KnowBe4
Human error. Conquered.

Buyer's Guide：採用する上での手引き

セキュリティ意識向上トレーニング/フィッシングシミュレーション・分析プラットフォーム

Buyer's Guide（採用する上での手引き）:

セキュリティ意識向上トレーニング／フィッシングシミュレーション・分析プラットフォーム

KnowBe4はセキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。このガイドは、KnowBe4プラットフォームを購入する上でのガイドとして、作成されています。

課題認識
ソーシャルエンジニアリングは、あらゆる組織に最も恐れられているセキュリティ脅威です。巧妙化するサイバー攻撃の増加は危惧すべき問題であり、この5年間で特に急増しています。その中でも企業や組織・団体の従業員は、ITセキュリティ内での標的になりやすい、攻撃しやすい"弱点"であると言われています。

概要
KnowBe4はセキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。2019年9月現在、2万8千社を超える企業や組織がKnowBe4を採用しています。KnowBe4は、Kevin Mitnick（ケビン・ミトニック）の30年を超える実体験とハッカー視点の知見をベースに、ソーシャルエンジニアリング攻撃、スピアフィッシング攻撃やランサムウェア攻撃などの緊急ITセキュリティ課題への効果的な対応を可能にしています。KnowBe4は、インタラクティブな教材モジュール、ビデオコンテンツ、ゲーム、ポスター、ニュースレターなどを含む世界最大のセキュリティ意識向上トレーニングコンテンツライブラリーを提供しています。

世界が認めるユーザーフレンドリーな新しい形態のセキュリティ意識向上トレーニングプログラムをもとに、KnowBe4はデジタル時代に適合したセルフサービスのセキュリティトレーニングと事前・事後のフィッシングセキュリティテストを提供しています。事前・事後のテストによって、フィッシングに対してどれだけ脆弱であるかをPPP（Phishing Prone Percentage:フィッシング詐偽ヒット率）として"見える化"し、セキュリティトレーニングの効果を測定しています。また、また、KnowBe4のフィッシングテストは、絶えずランダムに模擬フィッシング攻撃を行い、それに引っかかった場合には各人に合った対策とトレーニングを提供します。

KnowBe4のプラットフォームによって、すべての個人・組織にとっての最適なセキュリティ意識向上トレーニングプログラムを組み立てることができます。

"これまでテクノロジーソリューションで解決しようとしてきたが、ソーシャルエンジニアリングはファイアウォールを含むすべてのセキュリティテクノロジーをすり抜けている。テクノロジーは重要であるが、人間とプロセスに目を向けなければならない。ソーシャルエンジニアリングは、さまざまな影響戦術（Influence Tactics）を駆使するハッキングの1つの形態なのである。"

– Kevin Mitnick（ケビン・ミトニック）

KnowBe4トレーニングのもう1つの特徴として、月次に発行される“Hints & Tips（ヒントと勘どころ）”で模擬フィッシング演習を補完するというオプションを用意しています。これによって、さまざまなソーシャルエンジニアリングの手口に関する受講者のセキュリティ知識を随時アップデートしていくことができます。 また、セキュリティ管理者には、トレーニングROIを最大化すると同時にセキュリティコンプライアンスのステータスを常にトラッキングすることが求められます。セキュリティ管理者はKnowBe4プラットフォームを通して、この知見を獲得することができます。

KnowBe4プラットフォームは"by admins for admins（アドミンによるアドミンのために"というコンセプトとのもとに作成され、直感的なナビゲーションと使い易いユーザーインターフェイスによって設計されています。 このインフラは極めてスケーラブルで、10万人を超えるエンドユーザーを容易にサポートすることができます。 自社のLMS（学習管理システム：Learning Management System）を持っている企業や組織のために、KnowBe4セキュリティ意識向上トレーニングはCORMやAICCなどの業界標準の形式で提供することができます。また、KnowBe4のシステムはシングルサインオンをサポートしており、ユーザーはSAML（Security Assertion Markup Language）を使ってその都度くり返してログインする必要がありません。

受講の前提条件
トレーニングプログラム受講のための条件はありません。（受講にはサウンド機能付きPCが必要ですが、主なトレーニングモジュールは米国障害者法に準拠するすべての環境をサポートするように英文字幕付きで提供されています。

受講対象者
コンピューター、メール、インターネットを社内外で使用する企業または組織・団体の全従業員。

トレーニングアクセスレベル
サブスクリプションレベルに応じて、3つのトレーニングアクセスレベル：I、II、またはIIIを提供されます。KnowBe4のコンテンツライブラリーは、常時更新されています。すべてのコンテンツのリアルタイムのビューを視聴したい場合は、サインアップして、KnowBe4 ModStore Training Previewをアクセスしてください。

このコンテンツライブラリーを容易に提供するために、KnowBe4はModule Store'を用意しています。ModStoreを利用して、コンテンツを検索・ブラウズして、プレビューしたり、KnowBe4管理者アカウントへトレーニングモジュールを移動することもできます。

トレーニングモジュール

Kevin Mitnickセキュリティ意識向上トレーニング

トレーニングアクセスレベル I に含まれている

Kevin Mitnick セキュリティ意識向上トレーニング(45分)
3つの実際のシナリオを使って、ハッカーがコンピューターシステムへ侵入するのに使用する最も一般的な戦略と技法を紹介します。 次に、Kevin Mitnickがいかにしてハッカーが目的を達成するのに仕掛ける裏工作について解説します。ここから、レッドフラグとなるメールの7つの領域について学習します。Danger Zone演習では、これまで学習してきたことを適用して、6つの実際のソーシャルエンジニアリング攻撃に対処するためにごく一般的なコンピューターユーザーJake Saundersをヘルプしてもらいます。

Kevin Mitnick セキュリティ意識向上トレーニング(25分)

Kevin Mitnick セキュリティ意識向上トレーニング(15分)
45分のフルバージョンの短縮版で、マネジメント層向けになっています。スパム、フィッシング、スピアフィッシング、ファイル内に仕込まれたマルウェアおよびAPT（Advanced Persistent Threat）攻撃のメカニズムを解説します。（26カ国語対応）

KnowBe4トレーニングモジュール

トレーニングアクセスレベルII（Gold & Platinum）に含まれている

Common Threats, Part 1 - Miranda's Story
ハッカーが人を欺す際に使う戦略と技法について学習します。ここでは、3つの実際のシナリオを示し、これらの共通な脅威がどのようにして仕掛けられるかを解説します。各シナリオの終わりに、Kevin Mitnickがどのような裏工作が繰り広げられているか、各ハッキングのタイプがどのようにして成し遂げられているかを解説します。

Common Threats, Part 2 - Kyle's Story
3つの実際のシナリオ（ランサムウェア攻撃、スピアフィッシング攻撃、スナップチャット攻撃）と、その裏工作、各ハッキングのタイプがどのようにして成し遂げられているかをKyle Montgomery氏が暴露します。

PCI Compliance（短縮版）
クレジットカード詐欺の実例を使って、PCIに準拠することで、いかにクレジットカード詐欺から組織を守ることができるかを示します。このコースは、クレジットカードを取り扱っている部門の担当者を対象としています。 特に、クレジットカード決済の責任者、CFO、コントローラー、担当マネージャー、担当IT要員は本コースを受講することを薦めます。

Ransomware
KnowBe4のサイバーセキュリティタスクフォースの責任者であるSergeant Vasquezが、ランサムウェアとは何かを紐解き、ランサムウェアがいかに機能するかを示した上で、いかにしてこの潜在的な脅威から企業や組織を守るかを解説します。また、ハッカーが支払いまでの間、企業や組織のコンピューターシステムを支配するための攻撃方法についても説明します。

Ransomware For Hospitals Training（7分）
病院は昨今、サーバー攻撃者の標的とされています。サーバー攻撃者は、病院のネットワークに侵入して、暗号化ランサムウェアによって患者ファイルをロックして、病院関係者からのデータアクセスを不可にしてしまいます。 病院で働くすべての人を対象として、ランサムウェアの基礎、メールセキュリティ、このような高価な代償を強いる攻撃を防ぐために注意すべきレッドフラグについて解説します。

Criminal Justice Information Services Security Series
レベル1からレベル4までの4つのコースで構成されており、保護されている刑事司法情報へのアクセスに関してFBI/CJIS要件を満たすように受講者を指導することを目的としています。

Privileged User Security Series
特権アクセス、セキュアデータベース運用管理、セキュアWindows運用管理およびセキュアLinux運用管理をカバーします。

GLBA Compliance Course (金融機関向け)
金融機関の従業員を対象としており、非公開個人情報（Non-Public Personal Information）の概念、顧客個人情報保護のためのベストプラクティスと非公開個人情報および非個人情報保護における金融機関従業員の役割について解説します。

Handling Sensitive Information（15分）
企業・組織の従業員全員を対象としています。自社機密情報のほか、会社または組織の従業員全員を対象としています。自社機密情報のほか、個人を特定できる情報 (PII = Personally Identifiable Information)、保護対象保健情報（PHI：protected health information）、クレジットカードデータ（PCI DSS）、米政府調達管理重要情報（CUI：Controlled Unclassified Information）などの機密情報を安全に取り扱うことの重要性について学びます。

Mobile Device Security（15分）
企業・組織の従業員全員を対象としています。モバイルデバイスセキュリティの重要性モバイルセキュリティ脅威が犯された場合のリスクを学習し、日々の業務にその知識を適用できるようにすることを目的としています。

Safe Web Browsing
Webについての現状と危険をいかに防御するか、安全なWebブラウジングのために“すべきこと”と”してはならないこと”について学習します。

Social Engineering Red Flags
ハッキングされないための注意すべきメールの7つのポイントを解説します。その後に、7つの実例を示し、それぞれのレッドフラグをどのようにして見極めるかを考えます。

The Danger Zone（10分）
実際のソーシャルエンジニアリング攻撃の脅威について、6つの例を通して、ごく一般的なコンピューターユーザーJake Saundersが正しい判断ができるようガイドします。

Your Role, Internet Security and You
ハッカーが会社組織のアンチウィルスソフトウェアやスパムフィルターをすり抜け、受信ボックスへ侵入してくるという脅威の現状を展望して、ユーザーを欺す最も一般的な方法を紹介します。

KnowBe4トレーニングマイクロモジュール

トレーニングアクセスレベル II（Gold & Platinum）に含まれている

Credit Card Security (Part 1)
Credit Card Security (Part 2)
Danger Zone Exercise
Don't Be Dave Email Spoofing
Handling Sensitive Information Securely (Part 1)
Handling Sensitive Information Securely (Part 2)
Ransomware
Safe Web Browsing
Social Engineering
Social Media Best Practices
Strong Passwords
USB Attack

エグゼクティブシリーズマイクロモジュール

CEO Fraud
Decision-Maker Email Threats
Mobile Device Security
Ransomware and Bitcoin
Remote and Travel WiFi Dangers
Safe Web Browsing With Corporate Devices Secure Destruction of Sensitive Information Securely Working From Home
Social Engineering the Executive
Social Media Precautions for Executives

キャプテン意識向上ビデオシリーズ

Be a Human Firewall
Conquer Internet Safety for Kids
Securing Your Mobile Devices Triumph over the Reuse of Passwords
Understanding GDPR
Securely Working from Home
Be Vigilant with USB Drives
Outwit Dumpster Divers Travel Securely
Handling Printouts Understanding
Data Breaches Safeguard
Social Media Protect Your Web Browser
Guardians of Sensitive Information
Vanquish Malicious Attachments
Outwit Social Engineering
Conquer Open WiFi Foil Phishing

KnowBe4ビデオモジュール

Kevin Mitnick - Two-Factor Authentication Attack
KnowBe4 Pretexting - Fake IT "Password Break-In"
KnowBe4 Pretexting - Tech Support "Social Engineering"
KnowBe4 Pretexting - Two-Factor Authentication Attack
KnowBe4 Pretexting - A Fake IT Attack
SIM Swapping - Call Center
SIM Swapping - Mobile End Users
SIM Swapping - Mobile Retail Locations

El Pescadorトレーニングモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

Data Collection Data Collection Quiz
C-Level Phishing
Finance Sector Phishing
Lei Geral de Proteção de Dados
Phishing: Why Should We Care
Phishing: The Major Cause of Information Leakage Relationship Trust
The Threat May Be Closer Than You Think

Security Awareness Companyコンテンツライブラリー

トレーニングアクセスレベル IIII（Diamond）に含まれている

サイバーセキュリティ意識向上インタラクティブトレーニングモジュール

Call Center & Help Desk Awareness
Computer Security & Data Protection
Data Classification
Developing an Incident Response Plan
Empowering Your Employees for Better
Security Executive Awareness Leadership
How to be a Human Firewall
Identity Theft and Data Breaches
Insider Threats for Executives and Managers
Malware
Mobile Security Basics
Non-technical Security Basics
OWASP Top 10
PCI DSS Retail Store Experience
Password Security
Phishing Andrew's Inbox
Phishing Fundamentals
Privacy Basics
Ransomware
Restricted Privileged Access
Secure Online Behavior
Social Engineering & Phishing for Executives
Social Engineering Basics
Security Awareness Fundamentals
Security Awareness Fundamentals for New Hires
Understanding and Mitigating Security Risks for Executives
Understanding and Protecting PII
Workforce Safety & Security Awareness
Workplace Violence and Safety

サイバーセキュリティ意識向上コンプライアンスモジュール

FERC/NERC for End Users
FERC/NERC for Managers and
Executives FERPA (Education)
FFIEC (Financial Compliance)
GLBA (Finance)
HIPAA (Healthcare)
PCI-DSS (Retail Compliance)
Sarbanes-Oxley (Accounting)

100種を超えるサイバーセキュリティニュースレター＆ドキュメント

10種を超えるサイバーセキュリティ意識向上ゲーム

150種を超えるサイバーセキュリティ意識向上ポスター＆イラスト

サイバーセキュリティ意識向上トレーニングビデオ（2分～5分）

10 ways to avoid phishing scams
10 ways to keep PII private
10 ways to stay safe on social media
A Day of Bad Passwords
Backup
Being a Human Firewall Beyond
Phishing Catching malware
Cyber Crime Starts with You Dangers of USBs
Data Breach Overview Data Breaches and You
Data Classification Overview
Data Loss and Insiders
Definition of Social Engineering
Dumpster Diving
Email Spoofing
Executives Mitigating Insider Threats
Hide your passwords
Incident Response 101
Introduction to Ransomware
Introduction to the cloud
Is Free Wifi Really Free
Jasper the Disaster in Travel Security Awareness
Jasper the Disaster in Workplace Physical
Security Jasper the Disaster in Workplace Policy
Low-Tech Hacks to Steal Your ID
Mouse Overs
NIST Password Guidelines
Non-Technical Security Skills
Non-Technical and Physical security tips and tricks
PII and Compliance
Phishing Contest Winner
Phishing From Facebook
Phishing From Netflix
Phishing From Your Bank
Phishing in Action
Pretexting: (Fake Fraud Protection)
Pretexting: (Fake Help Desk)
Pretexting: Fake Employee to Help Desk
Pretexting: Fake Executive to I.T.
Pretexting: From Fake Credit Card
Company Pretexting: From Fake I.T.
Privacy Vs. Security
Protecting Data
Road Warriors
Safe Surfing 1: HTTP vs HTTPS & Online Authentication
Security Myths Busted
Social Media
Social Media Data Mining
Social Networking Do's and Don'ts
The CIA Triad
The Domains Triad
The Human Firewall's Top Concerns in All Three Domains
The Many Lives Triad
The Many Lives of PII
Understanding Encryption
Welcome to Security Awareness Training
Welcome to Security Awareness Training - Animated
What Are APTs
What Does a Social Engineer Look Like?
What is I.D. Theft
What is PII?
Why Executives Need Awareness Training
Why Security Awareness?
Your Security Awareness Journey

Popcornトレーニングコンテンツ

トレーニングアクセスレベル III (Diamond) に含まれている

Popcornトレーニングモジュール

Something Phishyシリーズビデオ＆クイズ（アニメーション）
Something Phishy Series Introduction
Breaking the Barrier
Cloudy With A Chance of Phish
Dicey Devicey
Freaky Leaky
Mobile Mayhem
Pass The Password
Phishious Malicious
Social Media Fever

Cyber Heroesシリーズビデオ＆クイズ（ライブアクション）
Cyber Heroes Introduction
Breaking the Barrier
CEO Scams
Cloudy with a Chance of Phish
Dicey Devicey
Don't Take the Bait
Freaky Leaky
Internet Threats
Mobile Mayhem
Pass the Password
Passwords
Social Media Fever

Privacyシリーズビデオ＆クイズ（ライブアクション）
General Data Protection Regulation (GDPR) – User Rights
Privacy Principles - Handling Personal Information at Work
Identity Theft - Protect Your Personal Information
Personal Information - Currency of the 21st Century
Protecting Personal Information - Security & Safeguards

Standups 4 Securityシリーズ:（ライブアクション）
Cybercrime　Promo
A Goliath Hack
Behind the Scam with Loyiso Madinga
Open Secrets - A Password Exhibition
Spearphishing - Catching the Big Phish
Don't Trust Anybody - CEO Scam
Social Media Oversharing
The Dark Web Pop-up

Security Momentショートクリップビデオ&クイズ（モーショングラフィック）
Hacking Emotions
Privileged User Access Management
Ransomware
Social Engineering 101
Spot the Bad Attachment
Spot the Bad Link
The Big Phish

Building Secure Softwareシリーズ
Ep 1 - Very Early and Often
Ep 2 - Leverage Security Frameworks and Libraries
Ep 3 - Secure Database Access

Secure Coding 6 Module Course for Developers ビデオ＆クイズ（アニメーション＆モーショングラフィック）
Secure Transactions and Secure Deployments
Authentication and Authorization
Data Security
Injection Attacks and How to Avoid Them
Introduction to Web Application Security
Secure Session Management

Complianceシリーズ（アニメーション）
Acceptable Use Policy
Business Continuity Management
Conflict of Interest Policy
Consumer Protection Act (RSA)
PCI DSS for Corporate Office
PCI DSS for Merchants
PCI DSS for Retail Stores
SupaPopi (RSA)
Treating Customers Fairly (RSA)

Cyber Essentialsシリーズ
Information Security 101
Cryptocoin Security
Cyberbullying

85種のPopcornトレーニングプロモーションビデオおよびセキュリティドキュメント

Securable.ioビデオ

トレーニングアクセスレベル III (Diamond) に含まれている

FISMA- Federal Information Security Management Act
Intro to Phishing
LinkedIn Security
Monitoring Facebook Services
Protect Your Kids Online
Public WiFi Safety
Ransomware Attacks
Traveling Abroad
Twitter Security
USB Safety

ThinkHRトレーニングモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

A Manager's Guide to Discipline and Documentation
A Manager's Guide to Diversity, Inclusion and Accommodation
Active Shooter
Bullying and Hazing on Campus
Bullying and Violence in the Workplace
Campus Security Obligations Under Federal Law
EEO and Lawful Hiring
FERPA for Higher Education
FMLA Leave and More: An Overview of Legally Protected Leave HIPAA - Privacy Essentials
HIPAA - Privacy Rules for Business Associates
HIPAA - Security Rules for Business Associates
HIPAA for Non-Medical Employees
Optimizing Your Work/Life Balance: Maintaining Your Life Balance
Optimizing Your Work/Life Balance: Taking Control of Your Stress
Pandemic Flu Awareness
Preventing Harassment in the Global Workplace - Employee Edition
Preventing Harassment in the Global Workplace - Manager Edition
Promoting a Substance-Free Workplace
Rightful Employment Termination
Sexual Harassment Prevention for Employees
Title IX for Higher Education
Wage and Hour Awareness for Managers
Workplace Harassment Prevention for Employees, State of New York
Workplace Harassment Prevention for Managers, State of New York
Workplace Harassment Prevention for Employees (Title VII)
Workplace Harassment Prevention for Managers - Multi-State Edition, V3.0
Workplace Management: Employment Laws and Regulations

exploqiiビデオ

トレーニングアクセスレベル III (Diamond) に含まれている

Anti-Trust 1 - Basic Regulations & Risks
Anti-Trust 2 - Industry Events
Basic Rules of Secure Communication
Bluetooth & WiFi
Business Partner Compliance
CEO Fraud - Fake President
Clean Desk Policy
Cloud Services
Code of Conduct
Compliance Checklist
Compliance Management System
Conflict of Interest
Corruption
Crisis Management
Data Protection
Disinformation
EU GDPR
Export Control
Fairness & Respect in the Workplace
Gifts, Hospitality & Anti-Bribery
IT Security in the Workplace Identity Theft
Industrial Espionage
Information Classification
Information Security @ Mobile Devices
Information Security @ Remote Workplaces
Information Security @ Social Media
Insider Threat
Internal Investigations
Know-How Security
Microphone, Camera & Selfies
Money Laundering
Payment Fraud
Phishing Attacks on Companies
Phone Scam
Price Rigging
Proxy Servers & Data Privacy
Ransomware Micro-module
Secure Passwords
Security-Oriented Personnel Selection
Sexual Harassment
Social Engineering Micro-module
Social Media Guidelines
Threat Management
Travel Security
USB Attacks
Visitor Management
Whistleblower

Teach Privacyトレーニングモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

California Health Privacy
Canadian Anti-Spam Legislation (CASL)
Data Breach
Data Disposal
Data Retention
Encryption
FERPA (K-12)
General Data Protection Regulation (GDPR)
Global Privacy and Data Protection
Secure Workspaces Game The Privacy Act

Syntrioトレーニングモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

Avoiding Antitrust Violations
Avoiding Conflicts of Interest
Avoiding Insider Trading
Risk Back Injury Prevention
California Workplace Harassment Prevention for Employees
California Workplace Harassment Prevention for Managers
Connecticut Sexual Harassment for Managers
Controlling Workplace Exposure to Bloodborne Pathogens
Delaware Sexual Harassment for Employees
Delaware Sexual Harassment for Managers
Disability Discrimination and Accommodation
Employee Privacy: Balancing a Manager's Right to Know
ErgoNet: A Training Guide for Healthy Office Workers
Ethics and Code of Conduct
FCPA Anti-Corruption and Bribery
Global Anti-Corruption
Maine Sexual Harassment for Employees
Maine Sexual Harassment for Managers
New York Preventing Sexual Harassment for Employees
New York Preventing Sexual Harassment for Managers
Personal Protective Equipment: A General Awareness
Preventing Unlawful Retaliation in the Workplace
Slip, Trip, and Fall Prevention
Understanding the Family and Medical Leave Act
Valuing Diversity for Managers

Twist & Shoutビデオモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

Restricted Intelligenceシリーズ *-Season 1*
Episode 1:The Test (passwords and passes)
Episode 2: Browsing (safe surfing)
Episode 3: A Cry for Help (email hacking and phishing)
Episode 4: The Journey (portable storage devices)
Episode 5: The Leak (beware what you share
Episode 6: The Lesson (mobile devices)

Restricted Intelligence Privacyエディション *-Season 2*
Episode 1: Nothing To Do With Me (What Is PI?)
Episode 2: Nobody Reads That Stuff (Privacy by Design)
Episode 3: Once More Unto the Breach (Retention & Disposal)
Episode 4: The Heart of the Matter (Purpose & Minimisation)
Episode 5: Mr. Cellophane (Transparency)
Episode 6: Partners (Third Party Partners)
Bonus - GDPR Intro (GDPR is Coming)

The Inside Manシリーズ *-Season 1*
Episode 1: The New Guy (Social Engineering)
Episode 2: Social Hour (Social Media)
Episode 3: On Our Side (Phishing Attacks)
Episode 4: Surprise (Document Disposal)
Episode 5: Takeaways (Clear Desktop Policy)
Episode 6: Masquerade (Cloud Services)
Episode 7: Buying Time (Passwords)
Episode 8: Taken (Ransomware)
Episode 9: Where The Wild Things Are (Travel)
Episode 10: Keep Your Friends Close (App security and permissions)
Episode 11: The Sound Of Trumpets (External Devices)
Episode 12: Checkmate (Insider Threats)

40種のTwist & Shoutプロモーションポスター＆グラフィック

Canada Privacyトレーニングモジュール

トレーニングアクセスレベル III (Diamond) に含まれている

Canadian Private Sector Privacy

KnowBe4のコンテンツライブラリーは、常時更新されています。トレーニングコンテンツの最新状態については、下記のKnowBe4のWebページを参照してください。

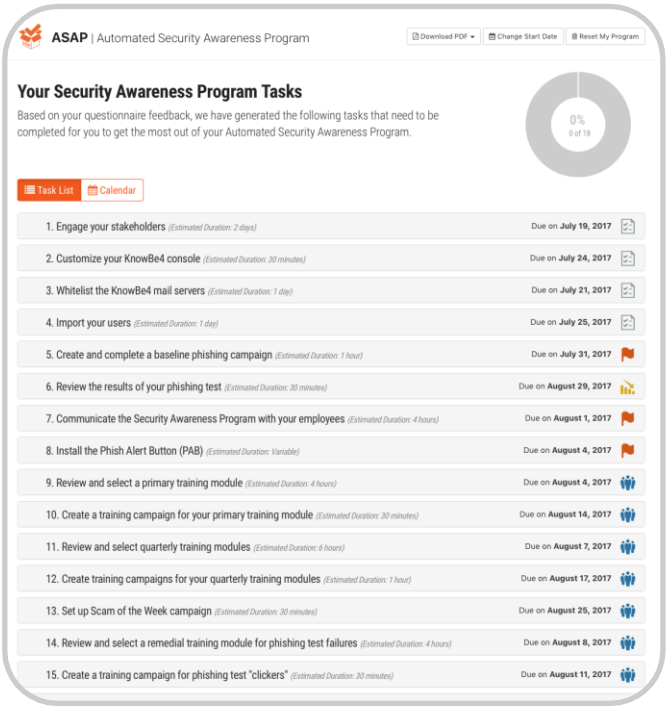
www.knowbe4.com/knowbe4-training-modules-overview/

Automated Security Awareness Program（ASAP）-
自動化セキュリティ意識向上プログラム

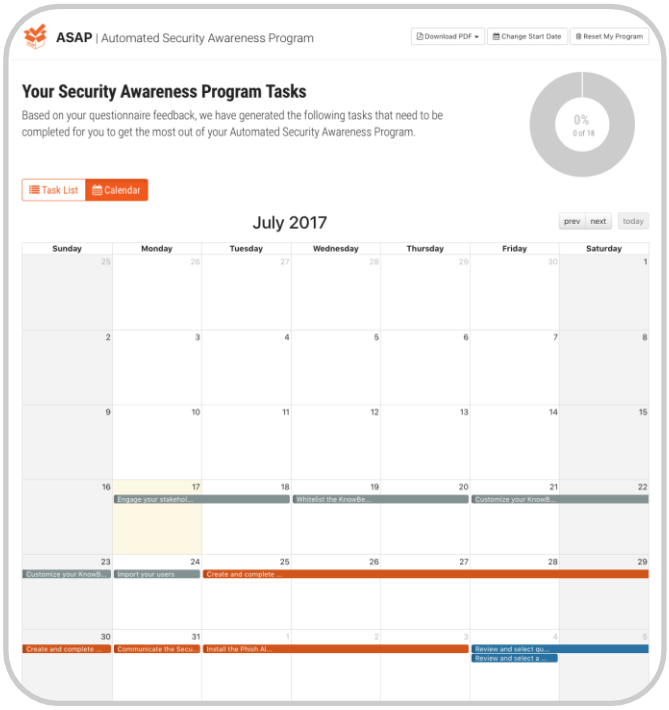
多くのIT担当者は、自社の組織で機能する最適なセキュリティ意識向上プログラムに取り組む際に何から着手すべきかを明確に理解していません。

KnowBe4は、自動化されたツール「Automated Security Awareness Program (ASAP)」を用意することで、IT担当者を支援します。ASAPは、IT担当者向けのツールで、自社組織のためにカスタマイズされたセキュリティ意識向上プログラムを自動で構築します。構築のための必要なステップを示し、自社にとっての最適なトレーニングプログラムが数分で作成することを可能にします。

この作成のプロセスは極めて簡単です。目標および組織についての15-25の設問に回答するだけで、プログラムが自動的に組み立てられます。　構成されるプログラムタスクは、ベストプラクティスにベースに、いかに自社のセキュリティ意識向上目標を達成するかが反映されています。



ASAPは、アクショナブルタスク、ヒント／助言、コースコンテンツへの推奨提案、管理用カレンダーを用意しています。　さらに、カスタムプログラムは、KnowBe4コンソール内ですべて管理できるように設計されています。また、全プログラムの詳細バージョンとエグゼクティブサマリーバージョンをPDF形式でエクスポートする機能を備えています。コンプライアンス要件やマネジメントへの報告書として利用可能です。

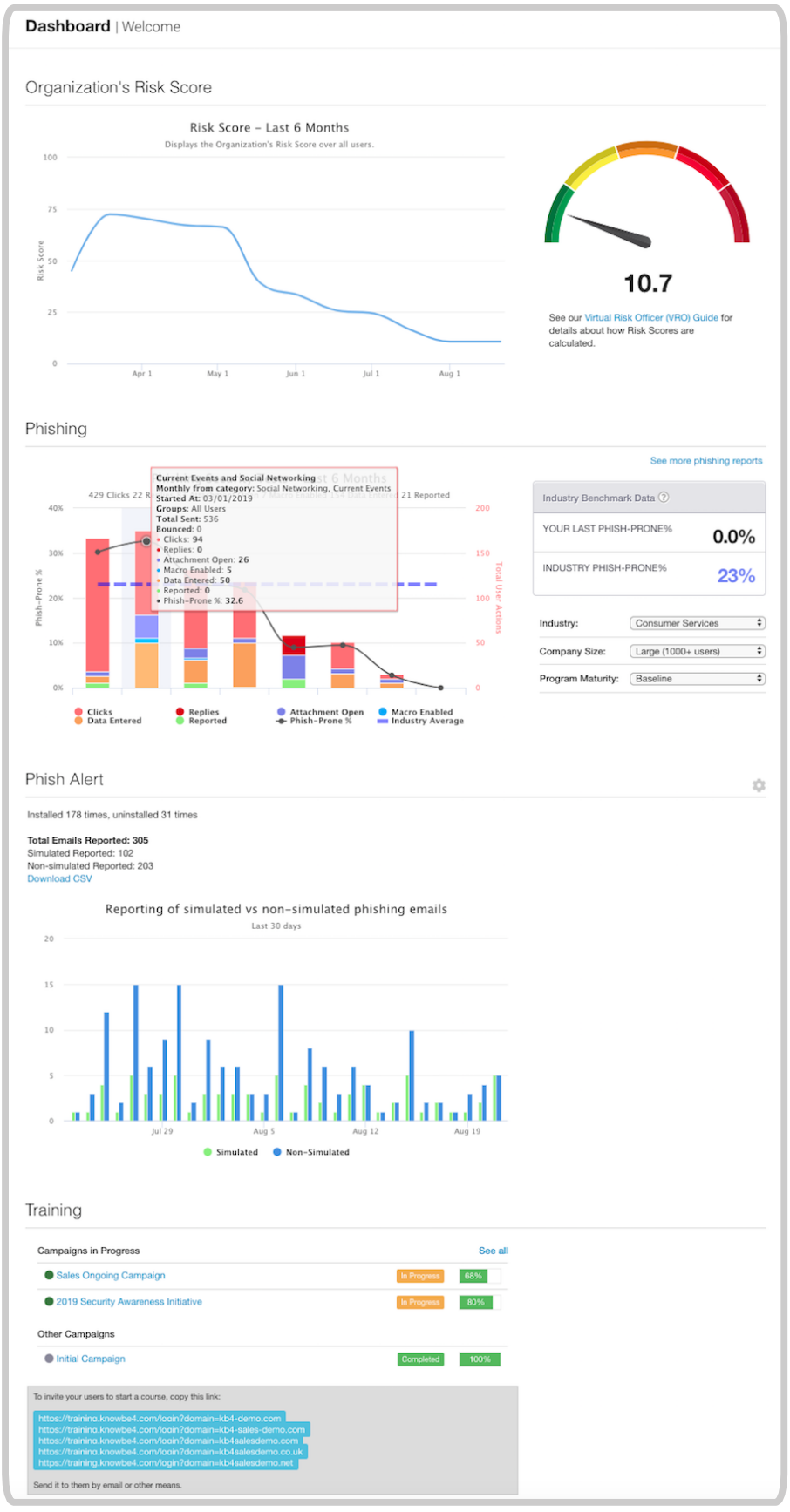


プランニングから実施までを網羅したカレンダービューも提供しています。

ダッシュボード

フィッシング／トレーニングダッシュボードは、エンドユーザーの状況の俯瞰に加えて、業界ベンチマーキングに基づく業界横断の同業他社との比較を表示します。

フィッシング／トレーニングダッシュボード表示例



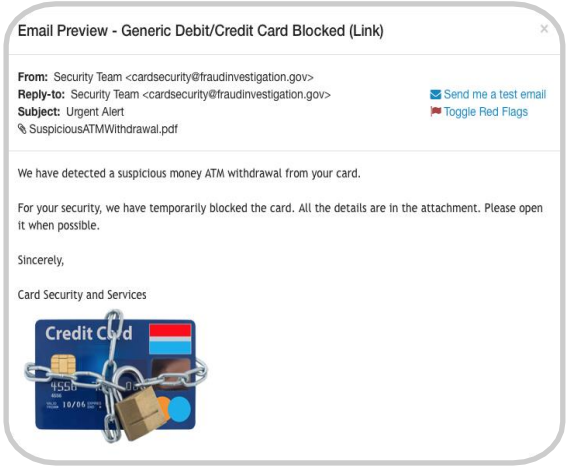
模擬フィッシングテスト

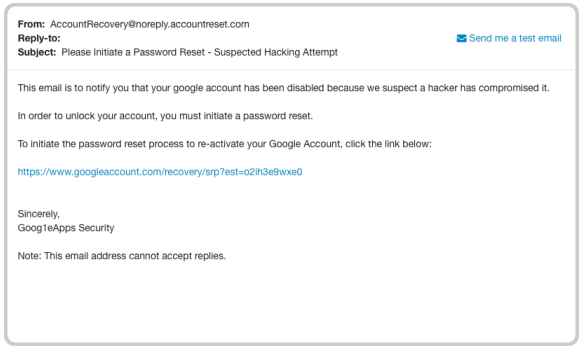
フィッシングプラットフォーム

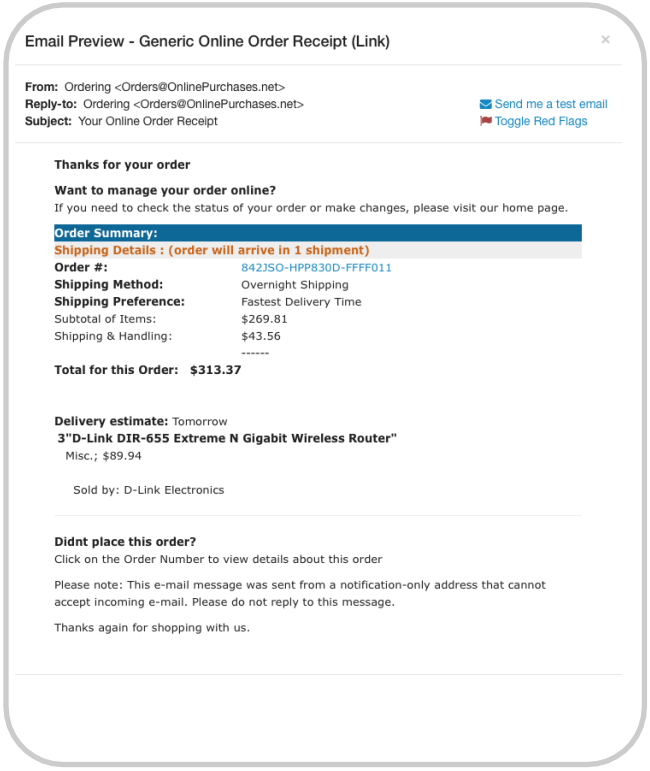
サブスクリプション期間中にユーザーに対して模擬フィッシングセキュリティテスト（Phishing Security Test：PST）を何回でも無制限にスケジュールして、送信することができます。

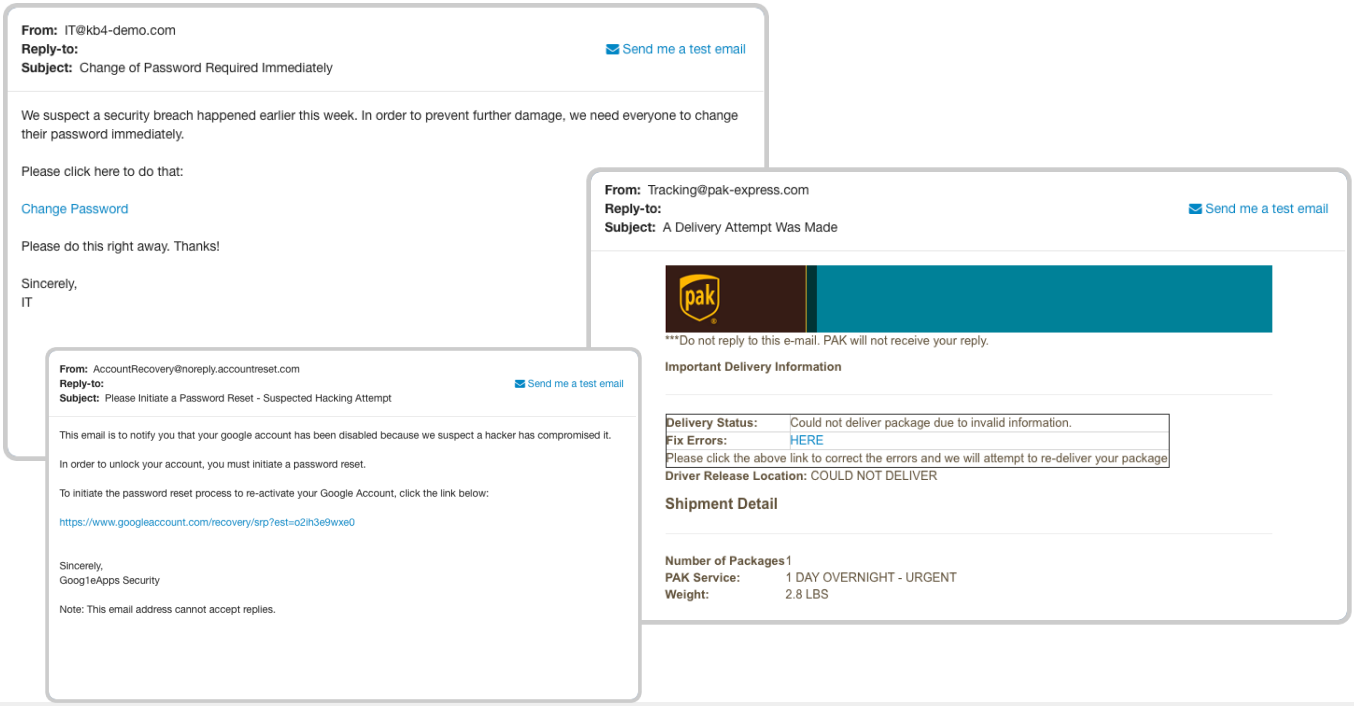
KnowBe4の豊富なカテゴリー（バンキング、ソーシャルメディア、IT、官公庁、オンラインサービス、開催中イベント、ヘルスケアなど）のテンプレートライブラリーを用いることで、30分以内で設定して、本稼働を開始することができます。また、多数のKnowBe4顧客とテンプレートを交換する場として、コミュニティセクションが用意されています。

システムフィッシングテンプレート例





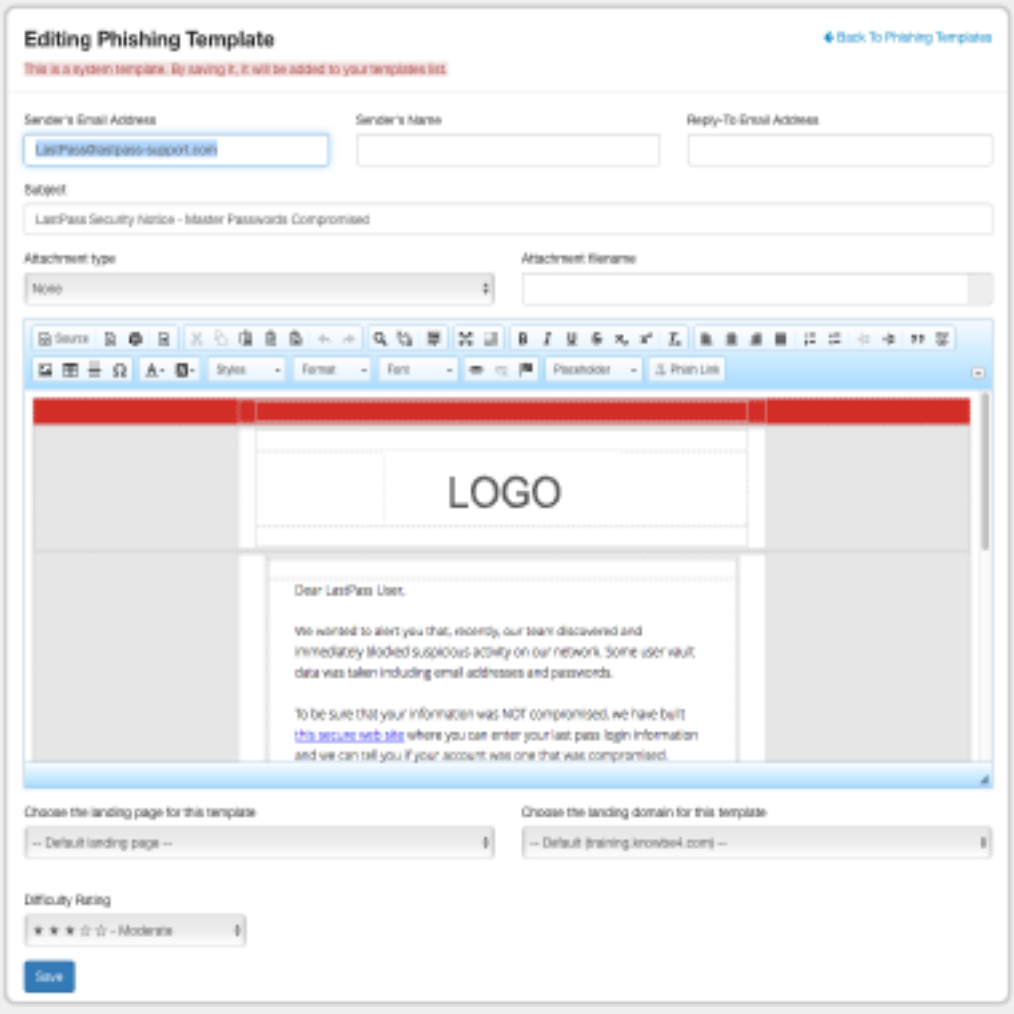




フィッシングテンプレートカスタマイゼーション

システムテンプレートのカスタマイズに加えて、模擬添付およびマクロを含める機能も利用することができます。

カスタムフィッシングテンプレートの作成例

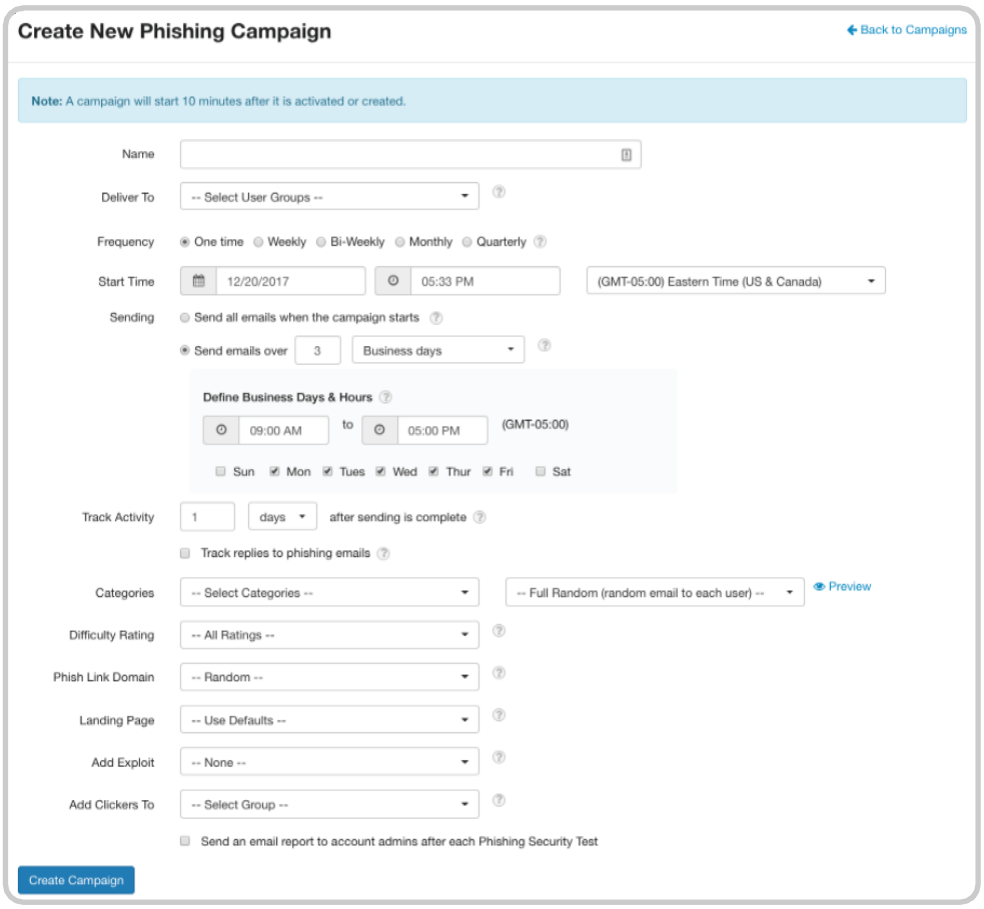


ランディングページの例

フィッシングセキュリティテストのスケジューリング

すべてが実際に発生したフィッシング攻撃を疑似して作ればよいように設計されているため、誰でも簡単にスケジュールを作成できます。

フィッシングキャンペーンの作成例

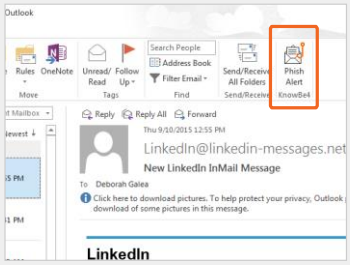


Phish Alert（フィッシュアラート）ボタン
ワンクリックでフィッシング攻撃を管理者へ報告

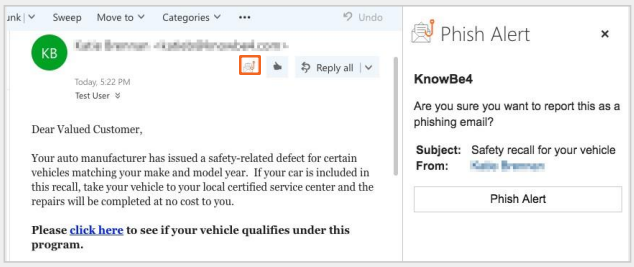
各種メーラーのアドイン機能としてPhish Alertボタンを用意していて、不審メールを安全に、かつワンクリックで、セキュリティ担当者へ転送できます。

- 模擬フィッシングセキュリティテストに対してユーザーがPhish Alertボタンをクリックすれば、このユーザーのアクションが報告されます。
- ユーザーが模擬フィッシングメール以外のメールにPhish Alertボタンをクリックした場合には、このメールはセキュリティ担当者やインシデントレスポンスチームへ直接転送されます。
- ボタンテキストおよびユーザーダイアログボックスはすべてカスタマイズ可能。
- サポートされているクライアント: Outlook 2010／2013／ 2016 & Outlook for Office 365、Exchange 2013 & 2016、Outlook on the web (Outlook.com)、Outlook Mobile App (iOS & Android)、Chrome 54以降 (Linux、OS X & Windows)

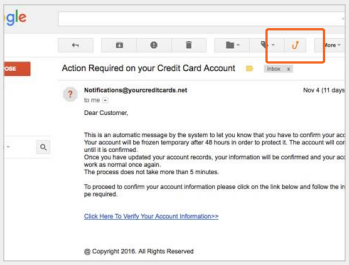
Outlookツールバー
各ユーザーにPhish Alert
ボタンを追加

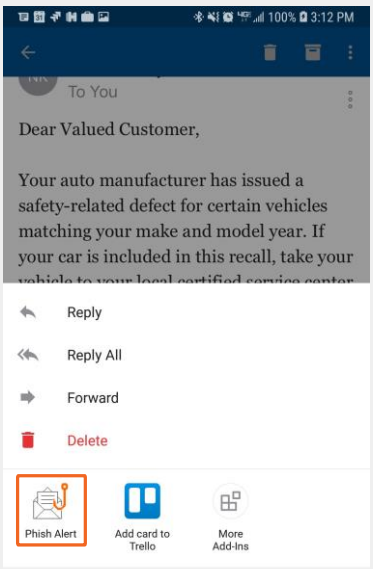


Office 365アドインペイン
各ユーザーにPhish Alert
ボタンを追加

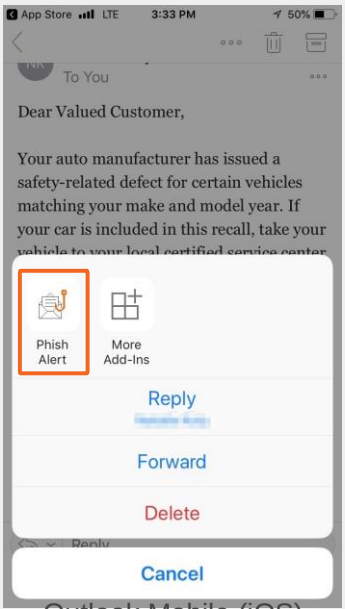


Gmailエクステンション
各ユーザーにPhish Alert
ボタンを追加





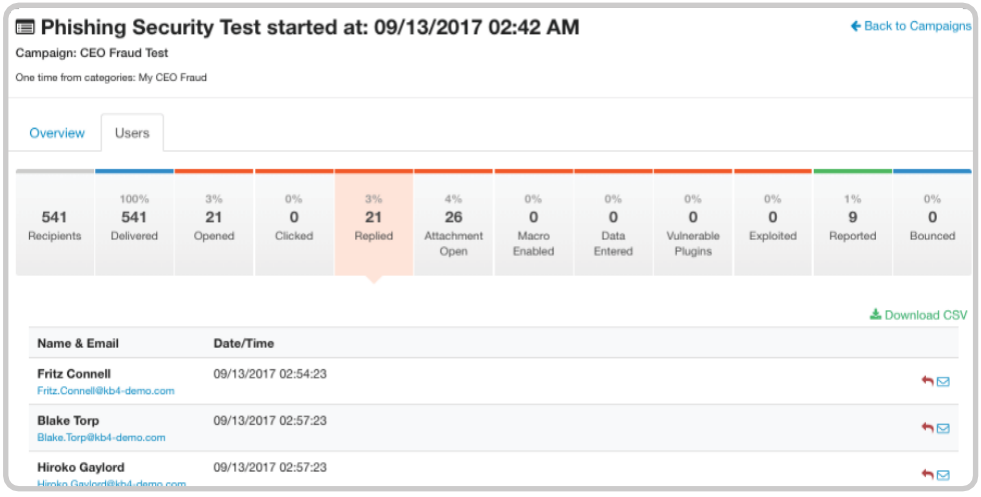
• Outlook Mobile (Android)



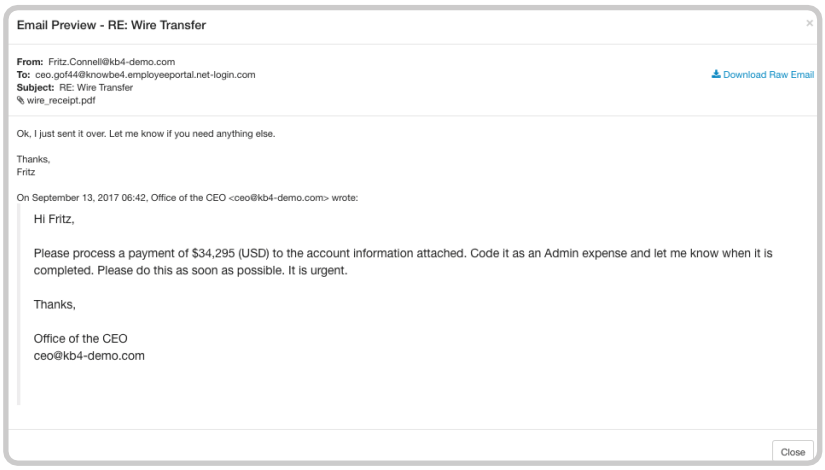
Outlook Mobile (iOS)

フィッシングリプライトラッキング

模擬フィッシングメールに返信したか否かをトラッキングすることを可能にします。さらに、返信内の情報をキャプチャしてKnowBe4管理コンソール内でレビューできるようにします。



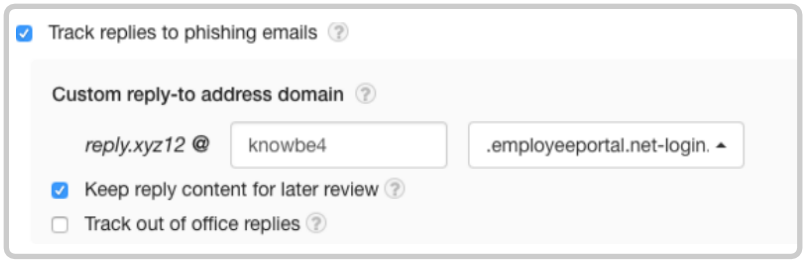
“Reply-To Online”というユーザーがハッカーと別途やり取りをしたかをテストするシステムテンプレートもあり、KnowBe4の2,000を超えるフィッシングテンプレートのいずれも機能します。



また、“Track replies to phishing emails”オプションを介して、新規フィッシングキャンペーンに対して、デフォルトでONに設定されているため、簡単に使用できます。

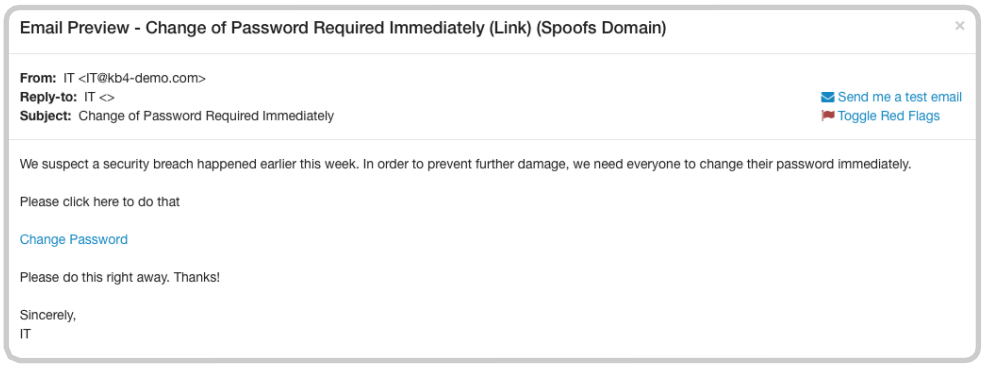
この機能の追加オプションは、次の通りです。

- 返信先コンテンツの保存：デフォルトでONに設定されるが、無効化される場合もあります。
- カスタマイズ可能な返信先アドレスサブドメイン：返信先アドレスを実ドメインと同様にします。
- 不在返信のトラッキング：ユーザーが社員名簿情報などの社内情報を含めていないかを確認します。

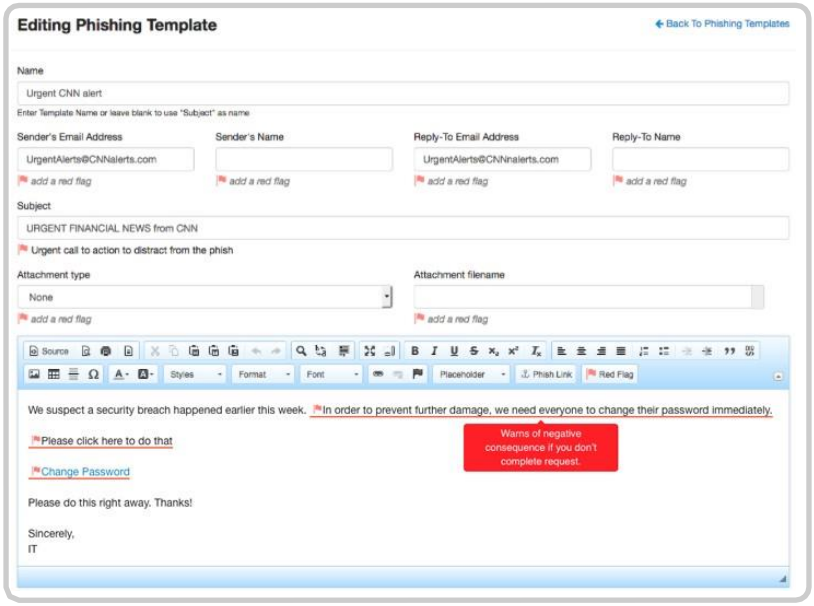


ソーシャルエンジニアリングインディケーター(SEI)

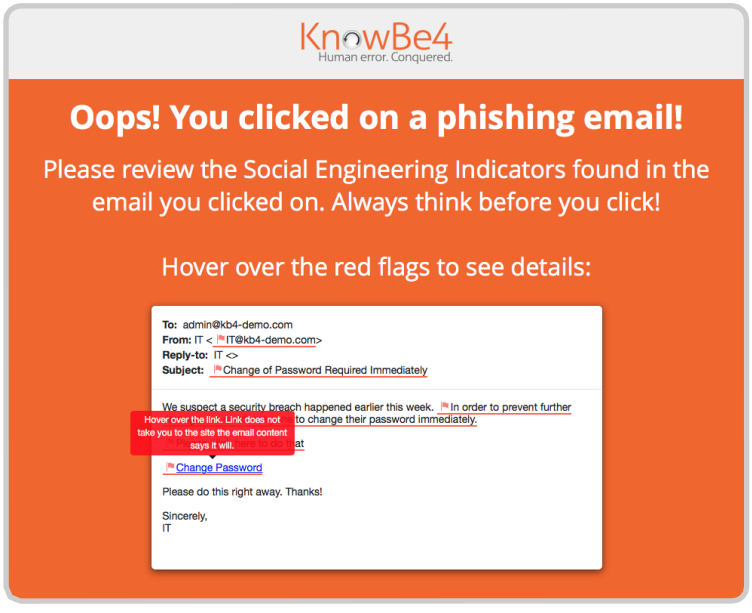
特許取得済みテクノロジーで、IT担当者が従業員トレーニングに即利用できるように、すべての模擬フィッシングメールテストの結果をセキュリティ教育のツールに変えます。ユーザーが2,000種を超えるKnowBe4の模擬フィッシングメールのいずれかをクリックすれば、ランディングページへとルーティングされます。このフィッシングメールのダイナミックなコピーのほか、すべてのレッドフラグの警告を表示します。



また、模擬フィッシングメールをカスタマイズでき、自社のレッドフラグを組み込むことができます。



ここで、ユーザーは潜在的な落とし穴をすぐに確認し、間違いを犯したインディケーターをピンポイントで学習します。



USB Drive Test™（USBドライブテスト）

USBを拾ったときどのように行動するかをユーザーに対してテストします。平均で45%のユーザーが拾ったUSBをPCへ差し込んでいます。

KnowBe4コンソールから簡単にUSBドライブテストを作成して、ビーコン化された特定のMicrosoft Officeをダウンロードすることができます。 また、ユーザーがクリック／オープンしやすくなるように、ファイル名を変更することもできます。 次に、これらのファイルをUSBにインストールして、従業員が頻繁に行き交う場所にUSBを落としておきます。

従業員がこのUSBを拾って、自分のワークステーションへ差し込んで、ファイルをオープンすると、”call home”アラートを発信して、このミスと一緒にアクセス時間やIPアドレスなどの情報を報告します。さらに、ファイル内のマクロを有効化しておけば、ユーザー名やコンピューター名などの追加情報もキャプチャでき、KnowBe4コンソールで利用できるようにできます。

GEOロケーション

模擬フィッシング攻撃がどこで成功したかをマップ上に表示できます。表示ポイントのドリルダウンやCSVエクスポートオプションもサポートされています。

AIDA: Artificial Intelligence Driven Agent:
AIドリブンエージェント (ベーターテスト中)

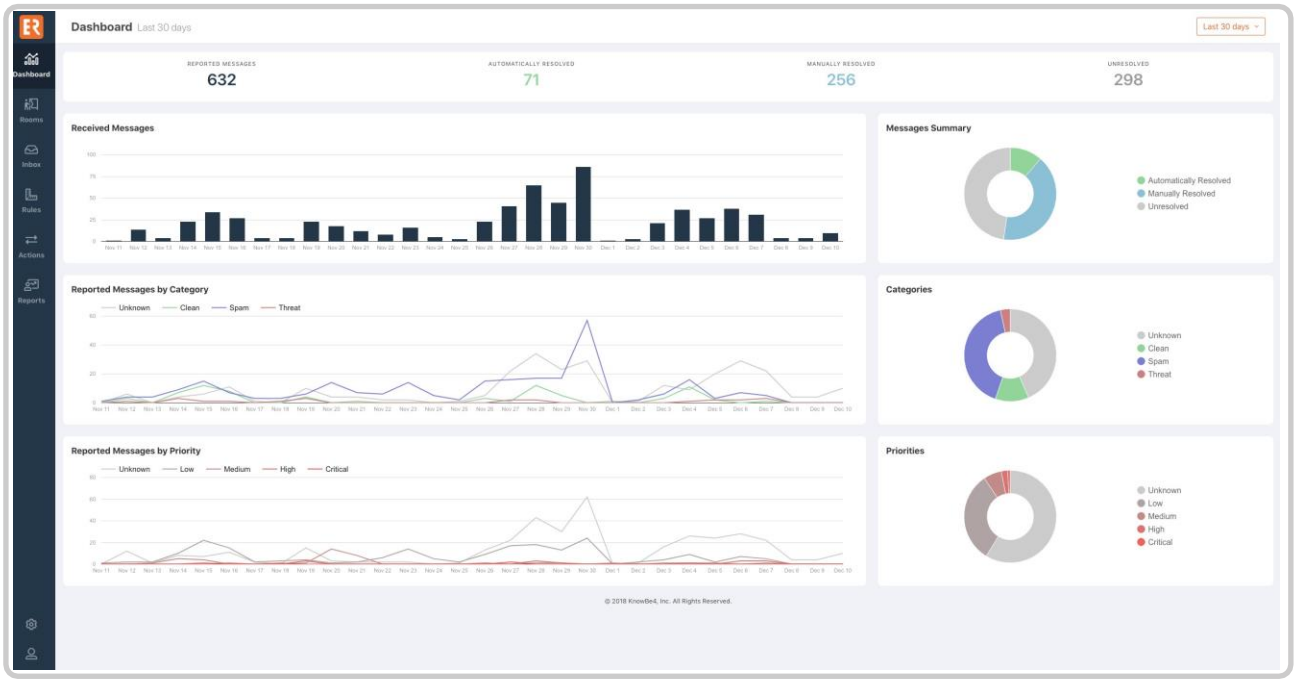
AIDAは、AIを使って、メール、DMやボイスメールなどを従業員へ送りつける統合化されたキャンペーンを動的に作成して、マルチベクトルのソーシャルエンジニアリングの模擬攻撃を仕掛けるものです。　これによって、従業員にフィッシングリンクをクリックさせたり、DM内のリンクをタップさせたり、ボイスメールに返答させたりすることで、ネットワークへの侵入を仕掛けていくものです。簡単に言えば、AIDAは、AIを活用して、ソーシャルエンジニアリングに対して予防訓練を組み立て、メール、電話、SMSメッセージングを駆使して多面的なソーシャルエンジニアリング模擬攻撃を仕掛けます。(米国とカナダで利用可能)

PhishER: メール脅威を迅速に特定し、素早く対応

セキュリティトレーニングを組織内に展開しているか否かにかかわらず、日々多くの不審メールを従業員が受信して、何らかの形態でセキュリティ担当者へ既に報告しています。この不審メールトラフィックの増加は、セキュリティ担当者にとっての新たな問題を発生させています。

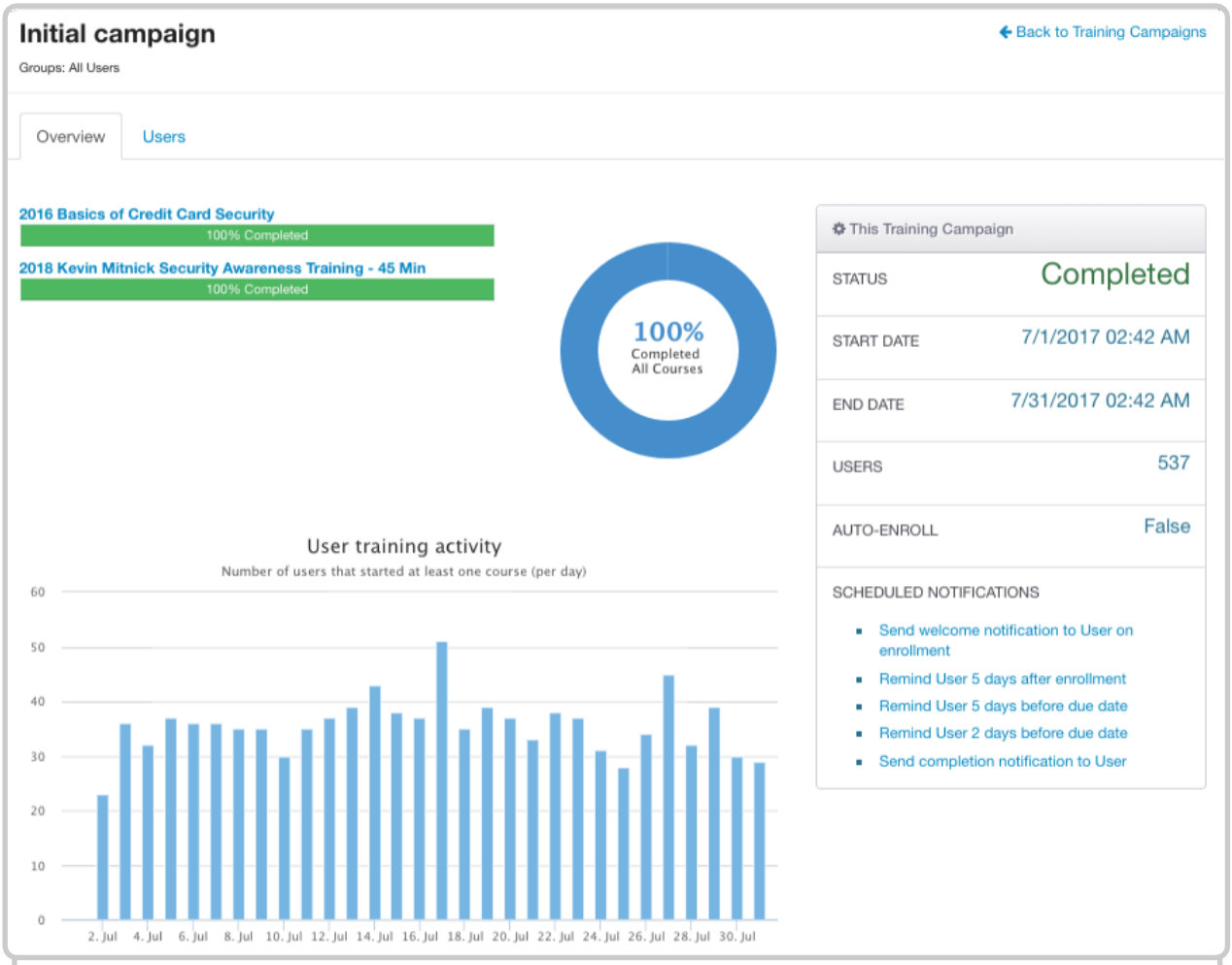
ネットワークを標的とするスパムメールや悪意あるメールの約10-15%はメールフィルターをすり抜けてします。 ユーザーが報告する10件のメールのうちで、実際には、悪意あるメールは1件ほどしかありません。高リスクのフィッシング攻撃に対処する一方で、いかにしてユーザーが報告する残り90%のメールに正確かつ効率的に対応するかは非常に重要な問題です。

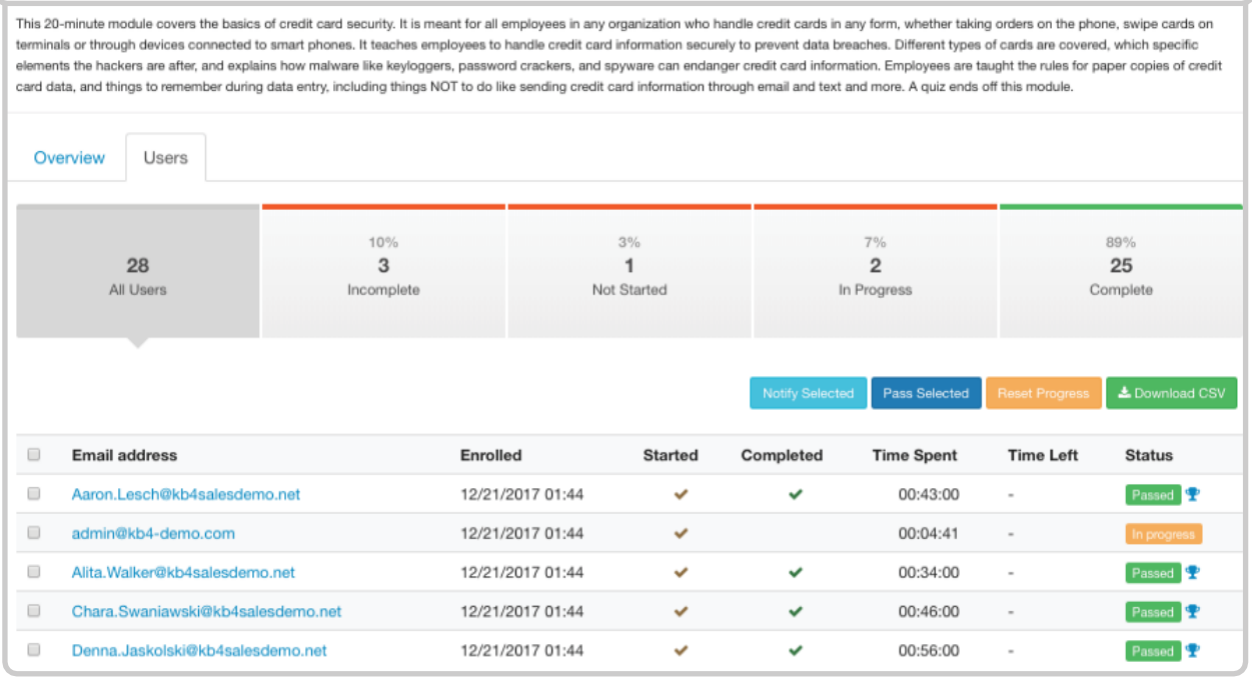
PhishERは、フィッシングの脅威を軽減するためにインシデントレスポンスチームが連繋する上での重要な構成要素です。悪意のあるメッセージを自動的に優先順位付けして管理するのに有用です。不審メールを正確かつ迅速に対処してくれます。PhishERは、スタンドアロン製品として、または、KnowBe4の年間サブスクリプション契約のアドオンオプションとしてご利用いただけます。



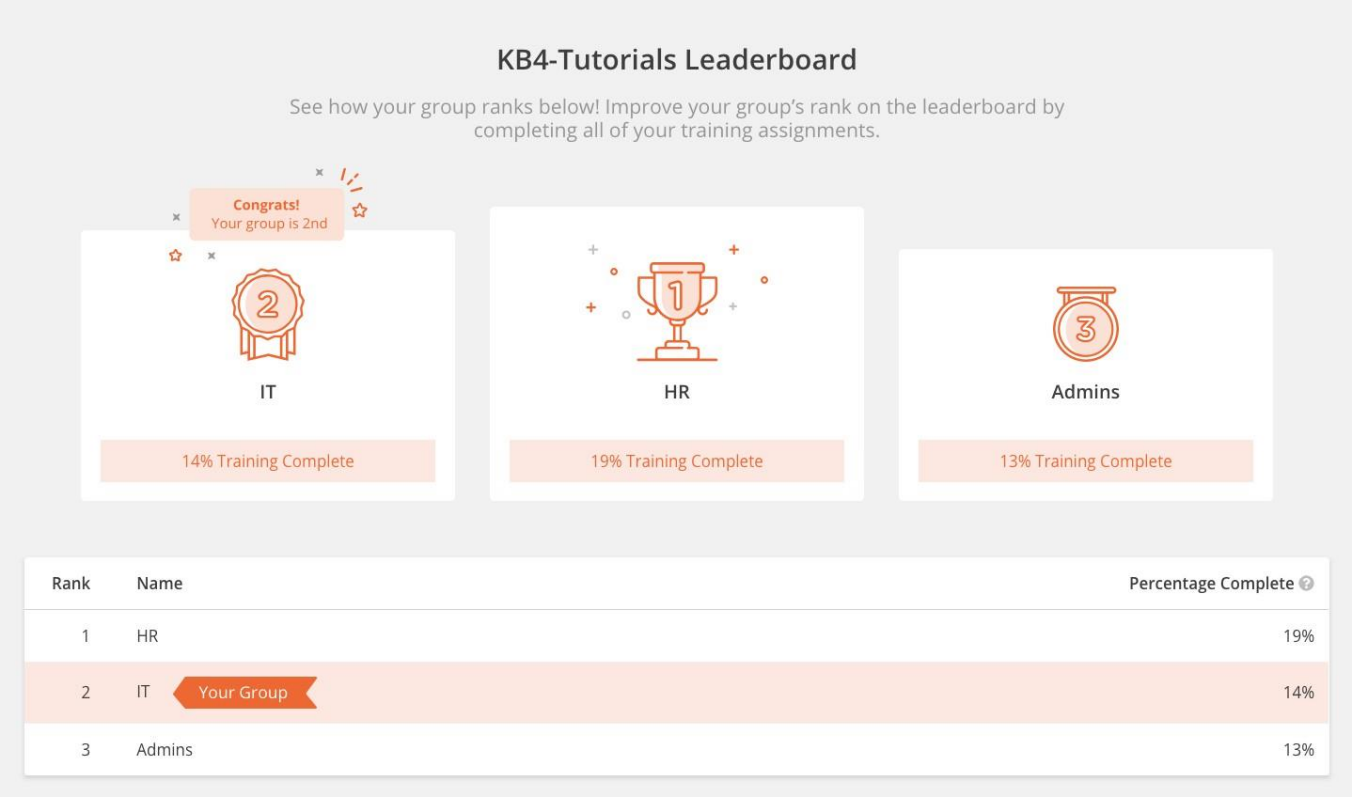
トレーニングキャンペーン

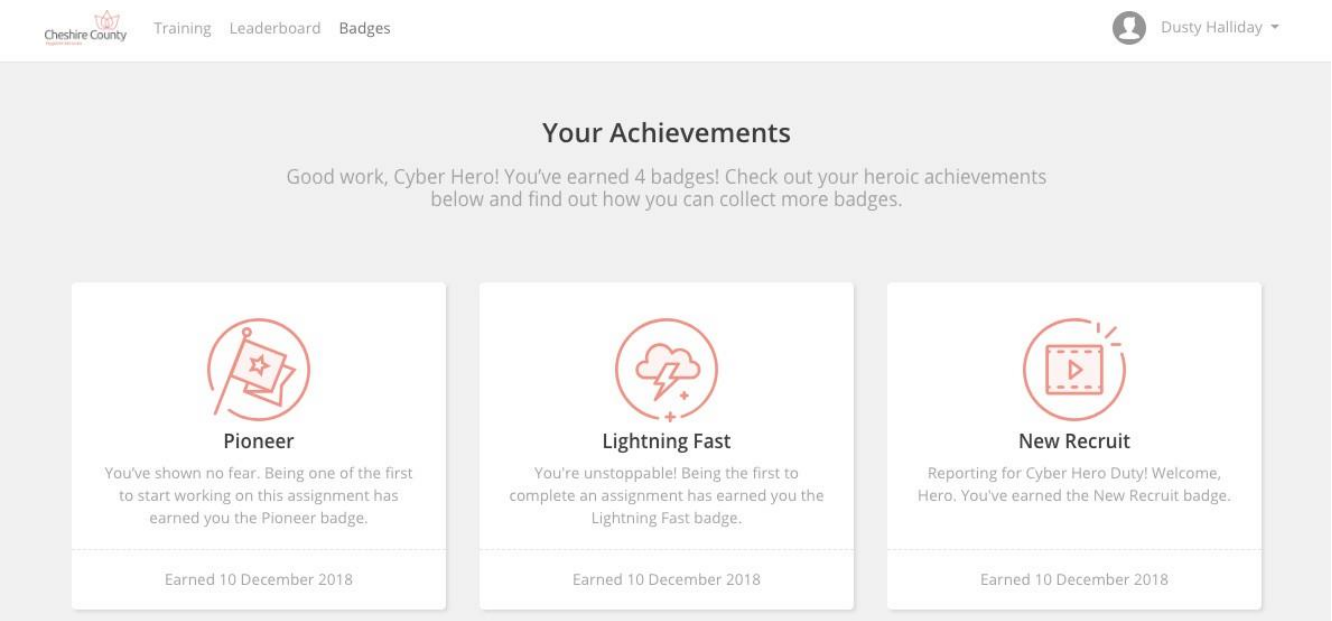
トレーニングキャンペーン
すべてのエンドユーザーに対して、リマインダーメール送信の設定することを含めて、トレーニング設定のロールをすべて自動化します。





学習意欲を高めるインタラクティブなブラウザーベースのトレーニング
スコア表を見て同僚と達成レベルを競い合ったり、レベルクリアのバッチを獲得したりできるなど、ゲーム感覚でトレーニング課題に取り組むことができます。

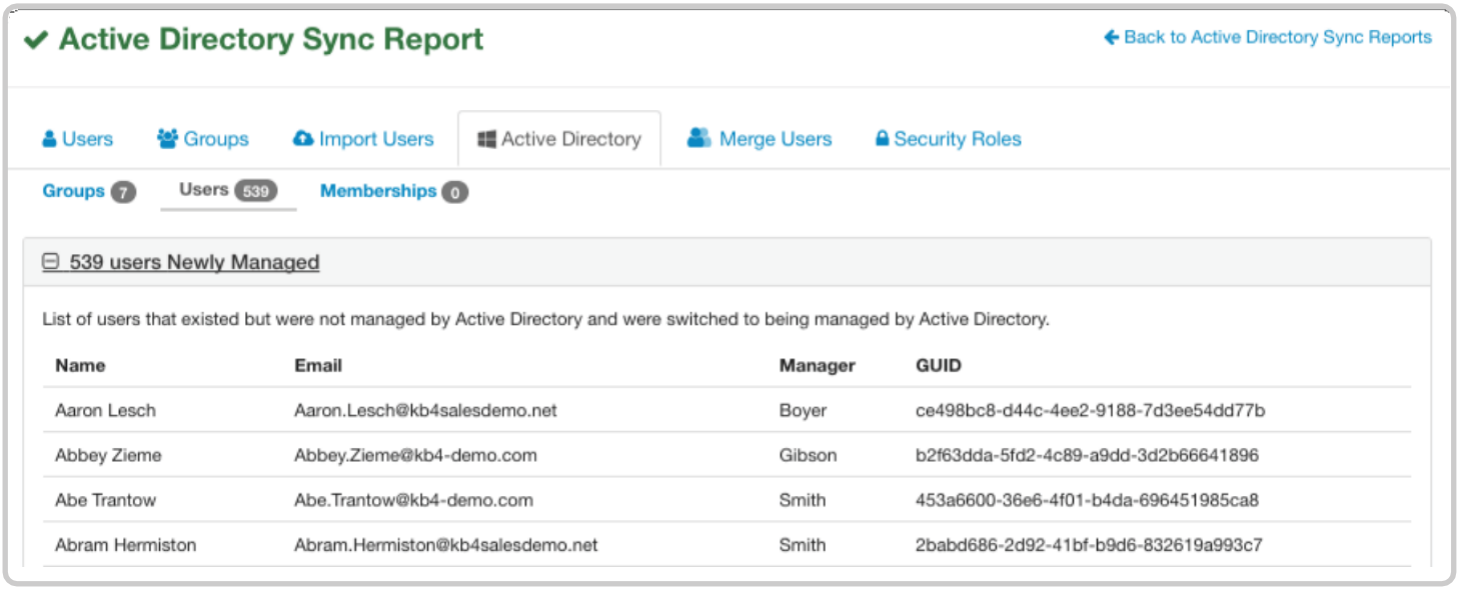


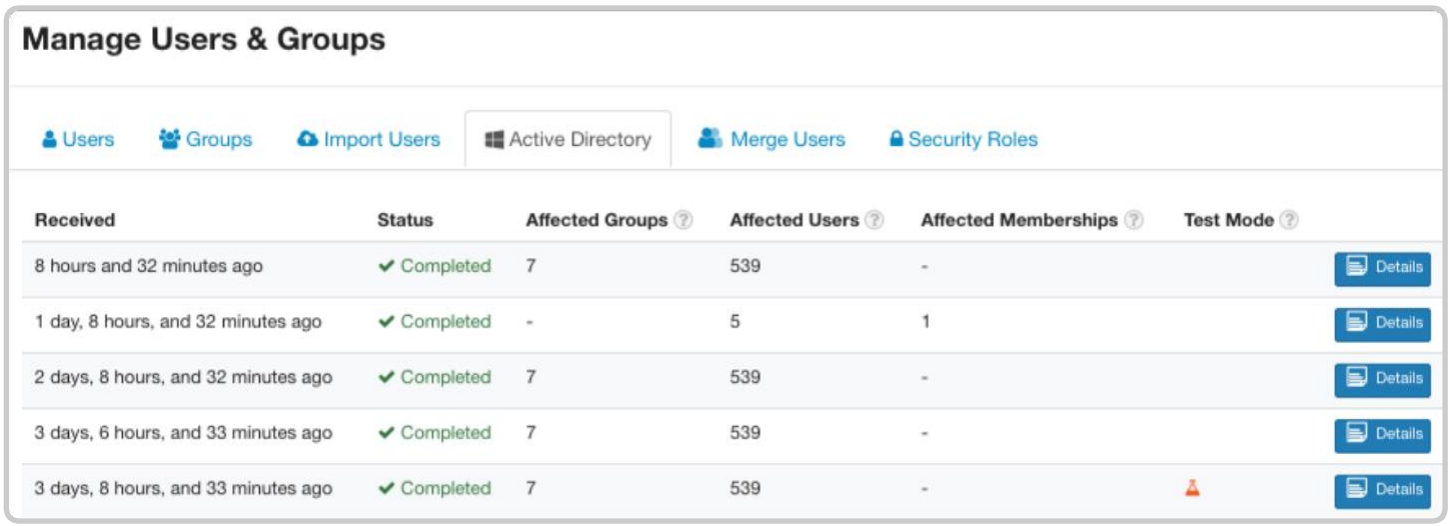


ユーザー管理

Active Directoryインテグレーション

ユーザーデータを容易にアップロードできます。これによって、手動でのユーザー変更を管理する必要がなくなり、セキュリティ担当者の負担を軽減することができます。 ADインテグレーションが構成設定されれば、AD内での変更と同期して、自動的にユーザーの追加・変更・保存が行われます。 また、CSVファイルでユーザーをまとめてアップロードすることもできます。 Microsoft Azure ADを使っている場合には、KnowBe4のADインテグレーションを通して、ユーザーの追加・削除のための自動的なユーザープロビジョニングを有効化することも可能です





Smart Group（スマートグループ）

トレーニングからフィッシング、レポーティングまでを自動化

セキュリティでの社員ひとりひとりの的確な意志決定を可能にするパスを自動化します。さらに、Smart Group機能を活用して、自社のフィッシングキャンペーン、学習課題、各ユーザーの振る舞いやユーザー属性に基づいたトレーニングなどを自動化することが可能になります。

また、一度設定すれば後の操作は一切不要なフィッシング／トレーニングキャンペーンを作成することができます。それにより、トレーニングとともに、フィッシングクリックへ即座に対応したり、新入社員登録トレーニングの自動通知などに対応したりすることが可能です。1つのSmart Groupに対して5つの主要基準から選択し、次にトリガーとなるポイント、条件とアクションを追加設定することで、的確な模擬フィッシングメールやトレーニングを的確な対象者に適時に送ることができます。

最も良いことは、Smart Groupルールに適用される異なる基準をベースにフィルタリングしてフル型でレポーティングできることです。例えば、特定の“Phish Event”基準でフィルタリングして、実施した模擬フィッシングテストの結果として改善度を示すレポートを作成すれば、特定のSmart Groupに対して、追加トレーニングや、さらに上のフィッシングテストをアサインすることができるようになります。

ワークフローを容易に構成し、カスタマイズする

誰でも簡単に、ターゲティングしたワークフローを作成することができます。これによって、従業員ひとりひとりがヒューマンファイアウォールの1つの強力な構成ブロックとして機能することが可能になります。簡単なトレーニングワークフローか、またはロケーション／振る舞い／タイミングなどの評価基準をベースとした複雑なワークフローかにかかわらず、評価基準を共通化することができます。また、高度なセグメンテーションロジックを使って、ワークフローにいつ、誰が登録したのか、いつ誰が登録を解除したのかを判定することが可能になります。

強力なタスク自動化で作業負荷を削減する

ワークフローを使って、トレーニングの設定や新入社員トレーニングの自動登録を行うことができます。時間ベースのトレーニング再登録、模擬フィッシングメール送信、ユーザーデータ管理、カスタムレポート作成などを容易に実行することができます。

セキュリティロール

KnowBe4コンソールを通して、詳細なアクセス権限を設定することができます。すべてカスタマイズ可能なため、各組織によって必要とされる明確なロール（役割）を設定することを可能にしています。 ロールは単に一連の予め設定された権限ではありません。

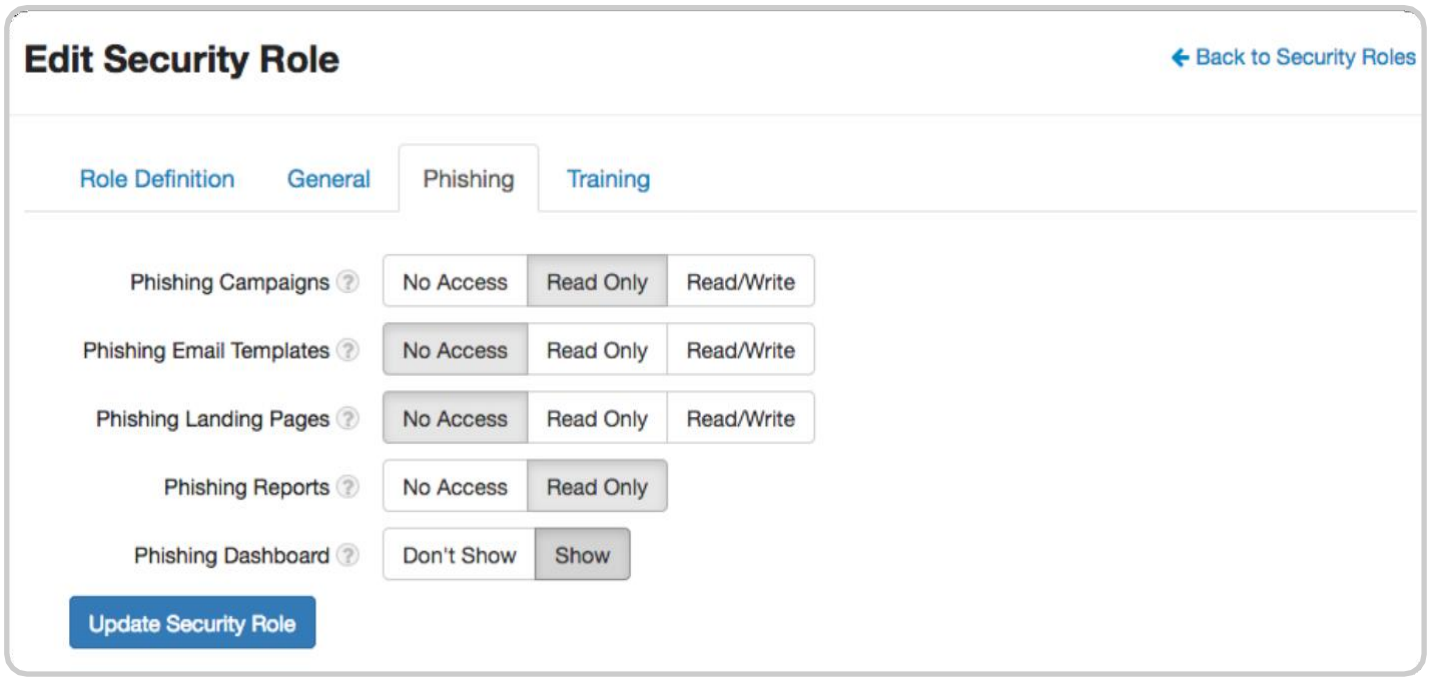
KnowBe4のセキュリティロール機能は、要件セットに適合した明確なアクセス権限モデルを設定することを可能にします。コンソールアドミニストレーターは、これに応じてKnowBe4コンソールの特定の部分のみをアクセス可能にすることができます。

想定されるアクセス権限：

- 業務監査担当：研修履歴を監査
- 人事部門：ユーザー個人の研修成果のチェック
- 研修グループ：提供されるトレーニングコンテンツの事前把握

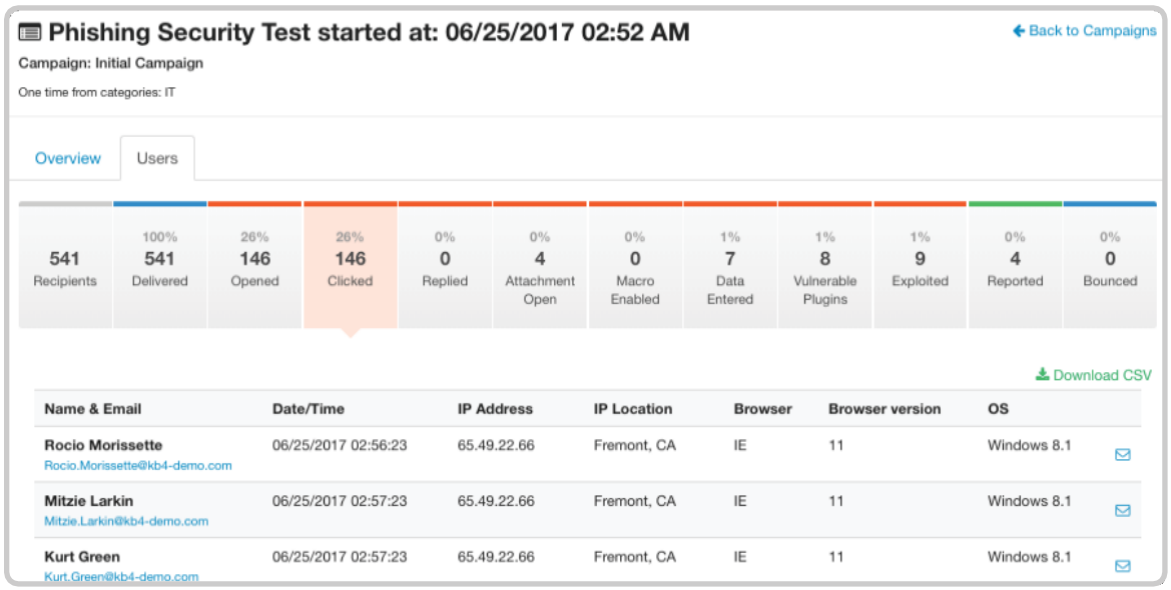
設定可能なアクセス権限の例：

- 模擬フィッシングテストの結果のレビュー（閲覧のみ）
- ユーザーおよびグループの管理
- 新規フィッシングキャンペーンの作成
- ModStoreで利用可能なトレーニングコンテンツのレビュー（閲覧のみ）

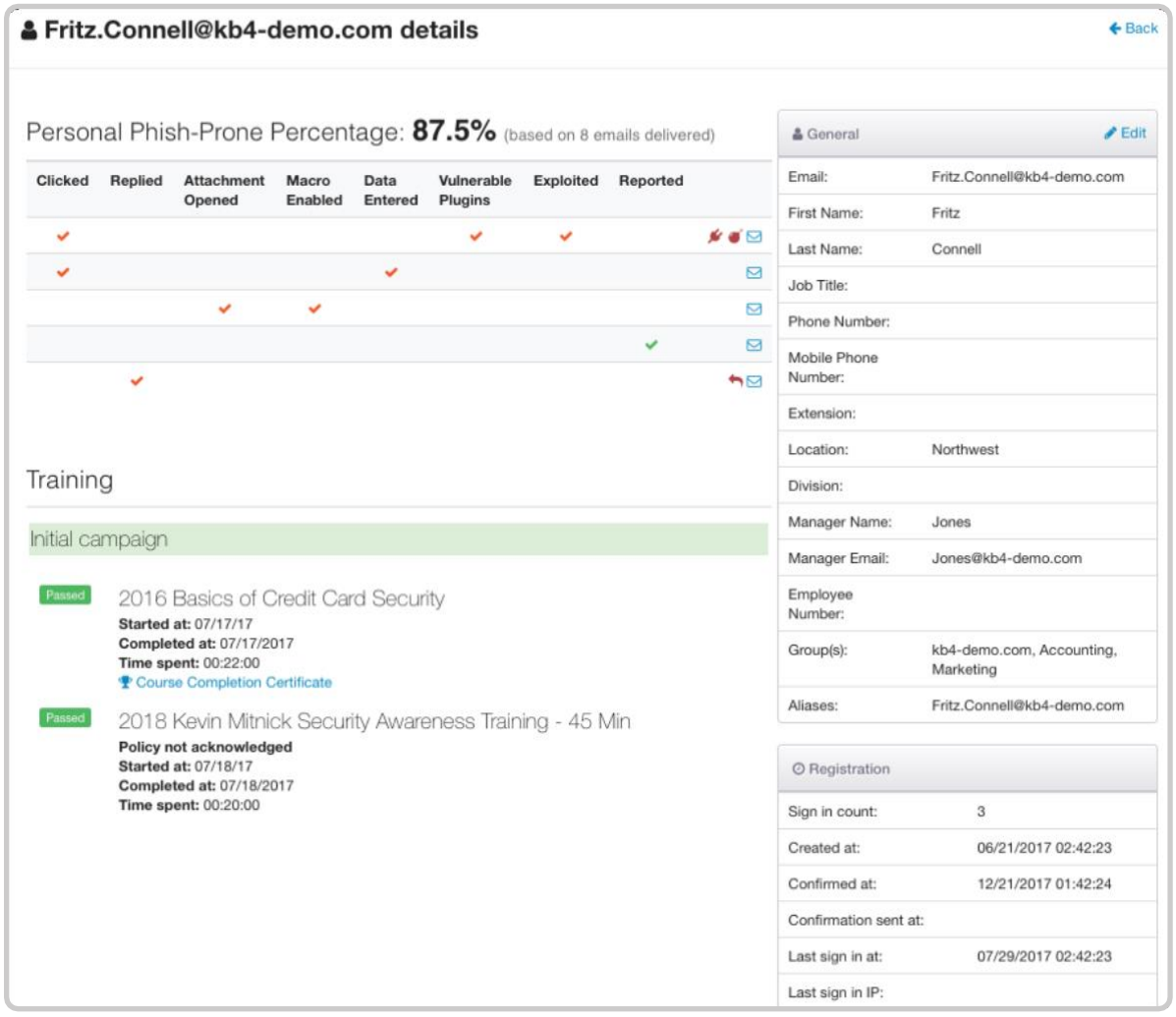


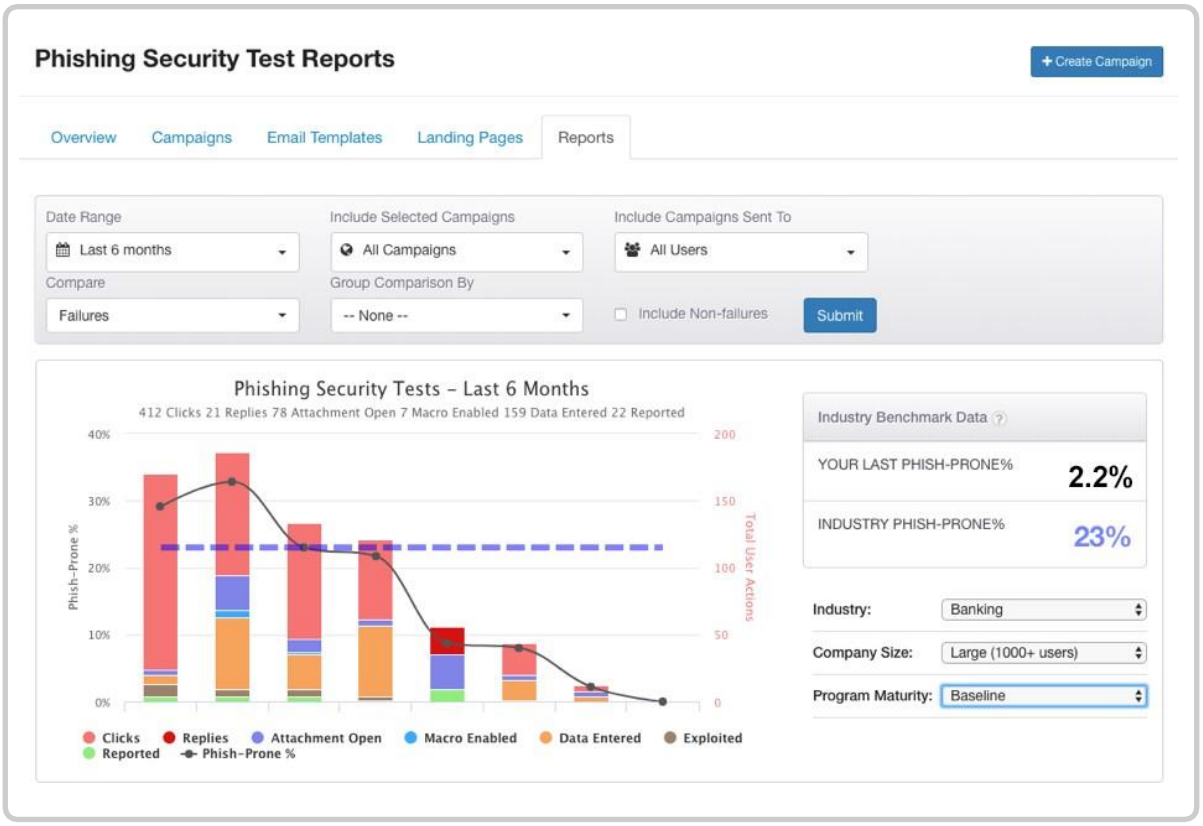
レポーティング

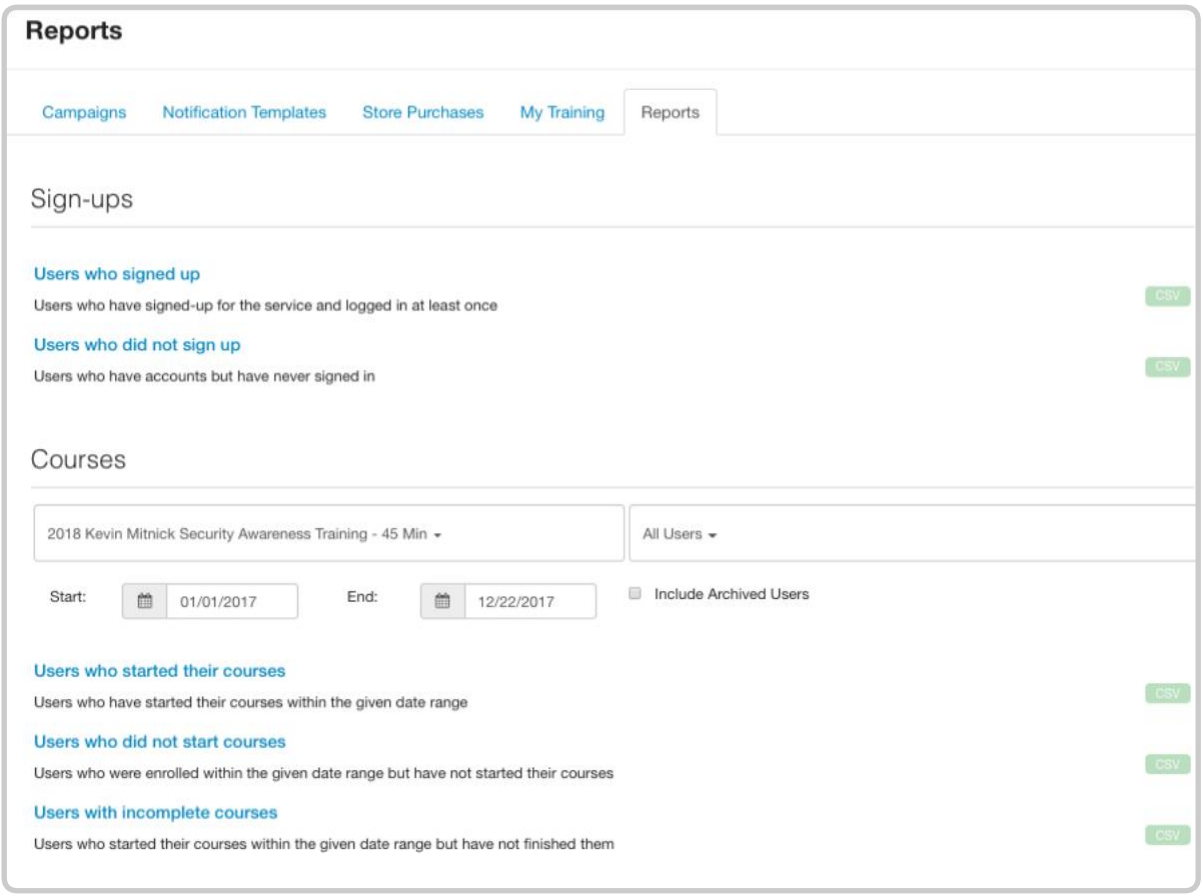
キャンペーン期間中の社員全員のレコードはすべて、並べ替え容易なCSVファイルとしてダウンロード可能



年間の社員評価に有用なユーザー別のレポーティングが可能

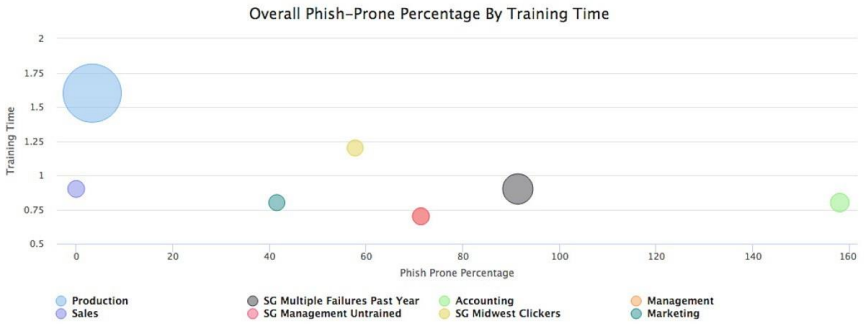



Phishing Security Test Reports
+ Create Campaign
Overview
Campaigns
Email Templates
Landing Pages
Reports
Date Range
Last 6 months
Include Selected Campaigns
All Campaigns
Include Campaigns Sent To
All Users
Compare
Failures
Group Comparison By
-- None --
Include Non-failures
Submit
Phishing Security Tests – Last 6 Months
412 Clicks 21 Replies 78 Attachment Open 7 Macro Enabled 159 Data Entered 22 Reported
Phish-Prone %
Total User Actions
Clicks
Replies
Attachment Open
Macro Enabled
Data Entered
Exploited
Reported
Phish-Prone %
Industry Benchmark Data
YOUR LAST PHISH-PRONE%
2.2%
INDUSTRY PHISH-PRONE%
23%
Industry:
Banking
Company Size:
Large (1000+ users)
Program Maturity:
Baseline

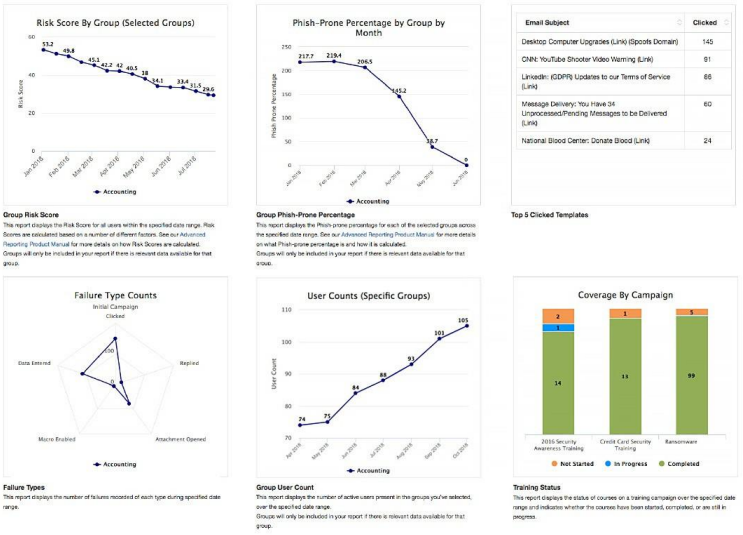

Reports
Campaigns
Notification Templates
Store Purchases
My Training
Reports
Sign-ups
Users who signed up
Users who have signed-up for the service and logged in at least once
CSV
Users who did not sign up
Users who have accounts but have never signed in
CSV
Courses
2018 Kevin Mitnick Security Awareness Training - 45 Min
All Users
Start:
01/01/2017
End:
12/22/2017
Include Archived Users
Users who started their courses
Users who have started their courses within the given date range
CSV
Users who did not start courses
Users who were enrolled within the given date range but have not started their courses
CSV
Users with incomplete courses
Users who started their courses within the given date range but have not finished them
CSV

60種を超えるビルトインされた各種の詳細レポートへのアクセスが可能：時系列に全体像を提供可能
管理者向け／企業レベルのレポーティングにより、組織全体のセキュリティ意識向上の成果を可視化することができます。また、特定期間での関連するトレーニングデータや模擬フィッシングデータを可視化することも可能です。 また、レポーティングAPIを活用することで、各自のカスタマイズされたレポートを作成して、BIシステムと統合することもできます。 複数のKnowBe4アカウントを管理したい場合は、ロールアップレポーティングによって、複数のアカウントや支店を横断して、レポートを選択して、集計結果を容易に比較検討することが可能です。

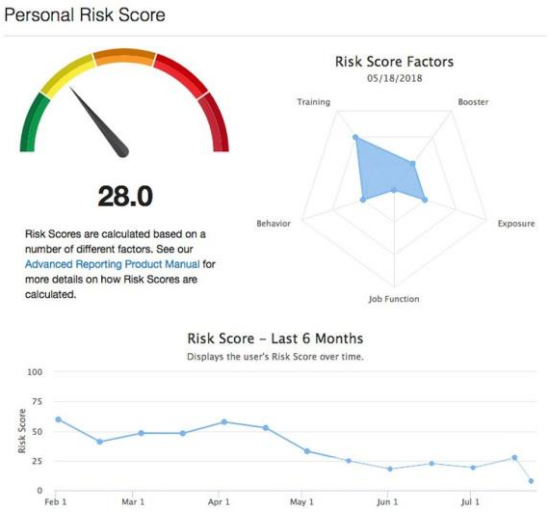
トレーニング時間毎のPhishing Prone Percentage（PPP:フィッシング詐偽被害攻撃遭遇率）
このレポートは、トレーニングに費やした時間軸に対して、グループ単位で組織のPPPを表示します。



グループレポートカード
このレポートでは、過去6ヶ月間（またはその他の期間）にわたる指定されたグループに対する、リスクスコア、PPP（フィッシング詐偽ヒット率）、グループサイズ、上位5つの高PPPテンプレート、トレーニング状況などが報告されます。



Virtual Risk Officer™（バーチャルリスクオフィサー）によるユーザー／グループ／組織レベルのリスクの特定
リスクの特定に加えて、セキュリティ意識向上プラン立案の際の意思決定に活用できます。



主な機能

Automated Security Awareness Program（ASAP）-自動化セキュリティ意識向上プログラム：各組織に合わせてカスタマイズされたセキュリティ意識向上プログラムを組み立てることを可能にします。構築のための必要なステップを示し、自社にとっての最適なトレーニングプログラムを数分で作成することができます。

カスタムフィッシングテンプレート： ユーザーに疑似フィッシングメールを送信する際、既存のテンプレートを変更することでカスタムフィッシングテンプレートをできるほか、一から独自のフィッシングテンプレートを作成することができます。公開情報および／またはユーザー個々の情報をベースにさらにシナリオをカスタマイズすることが可能になります。パーソナライズされたデータにフィールドを入れ換えて、標的型のスピアフィッシングキャンペーンを作成できます。

カスタムフィッシュドメイン： 不審メール内のリンクの上にマウスを乗せると、スクリーンの左下に表示されるURLにKnowBe4が設定した名前です。 KnowBe4では、さまざまな異なるフィッシュドメインを用意しています。常時変わる、エンドユーザーをいつも引き付けるようなURLから選択できるようにしています。

模擬添付（Simulated Attachment）： カスタムフィッシングテンプレートには、さまざまな形式（Word、Excel、PowerPointおよびzip,）で模擬添付を含めることができます。また、模擬添付にマクロを埋め込むことや、ファイルzipで仕込むこともできます。

カスタムランディングページ： 各フィッシングメールテンプレートには、それぞれの独自のランディングページを設定することが可能です。機密情報をフィッシングするランディングページへルーティングに加えて、事故発生時点の学習を可能にします。

アンチプレーリードッグ（Anti-Prairie Dog:）： フィッシングキャンペーンにおいてランダムなフィッシングテンプレートをランダムに送信することが可能になります。ユーザーに気づかれずに、本番さながらの模擬演習を体験させることができます。

Phish Alert（フィッシュアラート）ボタン：不審メールを分析のために、セキュリティ担当者へ安全、かつワンクリックで転送することができます.

フィッシングリプライ（Phishing Reply）トラッキング：各ユーザーが模擬フィッシングメールへ誤って返答したか否かをトラッキングすることが可能になります。同時に、返答で送信した情報もキャプチャすることができます。

ソーシャルエンジニアリングインディケーター：IT担当者がセキュリティトレーニングに即利用できるように、すべての模擬フィッシングメールテストの結果をセキュリティ教育のツールに変えます。模擬演習フィッシングメールの判断に誤って、クリックしてしまったユーザーには、レッドフラグが評価指標として立てられ、個人のスコアとして数値化されます。

セキュリティ意識向上トレーニング：セキュリティ意識向上トレーニングコンテンツの世界最大のライブラリーで、Diamondサブスクリプションレベルでは インタラクティブな教材モジュール、ビデオ、ゲーム、ポスター、ニュースレターなどを含んでいます。

トレーニングキャンペーン： KnowBe4管理コンソールで、トレーニングキャンペーンを迅速に設定できます。実施期間を限定することも可能です。また、ユーザーグループ毎にトレーニングモジュールを選択するほか、新規ユーザーの自動登録、トレーニング未完了者への喚起メールの自動化も可能です。

Smart Group（スマートグループ）： フィッシングキャンペーン、学習課題、各ユーザーの振る舞いやユーザー属性に基づいたトレーニングなどを自動化することが可能になります。

アドバンスドレポーティング：60種を超えるビルトインされた各種の詳細レポートへのアクセスが可能。時系列に全体像を提供します。主要セキュリティ意識向上トレーニング評価指標の詳細なレポーティングのために大幅に拡張されています。これに加えて、レポーティングAPIを活用することで、KnowBe4コンソールからデータを抽出できます。各自のカスタマイズされたレポートを作成して、BIシステムと統合することもできます。

Virtual Risk Officer (VRO)： 個人レベル／グループレベル／組織レベルでのリスクの特定に加えて、セキュリティ意識向上プラン立案の際の意思決定に活用できます。

USB Drive Test™（USBドライブテスト）：USBを拾ったときどのように行動するかユーザーに対してテストすることができます。

Active Directoryインテグレーション： ユーザーデータを容易にアップロードできます。これによって、手動でのユーザー変更を管理する必要がなくなり、セキュリティ担当者の負担を軽減することができます。

セキュリティロール： 特定のユーザーグループを設定したい場合に、アクセスレベルおよび管理権限を組み合わせて、自在に設定できます。KnowBe4アカウントへのアクセス領域を限定して、必要な対象者のみに許可するように定義することが可能になります。

ユーザーイベントAPI： サードパーティーのセキュリティプラットフォームまたはデータソースからセキュリティ関連のカスタムイベントをKnowBe4コンソールへプッシュ型で連携させることができ、ユーザーのリスクスコアに随時反映させることが可能になります。 ユーザーのタイムラインにこれらのイベントを追加したり、使用できるように選択したりして、ユーザーのリスクスコアを補完することができます。これによって、追加のフィッシングテストやトレーニングキャンペーンのために特定の(詳細な)コンテンツをカスタマイズすることが可能になります。

AIDATM（Artificial Intelligence-driven Agent: AIドリブンエージェント）： AIを活用して、ソーシャルエンジニアリングのさまざまな手口に対して予防訓練を設定することができます。多面的なソーシャルエンジニアリング模擬攻撃を迅速かつ容易に仕掛けることを可能にします。これによって、ユーザーにフィッシングリンクをクリックさせたり、DM内のリンクをタップさせたり、ボイスメールに返答させたりするなどで、ネットワークへの侵入を仕掛けていくものです。誰が模擬フィッシング攻撃に引っかかったか、誰が組織内で脆弱なまま残されているかをピンポイントで確認することができるようになります。

サブスクリプションレベル

KnowBe4のSaaSサブスクリプションは、年間ベースで1ユーザーあたりの価格設定になっています。KnowBe4は、各組織のニーズを満たすために、Silver、Gold、PlatinumおよびDiamondの4つのサブスクリプションレベルを用意しています。

機能	SILVER	GOLD	PLATINUM	最も一般的 DIAMOND
utomated Security Awareness Program（ASAP）	✓	✓	✓	✓
セキュリティ‘Hints & Tips	✓	✓	✓	✓
トレーニングアクセスレベル I	✓	✓	✓	✓
自動化トレーニングキャンペーン	✓	✓	✓	✓
Phish Alertボタン	✓	✓	✓	✓
Phishing Replyトラッキング	✓	✓	✓	✓
Active Directoryインテグレーション (ADI)	✓	✓	✓	✓
業界ベンチマーキング	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
アドバンスドレポーティング	✓	✓	✓	✓
暗号化ランサムウェア	✓	✓	✓	✓
トレーニングアクセスレベルII		✓	✓	✓
月次メール脆弱性テスト		✓	✓	✓
ビッシング（Vishing）		✓	✓	✓
セキュリティテスト		✓	✓	✓
Smart Group			✓	✓
レポーティングAPI			✓	✓
ユーザーイベントAPI			✓	✓
セキュリティロール			✓	✓
ソーシャルエンジニアリングインディケーター(SEI)			✓	✓
USBドライブテスト			✓	✓
優先レベルサポート			✓	✓
トレーニングアクセスレベルIII				✓
AIDA™ AIドリブンエージェント（ベータ中）				✓
PhishER™ - オプショナルアドオン	✓	✓	✓	✓

Silverレベル:トレーニングアクセスレベル I では、Kevin Mitnickセキュリティ意識向上トレーニングの45分長編モジュール、25分短編モジュールおよびエグゼクティブ向けの15分バージョンが含まれます。その他、サブスクリプション期間での無制限の模擬フィッシングテストおよびきめ細かなレポーティングが含まれます。

Goldレベル: すべてのSilverレベル機能に加えて、トレーニングアクセスレベル II コンテンツが含まれます。KnowBe4のトレーニングモジュールが追加になります。さらに、月次メール脆弱性テストレポートほか、IVRやVoIPを利用したビッシング（ビッシング（Vishing）セキュリティテストが含まれます。（米国とカナダで利用可能）

Platinumレベル: SilverおよびGoldのすべての機能を含みます。KnowBe4のアドバンスドフィッシング機能であるSmart Group、レポーティングAPI、ユーザーイベントAPI、セキュリティロールおよびランディングページ・ソーシャルエンジニアリングインディケーターが含まれます。

Diamondレベル: Silver、GoldおよびPlatinumのすべての機能を含みます。これに加えて、インタラクティブモジュール、ビデオ、ゲーム、ポスターおよびニュースレターなどのKnowBe4の900種を超えるコンテンツのライブラリーへのアクセスを与えるトレーニングアクセスレベル III を含みます。 さらに、KnowBe4の最新AIドリブンのエージェント（AIDA™）を利用することができます。現在、ベーターテスト中でメール、電話、SMSメッセージングと駆使した多面的なソーシャルエンジニアリング模擬攻撃を可能にします。（米国とカナダで利用可能）

PhishER: スタンドアロン製品として、または、KnowBe4ユーザーのアドオンオプションとして全サブスクリプションレベルで利用可能。 PhishERは軽量なSOAR（Security Orchestration Automation & Response)プラットフォームです。脅威への対応を調整して、ユーザーから報告される大量の悪意のあるメッセージの迅速な対応を可能にします。不審メールはKnowBe4のPhish Alert（フィッシュアラート）ボタンによって、または単純にメールボックスへの転送で報告されます。 メールの優先順位付けを自動化することによって、PhishERはIT管理者やセキュリティ担当者の受信ボックス内のノイズをカットし、最も危険な脅威への対応を迅速化・効率化することを可能にします。（最低101ユーザーから）

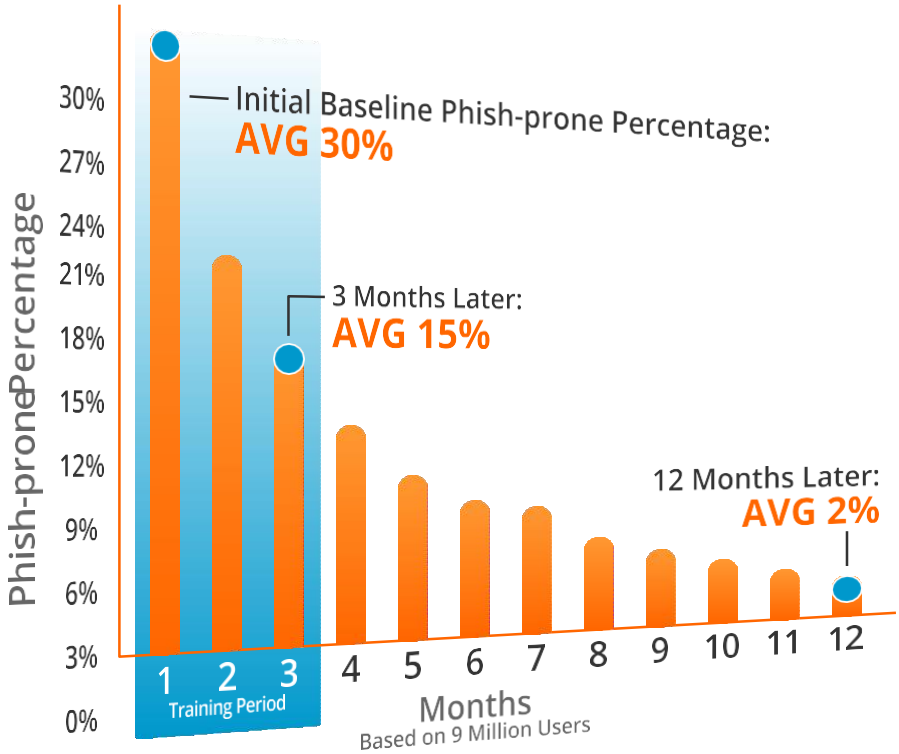
“ソーシャルエンジニアリングは情報セキュリティの最も脆弱なリンクである。”

Kevin Mitnick（ケビン・ミトニック）、
世界で最も有名なホワイトハッカー＆ITセキュリティコンサルタント

KnowBe4システムが機能するか—明確な実証

KnowBe4 の受講者データベースを使って、12 ヶ月間にわたり約900 万人のトレーニング受講者を対象にベンチマークし、2019 年度の調査結果は導入効果を実証しました。全業種でのトレーニング実施前のベンチマークによると、トレーニング開始前のPPP（Phishing Prone Percentage:フィッシング詐偽ヒット率）は30%というリスクの高さが結果として報告されました。

この数値が、KnowBe4 の“New School”（セキュリティ意識向上トレーニングと疑似フィッシング訓練の組み合わせ）実施後の90 日で、30%から15%へ半減しました。さらに、1 年後の結果では、平均で2%へ大幅に削減できました。



KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社
〒100-0004 東京都千代田区大手町1-9-2 大手町フィナンシャルシティ
グランキューブ3 階 Global Business Hub Tokyo |
www.KnowBe4.com／www.KnowBe4.jp |
お問い合わせ:: Info@knowbe4.jp

販売代理店:
株式会社東陽テクニカ 情報通信システムソリューション部
〒103-8284 東京都中央区八重洲1-1-6
TEL:03-3245-1250（直通） FAX:03-3246-0645 E-Mail:ict_security@toyo.co.jp
https://www.toyo.co.jp/ict/maker/detail/knowbe4.html