National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Обеспечение безопасности в Интернете

Почему кибербезопасность важна для меня?

Интернет и социальные сети — это замечательные платформы, которые помогают нам делиться информацией и оставаться на связи с друзьями и семьей.

Однако преступники и другие незаконные организации также используют эти платформы, чтобы попытаться получить Ваши деньги, Вашу информацию или запугать Вас.

Они могут действовать из любой точки мира, свободно говорить на большинстве языков и создавать убедительные поддельные веб-сайты. Они могут связаться с Вами по электронной почте, через социальные сети и текстовые сообщения и попытаться напугать или встревожить Вас, чтобы Вы не могли ясно мыслить.

Это означает, что Вам нужно быть начеку и знать о том, какие уловки они используют.

С какими распространенными проблемами я могу столкнуться в Интернете?

Вот некоторые из наиболее распространенных ситуаций, с которыми мы сталкиваемся.

- Вы получаете подозрительное электронное письмо или текстовое сообщение с просьбой перейти по ссылке.
    - Эти ссылки часто ведут на поддельные сайты, созданные для кражи Ваших учётных данных или финансовой информации.
- Вы получаете подозрительный звонок с просьбой предоставить личную информацию.
    - Как уже было сказано выше, звонящий притворится сотрудником Вашего банка и попросит предоставить информацию.
- Вы получаете сообщение от человека, выдающего себя за авторитетное лицо, которое пытается заставить Вас что-то сделать.
    - Часто этот человек угрожает Вам чем-либо.
- Кто-то проникает в один или несколько Ваших аккаунтов в Интернете (например, в электронную почту или социальные сети).
    - Если кто-то проникнет в Ваш аккаунт в Интернете, то он может украсть информацию, перенаправить платежи и потенциально атаковать Ваших друзей или семью, выдавая себя за Вас.
- Украдены данные Вашей кредитной карты, или Вас обманули, лишив денег в результате фиктивной продажи или инвестиции.
    - Мошенники надеются, что Вы увидите выгодную сделку и захотите заплатить, не задумываясь. Или, возможно, произошла утечка данных с реального веб-сайта, и Ваши данные попали в сеть.

Вот еще несколько сценариев:
Получите помощь прямо сейчас - Защитите свою онлайн-безопасность

Как обеспечить безопасность в Интернете?

- **Длинные и уникальные пароли.**
    - Чем длиннее пароль, тем он надежнее.
    - Создайте запоминающийся пароль длиной более 16 символов, объединив четыре случайных слова (например: TriangleRhinoOperationShoes) и добавив цифры, заглавные буквы и символы, если необходимо (например: Triangle&"Rhino"Operation2Shoes).
    - Главное, не повторяйте свои пароли. Если преступник получит один из Ваших паролей, он попробует использовать его и на других аккаунтах.
    - Используйте менеджер паролей, чтобы запоминать пароли за Вас и создавать новые.
    - Создавайте хорошие пароли - Защитите свою онлайн-безопасность
- **Включите двухуровневую аутентификацию.**
    - Это дополнительная информация - обычно код, отправляемый на Ваш телефон, который необходимо ввести при входе на веб-сайт.
    - Этот метод очень эффективен и может предотвратить большинство попыток проникновения в Ваши аккаунты.
    - Мы рекомендуем использовать «приложение для аутентификации», если оно поддерживается.
    - Настройте двухуровневую аутентификацию (2FA) — Защитите свою онлайн-безопасность
- **Оставайтесь конфиденциальными в сети.**
    - Лучший способ обеспечить безопасность в социальных сетях — включить настройки конфиденциальности.
    - Это не позволит случайным людям, включая киберпреступников, видеть Ваши публикации или отправлять Вам сообщения.
    - И всё же будьте осторожны при публикации личной информации о себе, своей семье или друзьях.
    - Убедитесь, что те люди, которые с Вами контактируют, являются теми, за кого себя выдают.
    - Остерегайтесь поддельных запросов на добавление в друзья. Будьте осторожны с людьми, утверждающими, что они журналисты, или с теми, кого Вы плохо знаете.
    - Защитите свою конфиденциальность в Интернете - Защитите свою онлайн-безопасность
- **Регулярно обновляйте свои устройства и программы.**

    - Обновление Вашего телефона, компьютера или программного обеспечения помогает устранить уязвимости и укрепить безопасность.
    - Преступники всегда ищут способы проникнуть в систему, а обновления устраняют уязвимости.
    - Регулярно перезагружайте свои устройства.
    - Регулярно обновляйте свои устройства и программы - Защитите свою онлайн-безопасность

- **Будьте осторожны с мошенниками.**
    - Лучший совет — знать о таких мошеннических схемах и быть начеку, если преступники попытаются связаться с Вами на любой онлайн-платформе.
    - Если что-то кажется странным, не взаимодействуйте с человеком, который с Вами связался. Будьте особенно осторожны, если у Вас просят денег, даже если в дружелюбной манере.
    - Обращайте внимание на странные ссылки и адреса электронной почты (например: Ваш банк не будет отправлять Вам электронное письмо с gmail аккаунта).
    - *Никогда* не нажимайте на ссылки в текстовых сообщениях.
    - Загружайте приложения на своё устройство только из официальных магазинов приложений.
    - Если у Вас возникли сомнения, свяжитесь с контактирующей с Вами организацией напрямую и не переходите по ссылкам или номерам телефонов, которые Вам присылают.
    - Старайтесь быть в курсе рисков безопасности в Интернете для себя, своего сообщества и любых групп, к которым Вы принадлежите.
- **Защищайте свою информацию.**
    - Используйте зашифрованные приложения для обмена сообщениями, такие как Signal. Это не позволит никому прочитать Ваши сообщения.
    - Делитесь информацией с веб-сайтом только в том случае, если адрес начинается с HTTPS. S значит «безопасный», что означает, что любая информация, передаваемая между Вами и веб-сайтом, зашифрована.
    - Рассмотрите возможность использования виртуальной частной сети (VPN), которая может защитить Ваши данные и скрыть Ваше местоположение.
    - Проверьте, к каким данным и разрешениям имеют доступ Ваши приложения. Например, фитнес-приложению не нужен доступ к Вашим контактам.

Что делать, если меня обманули или случилось что-то хуже?

Есть много мест, куда Вы можете обратиться за помощью. Ни одна из этих организаций не будет передавать Ваши данные третьим лицам без Вашего согласия.

- Вы можете сообщить о киберинцидентах в NCSC через портал CERT NZ, и мы можем помочь или связать Вас с другим агентством:
  Сообщить об инциденте | CERT NZ
- Если Вы потеряли деньги, то Вам следует немедленно обратиться в свой банк.

- Мошеннические текстовые сообщения можно бесплатно пересылать на номер 7726 — службу, которой управляет Департамент внутренних дел.