KnowBe4

The Outstanding ROI of PhishER Plus

My name is Stu Sjouwerman. I'm the Founder and CEO of KnowBe4, my 5th startup. I have been in IT for 40+ years, the last 25 of those in information security. At my last company, we built an antivirus engine from scratch and combined it with intrusion detection, prevention and a firewall. But we encountered a persistent problem that few organizations were addressing; end users being manipulated by bad actors. That's why I started KnowBe4: to help IT professionals manage the ongoing problem of social engineering.
In April 2021 we went public on the NASDAQ, and we were taken private in 2023.

Overcome the Phishing Tsunami

91% of cyberattacks start with a spear-phishing attack and phishing is responsible for two-thirds of ransomware infections. With advancements in AI making sophisticated phishing attacks exponentially more effective, it's critical you arm your IT and infosec teams with the tools to accurately and quickly mitigate phishing threats BEFORE they strike.

If your organization is combating phishing threats with manual workflows, you're dramatically increasing the risk that phishing presents to your organization. These outdated processes create four major challenges:

> "PhishER is a natural for our business. It significantly reduces our risk, it saves our technical teams a ton of time and it is very easy to configure and customize."
>
> – George Schneider, Information Security Manager

- **ALERT OVERLOAD**

  IT and infosec teams that rely on manual workflows take, on average, 27 minutes to manually triage a phishing email,[1] dramatically increasing the risk phishing presents to your organization.

- **STRESSING UNDER-RESOURCED IT TEAMS**

  61% of mid-sized organizations do not have a dedicated cybersecurity expert on staff, and on average, for every 10 IT employees at an organization, only one is dedicated to cybersecurity.[2]

- **INABILITY TO STOP THE TSUNAMI**

  Increasing percentages of phishing emails are making it past secure email gateways and into your users' inboxes: 56% of email-based attacks bypassed legacy security filters in 2022,[3] and 18.8% of phishing emails bypassed Microsoft Exchange Online Protection and Defender.[4]

- **SLOW RESPONSE TO TARGETED ATTACKS**

  The inability to mitigate a targeted phishing attack, such as a spear phishing campaign, in real time leaves your organization vulnerable. Multiple users are likely receiving the same phishing emails and your organization can't quarantine phishing emails from inboxes before a malicious link is clicked on.

[1]The Business Cost of Phishing, 2022 Report
[2]State of Cybersecurity for Mid-Sized Businesses, 2023
[3]ArmorBlox
[4]Check Point Email Research Team

This is why it's critical to implement KnowBe4's Security Orchestration, Automation and Response (SOAR) product designed specifically for phishing threat response and management: PhishER Plus

The Benefits And ROI Of KnowBe4's PhishER Plus/PhishER

Here are the cost savings, productivity gains and business benefits one enterprise organization experienced by implementing KnowBe4's PhishER, according to Forrester's Total Economic Impact of KnowBe4.[5]

Using KnowBe4's Phish Alert Button, the organization's employees report up to 2,000 suspicious emails in PhishER per month. About 88% of these user-reported emails are spam or threats. This helps the organization manage, escalate and remediate these large volumes by using the PhishRIP email quarantine feature to automatically quarantine and delete reported phishing emails from the mailboxes of affected users.

Time savings from automated email alert notification and response, valued at $411,302.

PhishER Plus saves the organization's incident response team an average of 25 minutes of investigation/ remediation work per email.

Increased collaboration between users and SecOps enables proactive threat response and reduced IT help desk tickets and the need for IT remediation work

Automated responses that allow you to quickly communicate with employees regarding emails they need to continue working.

Additional Organizations with Time Savings:

- **U.S.-Based Critical Infrastructure Organization**

  Saves 7 weeks' time annually for the IT team by automatically investigating, quarantining and removing malicious emails

- **Marketing Firm**

  Has reduced the number of suspicious emails that needed to be manually investigated from approximately 70 to 20 per month, resulting in a savings of at least 12.5 hours/month

- **Technology Organization**

  Uses PhishER's AI-driven analysis to automatically identify 70% of all user reported emails, allowing headcount and budget to be dedicated to other IT teams

- **Non-Profit Organization**

  Improved phishing attack response times and freed IT resources and headcount for other security priorities

- **Higher Education Institution**

  PhishER ripped over 150,000 malicious emails from users' inboxes before they ever had a chance to click on them

I strongly recommend you approve this PO.

More than 65,000 organizations globally use it successfully.

Warm regards,

Stu Sjouwerman
Founder and CEO

[5] Forrester Total Economic Impact of KnowBe4