and social engineering attacks.



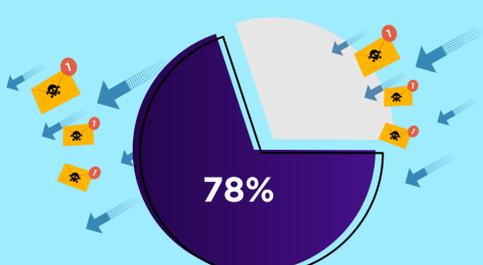
Human Vulnerabilities: These threats exploit human vulnerabilities.



Undetected Threats: 82% of soft threats bypass Secure Email Gateways.



Origin of Threats: 78% of malicious emails come from Office 365 and Google Workspace users.



3. Mitigating Risks Email Security Risks

Keepnet's Email Threat Simulator continuously tests your secure email gateway solutions with 700+ real-world attacks, identifying vulnerabilities and strengthening defenses.



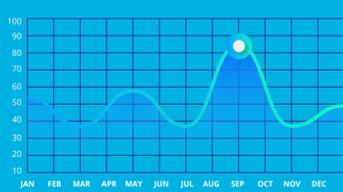
Harden Secure Gateway: Strengthen your secure gateway solutions against real-world threats.



Fix Misconfigurations: Detect and corrects issues in email configuration.



Monitor Progress: Track improvements and readiness against email attacks over time.



Reduce email risk using the following attack samples:

Malicious Attachment Simulation: Test the robustness of your security measures against malicious attachments.



Ransomware Simulation: Evaluate your defense capacity against known ransomware attacks.



APT Attack Simulation: Assess your response to advanced persistent threats.



Customized Testing: Customize attack vectors for tailored security testing.



Detailed Reporting: Receive comprehensive reports to understand vulnerabilities and improve the defense.



Investment Payoff: Boosts email blocking efficiency from 28% to 96%, maximizing your security investment.



Sign up for our **FREE 15-day** trial and discover how we can help you strengthen your secure email gateway solutions.



info@keepnetlabs.com