secdev foundation DSH vietnam VIETNET-ICT

Sổ tay dành cho học viên

Dự án Digital Safety Hub Vietnam

Sổ tay dành cho học viên
Dự án Digital Safety Hub Vietnam

BẢN QUYỀN THUỘC VỀ
VIETNET-ICT VÀ SECDEV FOUNDATION

Thông tin liên hệ:

TRUNG TÂM CÔNG NGHỆ THÔNG TIN
TRUYỀN THÔNG VIETNET (VIETNET-ICT)
Email: contact@vietnet-ict.org
Tel: 024 62694690

Trong thời đại công nghệ 4.0, việc ứng dụng công nghệ để chuyển đổi quản trị tổ chức là một yếu tố cần có để các tổ chức phi chính phủ, phi lợi nhuận phát triển hiệu quả và bền vững. Tuy nhiên, đi cùng với những ứng dụng công nghệ là những nguy cơ về an toàn mạng sẽ phải đối mặt.

Để hỗ trợ các tổ chức, Trung tâm Công nghệ Thông tin - Truyền thông Vietnet (Vietnet-ICT) hợp tác cùng với Quỹ SecDev (The SecDev Foundation), một tổ chức phi chính phủ Canada khởi động dự án "Digital Safety Hub" tại Việt Nam với mong muốn tổ chức các khoá tập huấn về an toàn số cho các tổ chức phi chính phủ, phi lợi nhuận trong mạng lưới có nhu cầu.

TẠI SAO AN TOÀN SỐ LẠI QUAN TRỌNG?

Tội phạm mạng và chiến lược số quốc gia đòi hỏi tất cả các cá nhân và tổ chức cần có sự chuẩn bị để trở nên an toàn trong thế giới số. Tất cả chúng ta đều nên được trang bị những kỹ năng công dân số.

ĐÀO TẠO AN TOÀN (KỸ THUẬT) SỐ LÀ GÌ?

Đào tạo an toàn số hướng tới trang bị cho các cá nhân và tổ chức các kiến thức từ đó cá nhân/tổ chức có thể xác định các rủi ro số của họ và biết cách bảo vệ dữ liệu số, thiết bị và tài khoản trực tuyến của họ. Một số lĩnh vực/ khái niệm có thể liệt kê như: mật khẩu mạnh, xác thực hai yếu tố, cách thức liên lạc an toàn, hiểu phần mềm độc hại và các cuộc tấn công mạng khác, đồng thời cộng tác trực tuyến với đồng nghiệp và người thụ hưởng một cách an toàn và bảo mật.

Giới thiệu chung về đơn vị tổ chức

VIETNET-ICT

Trung tâm CNTT-TT Vietnet (Vietnet-ICT): Là tổ chức phi chính phủ, phi lợi nhuận tại Việt Nam với sứ mệnh hỗ trợ cộng đồng, đặc biệt là nhóm dễ bị tổn thương tại Việt Nam tiếp cận và hưởng lợi từ các dịch vụ CNTT và truyền thông, thông qua thúc đẩy hợp tác đối tác và tăng lường năng lực.

SECDEV.FOUNDATION

Quỹ SecDev, Canada (The SecDev Foundation): Quỹ tại Canada, làm việc trong các lĩnh vực liên quan đến phát triển và công nghệ mới. Quỹ SecDev tập trung nghiên cứu, phát triển giải pháp dữ liệu để tạo ra những sự thay đổi tích cực và hoạt động chủ yếu tại các khu vực Trung Đông, Châu Á, và Đông Nam Á.

RỦI RO SỐ CỦA TÔI

Kiến thức cần nhớ:

Nhận thức được tầm quan trọng của ý thức bảo mật

SỬ DỤNG ma trận quản trị rủi ro **ĐỂ CÂN ĐỐI NGUỒN LỰC** khi **XỬ LÝ RỦI RO.**

Hãy kiểm kê những tài sản số mà bạn có vào những ô dưới đây:

CUỘC SỐNG SỐ ⟷ **TÀI SẢN SỐ**

Thiết bị	Phần mềm	Thông tin	Danh tính	Khác

BẠN CÓ NHIỀU HƠN BẠN NGHĨ!

Khi tham gia trên môi trường trực tuyến, những tài sản số của chúng ta sẽ gặp phải những rủi ro.

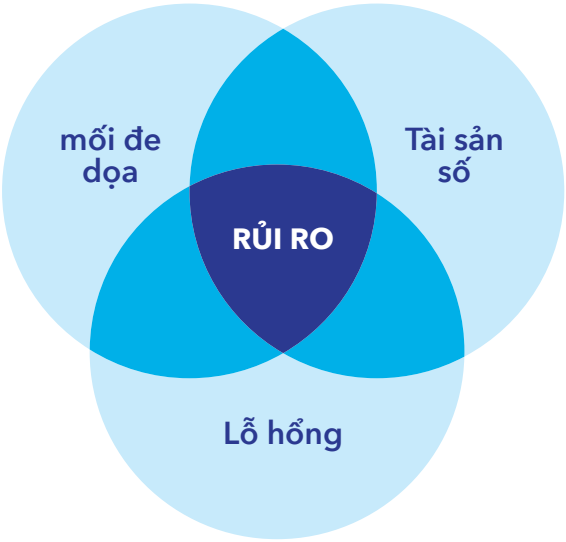
ĐIỀU QUAN TRỌNG LÀ Ý THỨC BẢO MẬT

MA TRẬN QUẢN LÝ RỦI RO

Cách dùng:
Bước 1: Xác định mức độ của rủi ro bằng cách xác định: (1) Xác suất của rủi ro; (2) Tác động của rủi ro

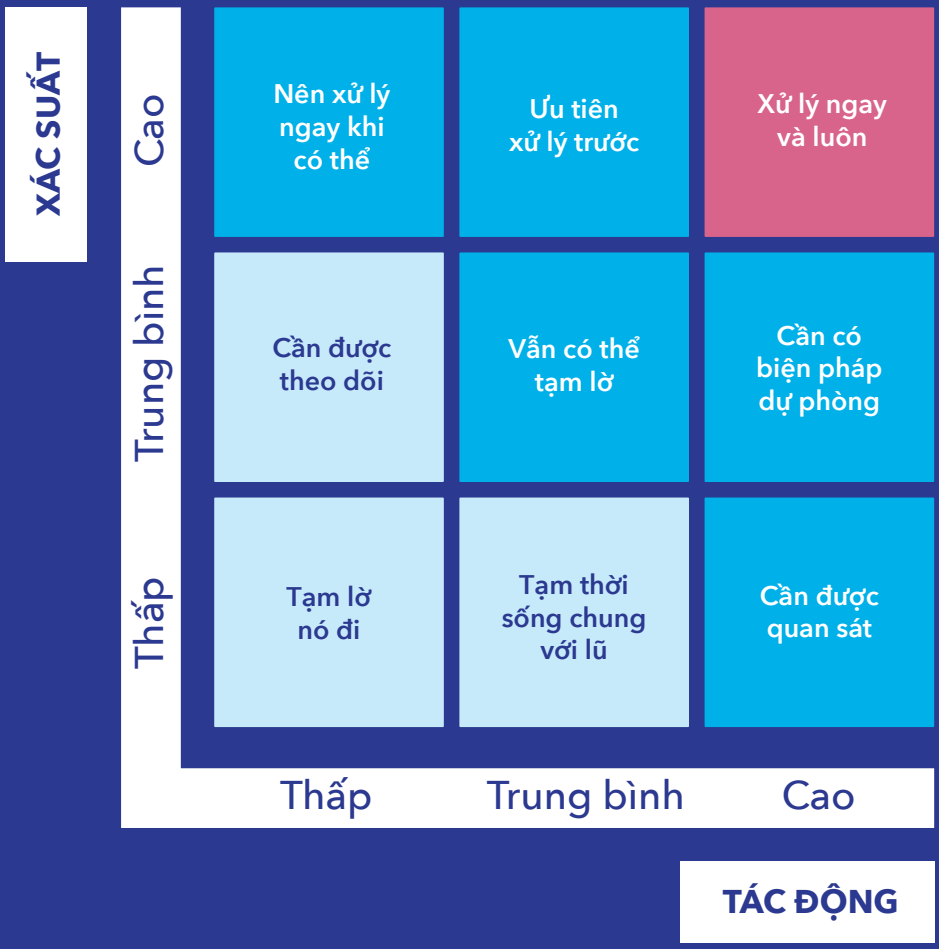
Bước 2: Sử dụng ma trận quản trị rủi ro để xác định chúng ta cần xử lý rủi ro ấy như thế nào

$$\text{Rủi ro} = \begin{matrix}\text{Giá trị tài sản}\\ + \\ \text{mối đe dọa}\\ + \\ \text{lỗ hổng}\end{matrix} - \text{ý thức bảo mật}$$



VÍ DỤ

MA TRẬN RỦI RO



MẬT KHẨU CỦA TÔI

Kiến thức cần nhớ:

Sử dụng mật khẩu mạnh + Xác thực hai yếu tố + Ứng dụng quản lý mật khẩu

Thực hành: Hãy chuyển những cụm từ dưới đây thành một mật khẩu mạnh nhé!

Homnayemtoitruong

Muathuthatdep

PASSWORD CHECK!

Với mỗi câu trả lời có, bạn được 1 điểm

- Cài mật khẩu trên tất cả các thiết bị
- Bật xác thực 2 yếu tố ở các tài khoản email và mạng xã hội (Nếu có một trong hai loại tài khoản chưa bật xác thực hai lớp, thì bạn không được tính điểm ở câu này)
- @Aa28 xxxxxxxx — Sử dụng một mật khẩu mạnh (Chữ và số: 12 chữ cái (viết hoa và viết thường), số, ký hiệu đặc biệt; không phải thông tin cá nhân dễ đoán về bạn)
- LOGIN — Không dùng tính năng tự thay đổi mật khẩu thường xuyên mà cài đặt thay đổi mật khẩu khi có đăng nhập bất thường
- Sử dụng ứng dụng quản lý mật khẩu (VD: Lastpass hoặc Keepass)

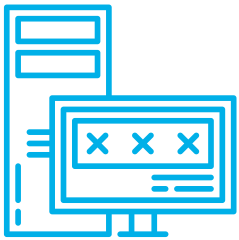
Nếu bạn được 4-5 điểm, xin chúc mừng, bạn thực hành rất tốt với mật khẩu.
Nếu bạn được 2-3 điểm, bạn cần chú ý hơn tới mật khẩu của mình.
Nếu bạn được 1 điểm, bạn cần thêm kiến thức về bảo mật mật khẩu ngay!

Để tìm hiểu ứng dụng quản lý mật khẩu là gì và dùng như thế nào, quét mã QR để đọc ngay!

Đáp án gợi ý:
H0MN4y3MT0ITRUON9
Mu4thuth@Td3p

DỮ LIỆU CỦA TÔI

HỎI NHANH ĐÁP GỌN DỮ LIỆU KHÔNG LỌT



Dữ liệu của tôi có thể phân loại như thế nào?

Đáp: Xác định các dữ liệu cần được lưu trữ, sắp xếp chúng ngăn nắp, gọn gàng và có thể phân loại dữ liệu thành các loại khác nhau tùy theo: (1) loại tài liệu; (2) mục đích sử dụng; và (3) mức độ quan trọng

Cách bảo vệ dữ liệu tại ổ?

Đáp: Mã hóa toàn bộ ổ đĩa để bảo vệ dữ liệu tại ổ bằng các phần mềm như VeraCrypt, BitLocker...

CyberSTAR

VeraCrypt

Windows 10 BitLocker

Tôi cần lưu ý gì khi sao lưu dữ liệu?

Thường xuyên sao lưu các dữ liệu quan trọng
Sao lưu dữ liệu thường xuyên với 3 bản sao lưu (1 trên đám mây và 2 trên các thiết bị/ ổ cứng).
Đảm bảo thiết bị chứa dữ liệu sao lưu không kết nối liên tục vào thiết bị lưu trữ bản gốc, cả về mặt vật lý hay thông qua mạng nội bộ

Xoá dữ liệu sao cho an toàn?

Khi bạn xóa một tệp khỏi máy tính hoặc điện thoại di động, chúng không biến mất hoàn toàn khỏi các thiết bị, những tệp này vẫn có thể bị khôi phục. Đây là lý do tại sao chúng ta không nên chỉ đơn giản xóa một tệp mà cần dùng ứng dụng chuyên dụng. CCleaner là một trong những chương trình đó. Dễ sử dụng, CCleaner cho phép bạn xóa các tệp riêng biệt hoặc định dạng toàn bộ ổ cứng trên thiết bị của bạn. (Lưu ý: Chúng ta không thể xóa an toàn ở những ổ cứng SSD)

THIẾT BỊ CỦA TÔI

NHỮNG THỰC HÀNH CƠ BẢN ĐỂ BẢO VỆ THIẾT BỊ

Đặt mật khẩu để đăng nhập ở các thiết bị (điện thoại và máy tính)

Đăng xuất khỏi thiết bị hoặc khóa máy khi không dùng nữa hay rời khỏi chỗ ngồi

Hạn chế quyền truy cập (tách tài khoản Admin và User), tạo tài khoản riêng biệt cho mọi người dùng cho các trường hợp phải sử dụng chung máy tính với người khác

Giữ các thiết bị (và toàn bộ các ứng dụng đã cài đặt) luôn ở chế độ cập nhật, sử dụng lựa chọn "cập nhật tự động" nếu có sẵn

Khi gửi các dữ liệu nhạy cảm, không truy cập vào wifi công cộng – Hãy sử dụng kết nối 3G hay 4G hoặc sử dụng VPN

Sử dụng các phần mềm bản quyền sẽ giúp tránh khỏi các rủi ro về bảo mật

Cấu hình thiết bị để khi bị mất cắp có thể theo dõi, xóa hay khóa từ xa

TIPS BỎ TÚI CHO BẠN
LƯU Ý CHO ĐIỆN THOẠI

- Nếu nghi ngờ máy của bạn bị xem trộm hoặc bị tạm lấy mất thẻ SIM, bạn có thể kiểm nghiệm bằng cách bí mật đánh dấu lên điện thoại hoặc dán tem lên điện thoại. Nếu điện thoại bị xâm nhập, thường những dấu hiệu này sẽ không giống ban đầu.
- LUÔN KHOÁ MÁY bằng mật mã hoặc PIN
- Không lưu thông tin nhạy cảm trên điện thoại. Điện thoại theo bạn khắp mọi nơi, nguy cơ mất điện thoại sẽ cao hơn những công cụ lưu trữ khác.
- Khi muốn cho hay bỏ điện thoại, hãy chắc chắn rằng bạn không để bất kỳ thông tin lưu trữ trên máy, thẻ SIM. Nếu bạn không muốn giữ thẻ SIM, tốt nhất hãy huỷ đi.
- Thường xuyên sao lưu dữ liệu trên điện thoại vào máy tính.
- Ghi lại số IMEI của điện thoại, số này giống như số CMND của điện thoại (xem bằng cách bấm *#606# hoặc vào xem tại Settings/Thiết đặt). Nhà mạng có thể lần ra tung tích của điện thoại thông qua số IMEI nên trong trường hợp bị mất điện thoại, nếu may mắn bạn có thể tìm lại được điện thoại.
- Khi mang điện thoại đi sửa, hãy lưu ý chọn người tin cậy. Lưu ý thoát các tài khoản trước khi mang đi sửa.

Bảo mật thiết bị bắt đầu ngay từ những thói quen cơ bản nhất. Hãy dành thời gian "khám phá" các thiết đặt trong máy, bạn nhé!

CUỘC TRÒ CHUYỆN SỐ CỦA TÔI

Mối đe dọa đối với thông tin liên lạc điện tử:

- Nghe lén từ phía máy khách
- Lỗ hổng và cửa sau trong phần mềm
- Thiết bị lưu trữ không an toàn
- Thu thập và sử dụng dữ liệu người dùng một cách không kiểm soát

TIPS:

- Đối với trình duyệt: Chọn các trình duyệt có tính an toàn cao hơn như FireFox, Chromia...

- Lựa chọn nền tảng messenger an toàn thông qua việc đánh giá các mối đe dọa đối với tổ chức và tính năng của nền tảng để giải quyết mối đe dọa đó để chọn nền tảng có sai sót tối thiểu và lợi thế tối đa. Lưu ý các nền tảng có mã hóa đầu cuối...

HỎI NHANH ĐÁP GỌN

LÀM SAO ĐỂ GỌI ĐIỆN & NHẮN TIN AN TOÀN?

? Bạn ơi, chỉ tôi mấy chiêu để gọi điện và nhắn tin an toàn đi.

Đáp: Nguyên tắc thứ nhất là không gọi điện hay nhắn tin bằng cách thông thường cho những chuyện "quan trọng". Nếu bạn làm theo cách thông thường thì 100% là các cuộc gọi và tin nhắn sẽ được lưu lại trong cơ sở dữ liệu của nhà mạng. Chúng ta nếu muốn bí mật là của riêng mình thì phải dùng cách khác.

? Cách nào vậy bạn ơi?

Đáp: Hãy dùng internet để liên lạc, có một số phần mềm liên lạc trên internet còn mã hoá đầu cuối các cuộc trò chuyện và tin nhắn

? Mã hoá đầu cuối là sao bạn ơi?

Đáp: Bạn có thể hiểu đơn giản là một hình thức bảo mật mà chỉ người gửi và người nhận có thể đọc được nội dung tin nhắn, cuộc gọi được truyền đi trong ứng dụng trò chuyện đó.

? Mình nên dùng ứng dụng nào bạn ơi?

Trước tiên, bạn hãy kiểm tra xem ứng dụng bạn định dùng có mã hoá không bằng cách tra cứu. Bạn có thể cân nhắc sử dụng những ứng dụng như Signal, Wire hoặc đơn giản như Skype.

Hãy luôn nhớ thần chú "Mã hoá đầu cuối" như yêu cầu bắt buộc cho các ứng dụng trò chuyện của mình nhé.

DANH TÍNH SỐ CỦA TÔI

Danh tính có thể được định nghĩa là "Tôi là ai và tôi làm gì". Nói cách khác, danh tính của tôi là tổng hợp dữ liệu của tôi, bao gồm ngày sinh, nơi tôi học tập hoặc nghiên cứu hoặc nơi tôi làm việc, cỡ giày của tôi, v.v. Cũng giống như vậy, người dùng Internet có danh tính số - là tổng hợp các thông tin, đặc điểm và lịch sử tương tác của họ, và về họ trên môi trường internet.

MÁCH BẠN MẸO LƯỚT WEB AN TOÀN

Về cơ bản, chuyện bạn lên mạng, xem những trang gì, bình luận ở đâu, làm việc gì (hay còn gọi là dấu chân số của bạn đó!) đều có thể bị theo dõi bởi nhà cung cấp dịch vụ mạng và những hacker "lành nghề".

Nếu bạn không muốn ai biết bạn làm gì, ở đâu... thì sau đây là những mẹo nhỏ:

- Kết nối mạng an toàn
- Lướt web an toàn
- Kiểm tra đường link & download an toàn

1. Luôn luôn dùng mạng ảo VPN hoặc những chương trình tương tự như Psiphon 3, Tor để lên mạng. Những chương trình này sẽ giúp bạn ẩn danh và mã hoá những truy cập mạng.

2. Tránh dùng những mạng internet mở hay hostpot, điều này không những giúp bạn bảo vệ sự riêng tư mà còn tránh cho bạn nguy cơ bị đánh cắp tài khoản.

3. Thường xuyên cập nhật trình duyệt.

4. Kích hoạt chế độ không lưu lại lịch sử trong trình duyệt. Bằng cách này, tất cả lịch sử lướt web, lịch sử download, mật khẩu… của bạn sẽ không bị lưu lại.

5. Bạn có thể dùng công cụ tìm kiếm Start Page hoặc DuckDuckGo để tìm kiếm một cách "lặng lẽ", những công cụ tìm kiếm này bảo vệ tính riêng tư cao hơn các công cụ tìm kiếm thông dụng.

6. Khi bạn truy cập vào những trang web có tính rủi ro cao, hãy hạn chế sự hoạt động Java để tránh máy tính bị nhiễm mã độc.

7. Sử dụng HTTPS Everywhere để bảo mật kết nối giữa máy tính và website, tiện ích này yêu cầu trình duyệt luôn ưu tiên vào website bằng con đường an toàn nhất (thông qua https)

8. Bạn nên xoá hết lịch sử lướt web, và nếu giữ lại thì cũng chỉ giữ với một số lượng hạn chế. Lí do làm việc này là tránh để hacker dựa vào các lịch sử đó suy đoán được thói quen lướt mạng của bạn.

9. Trước khi vào bất cứ website nào hay download bất cứ thứ gì, nên kiểm tra đường link.

10. Không nên click vào một đường link không rõ xuất xứ, bạn nên sử dụng Virus Total để kiểm tra đường link trước khi quyết định download hay mở ra xem.

11. Mở file đã tải về thông qua chương trình diệt virus để kiểm tra có bị cài đặt mã độc hay không.


“Security is a process,
not a product”
"Bảo mật là một quá trình,
không phải là một sản phẩm"
- Bruce Schneier -

Thông tin liên hệ:

TRUNG TÂM CÔNG NGHỆ THÔNG TIN TRUYỀN THÔNG VIETNET (VIETNET-ICT)

Email: contact@vietnet-ict.org

Tel: 024 62694690

Nội dung:
Nhóm giảng viên dự án DSH

Thiết kế:
Thanh Nguyễn

BẢN QUYỀN THUỘC VỀ
VIETNET-ICT VÀ SECDEV FOUNDATION