National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Manter-se seguro online

Por que a cibersegurança é importante para mim?

A internet e as mídias sociais são plataformas incríveis que nos ajudam a compartilhar informações e a manter contato com amigos e familiares.

No entanto, criminosos e outras organizações ilegais também as usam para tentar obter seu dinheiro, suas informações ou para intimidá-lo.

Eles podem operar de qualquer parte do mundo, falam a maioria dos idiomas fluentemente e criam sites falsos e convincentes. Eles entram em contato com você por e-mail, redes sociais e mensagens de texto e tentam deixar você assustado ou ansioso, sem pensar com clareza.

Tudo isso faz com que você precise estar preparado e sempre ciente dos truques que eles usam.

Quais são alguns dos problemas comuns que posso encontrar online?

Essas são algumas das situações mais comuns que encontramos.

- Você recebe um e-mail ou mensagem de texto suspeitos solicitando que você clique em um link.
    - Esses links geralmente levam a sites falsos, projetados para roubar seu login ou informações financeiras.
- Você recebe uma ligação suspeita que pede informações pessoais.
    - Como mencionado acima, o interlocutor fingirá ser do seu banco e pedirá informações.
- Você recebe uma comunicação de alguém que finge ser uma pessoa com autoridade, tentando fazer com que você faça algo.
    - Muitas vezes a pessoa faz algum tipo de ameaça.
- Alguém entra em uma ou mais de suas contas online (por exemplo: e-mail ou redes sociais).
    - Se alguém entrar na sua conta online, poderá roubar informações, redirecionar pagamentos e possivelmente atingir seus amigos ou familiares fingindo ser você.
- Os detalhes do seu cartão de crédito são roubados ou você é enganado e perde dinheiro em uma venda ou investimento falso.
    - Os golpistas esperam que você encontre uma boa oferta e pague sem pensar. Ou talvez um site verdadeiro sofra uma violação de dados e seus dados sejam vazado online.

Há mais cenários aqui:
Obtenha ajuda agora - Tenha controle da sua presença online

Como posso permanecer seguro online?

- **Senhas longas e únicas.**

- Quanto mais longa for uma senha, mais forte ela será.
- Crie uma senha memorável com mais de 16 caracteres contendo quatro palavras aleatórias (por exemplo: TriangleRhinoOperationShoes) e adicionando números, letras maiusculas e símbolos, se necessário (por exemplo: Triangle&"Rhino"Operation2Shoes).
- É importante não repetir suas senhas. Se um criminoso conseguir uma de suas senhas, ele tentará usá-la em outras contas.
- Use um gerenciador de senhas para lembrar suas senhas e criar novas senhas.
- Crie boas senhas - Tenha controle de sua presença online

- **Ative a autenticação em duas etapas.**
  - Essa é uma informação extra – geralmente um código no seu telefone – que você precisa para fazer login em um site.
  - Essa técnica é incrivelmente forte e pode impedir a maioria das tentativas de acesso às suas contas.
  - Quando possível, recomendamos usar um "aplicativo autenticador".
  - Configure a autenticação em duas etapas (2FA) - Tenha controle da sua presença online
- **Mantenha sua privacidade online.**
  - A melhor opção para permanecer seguro nas redes sociais é ativar suas configurações de privacidade.
  - Isso impedirá que pessoas aleatórias, incluindo criminosos cibernéticos, vejam suas postagens ou lhe enviem mensagens.
  - Ainda assim, tenha cuidado ao publicar informações pessoais sobre você, sua família ou seus amigos.
  - Certifique-se de que os contatos são quem afirmam ser.
  - Cuidado com pedidos de amizade falsos. Tenha cuidado com pessoas que dizem ser jornalistas ou outras que você não conhece bem.
  - Proteja sua privacidade online - Tenha controle da sua presença online
- **Mantenha tudo atualizado.**
  - Quando você atualiza seu telefone, computador ou software, isso também preenche quaisquer falhas de segurança que possam existir.
  - Os criminosos estão sempre procurando maneiras de ter acesso e as atualizações corrigem as vulnerabilidades.
  - Reinicie seus dispositivos regularmente.
  - Mantenha suas atualizações em dia - Tenha controle da sua presença online
- **Cuidado com golpes.**
  - O melhor conselho é estar ciente desses golpes e ficar atento caso os criminosos tentem entrar em contato com você em alguma plataforma online.

    - Se algo parecer errado, não interaja com a pessoa que entrou em contato com você. Tenha cuidado principalmente se eles pedirem dinheiro, mesmo que pareçam amigáveis.
    - Procure por links e e-mails estranhos (por exemplo: seu banco não enviará um e-mail de uma conta de Gmail).
    - *Nunca* clique em links em mensagens de texto.
    - Baixe aplicativos para seu dispositivo apenas de lojas de aplicativos oficiais.
    - Em caso de dúvida, entre em contato diretamente com a organização e não siga nenhum link ou número de telefone que lhe for enviado.
    - Tente estar ciente dos riscos de segurança online para você, sua comunidade e quaisquer grupos aos quais você pertença.
- **Proteja suas informações.**
    - Use aplicativos de mensagens criptografadas, como o Signal. Isso impedirá que alguém leia suas mensagens.
    - Apenas compartilhe informações com um site se o endereço começar com HTTPS. O S significa "seguro" e quer dizer que qualquer informação trocada entre você e o site é criptografada.
    - Considere usar uma rede virtual privada (VPN) que pode proteger seus dados e ocultar sua localização.
    - Verifique a que dados e permissões seus aplicativos têm acesso. Por exemplo, um aplicativo de fitness não precisa ter acesso a seus contatos.

O que devo fazer se for enganado ou algo pior?

Há muitos lugares onde você pode procurar ajuda. Nenhuma dessas organizações compartilhará seus dados, a menos que você dê seu consentimento.

- Você pode relatar incidentes cibernéticos ao NCSC através do portal CERT NZ e podemos ajudar ou colocá-lo em contato com outra agência:
  Relatar um incidente| CERT NZ
- Se você perdeu dinheiro, entre em contato com seu banco imediatamente.
- Mensagens de texto fraudulentas podem ser encaminhadas gratuitamente para o 7726, um serviço administrado pelo Departamento de Assuntos Internos (DIA).