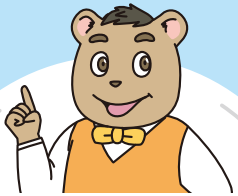


Hãy cảnh giác với an toàn thông tin và hưởng thụ sử dụng Internet

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
(MINISTRY OF INFORMATION AND COMMUNICATIONS)

VNCERT
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

http://www.vncert.vn

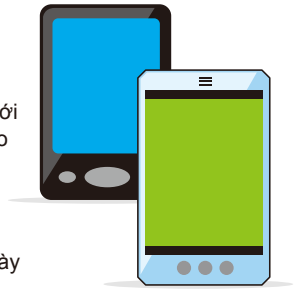
ASEAN · JAPAN
Information Security Awareness

Hiểu biết, bảo mật, cảnh giác

An toàn thông tin

Sử dụng Internet an toàn

An toàn cho điện thoại di động thông minh Smartphones



Điện thoại di động thông minh ngày càng phổ biến trên toàn cầu, và thị phần của loại diện thoại này ngày càng lớn khi so sánh doanh số của các loại điện thoại di động.

Điện thoại thông minh là những thiết bị tinh vi nếu đem so sánh với những phiên bản không dây trước đây. Điện thoại thông minh cho phép người dùng truy cập internet, tải về và sử dụng các phần mềm miễn phí.

Phiên bản mới của hệ điều hành OS và các ứng dụng trên điện thoại thông minh được nâng cấp thường xuyên. Việc nâng cấp này cho phép điện thoại thông minh ngày càng tinh vi và an toàn hơn.

*1 - OS là viết tắt của hệ điều hành, là một phần mềm điều khiển máy tính hoặc điện thoại thông minh. Ví dụ như trong máy tính, hệ điều hành quản lý các loại chức năng như các chức năng vào/ra (I/O) quản lý nhập vào từ bàn phím, chuyển ra màn hình, hoặc máy in.

*2 - Ứng dụng là một phần mềm cho mục đích cụ thể, chẳng hạn như xử lý văn bản, hoặc bảng tính. Người dùng có thể chọn các ứng dụng mà họ cần, và sử dụng chúng sau khi cài đặt trong hệ điều hành có chức năng cơ bản thường được sử dụng bởi tất cả các phần mềm.

*3 - Cập nhật có nghĩa là sửa đổi nhỏ của phần mềm để sửa lỗi, hoặc cung cấp thêm cải tiến chức năng. Bằng cách áp dụng chúng, người dùng có thể giữ cho phần mềm của họ được cập nhật. Cập nhật phần mềm bảo mật cho an toàn thông tin cũng quan trọng như vậy.

Nguy cơ và hiểm họa

1 Các loại mã độc trên điện thoại thông minh ngày càng gia tăng. Nếu điện thoại của bạn bị nhiễm mã độc, danh bạ điện thoại trong máy có thể bị gửi cho một máy chủ không rõ nguồn gốc, cũng như bạn dễ dàng mất tiền trong tài khoản.

2 Bên cạnh đó, khi tải các ứng dụng trên mạng, bạn phải điền các câu trả lời mà qua đó bạn bị lộ thông tin về địa chỉ hay nội dung của danh bạ điện thoại trong máy có thể bị gửi cho một máy chủ không rõ nguồn gốc. Ví dụ, có khi bạn được giới thiệu một ứng dụng được tặng để nâng cấp tuổi thọ của pin đang sử dụng, nhưng thật ra ứng dụng này đang tìm cách ăn cắp các thông tin cá nhân trong điện thoại thông minh để sử dụng vào việc khác.

Biện pháp đề phòng

- Đừng quên cập nhật các phiên bản mới nhất cho Hệ điều hành OS, các phần mềm ứng dụng và phòng chống virus trên điện thoại thông minh của bạn. Từ khi điện thoại thông minh chứa các thông tin địa chỉ và các thông tin nhạy cảm khác, người dùng cần thận trọng và quan tâm đến các biện pháp bảo mật như đối với một máy tính cá nhân.
- Trước khi tải các ứng dụng, bạn cần kiểm tra xem trang web có đáng tin cậy không và ai là nhà cung cấp các ứng dụng này, cũng như các điều khoản cho các thông tin phải cung cấp trước khi được sử dụng, v.v...

An toàn cho mạng kết nối LAN không dây

Trong những năm qua, máy tính cá nhân đã trở nên nhẹ hơn và điện thoại thông minh dần tràn ngập thị trường. Những tiến bộ này thúc đẩy sự phát triển nhanh chóng của mạng không dây cho phép kết nối internet bên ngoài các công sở và gần như khắp mọi nơi (trung tâm thương mại, sân bay, bến tầu…thậm trí cả ở nước ngoài, nếu thiết bị Wi-Fi tương thích về mặt kỹ thuật).

Nguy cơ và hiểm họa

1 Kể từ khi mạng cục bộ không dây được kết nối dễ dàng trong vùng phủ sóng vô tuyến, thông tin có thể bị khống chế, nếu không triển khai các biện pháp an toàn mạng hợp lý.

2 Ngoài ra, việc kết nối mạng không dây không cần mật khẩu cũng có thể làm thất thoát thông tin cá nhân và tạo tiền đề để tấn công máy chủ.

Biện pháp đề phòng

- Thiết lập cơ chế mã cho mạng cục bộ không dây (WPA2: Wi-Fi Protected Access 2, v.v…) có thể phòng chống được việc chặn bắt dữ liệu hay các truy cập trái phép . Việc giới hạn các thiết bị đầu cuối (sử dụng lọc địa chỉ MAC) cũng cho phép chặn các kết nối không rõ nguồn gốc.
- Khi bạn sử dụng mạng kết nối cục bộ không dây ở sân ba, ga tàu… Hãy kiểm tra xem nơi đó có áp dụng các biện pháp mã hóa thông tin không, và cần bỏ tính năng chia sẻ file trước khi sử dụng dịch vụ.

*4 - SSL là viết tắt của Secure Socket Layer là một giao thức để mã hóa dữ liệu được gửi trên web.

Lừa đảo chỉ bằng một cú nhấn chuột

Lừa đảo chỉ bằng một cú nhấn chuột là sự lừa gạt liên quan đến tiền nong khi bạn sử dụng các dịch vụ hiển thị trên màn hình. Bạn bị yêu cầu phải thanh toán sau khi chạm vào một biểu tượng trên màn hình hoặc một video trên trang web nào đó.

Gần đây, đã có những lừa đảo chỉ bằng một cú nhấn chuột thông qua các ứng dụng cho điện thoại thông minh và mạng xã hội giao như blogs/SNS.

C trường hợp Lừa đảo chỉ bằng một cú nhấp chuột cũng rất đa dạng, có khi hóa đơn đòi thanh toán sẽ biến mất với vài cú nhấn chuột, như sau khi điền tuổi thông tin cá nhân. Tuy nhiên có những trường hợp nghiêm trọng thì hóa đơn đòi thanh toán tiền không hề biến mất trên màn hiển thị cho tới khi người dùng phải ngắt tắt điện thoại

*1 - Blog là một dạng rút gọn của Weblog, qua đó người dùng có thể viết ý kiến hoặc cảm tưởng của họ như tạp chí, và người xem có thể tự do đưa ra ý kiến của mình trên bài viết đó.

*2 - SNS là viết tắt của dịch vụ mạng xã hội, cung cấp các trang web có nhiều chức năng như mở nhật ký hoặc thư viện ảnh của chúng ta cho công chúng, hoặc tạo ra cộng đồng mạng trong đó người dùng có thể tự do trao đổi ý kiến của mình.

Nguy cơ và hiểm họa

1 Cú nhấn chuột vào các biểu tượng bắt mắt trên màn hình hoặc bật xem một băng hình có thể bị đòi thanh toán một cách phi lý hoặc mở đường dẫn tới một trang lừa đảo.

2 Có trường hợp hóa đơn đòi thanh toán có ghi các số IP của thiết bị, cũng như các thông tin liên quan đến cá nhân nhằm khủng bố, bắt bạn phải thanh toán trong khi mất bình tĩnh.

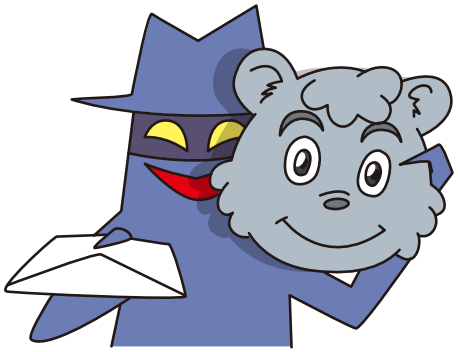
*3 - Địa chỉ IP là một số hiệu định danh được gán tự động cho các dụng cụ hoặc máy tính khi chúng được kết nối với internet..

Biện pháp đề phòng

- Sử dụng phần mềm lọc và các phần mềm chặn các web đen mới cấp nhật…cũng như, chỉ tải các ứng dụng cho điện thoại thông minh từ những nguồn tin cậy.
- Khi sử dụng máy tính, một cú nhấn chuột không bao giờ định danh tính của bạn…, và vì vậy bạn không có trách nhiệm phải thanh toán bất cứ thứ gì. Liên quan đến các ứng dụng cho điện thoại thông minh, đôi khi thông tin lưu trong thiết bị có khi bị thất thoát.
- Hãy tham khảo ý kiến tư vấn của dịch vụ tư vấn miễn phí của cộng đồng hoặc các nơi tin cậy nếu bạn liên tiếp bị gửi hóa đơn đòi thanh toán, sau khi sử dụng một số tiện ích không rõ nguồn gốc hoặc bị kiện đòi ra tòa … vì không thanh toán.

Tấn công có chủ đích bằng thư điện tử

Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus.



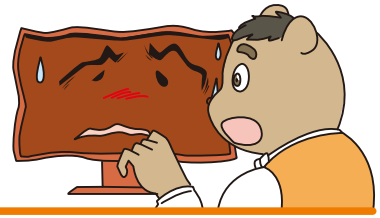
Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó.

Người dùng bị tấn công bằng thư điên tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus.

Nguy cơ và hiểm họa

1 Cách thức tấn công bằng thư điện tử ngày càng tinh vi. Chẳng hạn, tên tuổi của các cơ quan hay đối tác được sử dụng để đánh lừa là hoàn toàn có thật. Hơn nữa, nội dung trong các bức thư được gửi thì chỉ các bên liên quan mới được biết.

2 Nếu bạn mở tập tin đính kèm có chứa virus, bạn đã vô tình thiết lập kết nối với máy chủ khác và thông tin lưu trong máy tính có thể bị rò rỉ.



Biện pháp đề phòng

- Không mở các tập tin đính kèm cũng như các đường liên kết đáng ngờ kèm theo email.
- Nếu bạn đã chót mở một email đáng ngờ, đừng hoảng loạn và đừng bao giờ tắt nguồn đột ngột. Hãy ngắt kết nối mạng và hỏi người quản trị mạng để được giúp đỡ.
- Cài phần mềm diệt virus và thường xuyên cập nhật.
- Định kỳ, nên cấp nhật các phần mềm ứng dụng cùng với hệ điều hành OS.

DDoS Attacks

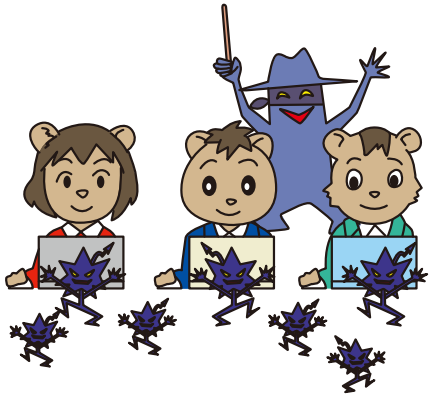
Một tấn công DDoS là tấn công mà một máy chủ cụ thể bị tấn công với số lượng lớn các gói tin từ nhiều máy tính từ nhiều nơi trên mạng Internet, khiến đường truyền bị quá tải hoặc vượt quá hiệu năng của máy tính dẫn đến máy tính mất khả năng cung cấp dịch vụ cho người dùng.

DDoS: Distributed Denial of Service

Nguy cơ và hiểm họa

1. Kẻ tấn công sẽ bí mật cài đặt mã độc vào các máy tính trung gian, chúng sẽ phát động tấn công máy chủ thông qua việc điều khiển các máy trung gian đó. Người dùng sử máy tính bị nhiễm mã độc đã vô tình tiếp tay cho cuộc tấn công mà không hề biết.

2. Máy tính bị nhiễm mã độc có thể tiến hành các cuộc tấn công DDoS khác, hoặc phát tán virus, gửi thư rác, thay đổi giao diện các trang web…



Biện pháp đề phòng

- Hãy cập nhật phiên bản hệ điều hành mới nhất cho máy tính hay điện thoại thông minh.
- Cài đặt và thường xuyên cập nhật phần mềm diệt virus.
- Định kỳ cập nhật các ứng dụng bổ sung cho hệ điều hành.

Văn hoá sử dụng Internet

Do sự gia tăng sử dụng SNS (dịch vụ mạng xã hội), các vấn đề trên mạng Internet không được tính đến trước đây đã xảy ra.

Có những trường hợp các cá nhân đăng tin lên internet có thể mang tính chất vu khống người khác và những người đăng tải thông tin đó đã phải đưa ra lời xin lỗi công khai.

Nguy cơ và hiểm họa

1. Có một khả năng xảy ra khi việc đăng tin không chủ định trên một SNS có thể dẫn đến thông tin cá nhân bị tiết lộ hoặc làm mất danh dự người khác hoặc vi phạm quyền riêng tư.

2. Một đăng tải không chủ định trên mạng Internet có thể dẫn đến hậu quả bồi thường thiệt hại, khiến trách của pháp luật hoặc thậm chí bị bắt giữ.

Biện pháp đề phòng

- Hãy cẩn thận không để tiết lộ thông tin cá nhân không cần thiết trên internet thông qua một SNS hoặc blog, twitter, v.v.… Việc đăng tải những hình ảnh có thể tiết lộ thông tin vị trí, do đó bạn nên thận trọng.
- Ngay cả trên internet, hãy chắc chắn cân nhắc về sự riêng tư và nhân phẩm của người khác và kiểm tra những nội dung đó trước khi đăng tải thông tin.

Tạo, quản lý và bảo vệ tài khoản của bạn đúng cách

Để sử dụng thư điện tử, mua sắm trực tuyến, sử dụng dịch vụ internet banking và các dịch vụ khác trên môi trường internet một cách an toàn, có khá nhiều phương thức để xác thực, trong đó, một trong những cách phổ biến là xác thực kết hợp đồng thời ID và sử dụng mật khẩu.

Có một sự gia tăng đáng kể các sự cố tấn công mạng nhằm lấy cắp thông tin tài khoản của người dùng như ID và mật khẩu.

Nguy cơ và hiểm họa

1. Kẻ gian có thể mạo danh người sử dụng để lấy cắp thông tin cũng như chuyển tiền gây thiệt hại về kinh tế nếu ID / mật khẩu sử dụng quá đơn giản (như ngày tháng năm sinh hay 9999, v.v…) hay được quản lý một cách cẩu thả (ví dụ như được viết trên giấy vàng và đính bên cạnh màn hình máy tính).

2. Sử dụng đồng thời mỗi một ID / mật khẩu cho nhiều trang khác nhau làm gia tăng nguy cơ trở thành nạn nhân của các cuộc tấn công mạng từ các nguồn khác nhau. Các thông tin quan trọng của cá nhân chứa đựng trong một trang mạng mà việc truyền tải không được áp dụng các biện pháp bảo mật bằng mã hóa sẽ rất dễ dàng bị đánh cắp.

Biện pháp đề phòng

- Rất nên tạo mật khẩu bằng ít nhất 8 kí tự khó đoán (chứa cả chữ và số, cũng như các ký hiệu khác) sau đó nên thay đổi mật khẩu thường kỳ.
- Không chia sẻ mật khẩu cho người khác, cũng như không sử dụng cùng một mật khẩu cho nhiều ứng dụng khác nhau.
- Nhưng khi bạn phải điền thông tin các nhân trên máy tính, nên chắc chắn là việc truyền tải phải được mã hóa. Cho nên các máy tính công cộng ở các quán cà fê, v.v…không phải là lựa chọn thích hợp.

Thư rác 1

Thư điên tử là một phương tiện liên lạc rất tiện dụng, cho phép người dùng có thể gửi và nhận thư mà không cần biết là người nhận đang ở đâu hay là ở cách ta bao xa. Tuy vậy, đôi khi người nhận lại nhận được quá nhiều email không cần thiết, còn gọi là thư rác.

Thư rác không chỉ làm ngắt quãng công việc, phương thức gửi thư rác còn ngày càng tinh vi để vượt qua các bộ lọc thư rác thông dụng, và còn có thể dẫn dắt người nhận tới những trang web đáng ngờ mà ở đó người ta không chỉ bị mất cắp tiền.

Thiết bị của nhà mạng còn có thể bị quá tải bởi số lượng lớn các thư rác được gửi đi và đến, điều đó dẫn đến sự ùn tắc việc gửi và nhận các thư tín quan trọng khác.

Nguy cơ và hiểm họa

1. Có những trường hợp một máy tính phát tán một lượng lớn thư rác. Trong đó, người dùng với địa chỉ emails ngắn gọn hoặc có tên dễ nhớ thường là nạn nhân của sự phát tán thư rác. Địa chỉ emails bị dùng để phát tán thư rác thường được thu thập từ các giả mạo dịch vụ tặng quà trên mạng hoặc thông qua các quy trình thông báo cắt các dịch vụ dùng thử trên mạng không có thật.

2. Thêm nữa, khi mở file đính kèm của một email hay nhấp chuột vào một đường dẫn gửi kèm trong email , người dùng có thể làm máy bị nhiễm vi-rus hay bị dẫn đến một trang web giả mạo.

Biện pháp đề phòng

- Địa chỉ thư tín của bạn nên chứa nhiều kí tự nhất có thể và các con số ngẫu nhiên để làm sao càng khó đoán càng tốt.
- Khi bạn cần sử dụng dịch vụ của một trang web mà bạn chưa tin cậy lắm, hãy dùng các địa chỉ email miễn phí của bạn để khai báo, thay vì dùng địa chỉ email quan trọng mà bạn thường dùng để trao đổi công việc.
- Hãy dùng các dịch vụ ngăn chặn thư rác của nhà mạng có các chức năng từ chối hoặc chống giả mạo, cũng như hãy sử dụng các phần mềm lọc thư rác.
- Hãy đừng đọc mà nên xóa ngay các thư rác nhận được. Đừng nhấp chuột vào các files đính kèm hay các đường links trong các email đáng ngờ. Vì khi đó, có thể bạn đã vô tình kích hoạt tiếp quá trình phát tán thư rác trên mạng.

Thư điện tử rác 2

Thư điện tử rác (thư rác) có thể không chỉ gây ra sự khó chịu cho người nhận hoặc làm gián đoạn công việc, mà chúng còn ngày càng trở nên có yếu tố độc hại và có thể dẫn dụ người dùng tới một trang trái phép với mục đích đánh cắp tiền bạc hoặc vượt qua bộ lọc thư rác đã thiết lập.

Điện thoại thông minh có thể bị nhiễm virút chứa trong các thư rác được điều khiển thao túng từ xa nhằm gửi một lượng lớn thư rác mà người dùng không hề biết.

Nguy cơ và hiểm họa

1 Có những trường hợp một máy tính sẽ ngẫu nhiên tạo ra một lượng lớn địa chỉ email và tiến hành gửi thư. Bởi vậy, việc sử dụng các địa chỉ email ngắn và tên phổ biến trong địa chỉ có thể dẫn đến khả năng tăng việc nhận thư rác.

2 Một số địa chỉ email hợp lệ để gửi thư rác được thu thập thông qua việc đăng ký một dịch vụ miễn phí giả mạo hoặc thông qua thủ tục ngừng đăng ký giả.
Ngoài ra, mở một tập tin đính kèm email hoặc truy cập vào một liên kết trong email có thể dẫn đến thăm một trang web trái phép hoặc dẫn đến nhiễm virus.

Biện pháp đề phòng

- Cố gắng ngăn chặn thư rác bằng cách sử dụng các dịch vụ chống thư rác như chức năng từ chối hoặc chức năng chống giả mạo bởi các nhà cung cấp dịch vụ Internet hoặc phần mềm lọc.
- Nếu bạn nhận được một email thư rác, hãy xóa nó mà không mở nó. Ngoài ra, không mở tệp đính kèm hoặc các liên kết truy cập cung cấp từ các email đáng ngờ. Cũng sẽ hiệu quả nếu bạn có thể chuyển tiếp các thư rác tới nhà cung cấp dịch vụ hoặc cơ quan quản lý.
- Hãy sử dụng các biện pháp cần thiết trên điện thoại thông minh cũng như máy tính.

Bảo vệ điện thoại thông minh và máy tính của bạn.

Điện thoại thông minh và máy tính là những công cụ hữu ích, Nhưng mặt khác chúng phải đối mặt với nhiều hiểm họa như trở thành bị nhiễm virus máy tính. Nhớ tuân thủ ba lời khuyên hàng đầu về an toàn thông tin để đảm bảo an toàn và bảo mật khi sử dụng máy tính và điện thoại thông minh.

Three top tips of information security

- Thận trọng khi xử lý thông tin cá nhân quan trọng.
- Bảo vệ máy tính của bạn với các bản cập nhật bảo mật mới nhất.
- Không truy cập các trang web đáng ngờ hoặc email không quen thuộc.

Các biện pháp an toàn thông tin có thể được ví như cài dây an toàn khi chúng ta đi xe hơi ngoài đường, đó là những gì chúng ta không được quên khi sử dụng điện thoại thông minh hoặc máy tính.