パブリック Wi-Fi を安全に使用するためのヒント

皆さんのオンラインを悪用する悪者がいます。パブリック Wi-Fi を使用する必要があるかどうかを検討するためのヒントについては、以下をお読みください。

コロナウイルスの発生と企業や図書館の閉鎖に対応して、多数の職員はオンラインでより多くの時間を費やしています。その結果、インターネットへの接続にパブリック Wi-Fi を使用する必要がある場合があります。パブリック Wi-Fi を使用する必要がある場合は、州の最高プライバシー責任者（最高プライバシー責任者）からの次の推奨事項を検討してデータを保護してください。

1. 正しいネットワークがあることを確認して下さい。

正しいネットワークに接続していることを確認してください。悪者は、名前を見れば無害に見えるネットワークを作りますが、実際には、インターネットサーフィンを見るためにネットワーク設定に接続するように誘導します。これは、ログイン認証情報またはパスワードを Web サイトに入力すると、ハッカーがユーザー情報を盗むことができることを意味します。これを防ぐには、ネットワーク名を注意深く読み、可能であれば、従業員に尋ねるか、ビジネスの看板を調べて、ネットワークが正当であることを確認してください。

人気のあるコーヒーチェーンのネットワークなど、よく知られているネットワークは、企業がサービスとしてネットワークを運用しているため、あまり疑われません。一般的に、既知のネットワークは、公共の場所でスマートフォンに現れるランダムな無料 Wi-Fi ネットワークよりも安全です。

2. 自動接続をオフにします。

多くのデバイス（スマートフォン、ラップトップ、タブレット）には自動接続設定があります。この設定により、デバイスを近くのネットワークに簡単に接続できます。これは信頼できるネットワークでは問題ありませんが、安全でないネットワークにデバイスが接続される可能性もあります。この機能はデバイスの設定機能で無効にできます。特に見知らぬ場所に旅行する場合は、これらの設定をオフにしておいてください。追加の予防策として、パブリック Wi-Fi の使用後に「ネットワークを忘れる」をチェックして下さい。

公共の場所で Bluetooth を監視する必要もあります。Bluetooth 接続により、さまざまなデバイスが相互に通信でき、ハッカーはオープン Bluetooth 信号を探してデバイスにアクセスできます。知らない場所にいるときは、スマートフォンや他のデバイスのこの機能をオフにしておいてください。

3. ファイル共有をオフにします

パブリック Wi-Fi を使用している間は、ファイル共有オプションがオフになっていることを確認してください。オペレーティングシステムに応じて、システム設定またはコントロールパネルからファイル共有をオフにすることができます。AirDrop は、オフにしておきたいファイル共有機能の例です。Windows / PC などの一部のオペレーティングシステムでは、新しいパブリックネットワークに初めて接続するときに「パブリック」オプションを選択することにより、ファイル共有がオフになります。

ファイル共有をオフにする手順

PC の場合：

1. ネットワークの 共有センター（共有センター）に行きます。
2. 次に、共有の詳細設定を変更します。
3. ファイルとプリンターの共有をオフにします。

Mac の場合:

1. System Preferences（システム環境設定）に移動します。
2. Sharing（共有）を選択します。
3. すべての選択を解除します。
4. 次に ファインダ で AirDrop をクリックし、「ユーザーに発見を許可する」を選択します。No One （誰もなし）を選択します。

iOS の場合、コントロールセンターで AirDrop を見つけてオフにします。

4. VPN を使用します。

デバイスに VPN（仮想プライベートネットワーク）をインストールすることを検討してください。VPN は、パブリック Wi-Fi でのデジタルプライバシーの最も安全なオプションです。それはデバイスを通過するデータを暗号化し、ネットワークを通過するときにデータが表示されないように保護「トンネル」として機能します。

5. 暗号化された Web サイトに関する FBI 警告– HTTPS。

アドレスが「https」で始まるウェブサイトについて FBI は、警告しています。「https」とロックアイコンの存在は、ウェブ トラフィックが暗号化されており、訪問者がデータを安全に共有できることを示しています。しかし、サイバー犯罪者は現在、安全に見せかけた悪意のある Web サイトを https に組み込んで信頼させてユーザーを誘導しています。

FBI の推奨事項：

- 電子メールの名前を単に信頼するのではなく、電子メールの内容の意図を疑ってください。
- 既知の連絡先からのリンクが記載された不審なメールを受信した場合は、連絡先に電話またはメールで連絡して、メッセージが正当であることを確認してください。不審なメールに直接返信しないでください。
- リンク内のつづりの間違いや間違ったドメインを確認しましょう（たとえば、「.gov」で終わるはずのアドレスが「.com」で終わっている場合など）。
- ブラウザーのアドレスバーにロックアイコンまたは「https」が表示されているという理由だけで Web サイトを信頼しないでください。

6. 機密情報へのアクセスはお薦め出来ません。

VPN を使用している場合でも、個人の銀行口座や、セキュリティで保護されていないパブリックネットワーク上の社会保障番号などの同様の機密個人データにアクセスすることはお勧めできません。セキュリティで保護されたパブリックネットワークでさえ、リスクを伴う可能性があります。パブリック Wi-Fi でこれらのアカウントにアクセスする必要がある場合は、最善の判断をしてください。金融取引の場合は、代わりにスマートフォンのホットスポット機能を使用することをお勧めします。

7. 安全と非安全。

基本的に 2 種類のパブリック Wi-Fi ネットワークがあります。安全と非安全。

安全なパブリックネットワークに可能な限り接続しましょう。セキュリティで保護されていないネットワークは、パスワードやログインなどのセキュリティ機能がなくても接続できます。安全なネットワークでは、通常、ユーザーは利用規約に同意するか、アカウントを登録するか、ネットワークに接続する前にパスワードを入力する必要があります。

8. ファイアウォールを有効にしておいてください。

ラップトップを使用している場合は、パブリック Wi-Fi を使用している間はファイアウォールを有効にしてください。ファイアウォールは、マルウェアの脅威からデバイスを保護するバリアとして機能します。ユーザーは、ポップアップや通知がでたりして Windows ファイアウォールを無効にしたまま忘れる時があります。PC の再起動で有効にしたい場合は、コントロールパネルの[システ

ムとセキュリティ]に移動し、”Windows Firewall” (Windows ファイアウォール)を選択します。Mac ユーザーの場合は、[システム環境設定]、[セキュリティとプライバシー]、[ファイアウォール]タブの順に移動して、機能を有効にします。

9. アンチウイルスソフトウェアを使用しましょう。

また、ラップトップに最新バージョンのアンチウイルスプログラムがインストールされていることを確認知して下さい。アンチウイルスプログラムは、共有ネットワークの使用中にシステムに侵入する可能性のあるマルウェアを検出することにより、パブリック Wi-Fi の使用中にユーザー保護に役立ちます。既知のウイルスがデバイスに搭載されたり、または疑わしいアクティビティ、攻撃がある場合、またはマルウェアがシステムに侵入した場合は、アラートによって警告が表示されます。

10. 二要素認証または多要素認証を使用しましょう。

個人情報を使用して Web サイトにログインするときは、(MFA)（多要素認証）を使用しましょう。これは、さらに保護する 2 番目の確認コード（携帯電話にテキストで送信されるか、アプリまたは物理キーによって提供される）を持っていることを意味します。そのため、ハッカーがユーザー名とパスワードを入手した場合でも、認証コードなしではアカウントにアクセスできません。

11. 個人のデバイスに絶えず注意しましょう。

ノートパソコン、タブレット、スマートフォンを公共の場所や車に放置しないでください。Wi-Fi ネットワークに予防策を講じている場合でも、人の物を盗んだり、情報をのぞき見したりする者を防ぐことはできません。周囲の環境に注意し、周りの人々に気をつけましましょう。

12. その他のオンラインの安全性のヒント。

特にパブリック Wi-Fi 接続を使用する場合、ネットで安全を確保するためのヒントをいくつか紹介しましょう。

- 強力なパスワードを使用しましょう。
- デバイスを暗号化しましょう。
- フィッシングメールに気を付けましょう。
- ソーシャルメディアに投稿する内容に注意しましょう。個人情報が多すぎると、ハッカーがパスワードを推測するのに役立ちます。
- 不要になった古い情報を削除しましょう。
- ネットワークから追加のソフトウェアまたはブラウザー拡張機能のインストールを求められた場合は、接続しないでください。
- 既知の問題から保護するために、最新のパッチとソフトウェアアップデートがデバイスにインストールされていることを確認してください。