WORK – Nâng cao kỹ năng số và hợp tác hiệu quả

1 LIVE – Tìm kiếm và đánh giá thông tin

2 **WORK – Nâng cao kỹ năng số và hợp tác hiệu quả**

3 PLAY – Giao tiếp an toàn trực tuyến

Nâng cao năng lực kỹ thuật số

Dự án: Nâng cao năng lực số của chính quyền địa phương, doanh nghiệp và người dân - Hướng tới một quốc gia số

Ngày 2, Buổi sáng

THE WORKSHOP

Quan điểm về năng lực kỹ thuật số

Sẵn sàng giúp đỡ người khác cải thiện năng lực kỹ thuật số của họ, xây dựng điểm mạnh và giảm thiểu điểm yếu của họ.

Không nản lòng trước tốc độ thay đổi nhanh chóng của công nghệ nhưng tin rằng người ta luôn có thể tìm hiểu thêm về cách công nghệ có thể được sử dụng trong xã hội ngày nay.

Sẵn sàng đánh giá tiềm năng của chính một người những người khác để liên tục học hỏi

Nâng cao năng lực kỹ thuật số

Nói về tầm quan trọng của việc nhận ra "tin tức giả" với những người khác

Sẵn sàng yêu cầu được dạy cách sử dụng ứng dụng (ví dụ: cách đặt lịch hẹn với bác sĩ trên internet) thay vì giao nhiệm vụ cho người khác.

Kiểm tra độ uy tín và tin cậy của nội dung số

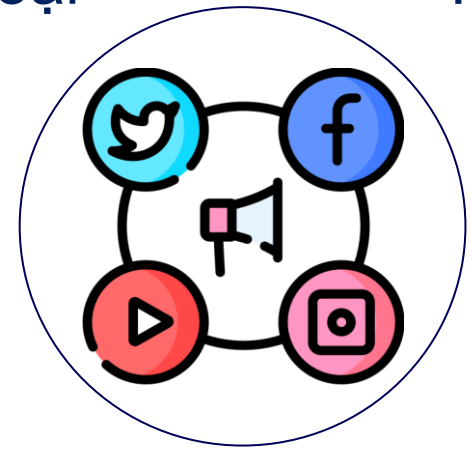
- Sẵn sàng chia sẻ kiến thức chuyên môn trên internet.
- Cởi mở chia sẻ nội dung kỹ thuật số.
- Không chia sẻ tài nguyên kỹ thuật số nếu không thể trích dẫn tác giả hoặc nguồn của chúng theo cách thích hợp.

Dịch vụ và công cụ truyền thông

Điện thoại

Thư điện tử

Hội nghị video



Mạng xã hội

Podcast

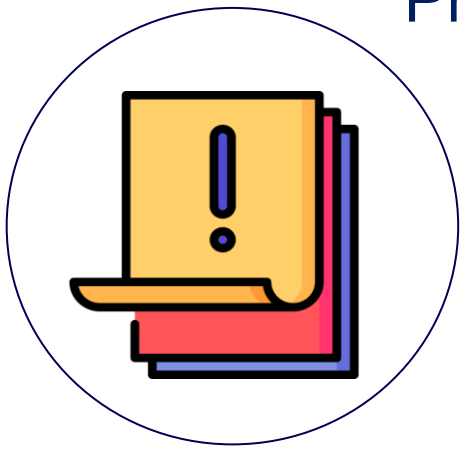
Sử dụng dịch vụ và công cụ truyền thông

Báo cáo & tóm tắt

Chia sẻ ý tưởng

Phản hồi & lời khuyên

Lên lịch họp



Mốc sự kiện quan trọng

Khái niệm về cộng tác từ xa

- Làm việc từ xa chính là việc người lao động sử dụng các thiết bị công nghệ liên lạc, giao tiếp hiện đại để làm việc ở bất cứ đâu để thực hiện công việc.

THE WORKSHOP

Lợi ích của cộng tác từ xa

- Giảm thiểu thời gian và chi phí di chuyển giữa nhà và văn phòng.
- Thời gian và không gian làm việc linh hoạt.
- Tăng độ tập trung với công việc.
- Giải tỏa căng thẳng.
- Cân bằng cuộc sống.
- Tiết kiệm chi phí thuê văn phòng.
- Gia tăng cơ hội làm việc với nhân viên ở các khu vực khác nhau.

Khó khăn của cộng tác từ xa

- Mất đi sự gắn bó với đồng nghiệp và môi trường làm việc
- Tăng chi phí khi làm việc ở nhà
- Nguy cơ mất cân bằng giữa cuộc sống và công việc
- Các nguồn gây xao nhãng
- Nguy cơ bảo mật thông tin

Quan điểm trong cộng tác từ xa

- Khuyến khích mọi người bày tỏ ý kiến của khi cộng tác trong môi trường kỹ thuật số.
- Hành động một cách đáng tin cậy để đạt được mục tiêu của nhóm khi tham gia xây dựng nguồn lực hoặc kiến thức.
- Sử dụng các công cụ kỹ thuật số thích hợp để thúc đẩy sự cộng tác giữa các thành viên trong nhóm.

Kỹ năng xã hội tốt → Giao tiếp rõ ràng → Khả năng làm sáng tỏ sự hiểu lầm

PLAY – Giao tiếp an toàn trực tuyến

1 LIVE – Tìm kiếm và đánh giá thông tin

2 WORK – Nâng cao kỹ năng số và hợp tác hiệu quả

3 PLAY – Giao tiếp an toàn trực tuyến

THE WORKSHOP

Người dân tham gia công nghệ số

Dự án: Nâng cao năng lực số của chính quyền địa phương, doanh nghiệp và người dân - Hướng tới một quốc gia số

Ngày 2, Buổi sáng

Các loại dịch vụ kỹ thuật số

Dịch vụ công

Dịch vụ cộng đồng

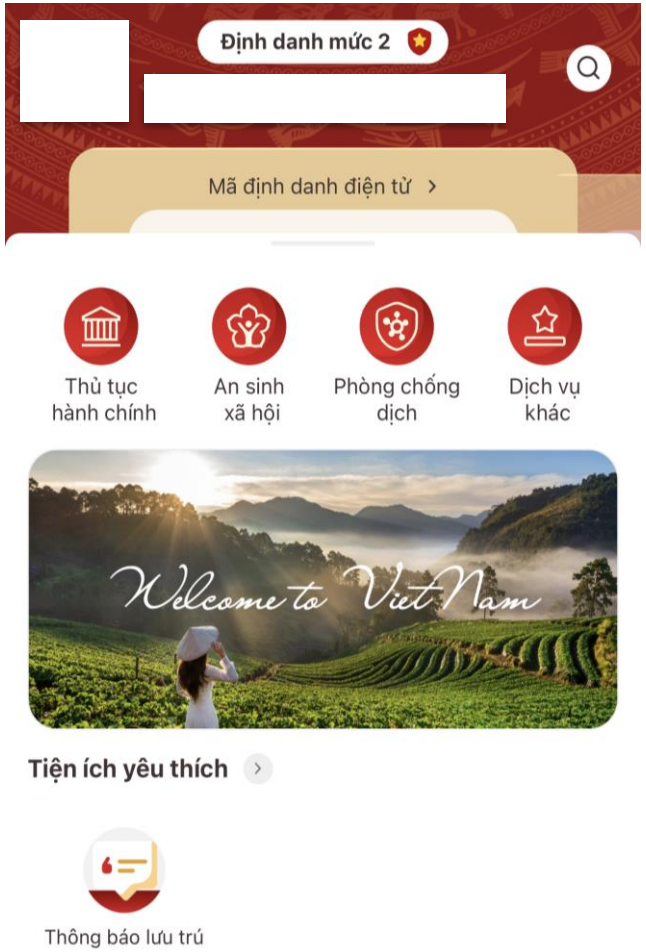
Dịch vụ tư nhân

Danh tính số là gì?

Ví dụ về danh tính số:

- Tên người dùng và mật khẩu.
- Các hoạt động tìm kiếm trực tuyến, chẳng hạn như giao dịch điện tử.
- Ngày sinh.
- Tiền sử bệnh.
- Lịch sử mua hàng.

Ở Việt Nam, danh tính số đang ngày càng phổ biến hơn

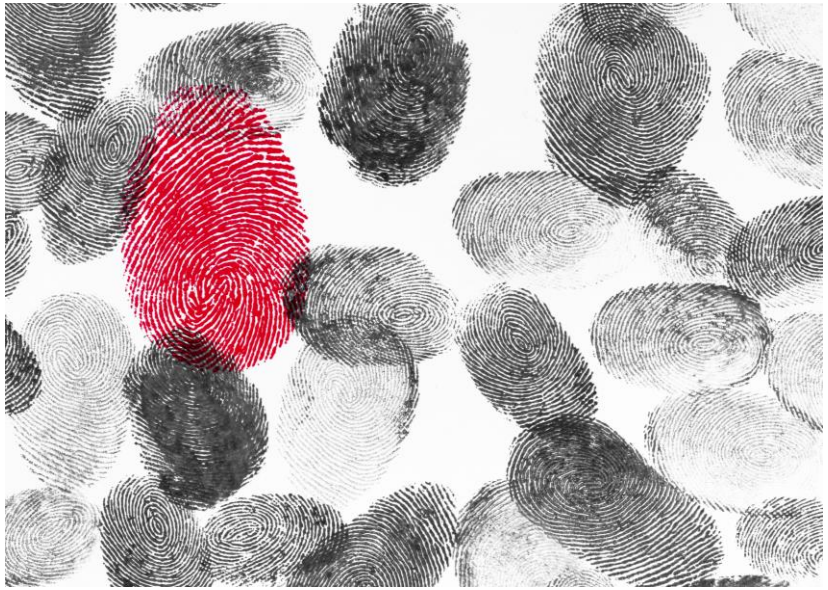


Ví dụ về danh tính số:

- Căn cước công dân.

Xác thực người dùng

- Phương pháp xác thực người dùng trên một trang web hoặc một dịch vụ trực tuyến hay quyền xác thực người dùng, là quá trình xác minh thông tin đăng nhập của một người dùng hoặc thiết bị cố gắng truy cập vào một hệ thống.



Làm thế nào để xác thực người dùng?

Truy tìm tập hợp dữ liệu xác định người dùng:

- Các hoạt động, hành động và đóng góp của người dùng trên internet (VD: các trang đã xem, lịch sử mua hàng).
- Dữ liệu cá nhân (VD: tên, tên người dùng, dữ liệu hồ sơ như tuổi, giới tính, sở thích).
- Dữ liệu ngữ cảnh (ví dụ: vị trí địa lý).

THE WORKSHOP

THE WORKSHOP

Khái niệm về cookie

- Cookie cho phép một website lưu các thông tin trên máy tính của người dùng và sau đó lấy lại nó.

Lợi ích và rủi ro

Các lợi ích và rủi ro khi quản lý một hoặc nhiều danh tính kỹ thuật số trên các hệ thống, ứng dụng và dịch vụ kỹ thuật số:

✓ Lợi ích: quy trình xác thực nhanh, tùy chọn của người dùng

X Rủi ro: bị đánh cắp danh tính, dữ liệu cá nhân bị bên thứ ba khai thác

Hướng dẫn tạo, xây dựng, và bảo vệ danh tính số

Các chiến lược sử dụng để kiểm soát, quản lý hoặc xóa dữ liệu được thu thập/quản lý bởi các hệ thống trực tuyến:

- Theo dõi các dịch vụ được sử dụng.
- Liệt kê các tài khoản trực tuyến.
- Xóa các tài khoản không được sử dụng.

Cách hạn chế và quản lý việc theo dõi các hoạt động của người dùng (bản thân) trên internet:

- Tính năng phần mềm: duyệt web riêng tư, xoá cookie.
- Công cụ nâng cao quyền riêng tư và các tính năng sản phẩm/dịch vụ: đồng ý tùy chỉnh đối với cookie, chọn không tham gia quảng cáo được cá nhân hóa.

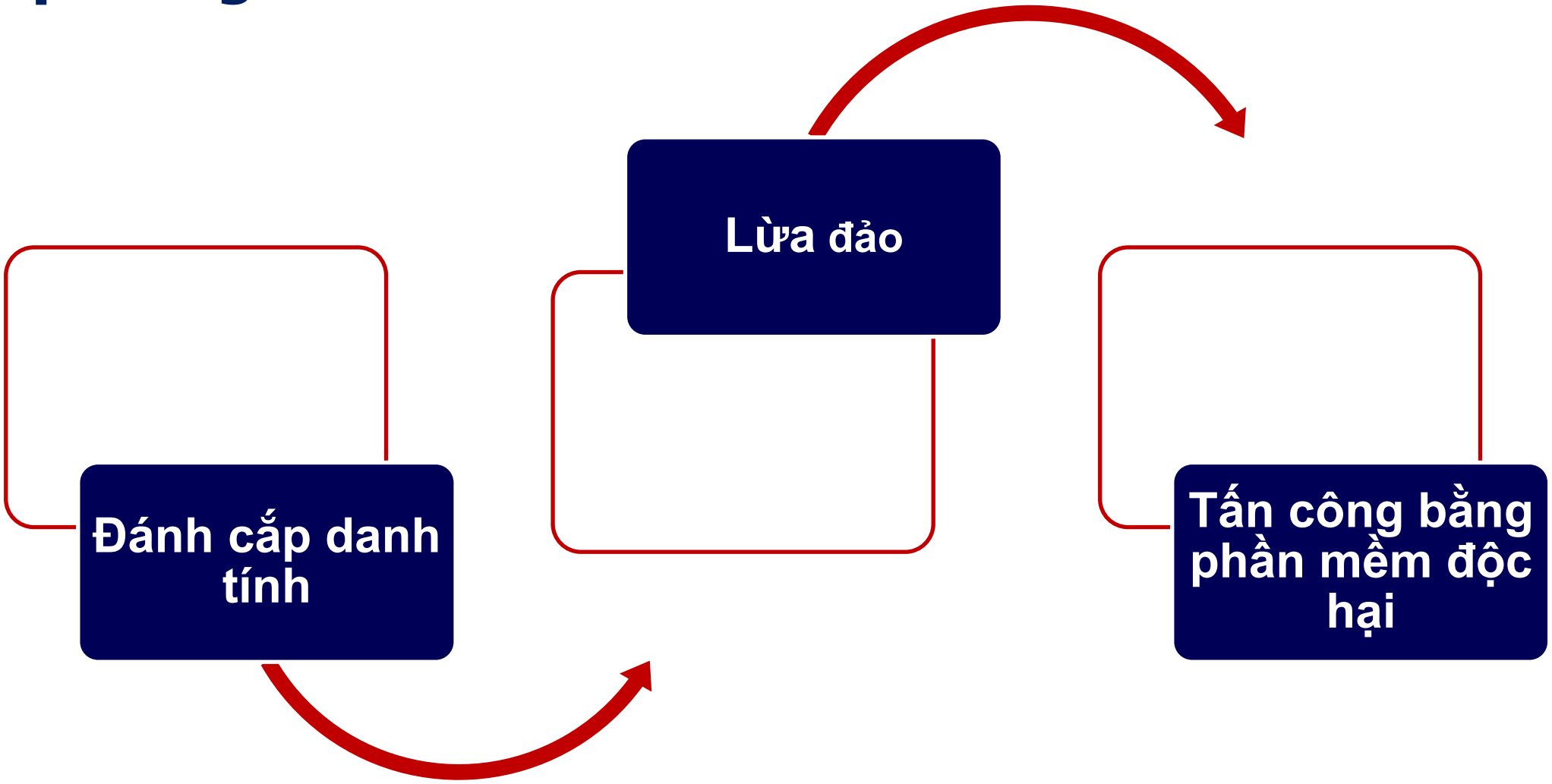
Bảo vệ các loại thiết bị

Dự án: Nâng cao năng lực số của chính quyền địa phương, doanh nghiệp và người dân - Hướng tới một quốc gia số

Ngày 2, Buổi sáng

THE WORKSHOP

Các rủi ro về an toàn khi sử dụng các thiết bị hoặc hệ thống có kết nối internet



Tại sao cần có nhận thức ATTT?

Đảm bảo ATTT tốt nhất theo qui tắc "90/10":

10% vấn đề ATTT phụ thuộc vào giải pháp kỹ thuật	90% vấn đề ATTT phụ thuộc vào con người tuân thủ tốt các chính sách ATTT

Ví dụ: cái khoá cửa là **10%**. Bạn phải ghi nhớ cách khoá, kiểm tra xem cửa đã được đóng hay chưa, chốt đã cài chưa, giữ chìa khoá cửa,... là **90%** còn lại.

Kết luận: cần cả **kỹ thuật** và **con người** để đảm bảo ATTT hiệu quả nhất !

Tại sao hacker có thể tấn công thành công?

Điểm yếu trong hệ thống

- Lỗ hổng ứng dụng (hệ điều hành, trình duyệt web,…)
- Lỗ hổng do cấu hình hệ thống không tốt
- Chính sách ATTT không tốt

Điểm yếu về nhận thức của người dùng

THE WORKSHOP

Bảo vệ an toàn dữ liệu, thông tin và thiết bị số

Chiến lược vệ sinh mạng thích hợp liên quan đến mật khẩu:

- VD: chọn những mật khẩu mạnh, khó đoán.

Cách cài đặt và kích hoạt phần mềm và dịch vụ bảo vệ:

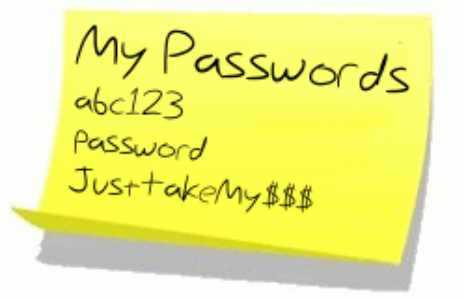
- Chống vi-rút (VD: McAfee, Bitdefender, Norton).
- Chống phần mềm độc hại: McAfee, Bitdefender, Norto.
- Tường lửa.

Cách kích hoạt xác thực hai yếu tố khi có sẵn:

- Mật khẩu sử dụng một lần.
- Mã OTP hoặc mã cùng với thông tin xác thực truy cập.

Mật khẩu của bạn bị mất như thế nào?

- Bị dò/đoán do mật khẩu đặt quá đơn giản
- Ghi mật khẩu ra giấy, file text
- Máy bị keylogger - phần mềm trộm mật khẩu
- Chia sẻ mật khẩu với người khác (với tính chất một mật khẩu có thể vào được tất cả các hệ thống như nêu trên, thì phải rất cân nhắc khi cho người khác biết, và cần đổi ngay sau đó)
- Bị nghe trộm qua mạng
- Dùng chức năng ghi nhớ mật khẩu của ứng dụng
- Bị tấn công lừa đảo cung cấp mật khẩu



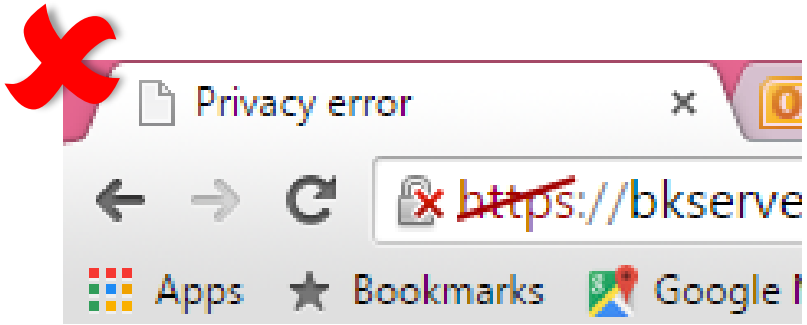
RMIT UNIVERSITY

Sử dụng mật khẩu an toàn (1)

- Đặt mật khẩu đủ mạnh, khó đoán nhưng dễ nhớ
- Không đặt mật khẩu trùng với ngày sinh nhật, tên,…
- Không ghi mật khẩu ra giấy hay file không mã hoá
- Đổi mật khẩu định kỳ
- Không chia sẻ mật khẩu
- Không ghi nhớ mật khẩu trên trình duyệt
- Sử dụng phần mềm giúp quản lý mật khẩu. Ví dụ: KeePass

Sử dụng mật khẩu an toàn (2)

- **HTTP hay HTTPS**
  - **HTTP:** không mã hoá, có nguy cơ bị nghe trộm mật khẩu qua mạng do mật khẩu ở dạng text bình thường.
  - **HTTPS:** có mã hoá bằng chức thư số, mật khẩu được bảo vệ.
- Nên sử dụng HTTPS thay cho http nếu website có hỗ trợ cả 2 giao thức
- Chú ý khi dùng HTTPS: thường thì trình duyệt có cảnh báo đối với các trường hợp chứng thư số sai, bị giả mạo, hết hạn,…



RMIT UNIVERSITY

Cách đặt mật khẩu mạnh, dễ nhớ

- Thay thế các chữ thành số hoặc ký tự đặc biệt theo quy tắc tương tự. Ví dụ: a -> @; A-4; i -> 1, !; s -> $; O -> 0; …
- Thêm các thành phần ngắn trước hoặc sau mật khẩu
- Ví dụ từ một mật khẩu đơn giản, biến đổi thành mật khẩu phức tạp:
  - password => Password => P@ssw0rd => !#P@ssw0rd

Các nguy cơ lộ, lọt và mất mát dữ liệu

- Dữ liệu không được phân loại đúng cách
- Dữ liệu xoá không đúng cách, bị khôi phục lại
- Chia sẻ dữ liệu không kiểm soát, chia sẻ dữ liệu trên Internet,…
- Mất, hỏng phương tiện lưu trữ (ổ cứng trên máy, ổ cứng di động, USB, thẻ nhớ, điện thoại, máy tính bảng,…)
- Virus phá hoại, lấy cắp thông tin
- Máy tính bị tấn công phá hoại, lấy cắp dữ liệu
- Cài đặt các phần mềm cho phép truy cập máy tính từ xa như Teamviewer, Logmein,… mà không giám sát khi có người truy cập.

Bảo vệ dữ liệu (1)

- Phân loại theo mức độ quan trọng của dữ liệu, có biện pháp bảo vệ phù hợp cho từng loại dữ liệu

Bảo vệ dữ liệu (2)

Chia sẻ file theo đúng qui định của công ty, phòng ban

- Không thực hiện tải lên (upload), hay chia sẻ tài liệu / dữ liệu quan trọng của nội bộ trên các trang mạng internet (google, facebook, mediafire, 4share, megaupload, rapidshare, slideshare, dropbox, fshare,…)
- Người sử dụng phải thực hiện chế độ xác thực người dùng khi chia sẻ máy in, chia sẻ thư mục. Tốt nhất là chỉ dùng các thư mục chia sẻ mà công ty qui định.

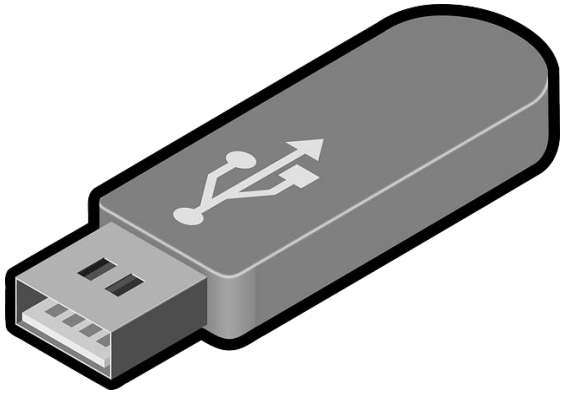
Mã hoá dữ liệu quan trọng

- Sử dụng một số công cụ như: TrueCrypt, BitLocker
- Đặt mật khẩu phức tạp với các tài liệu quan trọng (dạng Excel, Word)

RMIT UNIVERSITY

Bảo vệ dữ liệu (3)

- **Định kỳ sao lưu dữ liệu công việc theo qui định**
- **USB**
  - Hạn chế sử dụng USB, thẻ nhớ, ổ cứng di động,…
  - Trong trường hợp sử dụng:
  - Không nên lưu dữ liệu quan trọng
  - Dữ liệu quan trọng phải được mã hoá
  - Chỉ định cá nhân quản lý và chịu trách nhiệm
- **Máy tính**
  - Khoá máy (vật lý)
  - Đặt mật khẩu truy cập máy tính cho các tài khoản có trong máy
  - Khoá màn hình máy tính khi dời bàn làm việc.
  - Để thời gian tự khoá màn hình khi không sử dụng sau 5 phút.



RMIT UNIVERSITY

Bảo vệ an toàn dữ liệu, thông tin và thiết bị số

Cảnh giác không để máy tính hoặc thiết bị di động không có người trông coi ở những nơi công cộng.

Cần cân nhắc một số hành vi tự bảo vệ như không sử dụng mạng Wi-fi mở để thực hiện các giao dịch tài chính hoặc ngân hàng trực tuyến

Bảo vệ dữ liệu cá nhân và quyền riêng tư

Dự án: Nâng cao năng lực số của chính quyền địa phương, doanh nghiệp và người dân - Hướng tới một quốc gia số

Ngày 2, Buổi sáng

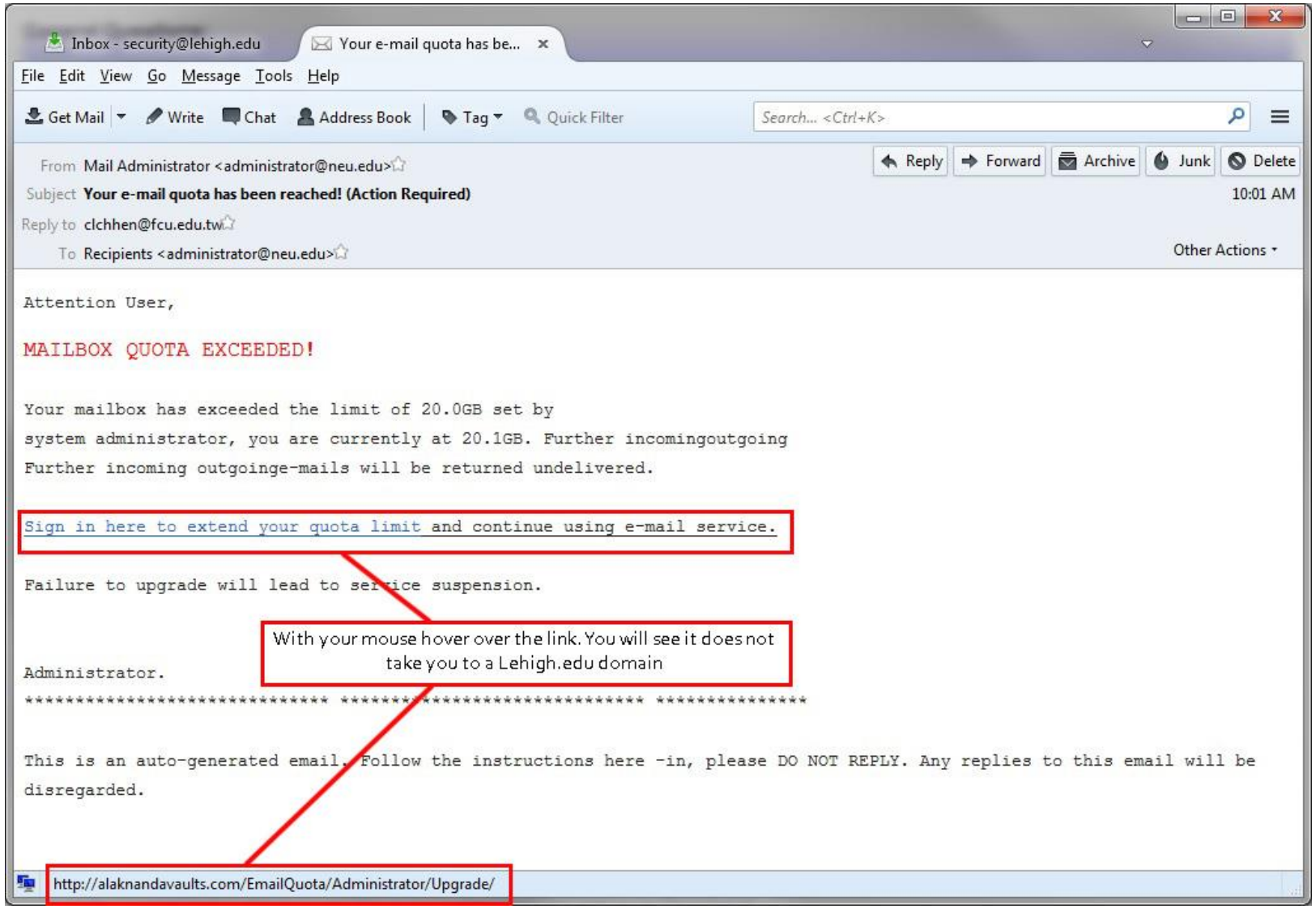
THE WORKSHOP

Bảo vệ an toàn dữ liệu cá nhân và riêng tư

1. Cách nhận dạng các thư điện tử đáng ngờ cố lấy thông tin nhạy cảm hoặc có thể chứa nội dung xấu.
2. Cách áp dụng các biện pháp bảo mật cơ bản trong thanh toán trực tuyến.
3. Cách kiểm tra xem độ an toàn của trang web yêu cầu cung cấp dữ liệu cá nhân.

Email lừa đảo lấy thông tin tài khoản

- Lừa lấy thông tin đăng nhập của người dùng bằng cách cho đăng nhập vào website giả mạo, khi người dùng click vào link trong email



Dấu hiệu Email lừa đảo

- Email không ghi rõ tên người nhận
- Người gửi không phải là người bạn biết, hay từ các địa chỉ bạn có liên hệ
- Nội dung Email không chính quy (ngay cả khi gửi từ người quen)
- Nội dung Email có các đường link không rõ ràng, link giả mạo
- Có chứa các file đính kèm "nghi ngờ" như: .zip, .exe, .vbs, .bin, .com, .pif, .zzx
- Có đường link hay file đính kèm xem thiệp điện tử không mong đợi.

- Không phản hồi các email yêu cầu cung cấp mật khẩu
- Không mở các file, bấm đường link nghi ngờ
- Xoá các email spam hay có nội dung nghi ngờ, forward email đó đến bộ phận IT xử lý.
- Cập nhật các bản vá cho các chương trình email như Outlook, ThunderBird,...
- Tìm cách xác minh các email cảm thấy nghi ngờ

RMIT UNIVERSITY

Sử dụng Internet an toàn

☑ **Không bấm** các đường link không rõ nguồn gốc, đặc biệt các đường link trong cửa sổ pop-up quảng cáo. Có thể sử dụng add-on, plug-in chặn quảng cáo (như Adblock)

☑ **Không chạy** các đoạn mã (script) không rõ nguồn gốc (ví dụ như các script trên mạng xã hội). Sử dụng các add-on, plug-in hỗ trợ chống tấn công qua Javascript

☑ Cập nhật thường xuyên các bản vá lỗ hổng trình duyệt và các add-on đi kèm như Flash, Java,…

☑ Tắt các add-on thừa trên trình duyệt.

☑ Cài đặt và sử dụng phần mềm diệt virus, tường lửa

☑ Sử dụng các phần mềm giúp kiểm tra đường link an toàn. Ví dụ: URL Void, Google Safe Browsing Diagnostic, …

☑ Tìm cách xác nhận lại thông tin khi thấy nghi ngờ, chú ý nguy cơ phát tán virus nhân dịp các sự kiện nổi bật, ngày lễ Tết,…

RMIT UNIVERSITY

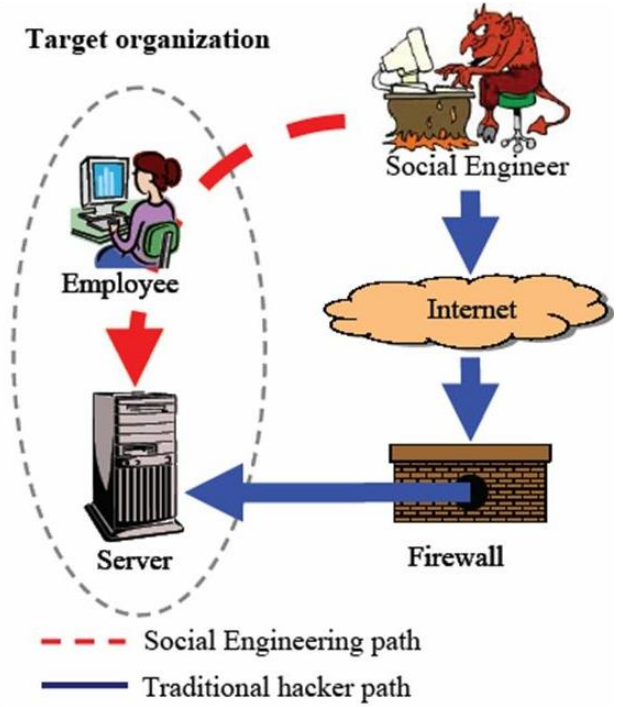
Một số phương thức tấn công

Tấn công thăm dò: sử dụng để thu thập thông tin, phát hiện ra các lỗ hổng trong hệ thống.

Tấn công truy cập: tấn công tác động vào hệ thống, như chiếm quyền điều khiển server, sửa đổi database,…

Tấn công từ chối dịch vụ (DoS, DDoS): tấn công gây quá tải, làm tê liệt dịch vụ được cung cấp.

Tấn công vào nhận thức người dùng (Social Engineering): là cách tấn công kết hợp đánh lừa người dùng. Ví dụ: gửi file, đường link đính kèm virus, khai thác thông tin bí mật,…



- Bản chất của cách tấn công trực tiếp vào hệ thống thường khó hơn, do đó hacker tìm cách đi vòng qua bằng cách lợi dụng sơ hở của người dung (hacker giả làm người quen gửi file chứa virus qua facebook, nhân viên mở file đó bằng máy tính trong công ty → hacker sẽ truy cập được hệ thống nội bộ công ty).

RMIT UNIVERSITY

Mã độc máy tính là gì?

Là chương trình phần mềm gây hại cho máy tính, dữ liệu của người sử dụng.

- **Worm:** sâu máy tính là một dạng mã độc máy tính có thể nhân bản chính nó từ máy tính này sang máy tính khác qua môi trường mạng, USB, đĩa CD…
- **Spyware, Adware, Ransomware:** phần mềm gián điệp, quảng cáo thu thập thông tin của người dùng rồi gửi ra ngoài, hiện các pop-up quảng cáo trên máy, thay đổi homepage trình duyệt, giả mạo,…
- **Trojan:** phần mềm thu thập thông tin từ máy tính, ví dụ như ghi nhận tất cả nội dung gõ từ bàn phím rồi gửi ra ngoài. Làm giảm độ an toàn của hệ thống bằng cách vô hiệu hoá phần mềm diệt virus hay tường lửa.
- **Virus file:** là phần mềm độc hại tự động chèn thêm chính nó vào các files thự thi trong máy, mỗi khi các file được gọi thực thi sẽ thực hiện lệnh của virus trước.

RMIT UNIVERSITY

Ransomware

Một dạng mã độc giả mạo, ngăn cản người dùng sử dụng dữ liệu máy tính.
Đánh lừa người dùng trả tiền để có thể sử dụng bình thường.

RMIT UNIVERSITY

Các con đường lây lan của mã độc

- Thiết bị USB, ổ đĩa di động…
- Web đen
- Phần mềm crack, keygen
- Email không rõ nguồn gốc (có thể chứa virus trong file đính kèm)
- Chia sẻ thư mục
- Lỗ hổng phần mềm
- …

RMIT UNIVERSITY

Phòng chống virus cho người sử dụng

- Cài đặt phần mềm diệt virus, thực hiện cập nhật mẫu virus hàng ngày
- Khi nghi ngờ bị virus, cần thông báo cho bộ phận IT xử lý.
- Không mở file, không bấm vào các đường link không rõ nguồn gốc
- Không tự ý tải và chạy các phần mềm crack, keygen
- Cập nhật thường xuyên các bản vá lỗ hổng phần mềm (Windows, Chrome, Firefox)

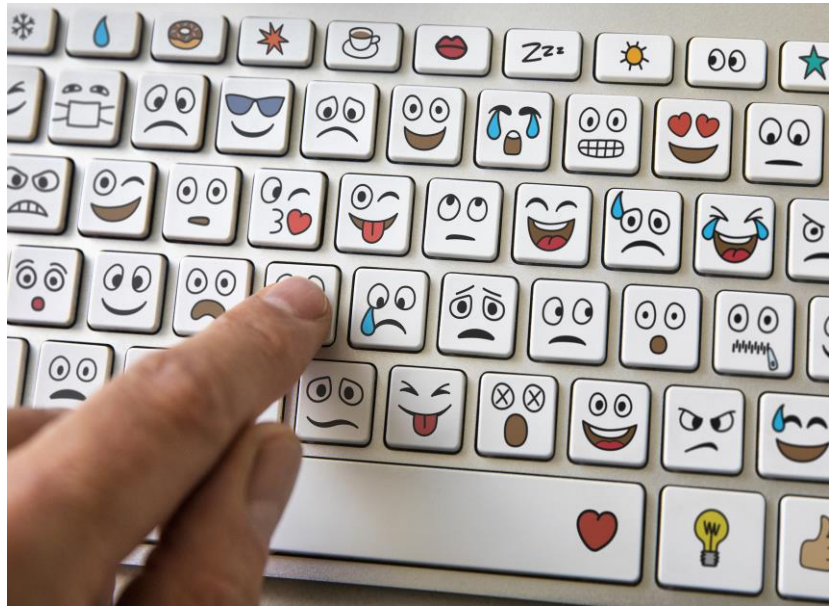
RMIT UNIVERSITY

Giao tiếp lịch sự trên Internet

Dự án: Nâng cao năng lực số của chính quyền địa phương, doanh nghiệp và người dân - Hướng tới một quốc gia số

Ngày 2, Buổi sáng

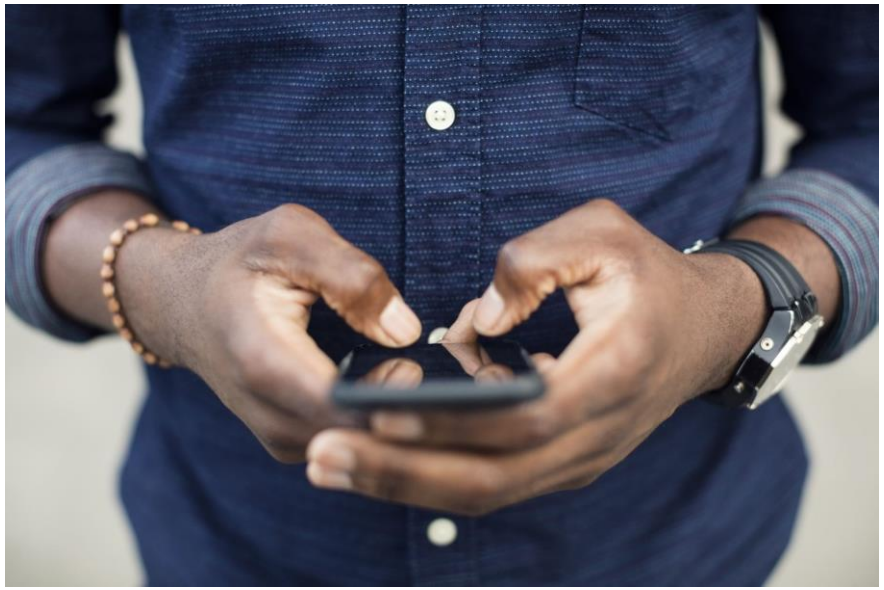
THE WORKSHOP



Khái niệm về các thông điệp không lời

Giao tiếp không lời bao gồm biểu cảm nét mặt, điệu bộ, các hình thái cận ngôn ngữ như độ lớn hoặc tông giọng, ngôn ngữ cơ thể, không gian giao tiếp hay khoảng cách cá nhân, ánh mắt nhìn, tiếp xúc (va chạm), ngoại hình và tạo tác.

- Phân loại thông điệp không lời
- Biểu tượng cảm xúc
- Hình dán



THE WORKSHOP

Quan điểm để xây dựng phép lịch sự khi sử dụng Internet

- Cần phải xác định và chia sẻ các quy tắc trong cộng đồng kỹ thuật số.
- Sử dụng quan điểm đồng cảm trong giao tiếp.
- Cởi mở và tôn trọng quan điểm của những người trên internet.
- Cởi mở với quan điểm của người khác ngay cả khi họ khác với quan điểm của mình.

Khái niệm về vấn nạn bắt nạt/ ức hiếp trên mạng

Bắt nạt qua mạng là khi bất cứ một cá nhân nào bị đe dọa, xâm hại, làm nhục, làm mất mặt/xấu hổ hoặc tra tấn bằng tinh thần qua tin nhắn, mạng Internet, các trang mạng xã hội và qua các thiết bị điện tử.

Phản hồi về tập huấn

Khảo sát đánh giá năng lực số

Chân thành
Cảm ơn!

Tuyên bố miễn trừ trách nhiệm

Bản thuyết trình này do Chính phủ Australia hỗ trợ thông qua Quỹ Hỗ trợ Cựu sinh viên Australia. Mọi quan điểm và nhận định trình bày trong bản thuyết trình này là của cá nhân tác giả và không nhất thiết thể hiện quan điểm của Chính phủ Australia.