livingsecurity

BUSINESS RISK

EMAIL & PHISHING VULNERABILITY

20% Of all employees are likely to click on phishing email links[1]

Challenge

Threat actors are becoming more sophisticated in their attempts to trick individuals to openly share personal and company information, thus resulting in an increase in data breaches. Historically organizations lean on phishing simulations to educate users on what to watch out for, however this alone is not shifting users away from clicking links in emails with clever subject lines, legitimate looking attachments, brand impersonations, or recognizing internal threats.

Solution

Living Security's Unify, Human Risk Management solution, enables security leaders to decrease their organizational risk by quantifying, responding to, and measuring human initiated risk to change behaviors.

Capabilities:

- Understand your riskiest individuals considering those with privileged access, non-malicious insider threats, and employees with larger attack surfaces.
- Share digestible and actionable risk metrics with other business leaders.
- Analyze phishing hygiene across your workforce.
- Identify which email behaviors lead to increased probability of clicking a phish.
- Take action to remediate behavior in a single platform.

[1] Terranova Security

Outcome

As a result of tracking and surfacing these insights your organization will see a **drop in the number of individuals with high risk of phishing and other email scams and an increase in vigilant behavior.**

Actionable insights improve cyber culture:

- Stop successful phishing and email scams before it turns into an incident.
- Prove ROI of Phishing, Email Security, and Security Awareness Programs

Integrations

Connect the following technology with Unify to understand, track, and reduce successful phishing and email scam attempts from occurring.

- Email Security
- LMS / Training
- Phishing Simulator

View available integrations

Insights Uncovered

Surface intelligence to drive change in your organization and reduce the likelihood of a successful phish.

- Quarantine activity
- Phishing proficiency
- Targeting susceptibility
- Phishing reporting analytics

Email & Phishing Vulnerability

- **Highlight** users who struggle to identify a phish
- **Analyze** susceptibility of users
- **Understand** which email behaviors lead to increased **probability of clicking a phish**
- **Act** on surfaced phishing insights to **reduce organization risk**

Objectives

- **Reduce susceptibility** to phishing attacks
- **Reduce** phishing click rate
- **Increase user reported phishing emails**
- **Identify most targeted users** across the email attack landscape

Behavior Change

- **Identification** of suspicious emails
- **Clicking** on URLs or attachments from unverified senders
- **Releasing** of quarantined emails
- **Reporting** of suspicious emails
- **Containing** suspicious emails

Insights

- Email **Behavior**
- **Quarantine Activity**
- **Phishing Proficiency**
- Targeting **Susceptibility**
- **Phishing Reporting Analytics**

Integrations

- **Email Security** (e.g. Proofpoint, Mimecast)
- **LMS/Training** (e.g. Living Security, Hoxhunt)
- **Phishing Simulator** (e.g. Living Security, Cofense)

LEARN HOW TO

MEASURABLY REDUCE CYBERSECURITY RISK

Get Started! See Unify in Action

About Living Security

Living Security's mission is to transform human risk to drive dramatic improvement in human behaviors, organizational security culture, and infosec program effectiveness. With our Human Risk Management platform, Living Security engages each employee with innovative and relevant context and content, while simultaneously providing the ability for leadership to identify, report on and directly mitigate the risk brought on by human behavior. Living Security is trusted by security-minded organizations like MasterCard, Verizon, MassMutual, Biogen, AmerisourceBergen, Hewlett Packard, and Target.

livingsecurity