

Monitor and Reduce Your Human Risk

Detect Dark Web Breaches

Identify Your Cybersecurity Champions

Report Phish Add-On



PHISHPROOF

By HATHR CYBER SECURITY



محاكاة تهديدات
التصيد الاحتيالي
وتدريب موظفيك



Monitor and
Reduce Your
Human Risk



Detect Dark Web Breaches

PHISHPROOF
By HATHR CYBER SECURITY

Knowledge Base

Welcome Checklist

PHISHING & TRAINING

- Dashboard
- Campaigns
- Employees
- Reporting
- Phishing Content
- Training Modules

CONFIGURATION

- Platform Settings
- Subscription & Billing

Human Risk Overview | Phishing Overview | Training Overview

Low Risk — 35%
Human Risk Score & Human Risk Factors

Human Risk Timeline & Forecast

Human Risk (5 Highest Risk)

EMPLOYEE EMAIL	FULL NAME	HUMAN RISK
dennis@cyberducks.com	Dennis Turner	85% - High Risk
alex@cyberducks.com	Alex Sasha	80% - High Risk
aisha@cyberducks.com	Aisha Khan	55% - Medium Risk
marcusporter@cyberducks.com	Marcus Porter Holloway	55% - Medium Risk
erin@cyberducks.com	Erin Ekersill	50% - Medium Risk

Employee Leaderboard (5 Highest Ranking)

EMPLOYEE EMAIL	FULL NAME	SCORE
hannah@cyberducks.com	Hannah Schultz	215
sofia@cyberducks.com	Sofia Morales	215
gabby@cyberducks.com	Gabriel Mendes	215
lukas@cyberducks.com	Lukas Schneider	190
ivana@cyberducks.com	Ivana Petrović	185

Dark Web Activity (5 Most Recent Breaches)

EMPLOYEE EMAIL	BREACHES	DETECTION DATE	STATUS
freja@cyberducks.com	2	20/07/2025	Employee Notified

Employee Reported Emails (5 Most Recent Reports)

REPORTED BY	REPORT DATE	ATTRIBUTION	ACTIONS
jonathan@cyberducks.com	19/08/2025	Analysis Required	
jonathan@cyberducks.com	14/08/2025	Analysis Required	



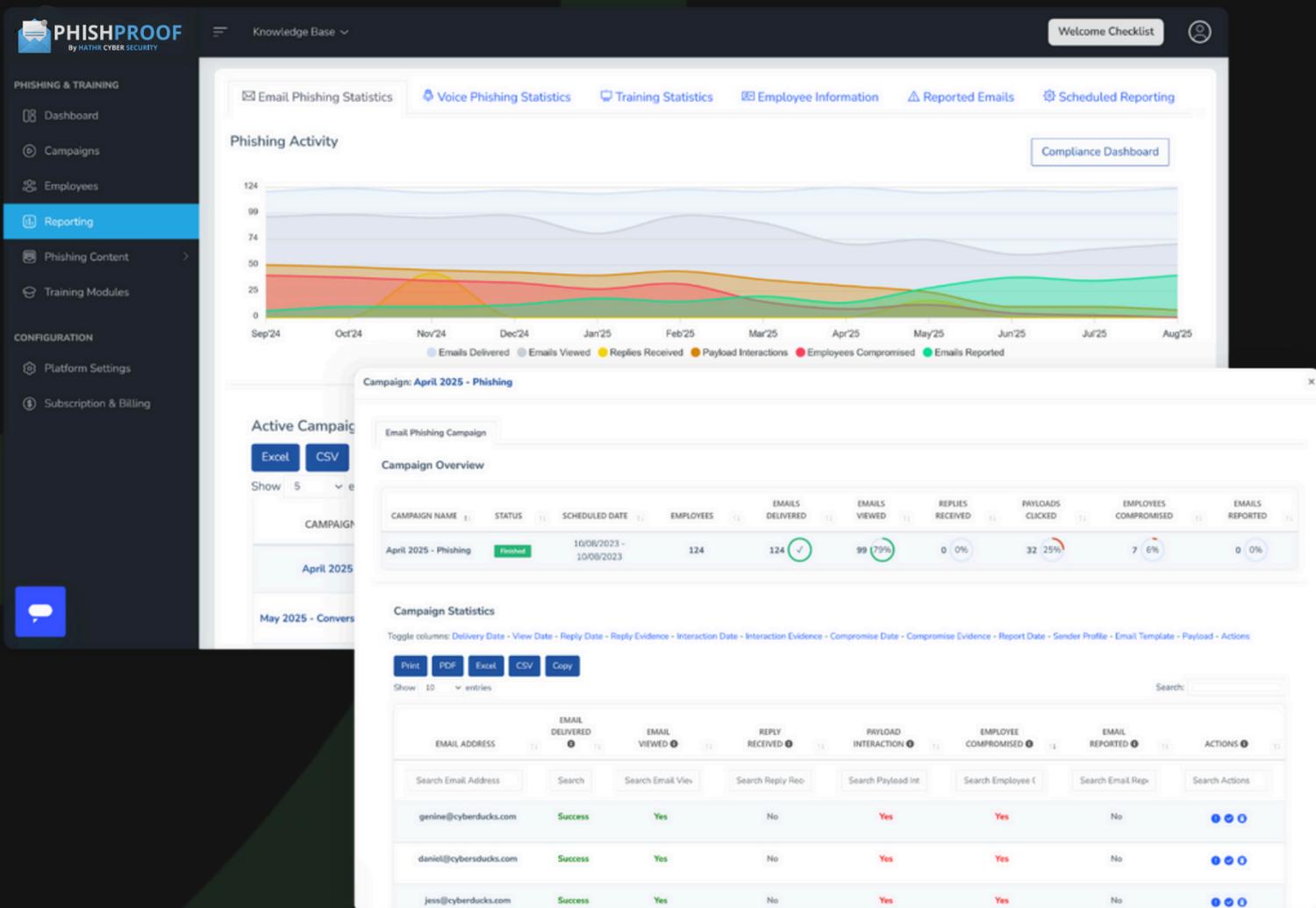
Identify Your
Cybersecurity
Champions



Report Phish Add-On

مقدمة

التصيد الاحتيالي اليوم ليس احتمالاً... بل تهديد يومي حقيقي. في عام 2025، لم يعد التصيد الاحتيالي مجرد ظاهرة عابرة، بل أصبح السلاح الأساسي في ترسانة مجرمي الإنترنت. تقنيات أذكى، ورسائل أكثر إقناعاً، وهجمات شديدة الاستهداف صُممت لاستغلال الموظفين قبل استهداف الأنظمة. هو منخفض التكلفة بالنسبة للمهاجمين، صعب الاكتشاف، وعالي التأثير على الأفراد والمؤسسات على حدٍ سواء. اليوم، التصيد الاحتيالي ليس احتمالاً... بل تهديد يومي واقعي. استجابتنا ليست رد فعل، بل نهج استباقي. من خلال محاكاة واقعية لهجمات التصيد، نحول موظفك من نقطة ضعف محتملة إلى خط الدفاع الأول، ونبني وعياً أمنياً حقيقياً من حيث تبدأ أغلب الهجمات: البريد الوارد.



أكثر من 135 قالب تصيّد مدعوم بالذكاء الاصطناعي

ابق متقدماً على التهديدات المتطورة من خلال مكتبة غنية تضم أكثر من 135 قالب تصيّد واقعي، مدعومة بالذكاء الاصطناعي ويتم تحديثها باستمرار لتعكس أحدث أساليب الهجمات المستخدمة في العالم الحقيقي.

تم تصميم كل قالب ليحاكي حملات التصيّد الحديثة بدقة عالية، مما يتيح محاكاة فعّالة تختبر وعي الموظفين، تكشف مناطق الخطر، وتبني سلوكيات أمنية مستدامة قبل أن يضرب المهاجمون الحقيقيون. ما الذي ستحصل عليه:

- ✓ أكثر من 135 قالب تصيّد حديث وجاهز للاستخدام
- ✓ واقعية معززة بالذكاء الاصطناعي وسيناريوهات تفاعلية متكيفة
- ✓ تحديثات منتظمة متوافقة مع أحدث توجهات التهديدات
- ✓ مصمّم لمحاكاة التصيّد على مستوى المؤسسات (Enterprise-Grade)

The screenshot displays a 'Phishing Email Library' interface with a grid of email templates. Each template includes an interaction rate, a payload type, and a preview of the email content. The templates shown are:

- Gmail-Blocked-Login**: Interaction Rate: 34%, Payload: Website. Preview: 'Sign-in attempt was blocked'.
- QR-Code-Office-365**: Interaction Rate: 12%, Payload: Website. Preview: 'Your organization requires Multi-Factor Authentication'.
- Expense-Claim-Discrepancy**: Interaction Rate: 11%, Payload: Info Request. Preview: 'EXPENSE CLAIM DISCREPANCY INFORMATION REQUEST'.
- Teams-Task-Assignment**: Interaction Rate: 46%, Payload: Website. Preview: 'quarterly Performance Reviews'.
- Spam-Filter-Quarantine**: Interaction Rate: 21%, Payload: Website. Preview: 'notification to inform you that emails addressed to you have been placed in quarantine'.
- DocuSign-Sign-Document**: Interaction Rate: 23%, Payload: Website. Preview: 'DocuSign' and 'Payroll sent you a document to review and sign'.
- Innapropriate-Email-Attach..**: Interaction Rate: 33%, Payload: Website. Preview: 'ge finds you well'.
- HR-Device-Violation**: Interaction Rate: 50%, Payload: Website. Preview: 'ge finds you well'.
- Google-Meeting-Invite**: Interaction Rate: 22%, Payload: Website. Preview: 'Meeting link'.

التصيد التفاعلي المدعوم بالذكاء الاصطناعي التوليدي

تُمكن Phish Proof من تنفيذ هجمات تصيد تفاعلية تحاكي أكثر أساليب التصيد تطورًا، حيث يقوم المهاجم بإنشاء تواصل متبادل ذهابًا وإيابًا لبناء الثقة مع الضحية قبل إرسال حمولة التصيد.

تعتمد هذه الميزة على الذكاء الاصطناعي وتستفيد من استخبارات المصادر المفتوحة (OSINT) لجعل محادثات التصيد واقعية ودقيقة من حيث السياق. كل تفاعل يكون فريدًا ومُخصَّصًا للموظفين، مع قدرة ذكية على الحفاظ على المصداقية عند طرح الأسئلة أو الشك.

يتوفر التصيد التفاعلي عبر كل من البريد الإلكتروني والمكالمات الصوتية، مما يوفر محاكاة شاملة تعكس التهديدات الحقيقية في العالم الواقعي.

 Pamela Turing <pamela[.]turing@ai-attacker[.]com> 10 minutes ago
Subject [Urgent] Expense Claim Discrepancy
Body Hey Mike,
I hope you're doing well! Do you have a moment to go over an expense claim discrepancy?
Best,
Pamela

 Mike Kirby <mike@victim[.]com> 5 minutes ago
Subject Re: [Urgent] Expense Claim Discrepancy
Body Hi Pamela,
Yikes! My apologies in advance if I made a mistake. I'm available now. What do you need?
Thanks,
Mike

 Pamela Turing <pamela[.]turing@ai-attacker[.]com> Received now
Subject Re: [Urgent] Expense Claim Discrepancy
Body Hey Mike,
Before I can go into the details, could you please provide your employment start date and your official job title. This is just a basic security measure we have in place to protect our employees' information.
Best,
Pamela

تعلم تفاعلي مُحفَّز بالألعاب مع شهادات امتثال

اكتشف مكتبتنا المتنامية باستمرار من مقاطع تدريب التوعية الأمنية المجانية، المقدمة عبر وحدات تعلم قصيرة وتفاعلية (Micro-Learning) مدعومة بأسلوب التحفيز بالألعاب (Gamification).

تم تصميم كل درس لتحويل مفاهيم الأمن المعقدة إلى تجارب تعلم بسيطة، جذابة، وقابلة للتطبيق العملي.

وتتضمن كل وحدة اختبارات قصيرة لقياس مستوى الفهم، وعند إتمامها يحصل الموظفون على شهادات امتثال فردية، مما يساعد المؤسسات على إثبات مستوى الوعي الأمني، الجاهزية، والالتزام بالمتطلبات التنظيمية.

الأثر الحقيقي:

- متوسط زمن إكمال الوحدة: 8 دقائق
- أكثر من 50 موضوعاً لبناء عادات أمنية مستدامة
- اختبارات قصيرة للتحقق من استيعاب المعرفة
- شهادات امتثال فردية لكل موظف

The image displays the PhishProof training platform interface. The top section shows a 'New Training Module' button and a 'Training Language' dropdown. Below this is the 'Training Module Library' with a grid of modules including Cyber Security, Phishing, Ransomware, Device Security, Multi-Factor Authentication, and Secure Internet Browsing. Each module card shows its estimated duration and skill level (Beginner or Intermediate). The bottom section shows a 'Learner Dashboard' for 'faisal@hathr.sa' with an average score of 91%, 14 assigned trainings, 7 completed trainings, and a badge score of 0. The dashboard also displays 'Badges Achieved' and two tables: 'Assigned Training' and 'Completed Training'.

Training Module	Estimated Time	Passing Score	Personal Best
Ransomware	7 Minutes	>= 70%	Not Attempted
Cyber-Security	7 Minutes	>= 70%	Not Attempted

Training Module	Personal Best	Completion Date	Certificate of Completion
Vishing	100%	يناير 04, 2026	Download Certificate
Remote-Working	100%	سبتمبر 11, 2025	Download Certificate
NCA	100%	يونيو 07, 2025	Download Certificate

الإمتثال والمعايير

الضوابط التي يمكن الامتثال بها
تساعدك منصة فث بروف على الامتثال للمعايير والضوابط
الوطنية والعالمية



Aramco CCC

ضوابط أمن المعلومات لشركة أرامكو

تدعم المنصة متطلبات برنامج CCC عبر أدوات توعية وتقييم سلوكي للموظفين، وتقديم تقارير تساعد على الامتثال للضوابط الأمنية الخاصة بشركات الطاقة والصناعة.



SAMA

إطار الأمن السيبراني للبنك المركزي السعودي

تتماشى المنصة مع متطلبات SAMA من خلال توفير تدريب دوري للموظفين، ومحاكاة لهجمات التصيد لقياس مدى الجاهزية والاستجابة للتهديدات.



ISO 27001

معايير أمن المعلومات العالمية

تساهم المنصة في تحقيق متطلبات معيار ISO 27001 عبر توفير أدوات للتوعية، وإجراءات لتقليل المخاطر البشرية وتحزيز الأمن الداخلي للمؤسسة.



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

NCA

الضوابط الأساسية للأمن السيبراني

تدعم المنصة متطلبات الهيئة الوطنية للأمن السيبراني من خلال رفع الوعي الأمني، واختبار الجاهزية ضد هجمات التصيد، مما يعزز الامتثال لضوابط التدريب والتوعية المستمرة.

أطر امتثال إضافية مدعومة

تدعم Phish Proof أيضًا الامتثال لعدد من الأطر والمعايير الإضافية، بما في ذلك PCI DSS، وإطار الأمن السيبراني لـ NIST، واللائحة العامة لحماية البيانات (GDPR)، وغيرها من المتطلبات الخاصة بمختلف القطاعات.

Platform Hathr

Your Security Choice in Your
Digital World



Contact us:

 29th floor, Al-Alya Towers, Tower B
intersection of Al Tahlia and Alya St
Riyadh, KSA

 www.hathr.sa  +966 552 300 849
 info@hathr.sa  +966 112 978 246

 [hathr_sa](#)
 [hathrr_sa](#)

 Home