National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

オンラインでの安全確保

サイバーセキュリティはなぜ重要なのでしょうか？

インターネットとソーシャルメディアは、情報を共有したり、友人や家族と連絡を取り合ったりするのに役立つ素晴らしい手段です。

一方で、犯罪者やその他の違法組織も、これらの手段を使ってお金を奪おうとしたり、個人情報を入手したり、また脅迫したりします。

彼らは世界中のどこからでも攻撃でき、殆どの言語を流暢に話せ、説得力のある偽のウェブサイトも作成できます。彼らは電子メール、ソーシャルメディア、テキストメッセージを通じてユーザーに接触し、ユーザーが冷静に考えることができないように、恐怖感や不安感を与えようとします。

つまり、常に準備を整え、彼らが使う罠にはまらないように注意する必要があります。

オンラインでよくある問題にはどのようなものがありますか？

これらはよく見られる事象の事例です。

- リンクをクリックするように求める疑わしい電子メールまたはテキストメッセージが届きます。
    - これらのリンクには、ログイン情報や財務情報を盗み取るために作成された偽のウェブサイトにつながるものが多いです。
- 個人情報を尋ねる不審な電話がかかってきます。
    - 電話の相手は銀行の職員を装って情報を尋ねてきます。
- 権威のある人を装って何かをさせようとする人物からの連絡を受けます。
    - そのようなケースでは、脅迫を受けることが多いです。
- 誰か他人がオンラインアカウント(メールやソーシャルメディアなど)に侵入します。
    - 誰か他人があなたのオンラインアカウントに侵入して、情報を盗み取ったり、支払いを違う支払先に変更したり、あなた自身になりすまして友人や家族をターゲットにしたりする可能性があります。
- クレジットカードの詳細が盗まれたり、偽の販売や投資で金銭を騙し取られたりします。
    - 詐欺犯は、お得な情報を見せて、何も考えずに支払いたくなることを期待しています。あるいは、実際のウェブサイトがデータ侵害に遭い、ご自身の詳細がオンラインで漏洩してしまうこともあります。

オンライン詐欺には、様々なケースがあります→
今援助を求める --オンライン時は自分主導に--

オンラインで安全を保つにはどうすればよいですか？

- **長くて分かりにくいパスワード。**
    - パスワードは長ければ長いほど強力になります。
    - 4 つのランダムな単語を結合して（例：TriangleRhinoOperationShoes）、必要に応じて数字、大文字、記号を追加して、16 文字以上の覚えやすいパスワードを作成します（例えば、Triangle&"Rhino"Operation2Shoes）。
    - 重要なのは、複数のアカウントで同じパスワードを使わないことです。犯人がパスワードの一つを入手した場合、他のアカウントでもそれを試します。
    - パスワードを記憶し、新しいパスワードを作成してくれるパスワードマネジャーを使用すると良いです。
    - 良いパスワードを作成しましょう -- オンライン時は自分主導に --
- **二要素認証を有効にします。**
    - 二要素認証とは、ウェブサイトにログインするために必要な追加情報（通常は携帯電話でのコード入力）です。
    - この認証は非常に強力で、アカウントへの侵入のほとんどを阻止できます。
    - サポートされている場合は、「認証アプリ」を使用することをお勧めします。
    - 二要素認証（2FA）を設定する -- オンライン時は自分主導に --
- **オンラインでプライバシーを守る。**
    - ソーシャル メディアで安全を保つための最善の選択肢は、プライバシー設定をオンにすることです。
    - これにより、サイバー犯を含む不特定多数の人があなたの投稿を閲覧したり、あなたにメッセージを送信したりすることが阻止されます。
    - 自分、家族と友達に関する情報を投稿する場合、投稿内容について注意する。
    - 連絡先が本人であることを確認してください。
    - 偽の友達リクエストに注意してください。特にジャーナリストを名乗る人や、よく知らない人には注意が必要です。
    - オンラインでプライバシーを保護 -- オンライン時は自分主導に --
- **常にすべての端末のプログラムを更新する。**
    - 携帯電話、コンピューター、またはソフトウェアを更新すると、セキュリティ上の穴も塞がれます。
    - 詐欺犯は常に侵入方法を探しており、アップデートによって脆弱性が修正されます。
    - デバイスを定期的に再起動してください。
    - 常にアップデートを行う -- オンライン時は自分主導に --
- **オンライン詐欺に注意してください。**

    - 最善策として、こうした詐欺には気を付けて、詐欺犯がオンライン プラットフォーム上で接触してきたときには注意を払うことです。
    - 何かおかしいと思われる場合は、接触してきた人と関わらないことです。たとえ友好的に見えても、お金を要求してきた場合には特に注意してください。
    - 不審なリンクやメール アドレスには注意が必要です。例えば、銀行員は Gmail アカウントからメールを送ったりはしません。
    - ショートメッセージにあるリンクを絶対にクリックしないでください。
    - 正規のアプリストアのみからアプリをダウンロードしてください。
    - 知らない人から企業名などを名乗る接触があり、少しでも疑問に思うとき、その企業に直接連絡して、確認すると良いです。送信されたリンクや電話番号にはアクセスしないでください。
    - 自分自身、コミュニティ、および所属するグループのオンラインセキュリティリスクについて常に認識するようにしましょう。
- **自分の情報を保護してください。**
    - Signal などの暗号化されたメッセージアプリを使用しましょう。これにより、他人があなたのメッセージを読むことができなくなります。
    - ウェブサイトで情報を共有するのは、アドレスが HTTPS で始まる場合のみにしましょう。「S」とは「セキュア」の略で、ウェブサイトで共有される情報はすべて暗号化されていることを意味します。
    - データを保護し、位置情報を隠すことができる仮想プライベートネットワーク(VPN)の使用を検討してください。
    - アプリがアクセスできるデータと権限を確認しましょう。たとえば、フィットネスアプリでは連絡先にアクセスする必要はありません。

詐欺に遭ったり、もっとひどい目に遭ったりしたらどうすればいいですか？

助けを求められるところはたくさんあります。これらの組織はすべて、あなたの同意がない限り、あなたの詳細情報を他と共有することはありません。

- サイバーインシデントについて、CERT NZ ポータルを通じて NCSC に報告することができ、NCSC はお助けをするか、他の機関と連絡を取れるようにご案内します。
  CERT NZ に事件について報告する
- お金を奪い取られた場合は、すぐに銀行に連絡してください。
- 詐欺関連のテキストメッセージを、内務省が運営する窓口である 7726 に無料で転送できます。