National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Giữ cho tổ chức của bạn an toàn trên mạng

Tại sao an ninh mạng lại quan trọng với các hội nhóm và tổ chức cộng đồng?

Trang này đưa ra lời khuyên và một số bước bạn có thể thực hiện để bảo vệ các hội nhóm, tổ chức cộng đồng của bạn tránh khỏi các mối đe dọa an ninh mạng. Ngoài ra còn có tài liệu hướng dẫn riêng dành cho các cá nhân để giữ cho họ an toàn trên mạng.

Lời khuyên này dựa trên những mối đe dọa phổ biến và nghiêm trọng nhất.

- Cập nhật – cập nhật phần mềm trên thiết bị của bạn để vá mọi lỗ hổng bảo mật.
    - Cập nhật các thiết bị của hội nhóm, tổ chức cộng đồng của bạn. Điều này bao gồm điện thoại, máy tính, bộ định tuyến WiFi (router) và bất kỳ thứ gì khác kết nối với internet - bao gồm các thiết bị thông minh.
    - Sử dụng tính năng cập nhật tự động khi có thể.
- Xác thực hai yếu tố (2FA) – tăng cường bảo mật cho tài khoản của bạn bằng cách yêu cầu mật khẩu và một bước nữa, chẳng hạn như mã số từ một ứng dụng trên điện thoại của bạn.
    - Lưu ý: Tính năng này còn được gọi là xác thực đa yếu tố (MFA), xác minh hai bước (2SV) và nhiều tên gọi khác.
    - Bật 2FA trên tất cả tài khoản của hội nhóm, tổ chức cộng đồng của bạn.
    - Nếu có thể, hãy cố gắng sử dụng một hình thức 2FA có khả năng chống lừa đảo (phishing), nghĩa là bạn không thể bị lừa cung cấp thông tin. Đây có thể là một khóa bảo mật vật lý hoặc một thứ gì đó ví dụ như dấu vân tay hoặc ID (nhận diện) khuôn mặt.
- Để ý các tài khoản trực tuyến của bạn – đảm bảo các thành viên cũ không còn giữ quyền truy cập vào các tài khoản sau khi họ rời khỏi hội nhóm, tổ chức cộng đồng.
    - Nếu có nhiều người truy cập cùng một tài khoản, hãy đảm bảo rằng tất cả họ đều có tên đăng nhập khác nhau và đều bật 2FA.
    - Lưu danh sách tất cả tài khoản người dùng và hủy kích hoạt (deactivate) bất kỳ tài khoản nào không cần thiết, chẳng hạn như khi nhân viên nghỉ việc.
    - Ghi lại danh sách các thiết bị bạn đã cung cấp cho các thành viên trong cộng đồng và nhớ lấy lại chúng và khôi phục cài đặt gốc (factory reset) khi người đó rời khỏi tổ chức. Bạn cũng có thể cần phải thay đổi mã số vật lý dùng để ra vào tòa nhà.
- Kiểm tra xem ai có quyền truy cập vào các tài khoản trực tuyến của bạn – những người trong hội nhóm, tổ chức cộng đồng của bạn chỉ nên có quyền truy cập vào những thứ họ cần.
    - Nếu tài khoản của một người nào đó bị tấn công (hack), các bước này sẽ hạn chế tác hại mà kẻ tấn công có thể gây ra.
    - Thường xuyên kiểm tra và loại bỏ các quyền (permission) không cần thiết.

- Nếu bạn có một tài khoản "quản trị viên" ("admin") duy nhất mà nhiều người cùng sử dụng, hãy theo dõi nó để biết có hoạt động bất thường nào không. Cố gắng hạn chế có những loại tài khoản như vậy, đặc biệt là đối với các công việc hàng ngày.
- Các quy tắc này cũng áp dụng với quyền truy cập của quản trị viên vào các thiết bị, chẳng hạn như router.

- Xem lại hợp đồng của bạn với các nhà cung cấp dịch vụ - bạn có thuê người vận hành dịch vụ CNTT cho bạn hay không.
  - Đảm bảo họ có sắp đặt các biện pháp bảo vệ an ninh mạng để đáp ứng các nhu cầu của hội nhóm, tổ chức cộng đồng của bạn.
- Biết cách thức mà tất cả các tài khoản và hệ thống của bạn hoạt động cùng nhau – việc nắm rõ các kết nối sẽ giúp bạn biết kẻ tấn công có thể xâm nhập vào đâu.
  - Xem lại các kết nối giữa các hệ thống của bạn, ví dụ như email, lưu trữ đám mây và các nền tảng kế toán.
  - Cân nhắc sử dụng Mạng riêng ảo (VPN) để tăng cường an toàn trên mạng. Sử dụng VPN sẽ ẩn hoạt động trực tuyến của bạn khỏi bất kỳ ai có thể đang cố gắng theo dõi bạn. Điều này đặc biệt hữu ích nếu bất kỳ thành viên nào trong hội nhóm, tổ chức cộng đồng của bạn kết nối từ xa.
- Đảm bảo mọi người trong cộng đồng của bạn đều 'thông minh trên mạng' ('cybersmart') – những người trong hội nhóm, tổ chức cộng đồng của bạn có nhiều khả năng bị nhắm mục tiêu hơn so với các hệ thống của bạn.
  - Đào tạo tất cả nhân viên về an ninh mạng cơ bản. Trang web Own Your Online Own Your Online | NCSC cung cấp nhiều lời khuyên và mẹo để giúp cho bạn an toàn trên mạng và hướng dẫn cách nhận biết các kiểu lừa đảo.
  - Nhắc nhở họ rằng điều này quan trọng đối với các tài khoản cá nhân của họ cũng như các tài khoản họ sử dụng cho tổ chức của bạn.
  - Chúng tôi cũng có hướng dẫn dành cho các cá nhân để giữ cho họ an toàn trên mạng.
- Lên kế hoạch ứng phó sự cố – có sẵn một kế hoạch ứng phó là việc quan trọng để mọi người không hoảng sợ khi có sự cố xảy ra.
  - Kế hoạch ứng phó sự cố nêu rõ ai sẽ làm gì khi xảy ra sự cố. Kế hoạch mẫu có sẵn tại đây Incident Management | NCSC
  - Bao gồm kế hoạch về những việc cần làm nếu điện thoại, máy tính hoặc các hệ thống khác bị hỏng. Luôn cập nhật kế hoạch này.
  - Lưu lại thông tin liên lạc của tất cả những người cần thiết và sao lưu các thông tin trong trường hợp phương thức chính để liên lạc với họ bị hỏng (chẳng hạn như email).
  - Đồng thời giữ bản kế hoạch này ở một nơi nào đó bên ngoài hệ thống của bạn, phòng trường hợp bạn không thể truy cập hệ thống được.