ATHENA

TRUNG TÂM ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

CÁC NGUY CƠ MẤT THÔNG TIN KHI GIAO DỊCH TRÊN MẠNG INTERNET

Trình bày : Võ Đỗ Thắng

Giám Đốc Trung tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng ATHENA

E-mail : thangvd@athenavn.com

Nội Dung

- Mất ANTT
- Một số thông tin về ANTT của ATHENA
- Mất ANTT từ đâu ?
- Môi trường làm việc di động và nguy cơ ANTT
- Một vài đề xuất
- Q&A

Mất ATTT là gì ?

- Thông tin bị những người không có quyền biết được *(wikileak…,thông tin, hình ảnh bị người khác bắt và sử dụng cho báo của họ, email, phone N# bị sử dụng cho quảng cáo.*
- Thông tin không truy cập được *(vì phương thức truy cập bị tê liệt, vì mất do xoá, do thiết bị lưu trữ bị hư hại, bị DoS…)*
- Thông tin bị sai lệch, bị thay đổi nội dung *(thư giả mạo, hồ sơ bị làm sai lệch, hình bị ghép…)*

Sự kiện về mất ANTT

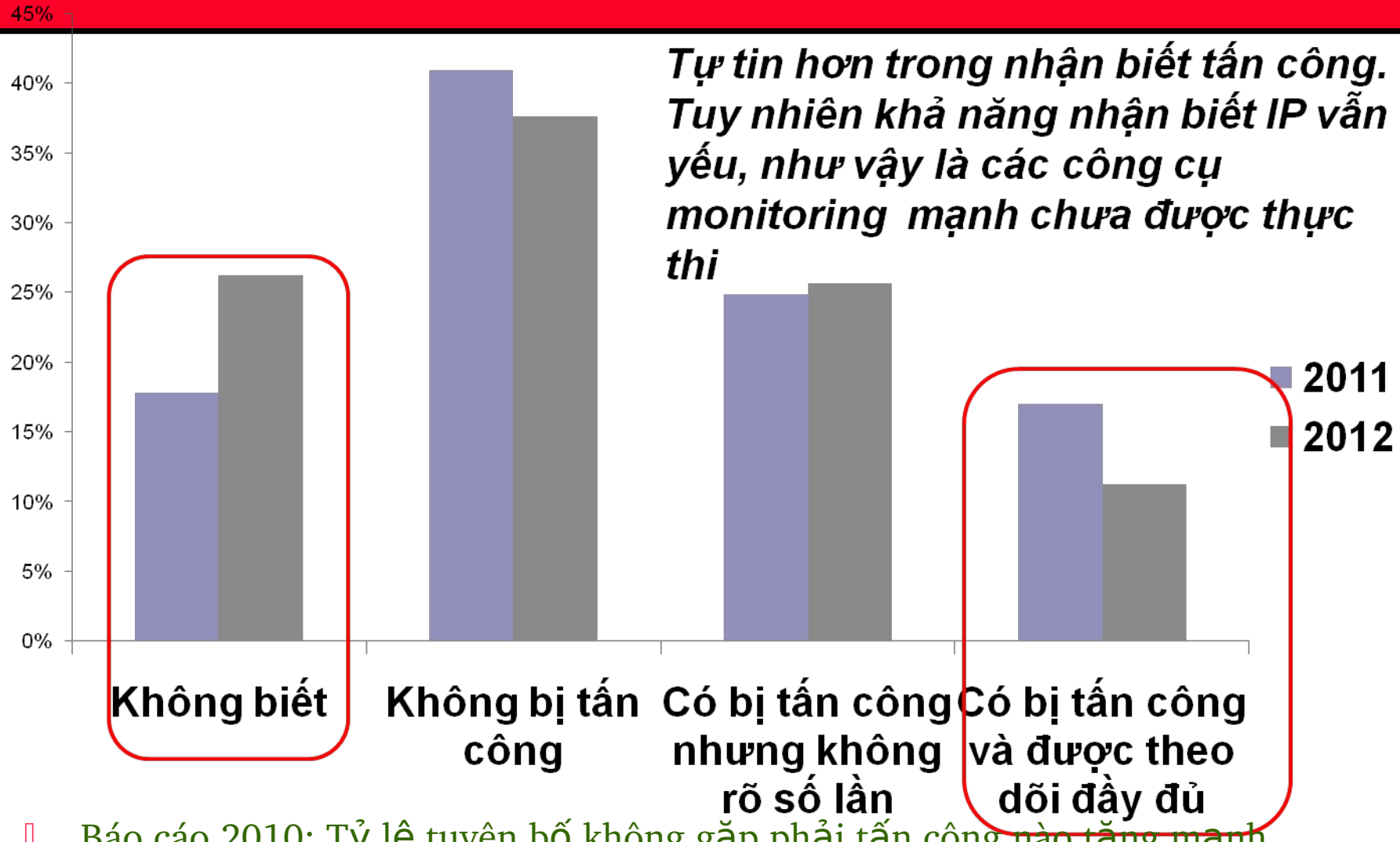
- Chị thị 897 CT-TTG của TTCP: Tăng cường các hoạt động bảo đảm an toàn thông tin số và các văn bản khác của CQ nhà nước
- Hàng trăm website chính phủ **gov.vn** bị hacker nước ngoài tấn công
- Việt Nam vẫn liên tục có tên trong nhiều danh sách quốc tế về các vấn đề liên quan đến ATTT, đặc biệt là vấn đề thư rác
- Bùng phát các hình thức lừa đảo mới qua nhiều phương thức như tin nhắn SMS, email, yahoo chat, website…
- Các hãng bảo mật của Việt Nam đồng loạt tung ra các giải pháp, phần mềm bảo vệ cho Mobile.

Sự kiện (tiếp)

- Một số tờ báo điện tử lớn của VN bị tấn công trong thời gian dài
- Hàng loạt các website, diễn đàn lớn của VN bị tấn công bằng nhiều phương thức khác nhau như DDOS và lấy cắp tên miền.
- Việt Nam đang trở thành địa bàn hoạt động của tội phạm công nghệ cao từ nước ngoài, tội phạm CNC tăng theo cấp số nhân
- Mất ATTT ngành ngân hàng tăng: các vụ việc cán bộ lợi dụng kẽ hở trong ATTT để đánh cắp tiền; ATM skimming rất phổ biến, …
- Nguy cơ lây nhiễm virus, mã độc hại, lừa đảo trực tuyến qua mạng xã hội đang ngày càng cao tại Việt Nam

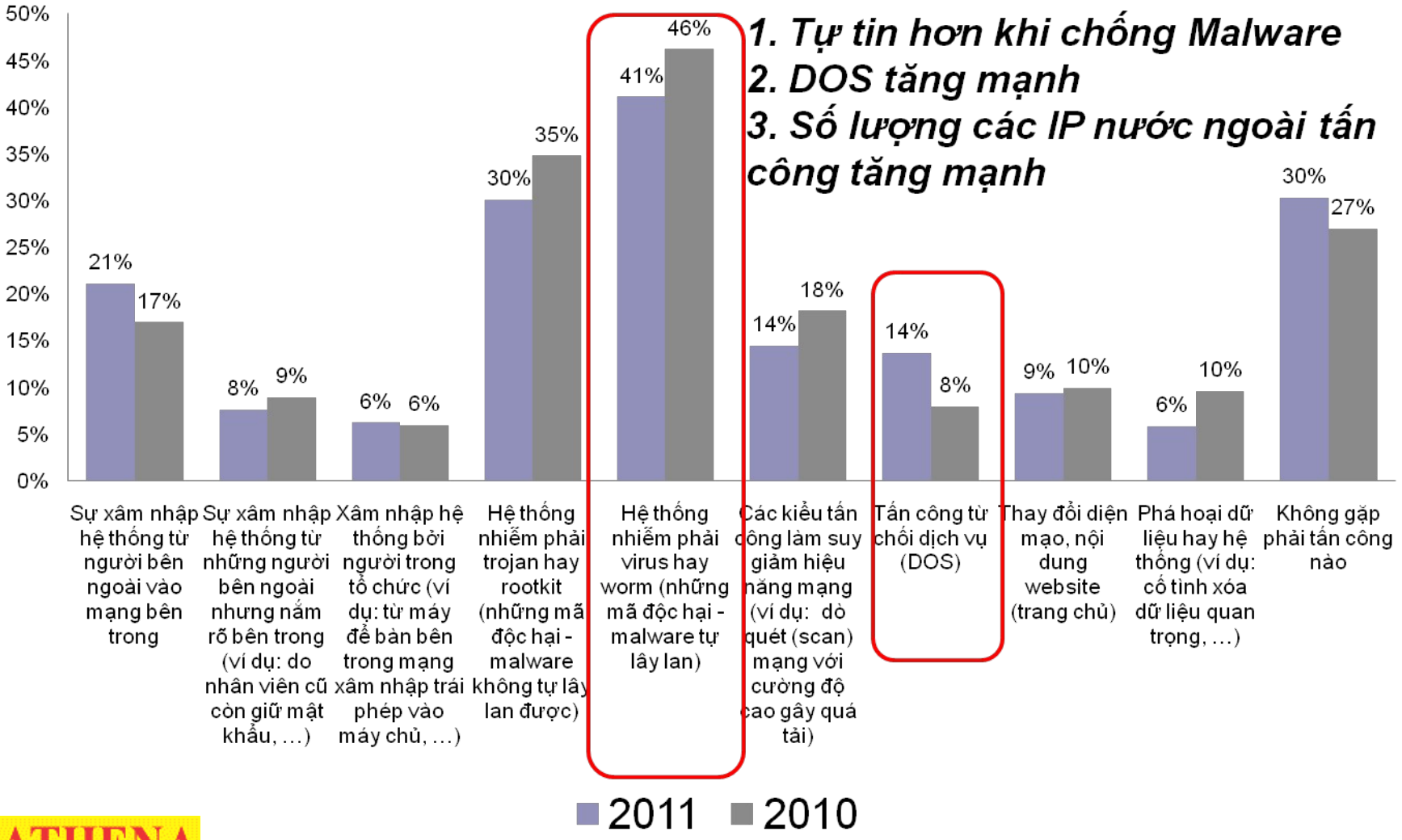
- MẤT AN NINH THÔNG TIN DO ĐÂU ?

Hệ thống của quý vị đã từng bị tấn công mạng (Cyber Attack) hay không (tính từ 1/2011)?



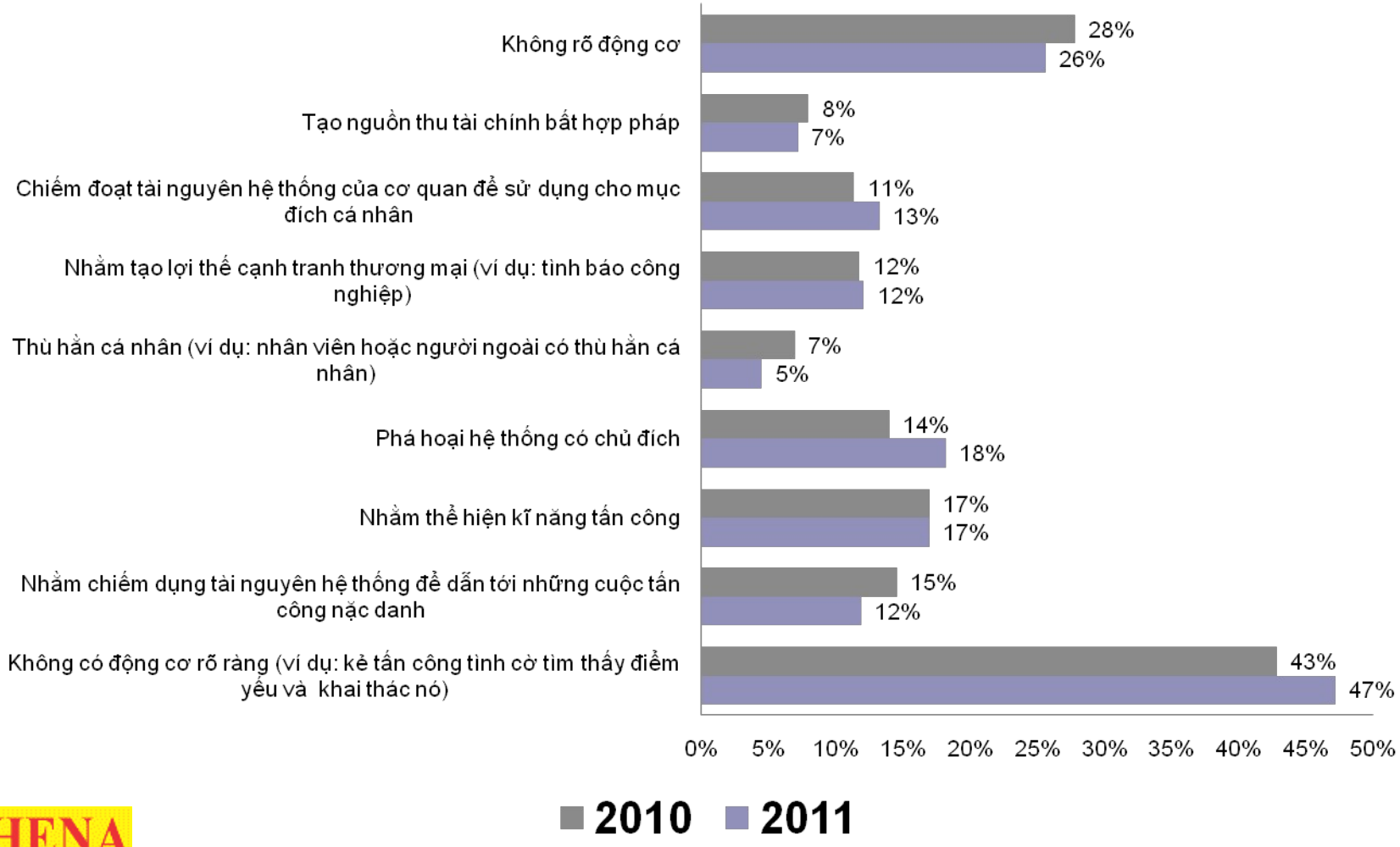
- Báo cáo 2010: Tỷ lệ tuyên bố không gặp phải tấn công nào tăng mạnh

Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2011



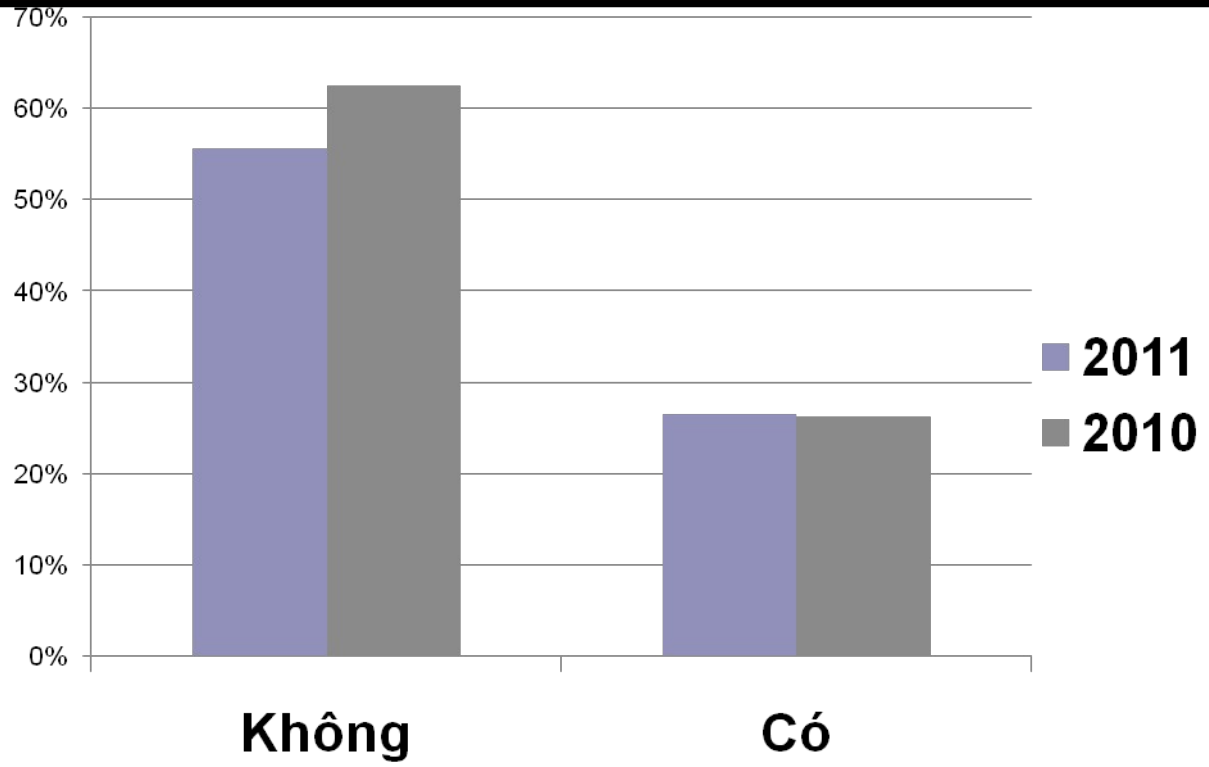
ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

Theo quý vị những động cơ nào được nghi ngờ là nguyên nhân gây ra những hành động trên?



ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

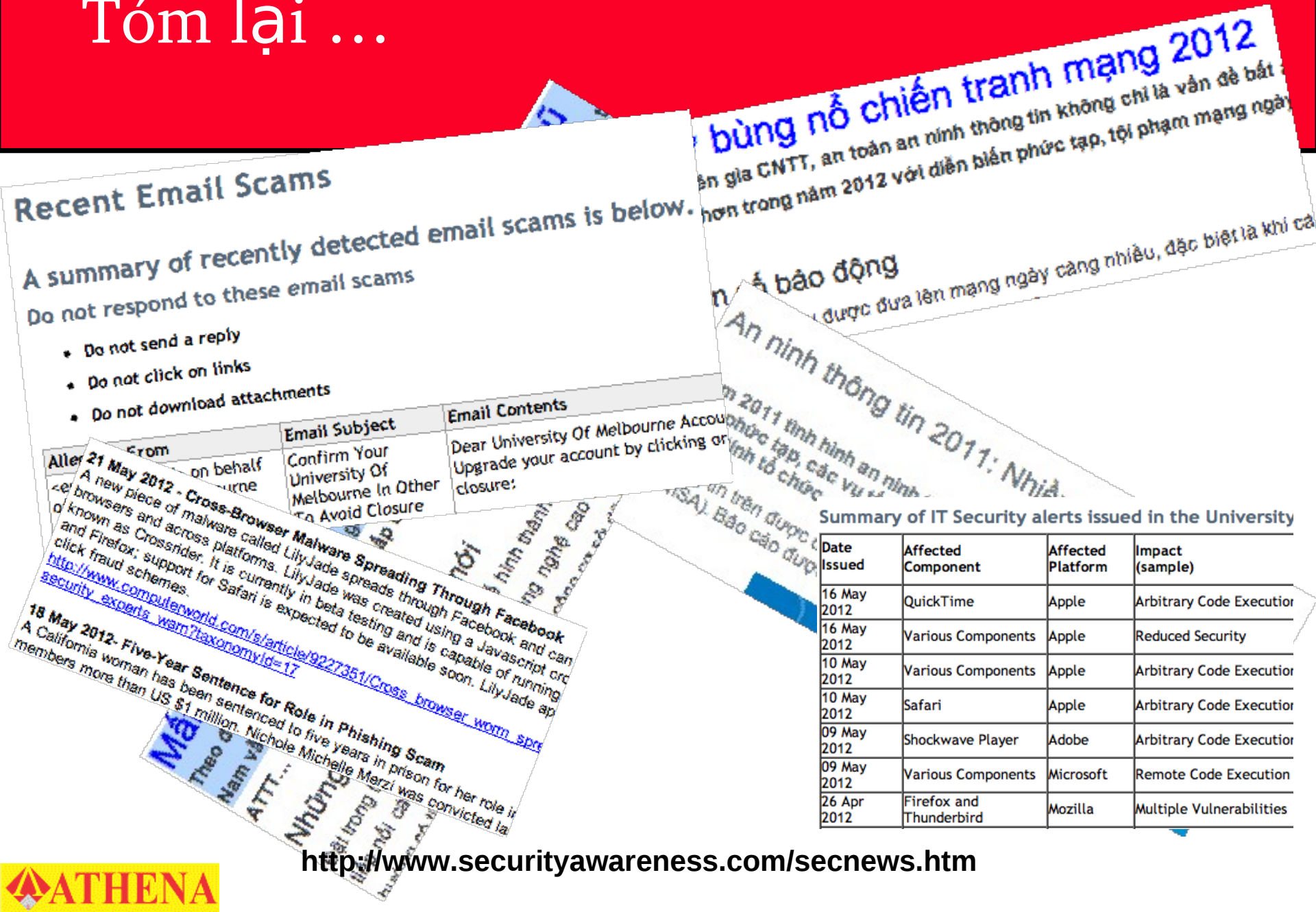
Tổ chức của quý vị có ước lượng được tương đối tổn thất tài chính khi bị tấn công không?



1. *Khả năng đánh giá tổn thất tài chính nhìn chung vẫn ở mức thấp, không thay đổi nhiều so với năm ngoái (chưa thực thi Đánh gía rủi ro)*
2. *Khi đi vào các tấn công cụ thể thì các tấn công bên ngoài như DOS, tấn công Web được cho là hay gây tổn thất, trong khi các tấn công bên trong bị coi nhẹ (Đặc điểm tâm lý 2011?)*

ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

Tóm lại …



Date Issued	Affected Component	Affected Platform	Impact (sample)
16 May 2012	QuickTime	Apple	Arbitrary Code Execution
16 May 2012	Various Components	Apple	Reduced Security
10 May 2012	Various Components	Apple	Arbitrary Code Execution
10 May 2012	Safari	Apple	Arbitrary Code Execution
09 May 2012	Shockwave Player	Adobe	Arbitrary Code Execution
09 May 2012	Various Components	Microsoft	Remote Code Execution
26 Apr 2012	Firefox and Thunderbird	Mozilla	Multiple Vulnerabilities

http://www.securityawareness.com/secnews.htm

ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

Bằng cách nào chúng ta bị hacked?

- Để một máy tính *(hay thiết bị tính toán có lập trình)* bị hacked, phải có một một ứng dụng nội gián
  Là ứng dụng của ta có sơ hở và bị trở thành nội gián không phụ thuộc vào chúng ta.
  Là ứng dụng do kẻ xấu cài đặt vào máy của ta với sự giúp sức của ta.

  Nếu máy tính của ta không bị đổi => chỉ có thể lừa (phishing) để chúng ta cung cấp thông tin, hoặc nghe thông tin trên đường truyền
  => Chúng ta có thể "sống" trong môi trường Internet hóa với "dày đặc" tin tặc như hiện nay

Bằng cách nào chúng ta tránh bị hacked?

- Ứng dụng của ta có sơ hở và bị trở thành nội gián không phụ thuộc vào chúng ta => vá lỗi phần mềm.
- Ứng dụng do kẻ xấu cài đặt vào máy của ta với sự giúp sức của ta => biết và thận trọng để không bị lừa *(click vào link của kẻ xấu, cài phần mềm xấu)*.
- Lừa (phishing) => nhận biết *(bằng công cụ, hiểu biết, thuê diệt web giả…)* website giả
- Nghe lén thông tin trên đường truyền

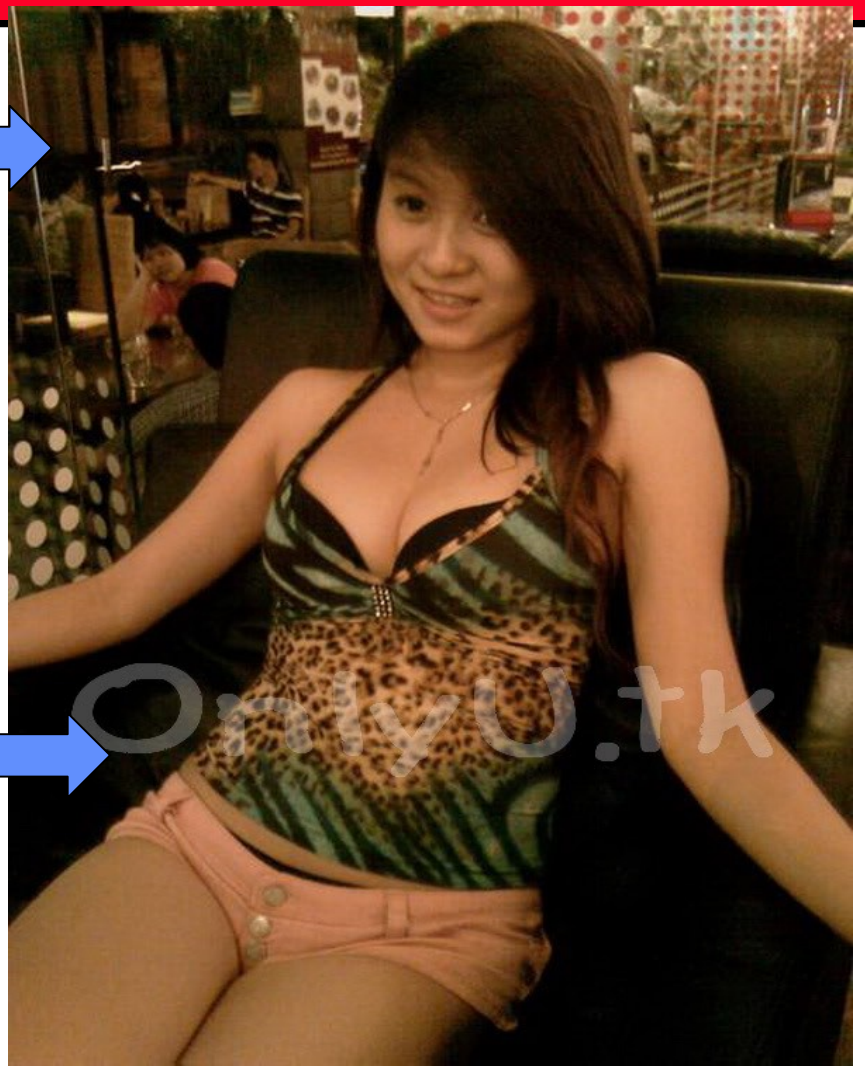
=> Mã hóa dữ liệu.

Tấn công mã độc

Click vào đây để xem bản full

...

Download bản đẹp ở đây...

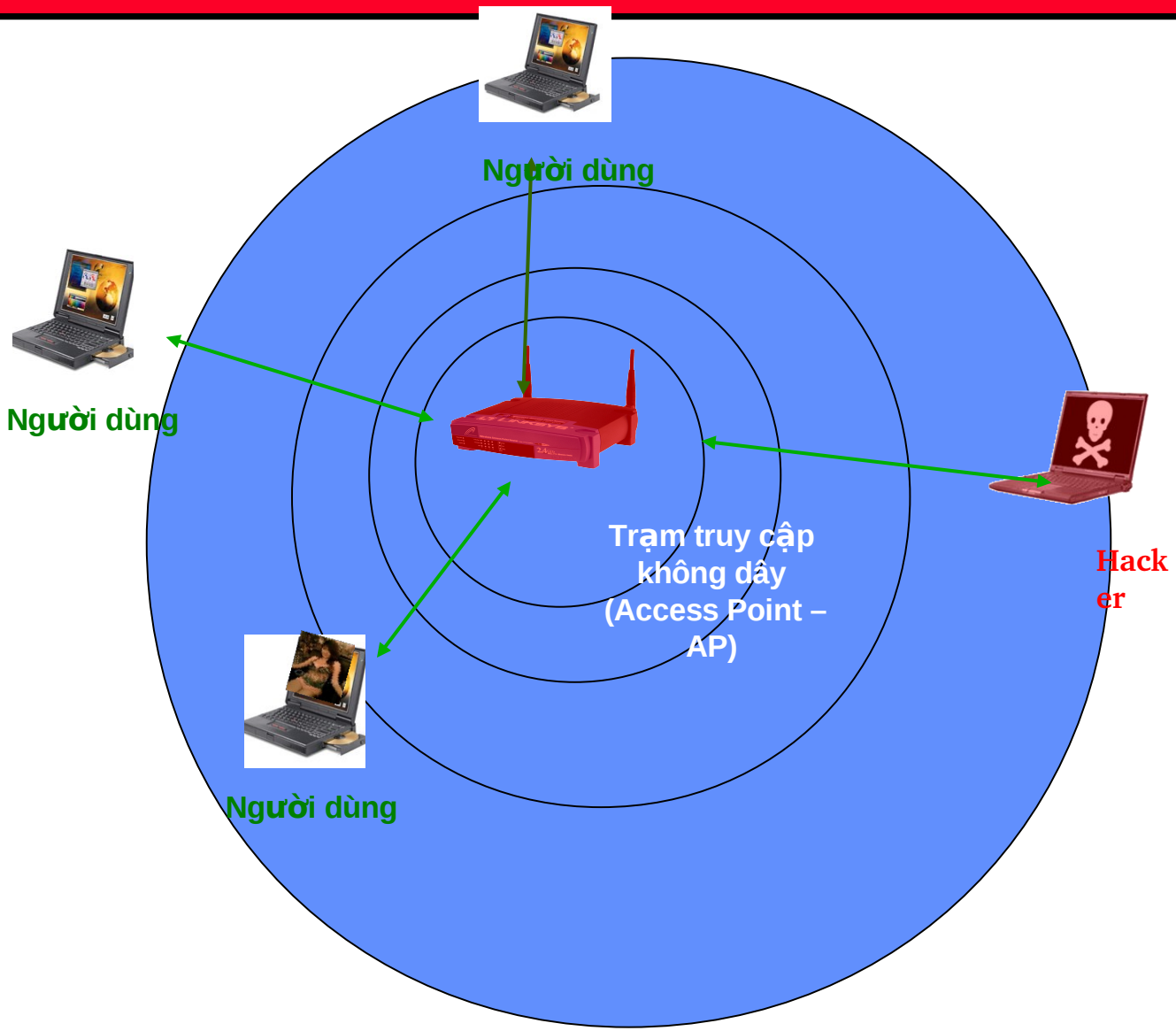


Môi trường làm việc freelance

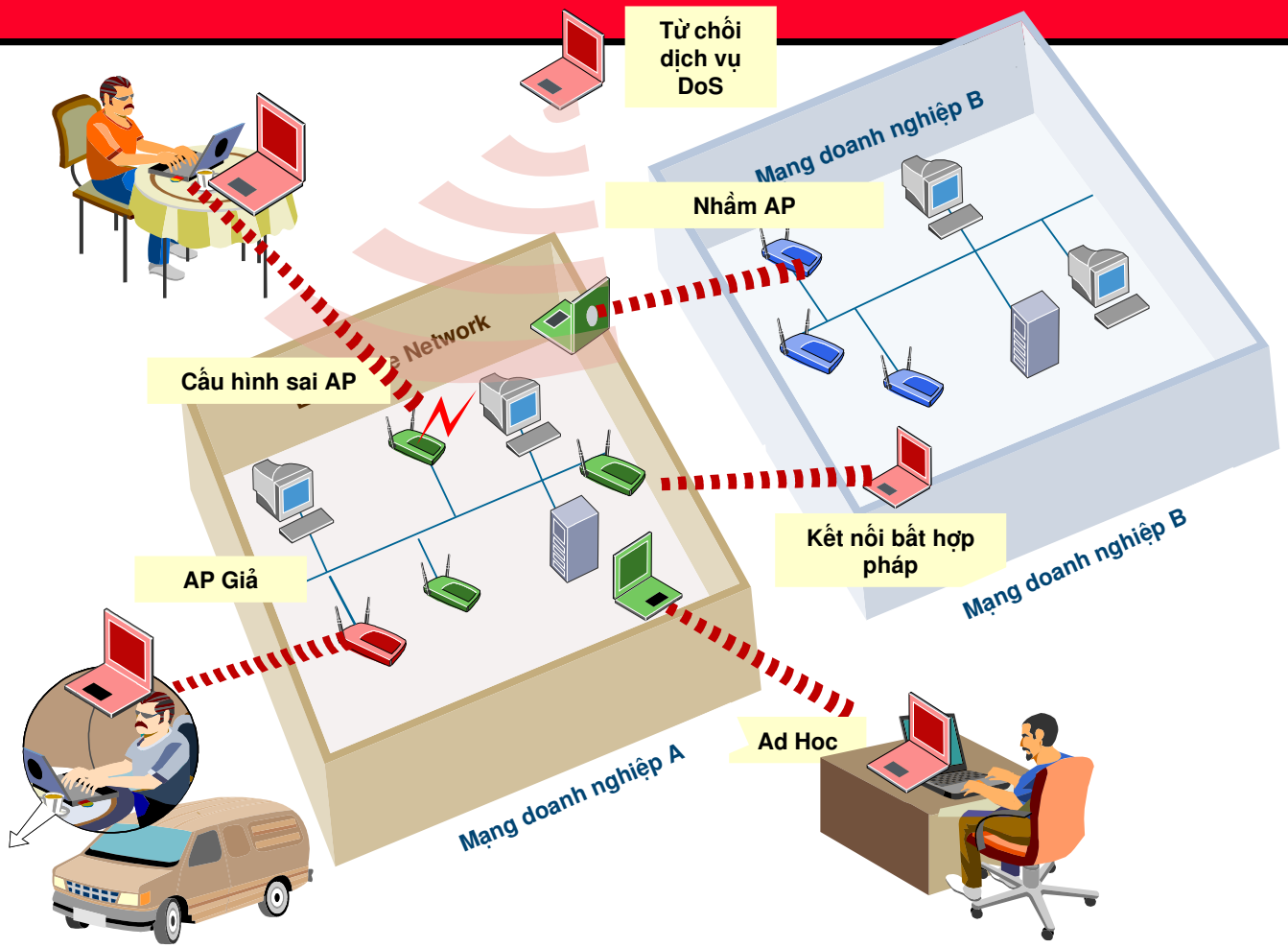
- Môi trường làm việc di động
- Sử dụng nhiều thiết bị khác nhau
- Kết quả 100% dạng số => dễ mất hết

ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

Rủi Ro Môi Trường Wifi



VÍ DỤ CÁC TẤN CÔNG WIFI



- Trạm truy cập AP giả mạo
- **Cấu hình sai AP**
  - **Kết nối ngang hàng wifi**
  - **Máy trạm gia nhập nhầm AP!**
  - **Người dùng bất hợp pháp**
- **Tấn công từ chối dịch vụ**

Tấn công giả mạo AP

Khai thác Thông tin từ Mạng Xã Hội

- Ngày 1/7/2012 , Mạng Xã Hội Bai du Trung Quốc đã âm thầm triển khai tại Việt Nam
- Có khả năng thu thập thông tin người dùng tại Việt Nam
- Có thể sử dụng thông tin người dùng để sử dụng cho mục đích xấu
- Theo báo người lao động ngày 1/7/2012
- http://nld.com.vn/20120701102825994p0c1002/baidu-tra-da-quan-bi-phan-ung-du-doi.htm

Tóm lược

- Thực hiện vá (patch) kịp thời và đầy đủ (tự động ???)
- Cân nhắc kỹ trước khi click vào link hoặc cài đặt phần mềm mới
- Mã hoá thông tin mỗi khi có thể: mã hóa tập tin, mã hoá thiết bị lưu trữ, xác thực khi sử dụng thiết bị, mã hoá đường truyền. Sử dụng 2 phương thức kết hợp để xác thực (token+mật khẩu)
- Triển khai xóa dữ liệu từ xa đề phòng mất thiết bị.

Hỏi đáp

ATHENA
ĐÀO TẠO QUẢN TRỊ MẠNG & AN NINH MẠNG QUỐC TẾ

LIÊN HỆ

- VÕ ĐỖ THẮNG
- Trung tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng ATHENA
- 2 Bis Đinh Tiên Hoàng, DaKao, Quận 1,Tp HCM
- www.athena.com.vn
- Tel : 38244041
- Hotline : 090 78 79 477