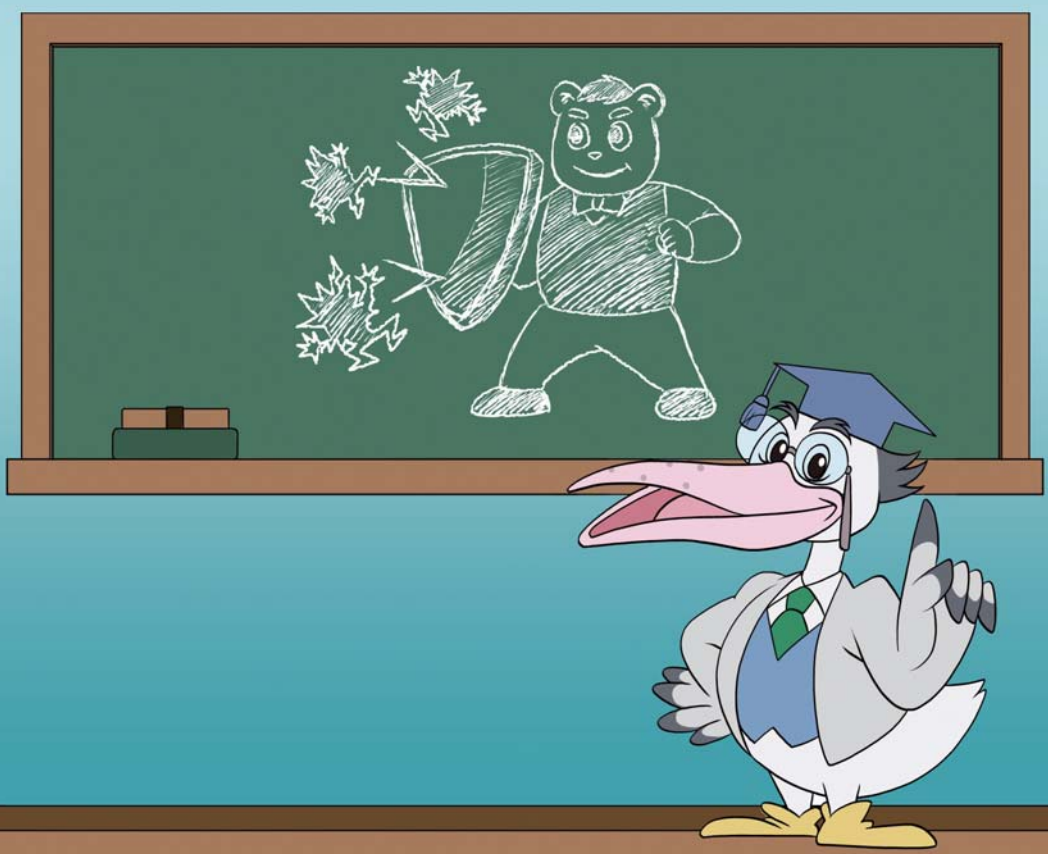
Truyện tranh
kèm hội thoại

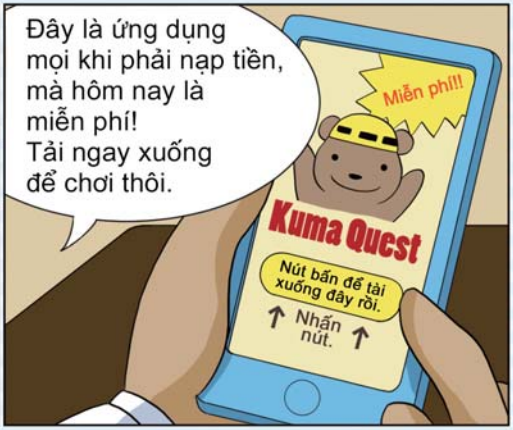
Cùng tìm hiểu về An toàn không gian mạng

Hiểu biết, bảo mật, cảnh giác



PHẦN1

An toàn với điện thoại thông minh



Vài ngày sau.


Sảy ra chuyện gì thế này?
Cảnh báo!
Điện thoại của bạn đã bị khóa, vì chúng tôi phát hiện một ứng dụng không hợp lệ trên điện thoại của bạn. Để mở khóa, hãy thanh toán 500.000 đ trong vòng 3 ngày. Điện thoại của bạn sẽ bị khóa cho tới khi bạn thực hiện xong việc thanh toán.


Trời ơi! Điện thoại thông minh của mình không hoạt động nữa.


Mình phải làm gì đây?


Một sự…vi phạm pháp luật.
Mình không rõ... cần phải hỏi ai bây giờ.


Được rồi, … mình sẽ thanh toán tiền và hi vọng sau đó mọi việc sẽ lại đâu vào đấy.


NGÂN HÀNG XXX
Mọi việc sẽ lại đâu vào đấy thôi mà. Nhưng sao mà đắt thế.
Ok, bây giờ điện thoại sẽ làm việc chứ.
...Hừm...
Cái gì thế này!?...
Điện thoại của bạn không mở khóa được.
Bác ơi! Giúp cháu với.
Có chuyện gì vậy?
Cháu thanh toán tiền rồi, mà điện thoại thông minh của cháu vẫn bị khóa.
Đây chính là một vụ lừa đảo rồi.
Các ứng dụng trên điện thoại di động mà không phải mua thường là có chứa vi-rus.
Nên bạn cần trang bị phần mềm diệt vi-rus và bạn chỉ nên tải các ứng dụng từ các trang web đáng tin cậy.
Chúng cháu hiểu rồi ạ!

NO.1 [Tổng hợp] An toàn với điện thoại thông minh

Chú ý!

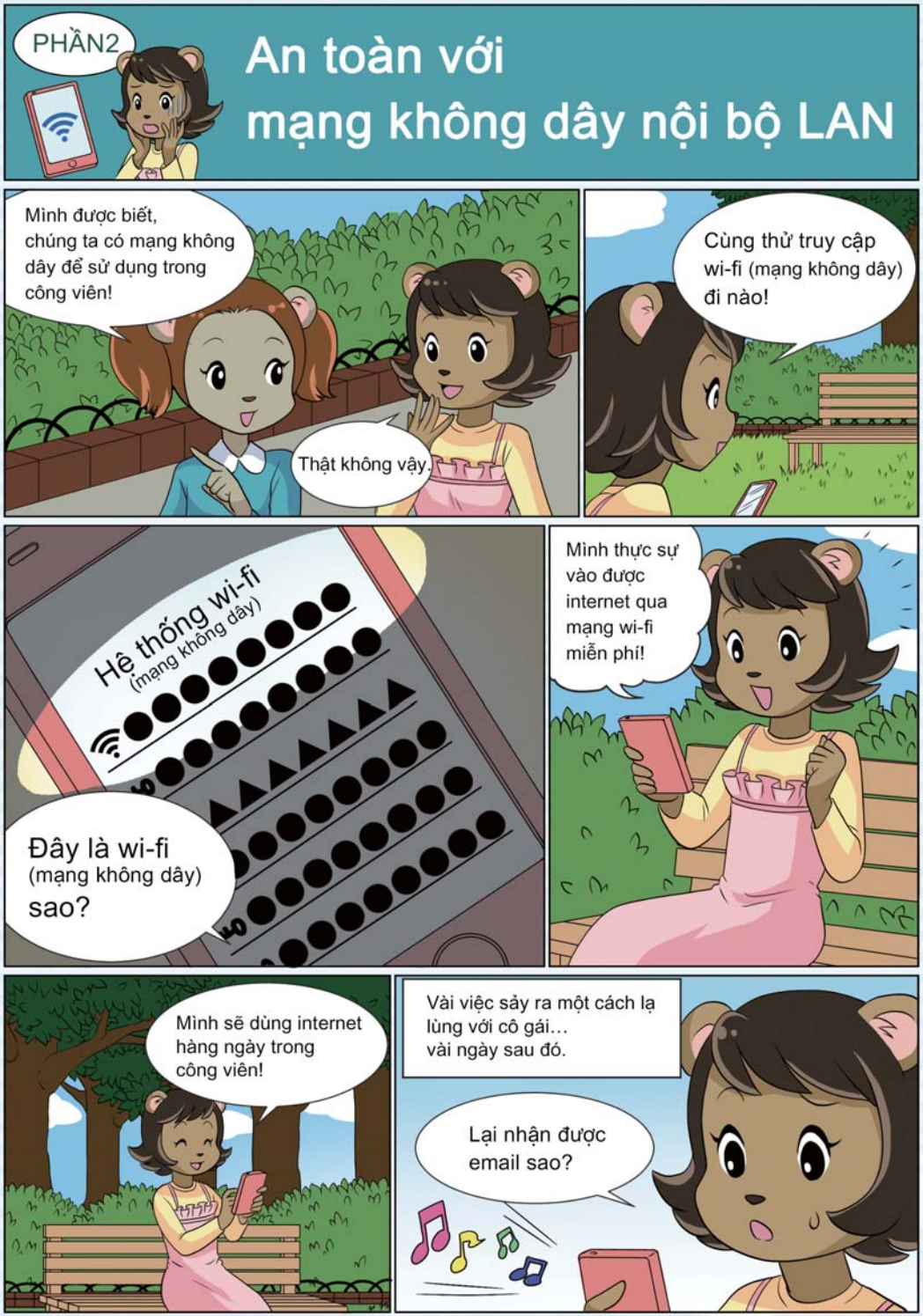
- Vi-rus độc hại được tìm thấy không chỉ trên máy tính, mà còn cả trong các máy điện thoại thông minh.
- Thiết bị của bạn có thể bị lây nhiễm từ các "Ứng dụng miễn phí"
- Thiết bị (máy tính và điện thoại thông minh) của bạn có thể bị lây nhiễm khi bạn không cập nhật hệ điều hành hay do không cập nhật các ứng dụng trên máy.

Giải pháp

- Hãy cài đặt phần mềm diệt vi-rus cho máy tính và điện thoại thông minh của bạn.
- Chỉ tải xuống các ứng dụng từ các trang web tin cẩn bằng cách kiểm tra tréo thông qua các nhà phát hành sản phẩm, các thông báo định kỳ đánh gía và so sánh các ứng dụng để xem doanh nghiệp phát triển dịch vụ đó có thực sự tồn tại và cập nhật các bình luận cho điểm dịch vụ, v.v...
- Luôn cập nhật phiên bản mới nhất cho các ứng dụng và hệ điều hành trên thiết bị của bạn.

Một vài gợi ý cụ thể.

- Mã độc 'đòi tiền chuộc' (là loại mã độc tự động khóa màn hình máy tính hay điện thoại của bạn, sau đó đòi phí mở khóa...) được ghi nhận 'bị phát tán khắp nơi'. Hãy chú ý: Mã độc đòi tiền chuộc 'ransomware' không chỉ nguy hiểm đối với máy tính, mà còn tác quái trên cả điện thoại thông minh.
- KHÔNG MỞ các tệp tin được đính kèm theo các tin nhắn rác, nếu không muốn thiết bị của bạn bị lây nhiễm vi-rus.


PHẦN2
An toàn với
mạng không dây nội bộ LAN
Mình được biết, chúng ta có mạng không dây để sử dụng trong công viên!
Thật không vậy.
Cùng thử truy cập wi-fi (mạng không dây) đi nào!
Hệ thống wi-fi
(mạng không dây)
Đây là wi-fi
(mạng không dây)
sao?
Mình thực sự vào được internet qua mạng wi-fi miễn phí!
Mình sẽ dùng internet hàng ngày trong công viên!
Vài việc sảy ra một cách lạ lùng với cô gái…
vài ngày sau đó.
Lại nhận được email sao?

Dạo này, mình nhận được quá nhiều thư rác.

Bạn nhận được những 320 email mới.

Còn sảy ra những việc lạ lùng khác nữa.

Mình vừa nhận được một cú điện thoại.

Đã có những 30 cuộc gọi…tới máy của mình rồi…!

Còn hơn thế nữa…

Bạn chắc chứ?

Mình quá kinh ngạc, vì đã thấy ảnh của bạn trên internet khi mình lướt web ngày hôm qua.

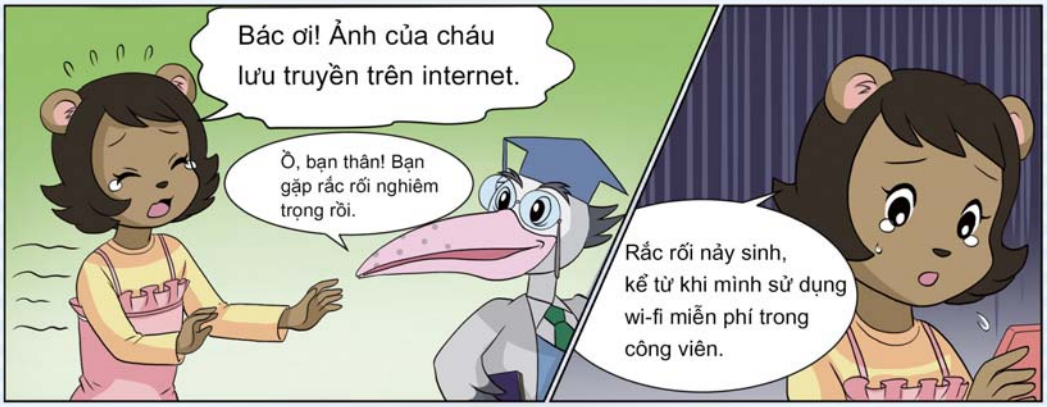
Thế đây là cái gì?

Mình chưa bao giờ đăng bức ảnh này lên bất cứ trang mạng xã hội nào cả.

Anh chàng Ẩn danh:

Hây, bạn không thấy cô bé này xinh ư?


Ô, ha ha...
Ôi, thánh thần ơi…!
Thật là phiền phức.


Bác ơi! Ảnh của cháu lưu truyền trên internet.
Ồ, bạn thân! Bạn gặp rắc rối nghiêm trọng rồi.
Rắc rối nảy sinh, kể từ khi mình sử dụng wi-fi miễn phí trong công viên.


Có thể đấy chính là nguyên nhân.
Truy cập internet thông qua wi-fi bất kỳ sẽ tiềm ẩn nguy cơ!
Vì vậy tốt nhất là chỉ nên sử dụng wi-fi đáng tin cậy, nếu nó đã được mã hóa.
Mình không hề biết rằng nó không an toàn. Mình đã sử dụng chỉ vì nó miễn phí.
Kể từ nay, mình cần cảnh giác với loại wi-fi miễn phí như thế này.

NO.2 [Tổng hợp] An toàn với mạng không dây nội bộ LAN

Chú ý!

- Một số điểm truy cập wi-fi miễn phí đã bị cài đặt mã độc.
- Cần nhận thức được rằng, ai đó có thể chặn thông tin của bạn, một khi bạn sử dụng các điểm truy cập mạng đã bị cài đặt mã độc.
- Ngay cả khi bạn được sử dụng mạng wi-fi nội bộ (khách sạn, nhà hàng...) có địa chỉ ISP cụ thể, trao đổi thông tin vẫn có thể bị can thiệp nếu thông tin của bạn không được mã hóa.

Giải pháp

- Không nên truy cập wi-fi công cộng bất kỳ, hoặc wi-fi không đáng tin cậy.
- Nếu cần phải sử dụng wi-fi công cộng, hãy dùng loại wi-fi công cộng có mã hóa thông tin được truyền tải.

Một vài gợi ý cụ thể.

- Chú ý chế độ đặt cấu hình thiết bị, khi bạn sử dụng wi-fi. Tệp thông tin của bạn có thể bị 'đọc trộm' bởi người sử dụng cùng hệ thống wi-fi, nếu bạn đặt chế độ "chia sẻ dữ liệu" trên máy tính PC hay điện thoại thông minh của bạn.
- Mạng không dây của bạn nên được cài đặt mật khẩu. Đừng để người không quen biết truy cập được vào mạng không dây (wi-fi) của riêng bạn.

Lừa đảo trên Internet

Phần3


NGÂN HÀNG xxxx
Xong! Mình vừa thanh toán trực tuyến xong, việc còn lại là đợi hàng đã mua được gửi đến thôi.
Mình vừa mua cái túi mà mình rất thích với giá cả được giảm tới 90%.
Ồ, thật thế không vậy.
Một tháng sau đó.
Hừm… Cái túi đã mua vẫn chưa được gửi đến.
Pi
Pi
Kiểm tra lại gian hàng trực tuyến xem nào.
Ồ, cái gì thế này?
Trang web này bị khóa rồi. Mình gọi điện thoại trực tiếp đến cửa hàng xem nào!
404 Not Found.
Trang web này hiện nay trong tình trạng không thể truy cập được.


Một tháng trước đây, tôi mua một cái túi trên trang trực tuyến của quầy hàng; mà cho đến tận hôm nay chưa nhận được hàng gửi tới.
Đáng tiếc là chúng tôi không có cửa hàng trực tuyến trên mạng. Tôi ngại rằng đã có sự nhầm lẫn nào đó…
Hừm…?
Bác ơi!
Đây chính là một trong những dạng lừa đảo trên internet.
Lừa đảo trên mạng tồn tại trên internet, ví dụ như thông qua mua bán trực tuyến…nhằm lấy cắp tiền của bạn.
Bạn cần phải KIỂM TRA xem đường dẫn URL của trang web hay người gửi thư điện tử là thật hay là giả mạo.
Làm gì có giá rẻ bất ngờ như vậy. Mình phải cảnh giác từ bây giờ.

NO.3 [Tổng hợp] Lừa đảo trên Internet

Chú ý!

- Bạn có thể đụng phải một cú lừa đảo trên mạng, khi bạn tiến hành mua sắm trực tuyến hay khi bạn sử dụng thanh toán ngân hàng trực tuyến.
- Gian lận trực tuyến dẫn người dùng đến các trang web ma giống như thật. Số lượng các trang fishing như vậy ngày càng nhiều.
- Bạn có thể bị dẫn đến trang web ma giống như thật hoặc bị làm nhiễm vi-rus, nếu bạn nhấp chuột vào các tệp đính kèm hoặc đường dẫn URL được thông báo hay mời chào trong các thư rác.

Giải pháp

- HÃY KiỂM TRA cẩn thận nguồn gốc của các đường dẫn URL hay người gửi thư điện tử là thật hay là mạo danh.
- ĐỪNG XEM các trang web khả nghi, hay các trang web sử dụng từ ngữ mập mờ hay rối rắm dễ gây nhầm lẫn, hoặc không thấy các thông tin để liên hệ (hay địa chỉ liên hệ là giả mạo).

Một vài gợi ý cụ thể.

- HÃY TỈNH TÁO trước các trang trực tuyến fishing, thường ngụy tạo các trang web của các ngân hàng thông dụng. Số lượng các trang lừa đảo này ngày càng tăng và thường được sử dụng để lấy cắp định danh ID và/hoặc mật khẩu của người dùng nhằm kiểm soát tài khoản trực tuyến (hay ăn cấp tiền từ tài khoản) của bạn.

Hướng dẫn sử dụng Mạng xã hội
(fachebook, twitter…)

Phần4


Nhưng mà… sao lại chọn một địa điểm như vậy để gặp mặt chứ?
Có vẻ như là… không có một ai ở quanh đây cả.
Ú òa!
Hello!
Vâng
Ối, ối…
Đưa tiền ra đây mau!
Ôi, không!


Mất hết tiền và giờ thì mình trở thành nhẫn túi mất rồi... Mình không muốn đi xem bộ sưu tập đó hôm nay nữa đâu!
Không hẹn nữa...
Mình cần phải hủy cuộc gặp gỡ ngày hôm nay thôi.
Gì thế này...! Sao anh bạn này lại biến mất vậy?
Hẹn gặp ngày mai nhé.
Đồng ý, tạm biệt.
Thỏ để Taro dời phòng chat.
Ồ, có phải bạn đã bị lừa khi hội thoại với một người giả mạo danh tính, đúng không?
Bị giả mạo danh tính?
Lấy cắp danh tính là việc dễ như trở bàn tay trên các mạng xã hội.
Bạn dễ dàng bị dính líu vào những vụ việc liên quan đến tội phạm, một khi danh tính của bạn bị đánh cắp.
Bạn tuyệt đối không nên liên hệ với những người không quen ở trên mạng xã hội. Trong mọi trường hợp, không nên hẹn gặp mặt những người mà mình không quen biết từ trước.
Mình ngốc quá... Mình sẽ phải cảnh giác hơn nữa khi sử dụng mạng xã hội.
Ôi, những mẫu model bằng nhựa sành điệu...

NO.4 [Tổng hợp] Hướng dẫn sử dụng Mạng xã hội

Chú ý!

- Kẻ mạo danh có thể xuất hiện bằng danh tính hấp dẫn với ảnh của một ai đó và liên hệ với bạn.
- Kẻ mạo danh có thể sẽ mời 'Tôi muốn hẹn gặp mặt bạn' và làm cho bạn bị dính líu vào những vụ việc mờ ám.
- Trong trường hợp xấu nhất, bạn dễ dàng bị dính líu vào những vụ tội phạm như bắt cóc trẻ em, buôn bán phụ nữ...

Giải pháp

- KHÔNG liên lạc với người không quen biết (qua mạng xã hội).
- KHÔNG gặp trực tiếp người không quen biết, ngay cả khi họ muốn xin phép được làm quen.

Một vài gợi ý cụ thể.

- Người lạ (trên mạng xã hội) thường hay liên hệ với bạn vì những vụ việc khuất tất không mong muốn.
- KHÔNG cho người lạ thông tin cá nhân của bạn như tên họ, ảnh, số điện thoại, địa chỉ, v.v...
- Kẻ mạo danh còn có thể trộm 'nick' của người quen thuộc, rồi tìm cách liên lạc với bạn...Trên mạng xã hội, nên biết cách kiểm tra xem có thật là người quen của mình đang 'chat' với mình không đã.


Có nhiều nguy cơ khi sử dụng internet.
Nhưng nếu sử dụng internet một cách hiểu biết, chúng ta có thể kết nối với mọi người vượt qua giới hạn về thời gian và lãnh thổ.
Hãy sử dụng internet một cách hiểu biết, bằng cách áp dụng các biện pháp an toàn mạng.

Hiểu biết, bảo mật, cảnh giác

知る　守る　続ける

Hãy sử dụng internet một cách hiểu biết, bằng cách áp dụng các biện pháp an toàn mạng.

ASEAN · JAPAN
Information Security Awareness