KEEPER®

サイバーレジリエンスの強化

グローバルなサイバーセキュリティ慣行についての洞察

概要

インターネット上のサービスは、私たちの生活のあらゆる領域、世界の隅々まで浸透しており、その中でもサイバーセキュリティは世界的な懸念事項になっています。Keeper Securityのレポート「**サイバーレジリエンスの強化: グローバルなサイバーセキュリティ慣行についての洞察**」は、サイバーセキュリティの一般的な傾向について調査したものであり、政府、企業、サイバーセキュリティの専門家などの関係者が、グローバルなサイバーセキュリティの脅威に対処するための、効果的な戦略を策定する上で役立ちます。

Keeperは、オーストラリア、ニュージーランド、シンガポール、インドネシア、日本、フランス、英国、米国、DACH (ドイツ、オーストリア、スイス) 地域の6000人に対して調査を実施し、現在のサイバーセキュリティに関する意識向上プログラムや教育プロジェクトの有効性についての洞察を得ました。サイバーセキュリティのベストプラクティスについて一生懸命に啓発しているのに、サイバー攻撃やオンライン詐欺が依然として多発している現状から、知識と実践の両方にまだ弱点があることがわかります。さまざまな対象者のセキュリティ行動と施策を評価することで、一般の人々の理解が不足している領域を特定できます。こうした情報は、効果的な啓発キャンペーンやトレーニングプログラムを作り、弱点を補強し、個人がインターネット上で安全に過ごすために必要です。

人々のサイバーセキュリティ行動を理解することで、サイバーレジリエンスを構築するための技術的な解決策やポリシーの策定と改善に役立ちます。例えばこの調査では、不便になったりパフォーマンスが低下したりするのを恐れて、かなりの数の人々がデバイスを更新していないことが明らかになっています。このデータは、テクノロジー企業がより簡易的でユーザーフレンドリーなプロセスを構築し、セキュリティを強化するための指針となります。同様に、多くのユーザーがパスワード管理を記憶や物理的なメモに頼っていることを考えると、パスワードマネージャーの導入を促進し、簡素化する必要があるのは明らかです。政策立案側ではこのデータを活用して、より安全なオンライン行動を奨励し、サイバー脅威から消費者を守るための規制やガイドラインポリシーを立案できます。

サイバーセキュリティの実践に関するグローバルな調査は、国際的な協力と知識の共有を促すものでもあります。サイバー脅威は国境を越えて存在するため、各国は他の場所で実施されている効果的な戦略や政策について学ぶことで大きな恩恵を受けることができます。各国が調査結果を共有し、解決策において協力することで、より回復力のあるグローバルなサイバーセキュリティインフラストラクチャを構築できます。共同で取り組むことで、個人のセキュリティを高めるだけでなく、より広範囲にわたってデジタルエコシステム全体の安定とセキュリティにも貢献します。

主な調査結果

調査データによると、サイバーセキュリティは依然として世界的に重要な問題であり、個人ではかなりの割合の人がオンライン詐欺やサイバー攻撃の被害に遭っています。また、サイバーセキュリティに関するユーザーの行動と認識の相違を明らかにするとともに、現在のセキュリティ施策の有効性やセキュリティの弱点のどこに対処すべきかについての知見も得られます。

サイバー脅威の蔓延

世界の回答者の半数以上が、過去1年間にオンライン詐欺やサイバー攻撃を経験したと答えています。

特に、4分の1以上 (26%) の回答者が偽の広告やオンライン景品の標的とされたことが注目されます。この攻撃手法が増加しているのは、世界的な景気後退が理由となっている可能性が高いでしょう。経済的に困窮している個人は、金銭的な救済や報酬を約束するオンライン詐欺に引っかかりやすい可能性があるからです。こうした傾向は、サイバー犯罪者がよく用いる手口に関する意識の向上と教育を緊急に行う必要性を浮き彫りにしています。

26%

もの回答者が偽の広告やオンライン景品の標的とされたことがあると回答

最も一般的な事例には、以下のようなものがあります。

偽の広告やオンラインプレゼント

フィッシング

スミッシング
(テキストによるフィッシング)

ヴィッシング
(電話によるフィッシング)

デバイスのアップデート状況

回答者の過半数は、デバイスを更新することに積極的であり、37%はアップデートが利用可能になり次第インストールし、35%は自動アップデートを有効にしています。

多くの人々が熱心にデバイスをアップデートしているのは心強いことです。それにもかかわらず、すぐにアップデートをしない人は知識不足、不便さ、パフォーマンスについての懸念などの障壁に直面しているという事実は、ユーザー教育を強化し、よりユーザーフレンドリーなアップデートの仕組みを導入することで、大きな効果が期待できることを示しています。

しかし、4分の1以上がアップデートを遅らせている主な理由には、以下のようなものがあります。

- アップデートについての知識がない
- 不便である
- パフォーマンスへの影響について懸念がある
- アップデートは重要でないと認識している
- デバイスストレージが不十分

KEEPER

パスワードの作成と管理

44%の回答者にとって、パスワード強度がパスワードを作成する際に考慮すべき重要な要素となっています。その他の要素としては、独自のパスワード作成手法を使用 (32%) やパスワードの覚えやすさ (31%) などがあり、世界のユーザーのほぼ3分の1が重視しています。しかし、ブラウザ内蔵パスワードマネージャーから推奨されるパスワードを使用している回答者は8%に過ぎず、パスワードマネージャーを使用してパスワードを生成しているのは12%に過ぎません。

驚くべきことに、パスワードの使い回しは危険な行為であると認識が広まっているにもかかわらず、41%が複数のアカウントでパスワードを使い回していることを認めています。.

パスワード変更の習慣については、30%が定期的にパスワードを更新していると回答しています。ウェブサイトからの要求に応じてパスワードを変更する人の割合はほぼ同じ割合 (29%) であり、28%はパスワードを忘れたときに変更し、8%はデータ漏洩後にパスワードを変更していると回答しています。

パスワードについてのこうした慣行は、引き続きサイバーセキュリティの大きな弱点になっています。パスワードを使い回したり、パスワード管理を記憶や物理的なメモに頼っていたりすることで、重大なセキュリティリスクに晒されることになります。多くの個人がパスワードのセキュリティと管理の堅牢さを信じているものの、実際の使用を見るとより良いツールと教育が急務であることは明らかです。パスワードマネージャーの利用を促進し、すべてのアカウントに強力でユニークなパスワードを作成し、その上で多要素認証 (MFA) が利用可能な場合は常に利用することで、こうしたリスクを大幅に軽減できる可能性があります。

41%

が複数のアカウントでパスワードを使い回していることを認めています

最も一般的なパスワード管理の方法は、以下の通りです

26%
記憶に頼っている

24%
書き留めている

19%
ブラウザや電話のメモアプリに保存している

パスワードの共有

パスワードの共有に関する世界の回答者からのフィードバックによると、回答者の半数以上 (61%) が以下のような方法を使用してパスワードを共有していることを認めています。

01 口頭または電話による

02 テキストメッセージまたはメッセージングアプリによる

03 書き留める

共有しがちなパスワードの上位5つは右の通りです。

銀行口座やクレジットカードのパスワードを共有していることを認めた人は、なんと15%にものぼりました。

パスワードの共有は、特にストリーミングサービスで一般的ですが、業界が最近この行為を取り締まっている事実を踏まえると、特に重要です。パスワードの共有は広く行われていますが、特にそれがパスワードの複数のアカウントでの使い回しなどの安全でない方法で行われた場合、かなりのセキュリティリスクをもたらします。パスワードマネージャーを使用してパスワードを安全に共有している回答者は7%に過ぎず、パスワード共有のベストプラクティスについて改善と教育が必要であることは明らかです。

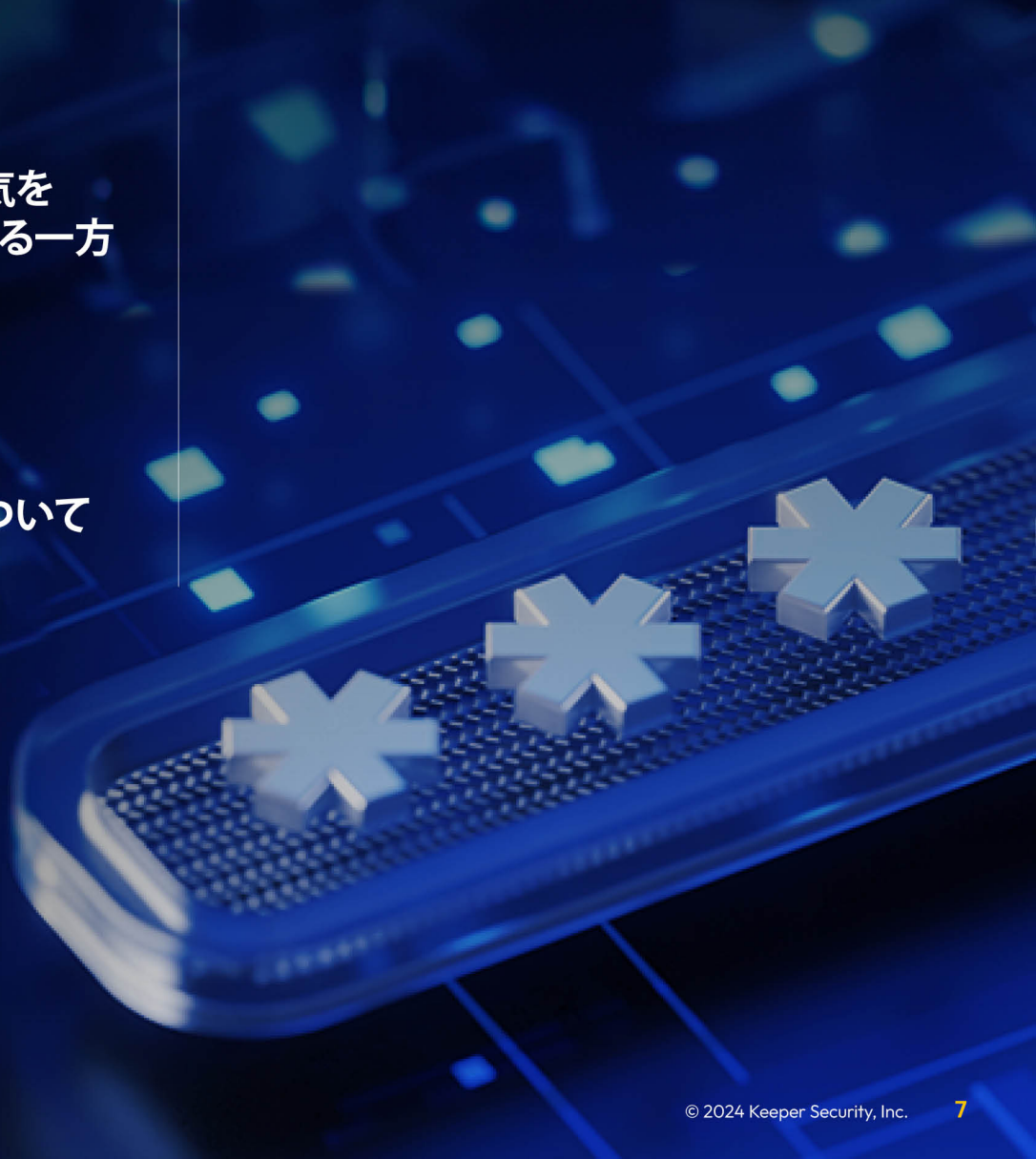
サイバーセキュリティへの信頼

85%
がパスワードは安全なものであると答えている

26%
がパスワードの習慣に気をつけていると回答している一方

13%
がパスワードの習慣について不注意である

特にパスワード管理に関しては、多くの人がサイバーセキュリティの施策を著しく過信しています。サイバーセキュリティに対するアプローチは多様で、一貫性がないことも少なくありませんが、回答者の85%がパスワードは安全なものであると答えており、83%がパスワードを適切に管理していると回答しています。さらに、回答者の過半数 (64%) がサイバーセキュリティのベストプラクティスの理解に自信があると回答しています。また、26%がパスワードの習慣に気をつけていると回答している一方で、13%がパスワードの習慣について不注意であったり、決まり悪く思ったりしていると回答しています。特に、ユーザーの62%が膨大なパスワード、アカウント、ログイン情報を管理することに懸念を抱いています。



結論

データからサイバーセキュリティにおける矛盾が明らかになっています。かなり多くの人々がサイバーセキュリティの知識と施策に自信を持っている一方で、サイバー攻撃や詐欺の被害に遭う人もまた絶えません。この矛盾は、知識だけではサイバーリスクを軽減するのに不十分であることを浮き彫りにしています。セキュリティのベストプラクティスの実践と厳格な遵守も同様に不可欠です。

この調査により、オンライン詐欺、フィッシング、偽の広告に関連するリスクについて、景気が悪くなって影響を受けやすい一般の人たちに向けて、もっと積極的に情報を伝えることが重要であることがわかります。同様に、セキュリティに関するアドバイスの適用を簡素化することが重要となります。例えば、使いにくさや知識不足といった問題を解決するために、もっと使いやすいデバイスの更新方法を開発して広めることが考えられます。

パスワードマネージャー利用の促進は、あまりに多くのパスワードやアカウントを管理することへの懸念を軽減する上で極めて重要です。こうしたツールを使うことで、簡単に強力でユニークなパスワードを作成したりMFAを使用したりできるので、パスワードの使い回しに伴う危険を防ぎ、安全にパスワードを保管できるようになります。

さらに、世界中のユーザーに対して、パスワードを安全でない方法で共有することのリスクについて啓発し、安全な代替手段を利用できるようにする必要があります。パスワードセキュリティの重要性を強調することは、サイバーセキュリティのレジリエンスを強化するために不可欠です。

Keeperのレポート「サイバーレジリエンスの強化: グローバルなサイバーセキュリティ慣行についての洞察」では、オンラインと職場の両方で、注意を要する場面で適切な行動が取れるよう人々を導く際にセキュリティ専門家が直面する課題が浮き彫りとなっています。

ユーザーの自信と意識の高さは称賛に値するものですが、行動面でも一貫して強化することが極めて重要です。ユーザーの行動面の問題点に対処し、教育や技術的な解決策を進めることで、サイバー攻撃やオンライン詐欺の脅威からの保護を強化できるようになります。

調査方法

このオンライン調査は、オーストラリア、ニュージーランド、シンガポール、インドネシア、日本、フランス、英国、米国、DACHの回答者6000人を対象とするもので、市場調査会社 OnePollにより、市場調査協会の規定に則って実施されました。この調査はOnePollの調査チームが監督、編集しました。OnePollは、MRSの企業パートナー、ESOMAR の企業メンバー、英国世論調査協議会のメンバーです。