BlackBerry
Intelligent Security. Everywhere.

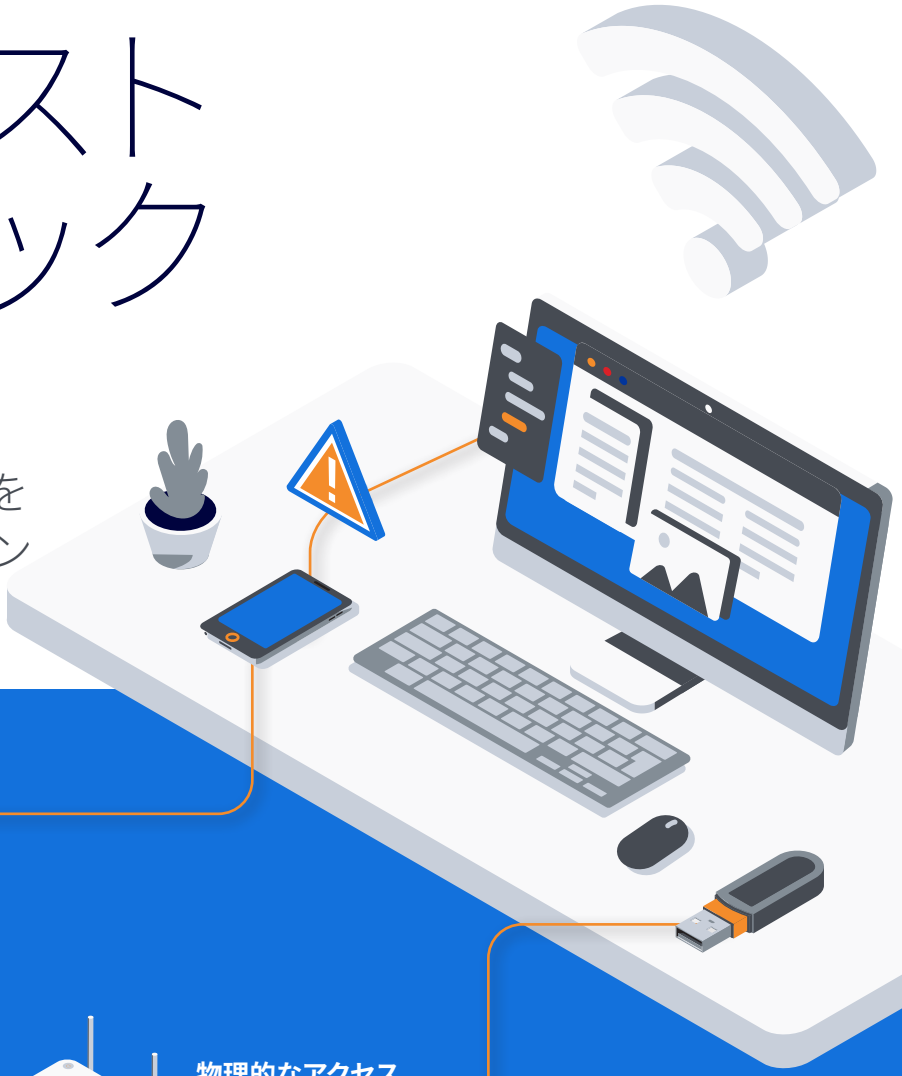
ホワイトペーパー

リモートワーカーのセキュリティのためのゼロトラストガイド

ゼロトラストプレイブックの手法を学んで
セキュアな在宅勤務を

ゼロトラストプレイブック

リモートワーカーは
ホームネットワークを保護し、
責任を持ってアプリケーションを
使用し、デバイスをロックダウン
する必要があります。



ソーシャルエンジニアリング

攻撃手法	ベストプラクティス
フィッシングメール	細心の注意を払う
サポート詐欺の電話	落ち着いて考える
偽のソーシャルメディアプロファイル	直感を信じる
偽の通知	

ワイヤレスインターフェイス

攻撃手法	ベストプラクティス
携帯電話ネットワーク	使用しないときは無効にする
Wi-Fi	デバイスを「削除」する
Bluetooth	パスワードを変更する

物理的なアクセス

攻撃手法	ベストプラクティス
USB メモリー	絶対に放置しない
ログイン済みアカウント	パスワードが有効なスクリーンロック
偽の通知	直感を信じる
USB 充電ケーブル	モバイルバッテリーを使用する

攻撃ベクトルに関するユーザーの意識向上

ここのところ、新型コロナウイルス（COVID-19）の感染拡大を受けて在宅勤務を行う従業員の数が増加しており、企業ネットワークが実質的に巨大化、分散化し、その保護は一層難しくなっています。

組織はゼロトラスト戦略とツールを実装して、モバイル従業員の増大が招くリスクの増加を軽減できると同時に、従業員自身も、適切なサイバー衛生を実践して絶えず注意を払うことによって、ゼロトラストプレイブックの手法を学ぶことができます。ゼロトラストセキュリティモデルとは、デフォルトで何も、誰も信頼しない戦略で、エンドユーザーはこれを採用することでセキュリティ水準を高めることができます。

リモートワーカーは、自身のセキュリティのためにも、毎日かなりの時間接続するであろう企業システムのセキュリティのためにも、ホームネットワークを保護し、責任を持ってアプリケーションを使用し、デバイスをロックダウンするのに必要な手段を講じなければなりません。

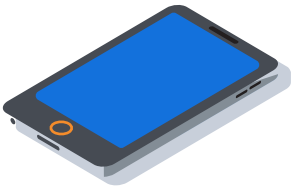
ホームネットワークで起きたことはすぐに企業に波及する可能性があります。特に、ベストプラクティスを遵守していなかったり、自宅内と企業ファイアウォール内の両方のセキュリティにどのような影響があるかを理解せずにアプリケーションを導入したりした場合にはなおさらです。

ゼロトラストセキュリティモデルでは、デフォルトで何も、誰も信頼しません。ゼロトラストセキュリティモデルの下では、すべてのユーザー、デバイス、ネットワークは検証されるまで敵対的であると想定され、その後もセキュリティ上の不備を防止するために継続的に検証されます。リモートワーカーは、そうではないことを証明できない限り、あらゆるものを潜在的な攻撃または侵害手段であると想定するゼロトラストの概念を適用することができます。

このホワイトペーパーは、リモートワーカーがいくつかの簡単なステップによって在宅勤務時のセキュリティ水準を向上させるための入門書として役立ちます。

攻撃ベクトルに関するユーザーの意識向上

攻撃者はさまざまな手段を利用して標的を感染させます。多くの場合、攻撃では以下に挙げるような戦術が 1 つ以上利用されるため、ゼロトラストのアプローチが不可欠です。該当する場合には本書内でさらに詳しく説明しますが、まず攻撃ベクトルに関する一般的な意識向上から始めましょう。



ソーシャルエンジニアリングにはさまざまな形態があり、悪意のあるフィッシングメールやサポート詐欺の電話から、偽のソーシャルメディアプロファイル、信頼できる組織から送信されたように見せかけた偽の通知にまで及びます。

ソーシャルエンジニアリング

ソーシャルエンジニアリングは、人間の性質という、軽減が難しい脆弱性の 1 つに付け込みます。ソーシャルエンジニアリングにはさまざまな形態があり、悪意のあるフィッシングメールやサポート詐欺の電話から、偽のソーシャルメディアプロファイル、信頼できる組織から送信されたように見せかけた偽の通知にまで及びます。私たちには生来、何かが本物のように見えればそれをそのまま信頼してしまう傾向があります。この判断は常に正しいとは限りません。攻撃者は、この性向を利用しようとします。

ソーシャルエンジニアリング活動の犠牲になる可能性を減らすための最善のアドバイスは、単に、行動する前に立ち止まって考えることです。ソーシャルエンジニアは、標的となるユーザーが集中していなかったり、ユーザーが細心の注意を払って行動していなかったりすることを期待しており、その攻撃は、宅配便の通知メール内のリンクをクリックするよう求めるプロンプトなど、日常業務を模していることがほとんどです。

落ち着いて、何かおかしいところがないか、兆候を探してください。何か怪しいと感じたなら、自分の直感を信じてください。行動を起こすことにプレッシャーを感じないようにしましょう。そして確信が持てないなら、行っている作業を止めて、IT セキュリティチームに連絡して支援を求めてください。ソーシャルエンジニアリングはさまざまな攻撃の 1 つの側面に過ぎないため、該当する場合は以下のセクションで他のリスク緩和ガイダンスを参照することができます。

デバイスへの物理的なアクセス

保護されていないデバイスに物理的にアクセスできる攻撃者は、悪意のあるソフトウェアをインストールしたり、アカウントを乗っ取ったりすることができます。このために用いられる方法としては、USB メモリーのようなリムーバブルストレージデバイスを差し込む、オンラインの場所から悪意のあるプログラムをインストールする、ユーザーが既にログインしているアカウントにアクセスするなど、さまざまな方法があります。

最善のアドバイスは、ごく短時間であったとしても絶対にデバイスを放置しないこと、そしてオフィスや自宅のような信頼できる環境にいても常に、自動タイムアウトを設定し、パスワードを有効にしたスクリーンロック機能を使用することです。

アプリケーションの脆弱性の悪用

デバイスに存在するアプリケーション内の脆弱性を悪用してリモートアクセスが取得される可能性があります。未知の脆弱性やパッチ未適用の脆弱性に対してできることは限られていますが、デバイスにインストールされているオペレーティングシステムとすべてのソフトウェアを完全に更新するよう徹底することができます。

最適な保護のため、OS とソフトウェアの自動更新を有効にして、新しいバージョンがいつ出るかを常にチェックしなくても済むようにしてください。そうすれば、利用可能になり次第、パッチを確実に受け取ることができます。

また、使用していないときはアプリを閉じてください。実行されていなければ、攻撃者が脆弱なアプリケーションを利用できる可能性が下がります。これには、閉じているように見えても実際にはバックグラウンドで実行されているアプリも含まれます。モバイルデバイスにまだアプリキラーをインストールしていない場合は、適切なプログラムを入手して、アプリを終了したいときに実際に終了されるようにしてください。これによって、バッテリーの寿命が大幅に向上する可能性もあります。

ただし、これはせいぜい表面的な解決策であることに注意してください。十分なシステム特権を持つ攻撃者であれば、アプリの終了後もアプリを実行することができます。本書の後半で、日常的に使用するデバイスで管理者特権が有効になっていないユーザープロファイルを作成し、攻撃者がそのような特権を利用できないようにすることがなぜ重要なのかについて説明します。また、既知の脆弱性と未知の脆弱性の両方の悪用を防止できるエンドポイント保護ソリューション一式をデバイスにインストールします。

悪意のあるアプリと過剰な権限

検証されていないサードパーティ Web サイトからダウンロードした悪意のあるアプリケーションや脆弱なアプリケーション、さらには正規のアプリストアに存在する一部のアプリケーションも、攻撃者によってデバイスの侵害目的で利用される可能性があります。繰り返しますが、ここでもアプリケーションをダウンロードする前に立ち止まって考えてください。最初に一般使用者によるアプリの評価を確認するのは良いことですが、アプリケーションのセキュリティを判断するという点では、必ずしも信頼できるものではありません。

セキュリティにおける一般的な経験則は、デバイスを脱獄してはならないというものです。この意味がわからないなら、心配する必要はありません。また、ダウンロードする前に、アプリケーションが要求する権限を確認してください。懐中電灯アプリが本当にカメラやマイク、メッセージ機能、連絡先にアクセスする必要があるでしょうか？恐らくありません。

ここでも、もし確信が持てないなら、操作を止め、IT セキュリティチームに連絡して支援を求めてください。また、デバイスに包括的なエンドポイント保護ソリューションがインストールされていることを確認してください。

悪意のある Web サイトと侵害された Web サイト

攻撃者によって制御されている Web サイトにアクセスした場合、感染が起きる可能性があります。このような攻撃は、その活動の性質に応じて「ドライブバイ」攻撃や「水飲み場型」攻撃と呼ばれることがよくあります。ほとんどの人は、普段の Web サーフィンのリスクやマルウェアに感染する可能性については理解していますが、正規のサイトであっても、侵害されていたり、悪意のある広告ライブラリをホストしていたりすれば、デバイスに感染する可能性があるということは理解していません。

感染防止のためにできることがいくつかあります。たとえば、ブラウザが最新バージョンに更新されていることを確認する、正規の広告ブロックプログラムをインストールする、リスクを伴う Web サーフィン行動に関わらないようにして適切な判断を下す、などです。もう一度繰り返しますが、ここでも堅牢なエンドポイントセキュリティソリューションをデバイスにインストールしておくと、間違いなく効果があります。

USB 充電ケーブルを介した感染

侵害された充電ステーションや PC に USB ケーブルでモバイルデバイスを接続すると、マルウェアの感染につながる恐れがあります。どうしても充電が必要で、充電しなければ動作するデバイスがなくなると考えるかもしれませんが、それはまったくの間違いです。リスクのある公共の充電ステーションに頼るよりも優れた代替手段が存在します。個人用のポータブル充電器は安価で、バックパックや自動車の小物入れに入れて容易に持ち運ぶことができます。

自分で持ち歩いていなくても、信頼できる友人が持っているかもしれません。最悪のシナリオでは、ただコンセントを見つけて、そこに直接つないで短時間充電しなければならない場合もあります。USB ケーブルは電力供給とデータ交換を目的として設計されているため、USB 接続を使用して充電を行う場合は常にリスク要素がありますが、USB ポートではなくコンセントに接続すればリスクが下がることに注意してください。万一電源に悪意がある場合でも、優れたエンドポイントセキュリティソリューションであれば追加の保護を提供できます。

...Bluetooth で接続するデバイスのデフォルトのパスワードと PIN を変更し、使用しなくなったデバイスと Wi-Fi を削除する ...

ワイヤレスインターフェイスを介した攻撃

ワイヤレスインターフェイス機能があるデバイスは、携帯電話ネットワーク接続、Wi-Fi、Bluetooth、または近距離無線通信（NFC）を介して攻撃を受ける可能性があります。これはいかなる形態の接続にも存在するリスクの性質です。これらの機能の中には、接続されていなくても有効になっていれば接続をスキャンするものがあり、このスキャン中に、攻撃に利用可能なデバイスの情報が公開される可能性があります。そのため、使用しないときは完全に無効にすることをお勧めします。

さらに、Bluetooth で接続するデバイスのデフォルトのパスワードと PIN を変更し、使用しなくなったデバイスと Wi-Fi を削除するほか、自動接続機能を有効にしていないことを確認する必要があります。また、NFC は非常に短距離でしか接続できませんが、その接続はセキュアではないため、使用しないときはオフにしておくようにしてください。

最後に、自身で制御できないものには一切接続しないことをお勧めします。親しい友人の Wi-Fi は例外かもしれませんが、その友人がセキュリティに精通しておらず、ネットワークをロックダウンしていない場合は、それでさえリスクがあります。よくあることですが、利便性はセキュリティにとって悩みの種であり、ある機能がデバイスで利用できるからといって、その機能がセキュアであるという意味では決してありません。ここでの最善のアドバイスは、使用しないときはオフにするということです。

悪意のあるコード

デバイスに感染するマルウェアの種類によっては、攻撃者は、所有者がデバイスで実行できることはほぼすべて実行でき、場合によっては所有者よりもはるかに多くの操作を実行できます。スパイウェアのような悪意のあるコードは、電話の通話や、会話などの他の音声を録音したり、キーストロークを記録してログイン認証情報などの情報を盗んだりすることができます。さらに、テキストメッセージを読み取り、それを使用して多要素認証を破ることができるスパイウェアもあります。

リモートアクセス型トロイの木馬（RAT）を使えば、攻撃者はデバイスの制御を完全に掌握し、デバイスの設定を変更したり、スクリーンショットを撮ったりすることができます。また、ユーザー本人になりすまして、ネットワーク内の他のデバイスを感染させることもできます。メール、ソーシャルメディア、テキストアプリにアクセスできれば、連絡先に含まれるユーザーを簡単に騙して本人からの連絡だと思い込ませることができます。

マルウェアでは、一般的なプライバシー上の懸念も生じます。特に、そのマルウェアによって攻撃者がユーザーの個人的なメール、テキストメッセージ、留守番電話、チャットアプリケーションのコンテンツ、および通話履歴にアクセスできるようになる場合は深刻です。さらに、位置データ、閲覧履歴、写真やビデオなどの保存されたメディア、機密の個人データ、さらにはデバイスを仕事に使用している場合には企業データさえも取得できるマルウェアもあります。

最後になりましたが、ランサムウェアがあります。マルウェアはすべて悪質ですが、その中でもランサムウェアはいくつかの点で恐らく最も悪質です。デバイスに感染すると、ランサムウェアはすべてのデータを暗号化した上で、通常はデバイスの所有者に対し、データを復元するための復号化キーの入手方法を指示するメッセージを生成します。しかし多くの場合、それと引き換えに非常に高額の身代金（ransom、ランサム）を要求します。そのため、ランサムウェアという名前で呼ばれます。

データを回復するために身代金を支払うかどうかの判断はデバイスの所有者にかかっていますが、身代金を支払うことについては賛否両論があり、どちらも固有のリスクを伴います。身代金を支払っても、データを取り戻すことができなかったり、将来さらなる支払いを要求されたりする可能性があります。支払わなかった場合は、デバイス上のすべてのものを失う恐れがあります。最善の緩和策は、できればランサムウェアにまったく感染しないことであることは明らかです。

ここでもセキュリティについて同じことが言えます。多くの問題は同じプロアクティブなアプローチによって解決でき、マルウェアもそうした問題の 1 つであるからです。つまり、オペレーティングシステムとソフトウェアを最新の状態に保ってパッチを適用すること、リスクのあるオンライン行動には関わらないこと、デバイスを放置しないこと、予防措置を講じずにメールに含まれるリンクをクリックしたり添付ドキュメントを開いたりしないことなどです。

しかしマルウェアに関して言えば、最善の対策は、デバイスで次世代のアンチウイルスソリューションを確実に実行することです。なぜ次世代なのでしょうか？ シグネチャベースのアンチウイルスは既知の脅威のみに対して保護する時代遅れのアプローチであり、新しい脅威に対しては保護しません。この点については後で掘り下げて説明します。

Web サイトが、リスクが高いか悪意があると評価されている場合、ユーザーに通知してくれるブラウザもあります。これらの警告に従って、そのようなサイトを避けることをお勧めします。

Web セキュリティの向上

攻撃手法	ベストプラクティス
リスクのある閲覧行動	控える
トレントでのメディア、音楽、映画のダウンロード	Web トレントを避ける
賭博サイト	リスクのあるサイトを避ける
短縮 URL	正規の URL 短縮
自動ダウンロード	自動ダウンロードをすべて無効にする

ここで「Web セキュリティの向上」と言う場合、その意味は、インターネットに接続し、使い慣れたサイバースペースの素晴らしい機能をすべて実行しながら、自身とそのデバイスを保護するということです。くどいようですがここでも、使用しないときにはデバイスをオフにし、ゼロトラストアプローチを適用してください。

リスクのある閲覧行動

デバイスの侵害リスクを大幅に減らすためにすべてのユーザーが実行できる最も簡単な対策の 1 つは、リスクのある Web 閲覧行動を控えることです。このためには、攻撃で悪用されることが多い Web サイトのタイプを認識し、可能であればそのような Web サイトを避ける必要があります。成人向け Web サイトに関係する最もリスクの高い閲覧行動についてはここで過度に強調する必要はないでしょうが、攻撃で使われることが多い Web サイトのタイプはほかにもたくさんあり、特に在宅勤務時にホームネットワークのセキュリティを保つという観点から見た場合、ユーザーはこれらに気付いていない可能性があります。

このようなサイトには、ユーザーが音楽や映画などのメディアをダウンロードできる Web トレントや、ソーシャルメディアでよく宣伝されている、アンケートやその他の目新しい「Gotta-see-this（ちょっとこれ見て）」とい誘い文句を含むサイト、賭博サイト、ポップアップが過剰に表示されるサイト、低俗なゴシップやニュース記事を勧めるサイトなどが含まれます。インターネットには悪意のある Web サイトが大量に存在することに加え、ユーザーは、人気のあるゲーム Web サイトやニュースサイト、エンターテイメントサイトなどの正規の Web サイトでさえ、マルウェアを拡散するために使用される場合があることを認識する必要があります。

閲覧するサイトを選択する際には注意を払い、デバイスでファイアウォールを有効にしている必要があります。また、セキュリティソフトウェアが有効になっていて最新の状態であること、またブラウザも最新の状態であり、セキュリティ機能が有効になっていることを確認する必要があります。ポップアップをクリックしないようにし、直感を信じてください。何かおかしいと感じたなら、恐らくそうなのです。「話がうますぎると思ったときは、恐らくそうなのである」という古いことわざは、ここでも当てはまります。

デバイスの侵害リスクを大幅に減らすためにすべてのユーザーが実行できる最も簡単な対策の 1 つは、リスクのある Web 閲覧行動を控えることです。

自動ダウンロードをすべて無効にする

これをさらに一歩先に進めて、オンライン時にさらに保護を強化するには、アプリケーションとブラウザで、画像、音声、ビデオ、ドキュメントファイルなど、すべてのメディアファイルの自動ダウンロードを無効にすることができます。データの転送に関係する何らかの処理を自動的に実行するよう設定している場合は、常にリスクが高まります。繰り返しますが、利便性はセキュリティにとって悩みの種です。

ソーシャルメディアフィードをスクロールして、面白そうなコンテンツをすべてクリックするのは楽しいことですが、自らを危険にさらす可能性があることを知っておかねばなりません。リスクが高くても構わないと考えるかもしれませんが、そのデバイスを仕事に使用している場合、会社をもリスクにさらしていることを認識する必要があります。組織のセキュリティポリシーを調べて、それに準拠していることを確認し、もし理解できないことがあるなら、セキュリティチームに説明してもらってください。

短縮 URL とドキュメントの確認

短縮 URL は、文字数制限のある Twitter などのソーシャルメディアサイトで特に人気がありますが、リンクの正確な転送先がすぐにはわからないため、ユーザーにとって潜在的な問題になります。さらに、ブランディングされたバニティ URL を作成するために使用されるカスタム URL 短縮ツールは、短縮されていない正当な URL のように見えるものの、実際には悪意のある Web サイトに転送するリンクを作成する目的でも使用できます。短縮 URL の大部分は恐らく悪意のあるものではありませんが、悪意のある短縮 URL をクリックしないように用心する必要があります。

多くの場合、マウスカーソルを短縮 URL に合わせると、クリックする前にその接続先のパスを表示することができます。正当な URL 短縮ツールであれば、通常はそのツールで作成された URL を短縮解除する手段が用意されています。また、URL 短縮解除サイトも多数存在します。どちらを使用した方が良いかについて組織のセキュリティチームに相談するか、特定のツールを選択する前に自身で入念に調査することをお勧めします。

アンチウイルススキャナーのデータに照らして URL をチェックする無料のツールも提供されており、これらを使えば、その Web サイトが悪意があるものかどうかや、マルウェアの配布に使用されているかを明らかにすることができます。これらのサービスの中には、ファイルとドキュメントをアップロードしてスキャンし、汚染されているかどうかを特定できるものもあります。

この場合も、ツールを使用する前に組織のセキュリティチームに問い合わせて推奨事項を確認してください。分析目的でこれらのツールにドキュメントを送信することは、データの取り扱いに関する企業のポリシー、機密保持契約、または規制要件に違反する可能性があるため、必ず最初に専門家のアドバイスを求めるようにしてください。エンドポイントセキュリティソリューションも、悪意のある URL やスプーフィングされた URL を介した攻撃からの保護に役立ちます。

アンチウイルススキャナーのデータに照らして URL をチェックする無料のツールが提供されており、これらを使えば、その Web サイトが悪意があるものかどうかや、マルウェアの配布に使用されているかを明らかにすることができます。

SSL/HTTPS と Web サイトのセキュリティ

かつては、暗号化接続を提供してセキュリティベストプラクティスに従っているサイトは、機密情報を交換する銀行や e コマースサイトなど、一部の Web サイトに限られていました。現在では、機密情報が関係するかどうかに関係なく、単にユーザーを攻撃から保護するという理由から、すべての Web サイトにこれらのベストプラクティスを導入すべきです。

Web サイト（特に上記のような機密情報の交換に関係する Web サイト）にアクセスする場合は、URL アドレスバーに「HTTPS」や鍵アイコンが表示されていることを確認し、その Web サイトではすべてのトラフィックが SSL（Secure Socket Layer）で暗号化されていることを確かめる必要があります。SSL は、サーバーとクライアント間の接続が確実に暗号化されるようにします。

つまり、ユーザーがどのようなアクティビティに関与するかに関係なく、Web サイトでセッション全体を暗号化しないもっともな理由はありません。また、この基本レベルのセキュリティが提供されていない場合、そのサイトには関わらないようにすることをお勧めします。ときどき、ある Web サイトのセキュリティ証明書の有効期限が切れているという警告が表示されることがありますが、これもそのサイトに関わらない方が良い理由となります。最も人気の高いいくつかのブラウザでは、Web サイトがセキュアでない場合は警告が表示されるのが一般的です。

Web サイトが、リスクが高いか悪意があると評価されている場合、ユーザーに通知してくれるブラウザもあります。これらの警告に従って、そのようなサイトを避けることをお勧めします。安全でない Web サイトを自動的にブロックする DNS フィルタリングを提供するツールやサービスも利用できます。組織のセキュリティチームに問い合わせて、推奨される DNS フィルタリングオプションを確認してください。ただし、前述の「リスクのある閲覧行動」のセクションで述べているように、自身やその家族がよく利用していたサイトが、悪用された履歴があるためにブロックされる場合がある点に注意してください。

... ユーザーがどのようなアクティビティに関与するかに関係なく、Web サイトでセッション全体を暗号化しないもっともな理由はありません。また、この基本レベルのセキュリティが提供されていない場合、そのサイトには関わらないようにすることをお勧めします。

メールのセキュリティと意識向上

攻撃手法
フィッシングとスピアフィッシング
ベストプラクティス
リンクをクリックしない
信頼されていない添付ファイルを開かない
画像の自動ダウンロードを無効にする
知らない人からの未承諾メールを開かない
スペルや文法の誤りに注意する

メールは主要な攻撃ベクトルの 1 つで、メールのセキュリティに関して注意を怠らないことがどれほど重要かということは、いくら強調してもしすぎることはありません。ここでも再びゼロトラストの考え方が重要になります。私たちエンドユーザーは、メールを使って日常的な連絡（多くの場合は膨大な連絡）を行うことに慣れすぎているため、気が緩みがちです。攻撃者はそこに付け込んで攻撃を成功させるのです。

フィッシングとスピアフィッシング

恐らく私たちのほとんどは、フィッシングキャンペーンに加担しているスパムメールがもたらすリスクを認識しています。要するに、フィッシングはソーシャルエンジニアリング（前述）の一形態で、攻撃者は受信者を騙して機密情報を開示させたり、マルウェアを実行させてデバイスや接続ネットワークを感染させたりしようとします。

スピアフィッシングは、標的に関係する部外秘の情報や固有の情報を利用することによってフィッシングのレベルを一段階引き上げ、攻撃の成功確率を大幅に向上させます。この場合、信頼できる正当な送信者から送信されたように見せかけるために細工されたスプーフィングメールが使用されることもあります。個人用または企業のメールアカウントが侵害されることもあり、その場合、メールは見かけ上、実際に信頼できるソースから送信されているように見えます。

フィッシングメールには、マルウェア感染につながる悪意のあるリンクや汚染されたドキュメントが含まれることもあれば、Web サイトへのアクセス方法のみが記載されていることもあります。このようなサイトは正当なサイトのように見えますが、攻撃者によって制御されており、標的となるユーザーはアカウント認証情報や他の機密情報を入力するよう求められます。

メール攻撃からの自衛方法

以下に、一般的なメール攻撃から自衛するためのガイドラインを示します。これは決してすべてを網羅したリストではないことに注意してください。より詳細なセキュリティ意識向上トレーニングを受ければ、すべてのユーザーにメリットがあります。どのようなリソースが利用できるかについては、組織のセキュリティチームに確認してください。また、セキュリティに関しては常にそうであるように、行動する前に落ち着いて考えてください。

メールの送信者を確認します。いくつかのフィッシングメールは、実在する組織の URL に似せた URL（たとえば「cdc.gov」の代わりに「cdc-gov.org」など）を使用して、正当な送信者に見せかけた攻撃者から送信されていました。メールはすべて潜在的に悪意があるものとして扱い、用心することをお勧めします。また、正当なメールアドレスでさえも侵害されている可能性があることを覚えておいてください。

- **リンクをクリックしない：**リンクにマウスカーソルを合わせるとアクセス先のアドレスを表示できますが、ベストプラクティスとして、信頼できる URL をブラウザに直接入力するだけにし、メール内のリンクは決してクリックしないようにします。信頼できるソースからのメールのように見えても、同じように対応します。
- **信頼されていない添付ファイルを開かない：**添付ファイルに注意してください。送信者に見覚えがない場合や、疑わしいメールに見える場合には特に用心します。悪意のある添付ファイルが送られてきた場合に備えて、そのようなファイルから保護できるエンドポイント保護ソリューションが実行されていることを確認します。
- **画像の自動ダウンロードを無効にする：**メールに悪意のあるコードが含まれていて、メールを開くだけでデバイスに感染する場合があります。信頼できる確認済みのソースからのみ画像をダウンロードすることをお勧めします。
- **知らない人からの未承諾メールを開かない：**このようなメールはスパムフォルダに移動して、侵害リスクを冒さないようにすることをお勧めします。不明なソースからの未承諾メールによって重要な連絡が行われることはめったにありません。
- **スペルや文法の誤りに注意する：**これらは、詐欺やメールベースの攻撃を示す危険信号です。「Dear Sir」のような一般的な挨拶や、「Dear Beloved」のような過度に私的に見える挨拶にも気を付けてください。これらもほぼ確実に悪意があることを示す兆候です。
- **即時の行動を要求したり、個人情報、パスワード、またはログイン認証情報を要求したりするメールを避ける：**多くの場合、攻撃者は標的に切迫感を植え付け、判断を誤らせようとします。

メールのセキュリティを確保するために組織でどのようなツールが提供されているかと、自身とその組織を保護するためにそれらのツールを効果的に使用する方法について、組織に確認してください。堅牢なエンドポイントセキュリティソリューションが、リストの上位に来るべきです。

メールのセキュリティを確保するために組織でどのようなツールが提供されているかと、自身とその組織を保護するためにそれらのツールを効果的に使用する方法について、組織に確認してください。堅牢なエンドポイントセキュリティソリューションが、リストの上位に来るべきです。

ホーム ネットワークの セキュリティ

攻撃手法	ベストプラクティス
ホーム Wi-Fi ルーターのセキュリティ モデムのセキュリティ	• デフォルトのパスワードを変更する • ファームウェアを更新する • 可能な場合は自動更新を有効にする

ホームネットワークのセットアップは比較的簡単ですが、ネットワークを確実に保護するには、実際にはユーザーの側でかなりの手順を踏む必要があります。ホームネットワークを適切に保護することは、ユーザーを攻撃から保護するだけでなく、攻撃が企業ネットワークに及ばないようにする上でも非常に重要です。リモートワーカーの急増により、このリスクが大幅に増加しています。

このセクションでは、ホームネットワークを保護するために対処する必要のある主要項目をゼロトラストの観点からいくつか取り上げます。ただしここでも、これは包括的なガイドラインではありません。特に在宅勤務で企業ネットワークに接続するユーザーは、組織のセキュリティチームに問い合わせて組織のガイドラインとプロトコル一式を確認し、セキュリティとデバイス使用に関するポリシーに準拠する必要があります。また、このガイドで概説する他のベストプラクティスに従って、攻撃の被害に遭うリスクを軽減する必要もあります。

ホーム Wi-Fi ルーターのセキュリティ

ホーム Wi-Fi ルーターのセットアップの大部分は簡単なプロセスで、開梱して接続すればすぐに使用できます。また多くの場合、セットアップはインターネットサービスプロバイダー（ISP）によって実行済みです。しかし、ルーターを保護するために必要なステップが一部守られていない可能性があるため、以下に挙げる手順が実行されているかどうかを再確認することをお勧めします。

まず、ルーターのデフォルトの管理者パスワードを変更してください。このようなデバイスは通常、すべての製造デバイスに同じパスワードが設定されて出荷されるためです。さらに、必ず固有の SSID 名をネットワークに付けてください。また、デバイスが最新バージョンに更新されていることを確認し、自動更新オプションがある場合は有効にしてください。自動更新オプションを使用できない場合は、更新が利用可能かどうかを定期的に確認するためのリマインダーを設定してください。

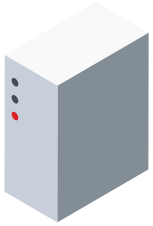
スマートテレビ、プリンター、自宅にあるインターネットに対応したその他の接続デバイスなど、ルーターに接続するありとあらゆるデバイスのデフォルトのパスワードを変更することもお勧めします。デバイスのセットアップ時に Wi-Fi に接続する必要がある場合は、デフォルトのパスワードが設定されている可能性が高いため、変更する必要があります。また、すべての接続デバイスでユニバーサルプラグアンドプレイ（UPnP）をオフにしてください。これはネットワーク上のすべての接続デバイスが互いを検出するのに便利な機能ですが、ホームネットワークの範囲内に好ましくないデバイスがある場合、そのようなデバイスによる接続に対して脆弱になります。

Wi-Fi ルーター自体については、接続を暗号化して、ルーターおよび共有データのセキュリティとプライバシーを強化することが重要です。WPA2 ／ WPA3 暗号化標準は、WEP ／ WPA よりもはるかに強力なセキュリティを提供するため、そちらを使用するようにしてください。その方法がわからない場合は、ISP の技術サポートに問い合わせます。ISP から提供されたデバイスではない場合は、デバイスを購入した店舗の技術サポートに問い合わせます。

また、MAC アドレスフィルタリングを有効にして、保護レイヤーを追加します。すべてのデバイスには固有の MAC アドレスが割り当てられているため、MAC アドレスフィルタリングを使用して、承認していないデバイスがネットワークに接続するのを防止します。また、ルーターのファイアウォールが有効になっていて、適切に構成されていることを確認します。Mac または PC にはファイアウォールが組み込まれていますが、ホームネットワークに接続されている他のスマートデバイスには恐らくファイアウォールがないため、ワイヤレスルーターのファイアウォールは重要な防御レイヤーです。これによって、ある朝目覚めたらスマート冷蔵庫がボットネットの一部になっていて、サービス拒否攻撃や大規模なスパムメール活動に関与していたというような事態が起きないようにします。

モデムのセキュリティ

ホームネットワークの Wi-Fi トラフィックはすべてルーターを経由しますが、ご利用の ISP でモデムが必要な場合（インターネット接続も提供するほとんどのケーブルテレビ会社でよくあるケースです）、トラフィックの大半はルーターの後にモデム経由でルーティングされることに気付いていないかもしれません。したがって、モデムも同様に保護する必要があります。その方法はメーカーによって異なり、同じメーカーでもモデルによって異なる場合がありますが、一般的には、暗号化のステップを除いてルーターと同じ対策を行います。つまり、デフォルトのパスワードを変更し、ファームウェアを更新し、可能であれば自動更新を有効にします。セットアップ手順にはセキュリティのためのステップがあるはずですが、なければ ISP に詳細を問い合わせる必要があります。



スマートテレビ、プリンター、インターネットに対応したその他の接続デバイスなど、ルーターに接続するありとあらゆるデバイスのデフォルトのパスワードを変更することをお勧めします。

デバイスとアカウントのセキュリティ

攻撃手法	ベストプラクティス
デバイスのセキュリティ	• デバイスを放置しない • 自動タイムアウトを有効にする • 強力なパスワード • 多要素認証（MFA）を選択する • パスワードマネージャー • 使用しないときは Wi-Fi、Bluetooth、および NFC を無効にする • すべてのデバイスが次世代のアンチウイルスソリューションを実行できることを確認する

このガイド全体に共通するテーマは、ユーザーは自身がデバイス上で関与するアクティビティに関して予防策を講じ、攻撃の被害者になるリスクを軽減する必要があるということです。これはゼロトラストの思考様式を適用する際の主要な戦略です。とはいえ、私たちが攻撃を受けやすい大きな要因は、好奇心から不注意まで、人間の純粋な性質にあります。したがって、ユーザーが確実にベストプラクティスに準拠し、デバイスとアカウントに対するリスクの軽減を目的に設計された機能とツールを活用することが重要です。以下に、デバイスのセキュリティを維持するために実行できるステップをいくつか示します。

デバイスのセキュリティ

デバイスを放置しないようにし、スクリーンロック機能を常に有効にして、デバイスにアクセスするには PIN やパスコードが要求されるようにしてください。また、別の作業で注意がそれてデバイスをロックし忘れた場合のために、自動タイムアウトを有効にし、短時間使用しない場合にデバイスをロックすることもお勧めします。

アカウントのアクセスに強力なパスワードを設定するほかに、多要素認証（MFA）オプションが利用可能な場合は常にこのオプションを選択してください。MFA を強力なパスワードと組み合わせても絶対的なセキュリティが提供される訳ではありませんが、不正使用のリスクが大幅に下がります。

パスワードマネージャーも優れた代替策です。パスワードマネージャーを使えば、ユーザーは推測しにくい強力なパスワードでアカウントを保護しながら、覚えるのは 1 つのパスワードだけで済むからです。その 1 つのパスワードには、大文字と小文字、数字、および特殊文字を組み合わせた長くて強力なパスフレーズ（32 文字以上）を推奨します。通常、パスワードマネージャーでは MFA が提供されており、これも強く推奨します。パスワードを再利用しないでください。また、いかなる理由があってもパスワードを共有しないでください。

ノートパソコンやデスクトップのようなデバイスの場合、ユーザープロファイルを 2 つセットアップして、1 つは管理者特権を持たない日常使用向けとして使用し、もう 1 つは管理者特権を持ち、デバイスやソフトウェアのメンテナンスタスクのために管理者特権が必要な限定的な状況で使用することをお勧めします。昇格された特権を持たないプロファイルでデバイスを使用することで、攻撃者がデバイスを完全に乗っ取る可能性を減らすことができます。

このガイドの前のセクションで説明したように、使用しないときは Wi-Fi、Bluetooth、および NFC を無効にし、特に旅行時にはサードパーティ製アプリからログアウトすることをお勧めします。可能であれば、旅行期間中には必要ないサードパーティ製アプリをアンインストールします。また、ユーザーが持ち運ぶデバイスにはディスク全体を暗号化するソリューションをインストールすることを強くお勧めします。そうすることで、デバイスの紛失または盗難時にも機密データを保護することができます。

デバイスに最新のオペレーティングシステムとソフトウェア更新プログラムがインストールされていることを確認し、可能な場合には自動更新を有効にしてください。サードパーティ製アプリに知らない連絡先を追加したり、未承諾メール内のリンクをクリックしたりしないでください。常にブラウザに直接 URL を入力して、目的の Web サイトに確実に移動するようにしてください。また、会社での連絡やファイル共有に、個人的にインストールしたアプリケーションやサードパーティ製アプリケーションを使用しないでください。承認されているコラボレーションおよびコミュニケーションソフトウェアについては、組織に問い合わせてください。

次世代のアンチウイルスソリューションを実行できるすべてのデバイスに、ソリューションがインストールおよび更新されていることを確認します。次世代のソリューションは、既知の攻撃のみを防御できる時代遅れのシグネチャベースのアンチウイルス製品よりも包括的な保護を提供します。また、デバイスがランサムウェアに感染した場合に備えて、重要なファイルの自動バックアップ／復旧機能がデバイスにあることを確認してください。デバイスの紛失または盗難時にもバックアップは重要です。また、デバイスの位置を特定したり、紛失したデバイスからデータをリモートワイプしたりできる機能があれば、情報漏洩対策のレベルをさらに引き上げることができます。

昇格された特権を持たないプロファイルでデバイスを使用することで、攻撃者がデバイスを完全に乗っ取る可能性を減らすことができます。

企業ネットワークへのセキュアな接続

分散した大規模な従業員を組織がサポートしていて、その従業員が管理対象デバイスと非管理対象（BYO）デバイスを組み合わせて勤務している可能性がある場合、企業のネットワークにセキュアに接続することは非常に重要です。従来の接続方式は、想定されているほどセキュアではない可能性があります。ここでも、ゼロトラストアプローチからヒントを得ることが重要です。

VPN のリスク

VPN によって従業員は組織のネットワークに便利な方法で簡単に接続できますが、このテクノロジーのセキュリティ上の制限による欠点が急速に明らかになりつつあります。トンネリングプロトコルが古く、トラフィックが IPv4 接続経由でルーティングされることによる IPv6 漏洩などの脆弱性のため、複雑な VPN 分散環境やパッチ適用の問題をサポートするために必要なリソースが増大しています。また、多要素認証に対応していないことから、接続を VPN に依存している組織ではリスクが増加する可能性があります。

さらに、一般的に BYO デバイスに VPN を使用するのはお勧めできません。適切な ID およびアクセス管理と、多要素認証を使用するとしても、VPN 経由で企業のシステムに接続すると、企業ネットワーク全体に対してかなりのレベルのアクセスを許可することになり、リスクを招きます。VPN 接続はセキュアであっても、感染したデバイスが軸として使用されて、組織の社内システムを感染させる恐れがあります。また、帯域幅の狭いコンシューマーレベルのインターネットを使用して在宅勤務にあたっている従業員の場合、VPN にはパフォーマンスの点で大きな問題があるため、生産性が低下する可能性もあります。

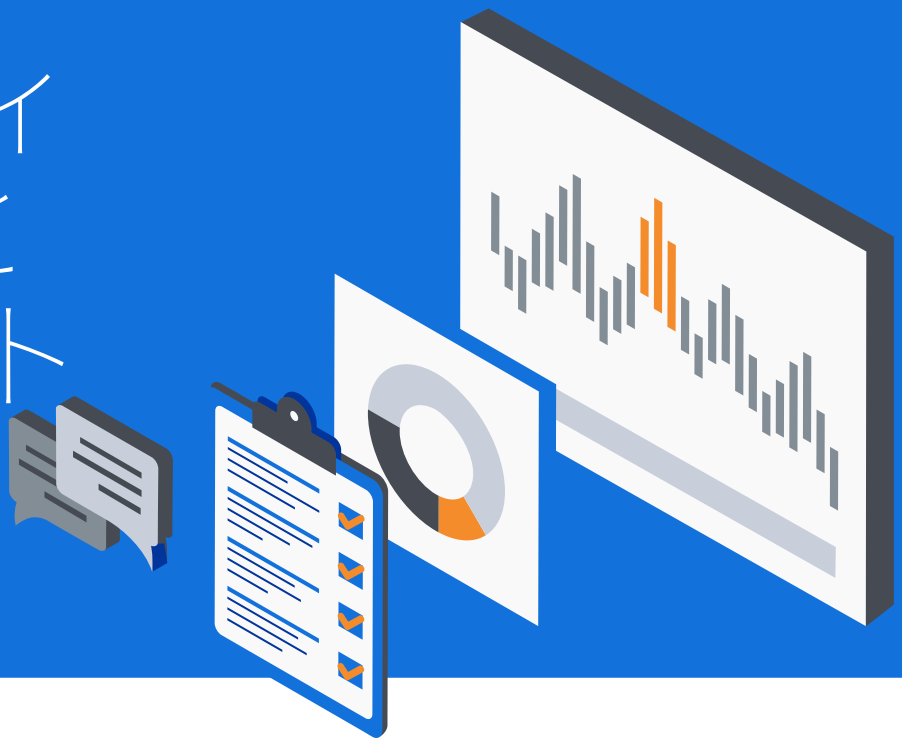
セキュアインターネットゲートウェイ

セキュアインターネットゲートウェイでは、企業ネットワーク上のあらゆるアプリケーション、デスクトップツール、ファイルにどこからでもセキュアにアクセスできるため、VPN に代わる現実的なソリューションです。リモートワーカーは、管理対象デバイスまたは個人用デバイスを使用してファイアウォール内側のコンテンツにアクセスすることができるため、従来の会社所有の管理対象環境で働いていたときのパフォーマンスが犠牲になることはありません。

また、これらはコンテナ化されたブラウザベースのソリューションであるため、企業資産を監査可能な方法でセキュアに 1 つの仮想デスクトップ環境に集約することができ、接続が断続的な場合にオフラインで作業するときにも、企業のアプリ、ツール、およびファイルすべてにアクセスすることができます。さらに、ターンキー型のアクセス管理も提供するため、ユーザーを迅速にオンボードまたはオフボードし、VPN よりも容易にエンドポイントをプロビジョニングすることができます。

VPN によって従業員は組織のネットワークに便利な方法で簡単に接続できますが、このテクノロジーのセキュリティ上の制限による欠点が急速に明らかになりつつあります。

セキュリティ意識向上とインシデントレポート



リモートワーカーをセキュアにサポートするためには、組織は、ゼロトラスト戦略の一環として、継続的なセキュリティ意識向上トレーニングと共に、明確に定義されたセキュリティインシデントレポートおよび対応機能を提供する必要があります。

継続的なセキュリティ意識向上プログラムでは、セキュリティベストプラクティスについて従業員を教育する ...

セキュリティ意識向上トレーニング

企業環境内またはリモートのどちらで働いているかにかかわらず、組織は従業員に対して継続的なセキュリティ意識向上トレーニングを実施する必要があります。継続的なセキュリティ意識向上プログラムでは、セキュリティベストプラクティスについて従業員を教育すると共に、プログラムが効果を上げているかどうかに関する監査可能なフィードバックを組織に提供するよう取り組む必要があります。セキュリティ意識向上トレーニングプログラムを提供する組織は数多くあり、中には無償で提供している組織もあります。

企業ネットワークに関わるすべての従業員、請負業者、インターン、およびパートナーは、セキュリティプロトコルを確認して理解し、セキュアな在宅勤務を確実に実現するための管理策に準拠する必要があります。セキュリティファーストの考え方を保ちます。あらゆるセキュリティリスクや安全リスクと同じように、最善のアプローチは予防です。すべての従業員は、自分が組織のセキュリティチームの最前線にいるという認識を持つ必要があります。

インシデントレポート

組織は、疑わしいセキュリティイベントによる潜在的な被害を減らし、社内の適切なチームにイベントをレポートする場合に従業員が取るべき手順を明確に定めて提供する必要があります。特に、在宅勤務中でセキュリティチームにすぐにアクセスできない従業員には、侵害された可能性があるデバイスを使用することなく、疑わしいセキュリティイベントをレポートするための機能が必要です。

まとめ

COVID-19 による危機が収まった後でさえ、在宅勤務がニューノーマルの重要な側面となる可能性があることを考えると、従業員は適切なサイバーセキュリティ衛生を確実に実践し、注意と警戒を怠らないようにする必要があります。このため、従業員が行うことすべてにゼロトラストアプローチを適用すると、優れたセキュリティプラクティスを確立する上で有利です。ホームネットワークで起きたことはすぐに企業に波及する可能性があるため、チームメンバーは、ホームネットワークを保護し、アプリケーションを責任を持って使用し、デバイスをロックダウンすることで、自分自身のセキュリティと企業ネットワークのセキュリティを実現する必要があります。

組織は、COVID-19 の危機が続く間、そして危機が去った後もリモートワーカーに企業ネットワークへのアクセスを提供するよう取り組みを続けています。その中で組織は、モビリティソリューションにより、ユーザーアクセスが関係する場所にゼロトラストフレームワークに基づいて最高レベルのセキュリティを確実に提供すると共に、セキュリティ維持のために従業員が必要とするトレーニングとサポートを提供する必要があります。全体的なプロセスは、IT 管理者と従業員にとって管理しやすいものである必要があります。なぜなら、新しいリモートユーザーが急増する可能性を考慮すると、ソリューションでユーザー、デバイス、およびアプリケーションを簡単にオンボード／オフボードできる必要があるためです。

いつもと同じように、BlackBerry チームはお客様をサポートする用意ができており、リモート従業員をセキュアに実現するためのオプションについて喜んでご提案いたします。また、弊社のホワイトペーパー「Seven Strategies to Securely Enable Remote Workers（在宅勤務をセキュアに実現するための 7 つの戦略）」もご覧いただけます。こちらの記事では、組織の IT 環境の内外に関わるあらゆるユーザー、デバイス、アプリケーション、およびシステムを制御する効果的なセキュリティコントロールを確実に導入するためのゼロトラスト戦略について考慮します。

BlackBerryについて

BlackBerry（NYSE：BB；TSX：BB）は、世界中の企業や政府機関向けに、インテリジェントなセキュリティソフトウェアとサービスを提供しています。現在、BlackBerryのソリューションは、1億5,000万台の自動車をはじめ、5億以上のエンドポイントを保護しています。カナダ・オンタリオ州ウォータールーに本社を置く同社は、AIと機械学習を活用して、サイバーセキュリティ、安全性、およびデータプライバシーソリューションの分野で革新的なソリューションを提供しています。さらに、エンドポイントのセキュリティ管理、暗号化、組み込みシステムなどの主要分野をリードしています。BlackBerryのビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

詳細については、BlackBerry.comにアクセスし、@BlackBerryをフォローしてください。

BlackBerry
Intelligent Security. Everywhere.

$$$20-0236 $ 200520

BlackBerry Intelligent Security. Everywhere.

ゼロトラスト プレイブック

リモートワーカーはホームネットワークを保護し、
責任を持ってアプリケーションを使用し、
デバイスをロックダウンする必要があります。

攻撃に対する意識向上

ソーシャルエンジニアリング

攻撃手法	ベストプラクティス
フィッシングメール	細心の注意を払う
サポート詐欺の電話	落ち着いて考える
偽のソーシャルメディアプロファイル	直感を信じる
偽の通知	

ワイヤレスインターフェイス

攻撃手法	ベストプラクティス
携帯電話ネットワーク	使用しないときは無効にする
Wi-Fi	デバイスを「削除」する
Bluetooth	パスワードを変更する

物理的なアクセス

攻撃手法	ベストプラクティス
USB メモリー	絶対に放置しない
ログイン済みアカウント	パスワードが有効なスクリーンロック
偽の通知	直感を信じる
USB 充電ケーブル	モバイルバッテリーを使用する

ルーターに接続するすべてのデバイスでデフォルトのパスワードを変更することをお勧めします。

デバイスの侵害リスクを
大幅に減らすためにすべての
ユーザーが実行できる
最も簡単な対策の 1 つは、
リスクのある Web 閲覧行動を
控えることです。

Web セキュリティの向上

攻撃手法	ベストプラクティス
リスクのある閲覧行動	控える
トレントでのメディア、音楽、映画のダウンロード	Web トレントを避ける
賭博サイト	リスクのあるサイトを避ける
短縮 URL	正規の URL 短縮
自動ダウンロード	自動ダウンロードをすべて無効にする

見出しを挿入

ソーシャルエンジニアリング

攻撃手法	ベストプラクティス
フィッシングメール	細心の注意を払う
サポート詐欺の電話	落ち着いて考える
偽のソーシャルメディアプロファイル	直感を信じる
偽の通知	

ワイヤレスインターフェイス

攻撃手法	ベストプラクティス
携帯電話ネットワーク	使用しないときは無効にする
Wi-Fi	デバイスを「削除」する
Bluetooth	パスワードを変更する