【米国リリース抄訳】 2020 年 4 月 20 日

最新フィッシングメール動向: 2020 年第 1 四半期にコロナウイルス関連のフィッシングメールが 600%増加

KnowBe4 が 2020 年度第 1 四半期版の「要注意件名」トップ 10 レポートを公開

※当資料は、2020 年 4 月 9 日に米国で発表されたニュースリリースの抄訳版です。
https://www.knowbe4.com/press/q1-2020-knowbe4-finds-coronavirus-related-phishing-email-attacks-up-600

米国フロリダ州タンパベイ(2020 年 4 月 9 日発) -
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のプロバイダーである KnowBe4 社(本社:米国フロリダ州タンパベイ、創立者兼 CEO:Stu Sjouwerman (ストゥ・シャワーマン))は、模擬フィッシング攻撃を通してどれくらい攻撃被害を受けやすいかを PPP (Phishing Prone Percentage:フィッシング詐偽ヒット率)としてアセスメントしています。この統計データを最新フィッシングメール動向として四半期毎に公表しています。本プレスリリースでは、2020 年第1四半期(2020 年 1 月－3 月期)の「要注意件名」統計レポートの注目ポイントを公開します。

本統計レポートによると、新型コロナウイルス(COVID-19)関連のフィッシングメール攻撃が 2020 年第 1 四半期(2020 年 1 月－3 月期)に 600%増と大幅に増加しています。同四半期での最もヒット率が高かったフィッシングメール件名はパスワードの即刻確認を通知する緊急メッセージで、45%というと驚くべきヒット率となっています。2 番目のヒット率が高かったフィッシングメール件名は、コロナウイルス関連のメッセージで、急激に増加して、10%に達しています。引き続き、ソーシャルメディア関連メッセージがフィッシングの手段として要注意のカテゴリーとなっています。また、同統計レポートによると、最もクリックされたソーシャルメディア関連のメール件名はログイン警告通知、パスワード再設定、不正アカウント侵害通知が上位を占めています。

KnowBe4 の CEO である Stu Sjouwerman はこの結果について、次のようにコメントしています。「サイバー犯罪者などの悪者は、あらゆる機会を利用してきます。彼らは、コロナウイルス禍のような危機的な状態における人の不安やストレスから発生する感情的な動揺を突いて、悪意あるリンクのクリックや添付ファイルの開封を仕掛けてきます。コロナウイルス関連のフィッシング攻撃の爆発的な増加は驚くべきことではないのです。今、人々はコロナウイルスに関する情報を欲し、

より多くの情報を知りたいと思っているのです。COVID-19 に関するメールは要注意です。受信したら、即座に IT 部門へ連絡してください。絶対に、リンクをクリックしたり、添付ファイルを開封したりしてはなりません。」

今回の統計では、KnowBe4 は、KnowBe4 の模擬フィッシング攻撃テストからの数万件のメール件名をチェックしています。また、KnowBe4 は、同社の Phish Alert ボタンを使ってエンドユーザーが IT 部門へ不審メートとして報告した実際のメールの件名についてもチェックしています。本統計データのポイントは以下のとおりです。

- **一般的に使われるフィッシングメール件名トップ 10**
  - 即時パスワード確認依頼
  - 米国疾病管理予防センター（CDC） 緊急警告：新型コロナウイルの感染実態
  - 有給休暇（PTO)内規変更
  - 定期サーバー保守 - インターネットアクセス不可
  - [[company_name]]緊急連絡システムのテスト
  - 休暇・病欠申請内規変更
  - [[email]] メールアカウントの利用停止
  - 人事部から重要なお知らせ： 必ず読んでください
  - 特別な人からバレンタインデーe カードを受信しました！
  - Microsoft チームの1つのチームメンバーに選出されました

**今回の統計データでの件名は英語ですが、日本語に翻訳してあります。同様なフィッシングテンプレートを日本語でも用意しています。*
***今回の統計データでの件名は、KnowBe4 がお客様用に用意した フィッシングテンプレートとKnowBe4 の顧客が各自でカスタマイズしたものの両方が含まれています。*

- **実際のメールの件名で最も一般的なもの**

模擬フィッシングメールに加えて、実際のメールの件名についても KnowBe4 では調査しています。以下は、KnowBe4 が 2020 年第1四半期で検出した実際のメールの件名で最も一般的なものです。

  - 新型コロナウイルス蔓延による延期ミーティングの一覧
  - SharePoint: 新型コロナウイルス（COVID-19）減税申請資料
  - 新型コロナウイルス（COVID-19）関連の機密情報
  - IT からのお知らせ: テレワーク- VPN 接続
  - Comcast: Carl Vargas からのお知らせ
  - Microsoft: ミーティングがすぐに開始されます
  - 人事通達: 新入社員対象の株購入プラン
  - Vodafone: 発信者警告: 本日受信のメッセージ
  - Amazon Chime: Vonage があなたを vonage_303136 参加に招待しています
  - Parking Authority: 駐車チケット: 料金支払い

**今回の統計データでの件名は英語ですが、日本語に翻訳してあります。英語名称（大文字、スペル）はそのままで表記しています。*
***実際のメールの件名とは、エンドユーザーが受け取った実際にメールで不審メールとしてIT 部門へ報告したメールの件名です。模擬フィッシングテストでのメールの件名ではありません。*

KnowBe4 についてさらに知りたい方は、www.knowbe4.com.をアクセスしてください。

＜KnowBe4 について＞

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訓練・分析を組み合わせた世界最大の統合プラットフォームのプロバイダーです。KnowBe4 は、IT／データセキュリティ・エキスパートである Stu Sjouwerman（ストゥ・シャワーマン）によって 2010 年 8 月に米国フロリダ州タンパベイで設立され、セキュリティの「人的要素：ヒューマンエラーの克服」にフォーカスして、ランサムウェア、CEO 攻撃/詐欺、ビジネスメール詐欺（BEC）を始めとする巧妙化するソーシャルエンジニアリング手口などの社員ひとり一人のセキュリティに対する認識を高めることで、「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援しています。世界で最も著名なサイバーセキュリティ・スペシャリストである Kevin Mitnick（ケビン・ミトニック）が CHO（Chief Hacking Officer）を務めています。同氏のハッカーの視点に立った知見をベースに KnowBe4 のトレーニングプログラムは組み立てられています。2020 年 4 月現在、3 万 2 千社を超える企業や団体が KnowBe4 を採用して、防御の最終ラインとして「人」による防御壁を構築しています。また、KnowBe4 はセキュリティ意識向上トレーニングのマーケットリーダーとして、その評価はガートナーが同社の 2019 年度マジッククアドラントで 3 年連続リーダーとして認定するほか、企業成長力や企業文化においても高い評価を獲得しています。
https://www.knowbe4.com/

<KnowBe4 Japan の問い合わせ先>

KnowBe4 Japan 合同会社　根岸
TEL:03-4588-6733　メール：info@knowbe4.jp
住所：千代田区大手町 1 丁目 9 番地 2 号　大手町フィナンシャルシティグランキューブ 3F
https://www.knowbe4.jp/