National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Garantir votre sécurité en ligne

Pourquoi la cybersécurité est-elle importante pour moi ?

Internet et les réseaux sociaux sont des outils formidables pour partager des informations et garder le contact avec nos amis et notre famille.

Cependant, des malfaiteurs et des organisations criminelles les utilisent également pour tenter de vous soutirer de l'argent ou vos données ou pour vous intimider.

Ils agissent depuis n'importe où dans le monde, maîtrisent parfaitement la plupart des langues et mettent en place de faux sites Internet convaincants. Ils prennent contact par e-mail, par les réseaux sociaux et par SMS et cherchent à provoquer la peur ou de l'angoisse en vous pour vous empêcher de raisonner clairement.

Vous devez faire preuve de vigilance et vous familiariser constamment avec les stratagèmes utilisés.

Quels sont les problèmes courants que je peux rencontrer en ligne ?

Voici quelques situations parmi les plus courantes.

- Vous recevez un e-mail ou un SMS suspect vous demandant de cliquer sur un lien.
    - Ces liens mènent souvent à de faux sites Internet conçus pour voler vos identifiants de connexion ou vos coordonnées bancaires.
- Vous recevez un appel suspect cherchant à obtenir vos informations personnelles.
    - Comme ci-dessus, l'appelant prétend travailler pour votre banque et vous demande des informations.
- Vous recevez une communication d'un individu se faisant passer pour un représentant de l'autorité et essayant de vous inciter à effectuer une action.
    - Souvent, la personne en question profère une menace implicite.
- Un individu accède à un ou plusieurs de vos comptes en ligne (par exemple : e-mail ou réseaux sociaux).
    - Lorsque quelqu'un accède à l'un de vos comptes en ligne, il peut voler des informations, rediriger des paiements et potentiellement cibler vos amis ou votre famille en se faisant passer pour vous.
- Les informations de votre carte de crédit sont volées ou vous êtes victime d'une arnaque lors d'une fausse vente ou d'un faux investissement.
    - Les escrocs veulent vous tenter avec une offre séduisante et vous inciter à payer sans réfléchir. Il arrive aussi qu'un site Internet authentique soit victime d'une violation de données et que vos informations soient divulguées en ligne.

D’autres scénarios sont disponibles ici :
Faites-vous aider maintenant - Maîtrisez votre vie en ligne

Comment garantir votre sécurité sur internet ?

- **Mots de passe longs et uniques.**
    - Plus un mot de passe est long, plus il est sécurisé.
    - Créez un mot de passe facile à retenir de plus de 16 caractères en associant quatre mots aléatoires (par exemple : TriangleRhinoOperationChaussures) et en ajoutant des chiffres, des majuscules et des symboles si nécessaire (par exemple : Triangle&"Rhino"Operation2Shoes).
    - Surtout, ne réutilisez pas vos mots de passe. Si un criminel se procure l’un de vos mots de passe, il l’essaiera également sur d’autres comptes.
    - Utilisez un gestionnaire de mots de passe pour mémoriser vos mots de passe et pour en créer de nouveaux.
    - Créez des mots de passe solides – Maîtrisez votre vie en ligne
- **Activez la double authentification ou vérification en deux étapes.**
    - La double authentification consiste en une information supplémentaire - généralement un code envoyé sur votre téléphone – dont vous avez besoin pour vous connecter à un site Internet.
    - Cette méthode est particulièrement fiable et peut bloquer la plupart des tentatives d’accès à votre compte.
    - Nous vous recommandons d’utiliser une application d’authentification, lorsqu’elle est prise en charge.
    - Configurez une double authentification (2FA) - Maîtrisez votre vie en ligne
- **Maintenez votre confidentialité en ligne.**
    - Le meilleur moyen pour garantir votre sécurité sur les réseaux sociaux est d’activer vos paramètres de confidentialité.
    - Vous empêchez ainsi des personnes inconnues, y compris des cybercriminels, de voir vos publications ou de vous envoyer des messages.
    - Faites preuve de prudence à propos de la publication d’informations personnelles vous concernant ou concernant votre famille ou vos amis.
    - Vérifiez l'identité des personnes qui vous contactent.
    - Faites attention aux fausses demandes d'ami. Méfiez-vous des personnes qui prétendent être des journalistes ou des personnes que vous ne connaissez pas bien.
    - Protégez votre confidentialité en ligne – Maîtrisez votre vie en ligne
- **Soyez toujours à jour.**
    - Lorsque vous mettez à jour votre téléphone, votre ordinateur ou votre logiciel, vous comblez également toutes les failles de sécurité éventuelles.

    - Les malfaiteurs cherchent en permanence le moyen d'accéder à vos données et les mises à jour rectifient les vulnérabilités.
    - Redémarrez régulièrement vos appareils.
    - Restez à jour - Maîtrisez votre vie en ligne

- **Faites preuve de vigilance.**
    - Il faut avant tout être conscient de ces escroqueries et rester attentif au cas où des individus malintentionnés tenteraient de vous contacter sur une plateforme en ligne.
    - Au moindre soupçon, cessez de communiquer avec la personne qui vous a contacté·e. Soyez particulièrement prudent·e si on vous demande de l'argent même si votre interlocuteur vous semble très sympathique.
    - Faites attention aux liens et aux adresses e-mail inhabituels (par exemple : votre banque ne vous enverra jamais d'e-mail à partir d'un compte Gmail).
    - Ne cliquez *jamais* sur les liens inclus dans les SMS.
    - Les applications ne doivent être téléchargées qu'à partir des magasins officiels.
    - En cas de doute, contactez directement l'organisation indiquée et n'utilisez aucun lien ou numéro de téléphone qui vous est envoyé.
    - Efforcez-vous de rester vigilant à propos des risques de sécurité vous affectant ou affectant votre communauté ou tous les groupes auxquels vous appartenez.
- **Protégez vos informations.**
    - Utilisez des applications de messagerie chiffrées comme Signal. Vous empêchez ainsi la lecture non autorisée de vos messages.
    - Ne partagez des informations avec un site Internet que si l'adresse commence par HTTPS. Le S signifie « sécurisé » et toutes les informations envoyées entre vous et le site Internet sont chiffrées.
    - Envisagez d'utiliser un réseau privé virtuel (VPN) capable de protéger vos données et masquer votre emplacement.
    - Vérifiez les données et les autorisations auxquelles vos applications ont accès. Par exemple, une application de fitness n'a pas besoin d'accéder à vos contacts.

Que dois-je faire si je suis victime d'une arnaque ou pire ?

Plusieurs entités sont là pour vous aider. Aucune de ces entités ne partagera vos données avec qui que ce soit sans votre consentement.

- Vous pouvez signaler les incidents de cybersécurité au bureau national de la cyber-sécurité, le NCSC via le portail CERT NZ. Nous sommes en mesure de vous aider ou de vous mettre en contact avec une autre agence :
  Signalez un incident | CERT NZ
- Si vous avez envoyé de l'argent, vous devez contacter immédiatement votre banque.
- Les SMS frauduleux peuvent être transmis gratuitement au 7726, un service géré par le ministère de l'Intérieur.