National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Giữ an toàn trên mạng

Tại sao an ninh mạng lại quan trọng đối với tôi?

Internet và mạng xã hội là những nền tảng tuyệt vời giúp chúng ta chia sẻ thông tin và giữ liên lạc với bạn bè và gia đình.

Tuy nhiên, tội phạm và các tổ chức phi pháp khác cũng sử dụng nó để lấy cắp tiền, thông tin của bạn hoặc đe dọa bạn.

Chúng có thể hoạt động ở bất kỳ nơi nào trên thế giới, nói lưu loát hầu hết các ngôn ngữ và tạo ra các trang web giả mạo rất giống thật. Chúng sẽ liên lạc với bạn qua email, mạng xã hội và tin nhắn và sẽ cố gắng làm cho bạn cảm thấy sợ hãi hoặc lo lắng, để bạn không thể suy nghĩ sáng suốt.

Tất cả những điều này có nghĩa là bạn phải có sự chuẩn bị và luôn luôn nhận biết được những mánh khóe mà chúng sử dụng.

Một số vấn đề phổ biến mà tôi có thể gặp phải trên mạng là gì?

Đây là một số tình huống phổ biến nhất mà chúng tôi thấy.

- Bạn nhận được một email hoặc tin nhắn đáng ngờ yêu cầu bạn nhấp vào một đường link.
    - Các đường link này thường dẫn đến các trang web giả mạo được thiết kế để đánh cắp thông tin đăng nhập hoặc thông tin tài chính của bạn.
- Bạn nhận được một cuộc gọi đáng ngờ yêu cầu cung cấp thông tin cá nhân.
    - Cũng như trên, người gọi sẽ giả vờ là người của ngân hàng của bạn và yêu cầu cung cấp thông tin.
- Một người nào đó giả vờ là người có thẩm quyền liên lạc với bạn, cố gắng bảo bạn làm điều gì đó.
    - Thông thường người đó sẽ đưa ra một lời đe dọa nào đó.
- Một người nào đó xâm nhập vào một hoặc nhiều tài khoản trực tuyến của bạn (ví dụ: email hoặc mạng xã hội).
    - Nếu ai đó xâm nhập vào tài khoản trực tuyến của bạn, họ có thể đánh cắp thông tin, chuyển hướng thanh toán và có thể nhắm mục tiêu vào bạn bè hoặc gia đình của bạn bằng cách họ giả mạo là bạn.
- Thông tin thẻ tín dụng của bạn bị đánh cắp hoặc bạn bị lừa tiền trong một giao dịch mua bán hoặc đầu tư giả mạo.
    - Những kẻ lừa đảo hy vọng bạn sẽ cho rằng đó là một giao dịch tốt và sẽ muốn trả tiền mà không cần suy nghĩ. Hoặc có thể một trang web thực sự bị dính vào một sự cố xâm nhập dữ liệu và thông tin của bạn bị rò rỉ trên mạng.

Xem thêm các tình huống khác tại đây:
Nhận trợ giúp ngay bây giờ - Own Your Online

Làm cách nào để tôi an toàn trên mạng?

- **Mật khẩu dài và độc nhất cho từng tài khoản.**
    - Mật khẩu càng dài thì càng mạnh.
    - Tạo mật khẩu dễ nhớ và nhiều hơn 16 ký tự bằng cách nối bốn từ ngẫu nhiên với nhau (ví dụ: TriangleRhinoOperationShoes) và thêm số, chữ in hoa và ký hiệu nếu cần (ví dụ: Triangle&"Rhino"Operation2Shoes).
    - Điều quan trọng là không lặp lại mật khẩu của bạn. Nếu bọn tội phạm có được một trong những mật khẩu của bạn, chúng sẽ thử mật khẩu đó ở các tài khoản khác.
    - Sử dụng một công cụ quản lý mật khẩu (password manager) để ghi nhớ các mật khẩu của bạn và tạo ra các mật khẩu mới cho bạn.
    - Tạo mật khẩu tốt - Own Your Online
- **Bật xác thực hai yếu tố (2FA).**
    - Đây là một lớp bảo vệ bổ sung – thường là mật mã gửi vào điện thoại của bạn – bạn cần có nó để đăng nhập vào trang web.
    - Kỹ thuật này cực kỳ mạnh mẽ và có thể ngăn chặn hầu hết các nỗ lực xâm nhập vào tài khoản của bạn.
    - Chúng tôi khuyên bạn nên sử dụng một 'ứng dụng xác thực' ('authenticator app'), nếu điều này được hỗ trợ.
    - Thiết lập xác thực hai yếu tố (2FA) - Own Your Online
- **Giữ gìn sự riêng tư trên mạng.**
    - Cách tốt nhất để giữ an toàn trên mạng xã hội là bật các cài đặt quyền riêng tư của bạn.
    - Điều này sẽ ngăn chặn những người lạ, trong đó có bọn tội phạm trên mạng, có thể xem bài đăng của bạn hoặc gửi tin nhắn cho bạn.
    - Vẫn phải cẩn thận khi đăng thông tin cá nhân về bản thân, gia đình hoặc bạn bè của bạn.
    - Đảm bảo đúng người như lời họ tự nhận.
    - Cảnh giác với các yêu cầu kết bạn giả mạo. Cẩn thận với những người tự xưng là nhà báo hoặc những người khác mà bạn không biết rõ.
    - Bảo vệ sự riêng tư của bạn trên mạng - Own Your Online
- **Cập nhật mọi thứ.**
    - Khi bạn cập nhật điện thoại, máy tính hoặc phần mềm, nó sẽ vá các lỗ hổng bảo mật có thể có.
    - Bọn tội phạm luôn tìm cách xâm nhập và gây hại thông qua các lỗ hổng.
    - Khởi động lại thiết bị của bạn thường xuyên.
    - Cập nhật kịp thời - Own Your Online

- **Nhận biết những thủ đoạn lừa đảo.**
    - Lời khuyên tốt nhất là hãy nhận biết những thủ đoạn lừa đảo này và luôn đề phòng nếu bọn tội phạm cố gắng liên lạc với bạn trên bất kỳ nền tảng trực tuyến nào.
    - Nếu có bất cứ điều gì có vẻ không ổn, đừng tương tác với người đã liên lạc với bạn. Đặc biệt phải cẩn thận nếu họ hỏi, xin tiền, ngay cả khi họ có vẻ thân thiện.
    - Cảnh giác với những đường link và địa chỉ email lạ (ví dụ: ngân hàng của bạn sẽ không gửi email cho bạn từ một tài khoản gmail).
    - *Không bao giờ* nhấp vào đường link trong tin nhắn.
    - Chỉ tải các ứng dụng (app) về thiết bị của bạn từ cửa hàng ứng dụng chính thức (app store).
    - Nếu nghi ngờ, hãy liên hệ trực tiếp với cơ quan chính thức và không làm theo bất kỳ đường link hoặc số điện thoại nào mà bạn nhận được.
    - Cố gắng nhận thức được các rủi ro bảo mật trực tuyến cho bản thân, cộng đồng của bạn và bất kỳ hội nhóm nào mà bạn tham gia.
- **Bảo vệ thông tin của bạn.**
    - Sử dụng các ứng dụng nhắn tin được mã hóa, chẳng hạn như Signal. Điều này sẽ ngăn không cho người khác đọc được tin nhắn của bạn.
    - Chỉ chia sẻ thông tin trên một trang web nếu địa chỉ của nó bắt đầu bằng HTTPS. Chữ S là viết tắt của từ "secure" (bảo mật) và có nghĩa là mọi thông tin qua lại giữa bạn và trang web đều được mã hóa.
    - Cân nhắc sử dụng mạng riêng ảo (VPN), nó có thể bảo vệ dữ liệu và ẩn vị trí của bạn.
    - Kiểm tra các ứng dụng của bạn có quyền truy cập vào các dữ liệu gì và được cấp những quyền gì. Ví dụ, một ứng dụng tập thể dục thì không cần quyền truy cập vào danh bạ của bạn.

Tôi phải làm gì nếu bị lừa đảo hoặc tệ hơn thế?

Có rất nhiều nơi bạn có thể tìm đến để được giúp đỡ. Tất cả các tổ chức này sẽ không chia sẻ thông tin của bạn với bất kỳ ai khác, trừ khi bạn đồng ý.

- Bạn có thể báo cáo các sự cố mạng cho NCSC thông qua trang CERT NZ và chúng tôi có thể giúp đỡ hoặc kết nối bạn với một cơ quan khác:
  Báo cáo sự cố | CERT NZ
- Nếu bạn bị mất tiền, bạn nên liên hệ ngay với ngân hàng của bạn.
- Bạn có thể chuyển tiếp (forward) miễn phí các tin nhắn lừa đảo đến số 7726, một dịch vụ do Bộ Nội vụ điều hành.