National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

온라인 안전

사이버 보안이 중요한 이유는?

인터넷과 소셜 미디어는 우리가 정보를 공유하고 친구 및 가족과 연락하며 지내는 데 도움이 되는 놀라운 플랫폼입니다.

하지만 범죄자와 기타 다른 불법 조직도 이것을 이용해 여러분의 돈이나 정보를 훔치거나 겁을 먹게 하려고 합니다.

이들은 세계 어느 곳에서나 활동하고, 대부분의 언어를 유창하게 구사하며, 그럴듯한 가짜 웹사이트를 만들어 둘 수도 있습니다. 이들은 이메일, 소셜 미디어, 문자 메시지를 통해 우리에게 접촉하여 두려움이나 불안감을 줌으로써 올바른 사리판단을 못하게 만들려고 할 것입니다.

그래서 우리는 이에 대비해 항상 이들의 수법을 알고 있을 필요가 있습니다.

온라인에서 흔히 접할 수 있는 문제로는 어떤 것이 있나?

다음은 가장 일반적으로 일어나는 상황의 몇 가지 예입니다.

- 링크를 클릭하라는 수상한 이메일이나 문자 메시지를 받음
    - 이러한 링크는 종종 로그인 정보나 금융 정보를 훔치려는 목적으로 설계된 가짜 웹사이트로 연결됩니다.
- 개인정보를 묻는 미심쩍은 전화가 옴
    - 위의 경우와 마찬가지로, 전화를 건 사람은 은행 직원인 척하며 정보를 묻습니다.
- 누군가가 권한을 가진 사람인 척하며 연락해 와 우리에게 무언가를 하게 만들려고 시도함
    - 종종 이 사람은 어떤 형태의 위협을 합니다.
- 누군가가 우리의 온라인 계정(예: 이메일 또는 소셜 미디어)에 접속
    - 누군가가 우리의 온라인 계정에 침입하면 정보를 훔치고 돈을 빼돌릴 수 있고, 본인인 척하며 우리의 친구나 가족을 표적으로 삼을 가능성도 있습니다.
- 신용카드 정보를 절취당하거나 허위 판매 또는 허위 투자로 스캠 사기를 당함
    - 사기꾼들은 우리가 좋은 거래라 판단하고 생각 없이 돈을 건네주기를 원합니다. 아니면 실제 웹사이트가 해킹되어 개인정보가 온라인에 유출될 수도 있습니다.

더 많은 시나리오가 여기에 나옵니다.

지금 도움 받기 - Own Your Online

온라인 보안 유지를 위해서는 어떻게 해야 하나?

- **길고 고유한 비밀번호**
    - 비밀번호는 길수록 더 강력합니다.
    - 임의의 단어 4 개를 결합하고(예: TriangleRhinoOperationShoes), 필요하면 숫자와 대문자 및 기호를 추가하여 16 자 이상의 기억하기 쉬운 비밀번호를 만드세요(예: Triangle&"Rhino"Operation2Shoes).

    - 중요한 점은 비밀번호를 반복해서 사용하지 않는 것입니다. 범죄자가 우리의 비밀번호 중 하나를 얻으면 다른 계정에도 이것으로 로그인을 시도할 것입니다.
    - 비밀번호 관리자를 통해 비밀번호를 기억하고, 새 비밀번호를 만드세요.
    - 좋은 비밀번호 만들기 - Own Your Online
- **2 단계 인증 기능 사용**
    - 이것은 웹사이트 로그인에 필요한 추가 정보로, 일반적으로 휴대폰에 나오는 코드입니다.
    - 이 기술은 놀라울 정도로 강력해서 우리의 계정에 침입하려는 대부분의 시도를 봉쇄할 수 있습니다.
    - '인증 앱'이 지원된다면 이것을 사용하는 것이 좋습니다.
    - 2 단계 인증(2FA) 설정하기 - Own Your Online
- **온라인에서 개인정보 보호 상태 유지**
    - 소셜 미디어에서 보안을 유지하는 가장 좋은 방법은 개인정보 보호 설정을 적용하는 것입니다.
    - 이렇게 하면 사이버 범죄자를 포함해 아무나 내 게시물을 보거나 나에게 메시지를 보내는 일을 막을 수 있습니다.
    - 그럼에도 자신이나 가족 또는 친구에 대한 개인정보를 게시할 때는 조심하세요.
    - 상대방이 허위 인물이 아닌지 확인하세요.
    - 가짜 친구 요청에 주의하세요. 언론인이라고 주장하는 사람이나 잘 모르는 사람을 조심하세요.
    - 온라인 개인정보 보호 - Own Your Online
- **모든 것을 최신 상태로 유지**
    - 휴대폰, 컴퓨터나 소프트웨어를 업데이트하면 존재할지 모를 보안 허점도 메워집니다.
    - 범죄자들은 항상 침입할 방법을 찾고 있는데 업데이트를 하면 취약점을 없앨 수 있습니다.
    - 기기를 규칙적으로 다시 시작하세요.
    - 최신 업데이트 하기 - Own Your Online
- **스캠에 주의**
    - 가장 좋은 조언은 이러한 스캠에 대해 인지하고 주의하는 것입니다.
    - 낌새가 이상하면 접촉해 온 그 사람과 대화하지 마세요. 그 사람이 친근하게 대하더라도 돈을 요구한다면 특히 조심하세요.
    - 수상한 링크와 이메일 주소에 주의하세요(예: 은행은 Gmail 계정을 써서 이메일을 보내지 않음).
    - 문자 메시지 안에 나오는 링크를 *절대* 클릭하지 마세요.
    - 공식 앱 스토어에서만 기기 앱을 다운로드하세요.
    - 미심쩍으면 접촉해 온 그 기관에 직접 연락하되 받은 링크를 따라가거나 그 전화번호로 전화를 걸지 마세요.
    - 자신과 지역사회, 소속 단체에 대한 온라인 보안 위험을 항상 인지하도록 노력하세요.
- **개인정보 보호**

- Signal 과 같은 암호화 메신저 앱을 사용하세요. 그러면 다른 사람이 메시지를 훔쳐 읽을 수 없게 됩니다.
- 주소가 HTTPS 로 시작하는 웹사이트에만 정보를 공유하세요. S 는 '보안(secure)'을 나타내는데 사용자와 웹사이트 간에 전송되는 모든 정보가 암호화된다는 것을 의미합니다.
- 가상 사설망(VPN)을 사용하는 것을 고려해 보세요. 데이터를 보호하고 사용자의 위치를 숨길 수 있습니다.
- 앱이 어떤 데이터와 권한을 액세스할 수 있는지 확인하세요. 예를 들어, 피트니스 앱이라면 연락처에 대한 접근 권한이 있을 필요가 없습니다.

스캠 사기나 이보다 더 나쁜 일을 당하면 어떻게 해야 하나?

도움을 받을 수 있는 곳이 많이 있습니다. 이러한 기관은 본인이 동의하지 않는 한, 당사자의 세부 정보를 다른 사람과 공유하지 않습니다.

- CERT NZ 포털을 통해 NCSC 에 사이버 사고를 신고할 수 있습니다. 신고를 하면 직접 도와드리거나 다른 기관을 연결해 드립니다.
  사고 신고 | CERT NZ
- 돈을 사기당했다면 즉시 은행에 연락해야 합니다.
- 스캠 문자 메시지는 내무부에서 운영하는 서비스인 7726 으로 전달할 수 있습니다(송신 요금 무료).