Số 55
04/2017

BẢN TIN danCISCO

Được phát hành bởi Công Ty TNHH Tư Vấn và Dịch Vụ Chuyên Việt

7 vấn đề bảo mật cần lưu tâm trong năm 2017

Năm 2016 dậy sóng bởi những vụ tấn công DDoS lớn chưa từng có từ "đội quân ma" IoT, lỗ hổng bảo mật trên WordPress đe dọa hàng triệu blogger đối mặt với rủi ro khó lường, mã độc ransomware bùng phát tống tiền khắp nơi, những cáo buộc về việc cá nhân sử dụng email riêng trong công việc gây mất anh ninh quốc gia, và tấn công mạng làm sai lệch kết quả bầu cử tổng thống Mỹ mới đây. Không có biểu hiện gì cho thấy bức tranh bảo mật 2017 sẽ sáng lên.

Thậm chí, theo nhiều chuyên gia bảo mật, tình hình năm nay còn tồi tệ hơn với nhiều diễn biến an ninh mạng phức tạp, từ những mánh lới phi kỹ thuật (social engineering) được hacker khai thác triệt để cho tới những cách thức tiêm nhiễm malware mới tinh vi hơn, khai thác lỗ hổng truy cập cơ sở dữ liệu dễ bị tổn thương, lợi dụng công nghệ di động xâm nhập vào hệ thống của các tổ chức, doanh nghiệp và người dùng mục tiêu.

[Trang 11]

10 LÝ DO BẠN NÊN LỰA CHỌN KHÓA HỌC CCNAX TRỰC TUYẾN TẠI VNPRO

[Trang 07]

Chương trình ưu đãi các khóa học:

Lớp sáng, chiều:

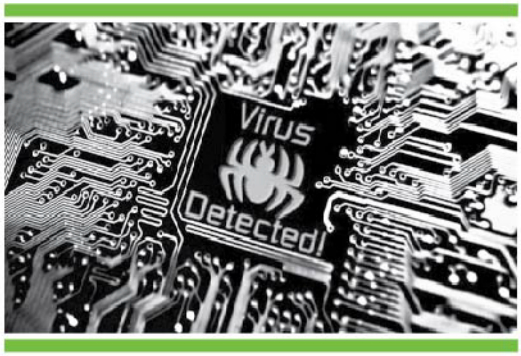
* Tặng Áo Thun.
* Tặng Giáo Trình.

Lớp tối:

a. Ưu đãi 30% HP dành cho Sinh Viên
b. Ưu đãi lên đến 20% HP dành cho Học viên cũ.
c. Ưu đãi dành cho khách hàng doanh nghiệp.
d. Tặng Balo, giáo trình.

Hầu hết các phần mềm bảo mật lớn đều bị CIA vượt qua

[Trang 03]



TIN TỨC SỰ KIỆN KHÁC

Buffalo tung router không dây hỗ trợ truyền phát 4K

Chuyên gia thiết bị số Buffalo vừa qua đã giới thiệu bộ định tuyến không dây mới có tên mã "WXR - 1900DHP 3", hỗ trợ truyền phát nội dung có độ phân giải 4K, dự kiến khởi bán cuối tháng 3/2017 tại Nhật Bản với giá 18.700 JPY (tương đương 162 USD).

Router tương thích cấu hình Wi-Fi IEEE 802.11a / b / g / n / ac, cùng 3 ăng-ten theo tiêu chuẩn 11ac, thiết bị hứa hẹn cung cấp đường truyền tốc độ cao cực kỳ ổn định với các thiết bị di động hoặc không dây. Bên cạnh đó, tính năng "tự động chống nhiễu sóng" giúp thiết bị hạn chế sự can thiệp của tín hiệu từ những đồ điện tử khác, chẳng hạn như lò vi sóng.

Cùng với "QoS cải tiến", router hoàn toàn có khả năng truyền phát tín hiệu video 4K. Hiện ở Nhật, chỉ có dịch vụ VOD Hikari TV cung cấp độ phân giải thời thượng này. Nhưng, với một đường truyền mạnh, người dùng vẫn sẽ có thể tận hưởng các điểm ảnh Ultra HD trên Netflix hay YouTube trong tương lai gần. Ngoài ra, với cổng USB, router có thể được nối với một USB DAC để chuyển âm thanh chất lượng cao lên các NAS cũng như chơi nhạc hi-res 192 kHz / 24 bit.

Trái tim của router là một vi xử lý lõi kép có clock-rate 1GHz, vận hành cùng 2 chip giao tiếp ở băng tần 5GHz và 2.4GHz. Thiết bị có khả năng điều biến thông tin (module) chuẩn 256 QAM và truyền tải tín hiệu ở tốc độ lên tới 1.300 Mbps trên band 5GHz hoặc lên tới 600Mbps trên band 2.4GHz. Thêm nữa, router cung cấp tính năng "chuyển băng tần", giúp người dùng linh hoạt chuyển đổi qua lại hai băng tần mỗi khi tắc nghẽn.

Về khả năng kết nối, máy có 4 cổng Ethernet (4x 1.000 Mbps) và 1 cổng Internet (1x 1.000 Mbps). Điện năng tiêu thụ trung bình khoảng 23,9 W. Thông số kích cỡ và cân nặng lần lượt là 41 × 185 × 185mm và 560g.

Theo buffalo

Hầu hết các phần mềm bảo mật lớn đều bị CIA vượt qua

WikiLeaks gần đây đã tung ra hàng loạt tài liệu của CIA, trong đó có đề cập đến việc một loạt các phần mềm diệt Virus và các sản phẩm bảo mật có thể bị CIA khai thác hoặc dễ dàng vượt qua.

Các sản phẩm này bao gồm:

- Comodo
- Avast
- F-Secure
- Zemana Antilogger
- Zone Alarm
- Trend Micro
- Symantec
- Rising
- Panda Security
- Norton
- Malwarebytes Anti-Malware
- EMET (Enhanced Mitigation Experience Toolkit)
- Microsoft Security Essentials
- McAfee
- Kaspersky
- GDATA
- ESET
- ClamAV
- Bitdefender
- Avira
- AVG

Chúng ta có thể nhận ra được rất nhiều trong số đó. Danh sách này cũng bao gồm luôn cả phần mềm diệt virus "Security Essentials" của Microsoft được tích hợp sẵn vào Windows Defenders trong cả Windows 8 và Windows 10, cũng như EMET, công cụ bảo mật chống khai thác thông tin (chủ yếu dành cho khách hàng doanh nghiệp).

Nhóm bảo mật của Project Zero thuộc Google cũng tìm ra rằng phần mềm diệt virus đôi khi lại là những phần mềm dễ tổn hại nhất trên hệ thống của bạn. Không chỉ bởi vì một số các công ty thiếu cẩn thận trong khi code mà phần lớn là bởi họ dùng những kỹ thuật tương tự nhau để "khiến người dùng an toàn hơn" khiến khả năng tổn thương hệ thống của người dùng trở nên lớn hơn.

Điều quan trọng nhất để giữ bản thân an toàn đó chính là cần phải cẩn thận về phần mềm cài đặt trên hệ thống, sử dụng tài khoản mặc định là tài khoản hạn chế quyền truy cập, nâng cấp hệ điều hành thường xuyên. Những điều này sẽ giúp chúng ta bớt đi các vấn đề về bị tấn công hoặc malware.

Theo tomshardware

Routing & Switching

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Chương trình CCNA R&S

CISCO CERTIFIED CCNP

Chương trình CCNP ROUTE

CISCO CERTIFIED CCNP

Chương trình CCNP SWITCH

CISCO CERTIFIED CCNP

Chương trình CCNP TSHOOT

CISCO CERTIFIED CCIE ROUTING AND SWITCHING

Chương trình CCIE

Security

CISCO CERTIFIED CCNA SECURITY

Chương trình CCNA Security

CISCO CERTIFIED CCNP SECURITY

Chương trình SECURE

CISCO CERTIFIED CCNP SECURITY

Chương trình FIREWALL

CCNA Voice

CISCO CERTIFIED CCNA VOICE

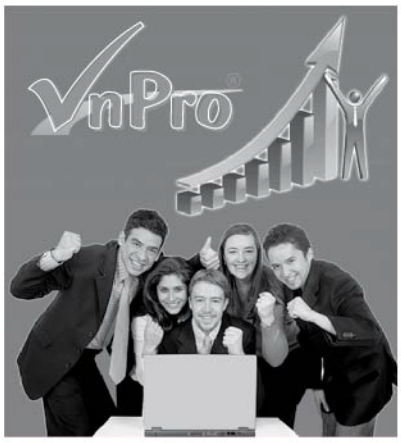
Chương trình ưu đãi các khóa học:

Lớp sáng, chiều:

* Tặng Áo Thun.
* Tặng Giáo Trình.

Lớp tối:

a. Ưu đãi 30% HP dành cho Sinh Viên
b. Ưu đãi lên đến 20% HP dành cho Học viên cũ.
c. Ưu đãi dành cho khách hàng doanh nghiệp.
d. Tặng Balo, giáo trình.

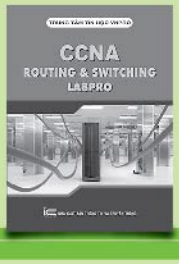


Cam kết lợi ích khi học tại VnPro

- Giáo trình giảng dạy chuẩn quốc tế và LabPro tiếng Việt.
- Thực hành >70% thời lượng chương trình và trực tiếp 100% trên thiết bị chính hãng, hiện đại. (>100 giờ lab)
- Được thực hành miễn phí ngoài giờ.
- Chứng chỉ VnPro được công nhận trên toàn quốc.
- Thi đậu quốc tế sau khi hoàn tất khóa học.

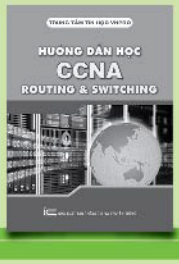
Là trung tâm duy nhất trong cả nước phát hành hơn 20 quyển sách mạng LabPro tiếng Việt. Giáo trình VnPro được cập nhật, nâng cấp thường xuyên theo chuẩn giáo trình quốc tế

GIẢM* NGAY 10%

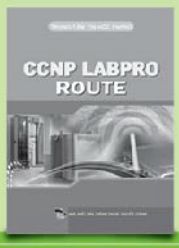


CCNA Routing & Switching
Giá: 150.000 VNĐ

CCDA
Giá: 250.000 VNĐ

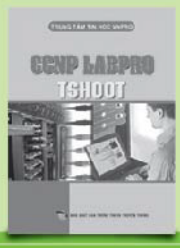


Hướng dẫn học CCNA Routing & Switching
Giá: 180.000 VNĐ



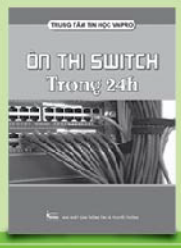
CCNP LABPRO ROUTE
Giá: 120.000 VNĐ

CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

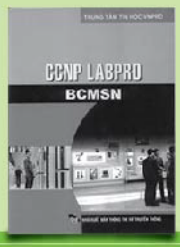
Ôn thi Route
Giá: 90.000 VNĐ



Ôn thi Switch
Giá: 100.000 VNĐ

Ôn thi Tshoot
Giá: 80.000 VNĐ

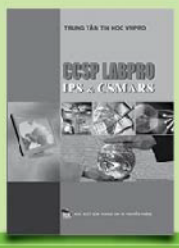
CCNP LABPRO BSCI
Giá: 95.000 VNĐ



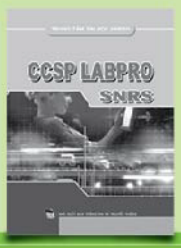
CCNP LABPRO BCMSN
Giá: 70.000 VNĐ

CCNP LABPRO ISCW
Giá: 120.000 VNĐ

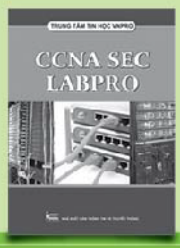
CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ



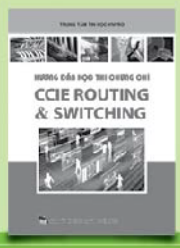
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



CCSP LABPRO SNRS
Giá: 140.000 VNĐ



CCNA SEC LABPRO
Giá: 150.000 VNĐ



CCIE R&S
Giá: 150.000 VNĐ

CWNA
Giá: 90.000 VNĐ

Chương trình ưu đãi sách: Áp dụng chính sách là giảm 10% khi đặt sách online

* Khi mua sách LabPro online. Link mua sách online:***http://www.vnpro.vn/sach-labpro/***

10 LÝ DO BẠN NÊN LỰA CHỌN KHÓA HỌC CCNAX TRỰC TUYẾN TẠI VNPRO

Bạn ở xa nhưng bạn muốn học CCNAX tại VnPro?

- Bạn muốn nâng cao kiến thức chuyên môn nhưng không có thời gian?
- Bạn muốn học Online nhưng vẫn đảm bảo đầy đủ kiến thức và thực hành như thực tế?
- Sau đây là 10 lý do bạn nên lựa chọn khóa học CCNAX Online tại VnPro!

1. VnPro là Trung Tâm uy tín với hơn 14 năm kinh nghiệm về đào tạo quản trị mạng Cisco.

- Với hơn 14 năm kinh nghiệm trong lĩnh vực quản trị mạng Cisco, VnPro luôn đi đầu trong việc ứng dụng công nghệ vào công tác giảng dạy nhằm mang lại chất lượng đào tạo tốt nhất dành cho học viên.

2. Đội ngũ giảng viên giàu kinh nghiệm thực tế, được đào tạo nghiệp vụ sư phạm chuyên nghiệp.

- Với đội ngũ giảng viên là những chuyên gia cao cấp đầu ngành, đã và đang làm việc cho các tập đoàn, công ty công nghệ hàng đầu tại Việt Nam. Với những kinh nghiệm thực tế kết hợp với kỹ năng sư phạm được đào tạo bài bản, đội ngũ giảng viên của VnPro luôn sẵn sàng truyền lại ngọn lửa đam mê cho học viên.

3. Chương trình đào tạo bài bản, được thiết kế riêng cho khóa học trực tuyến phù hợp với nhiều đối tượng khác nhau.

- Bằng kinh nghiệm thực tế của đội ngũ giảng viên kết hợp với giáo trình chuẩn của Cisco, VnPro cho ra đời chương trình CCNAX Online phù hợp với tình hình hình thực tế của Việt Nam. Dù sinh viên, hay người đi làm đều có thể tiếp thu một cách tốt và nhanh nhất.

4. Học trực tuyến, thực hành trực tuyến, kiến thức thực tế.

- Từ các bài giảng trực tuyến, đến việc sử dụng công cụ LabOnline PRO để thực hành học viên sẽ dễ dàng nắm bắt kiến thức được truyền tải từ giảng viên một cách tốt nhất.

5. Phần mềm đào tạo Online chuyên nghiệp và có bản quyền.

- Phần mềm đào tạo Online tại VnPro được giới công nghệ đánh giá là phần mềm tốt nhất cho công việc đào tạo giảng dạy online hiện nay.

6. Tương tác trực tiếp với giảng viên như trên lớp học thực tế.

- Với phần mềm đào tạo Online tại VnPro học viên có thể tương tác với giảng viên như trên lớp học thật. Học viên có thể dễ dàng giơ tay để trao đổi riêng với giảng viên hoặc trao đổi chung với cả lớp khi cần thiết.

7. Trao đổi và làm việc nhóm với các thành viên của lớp dễ dàng.

- Học viên có thể trao đổi riêng theo từng nhóm với sự hướng dẫn của giảng viên. Việc trao đổi nhóm này sẽ giúp cho học viên dễ dàng làm các bài tập lớn từ giảng viên đưa xuống nhằm tiếp thu tốt nhất kiến thức từ bài học mang lại.

8. Học trực tiếp trên SmartPhone.

- Với ứng dụng trên AppStore và cả Android, học viên có thể học online ngay trên chiếc SmartPhone của mình mà không cần phải lúc nào cũng mang theo laptop.

9. Linh hoạt về thời gian và địa điểm học

- Vì có thể học bằng SmartPhone và xem lại toàn bộ buổi học qua các video của VnPro nên giúp cho việc học tập của học viên trở nên linh hoạt hơn nữa. Không còn bị giới hạn bởi không gian và thời gian dù là quán café, ở nhà, công ty, hay thậm chí bạn đang ở trên xe ô tô. Chỉ cần có mạng internet và 1 chiếc Smartphone là có thể học CCNAX.

10. Được VnPro cấp chứng chỉ hoàn thành khóa học.

- Học viên sẽ được cấp chứng chỉ hoàn thành khóa học sau khi vượt qua được tất cả các bài Test. Chứng chỉ do VnPro cấp luôn được các nhà tuyển dụng đánh giá rất cao.

Bộ phận Marketing – Phòng Kinh Doanh

VNPRO TRIỂN KHAI ĐÀO TẠO NÂNG CAO NGHIỆP VỤ SƯ PHẠM CHO ĐỘI NGŨ GIẢNG VIÊN

Bên cạnh sứ mệnh đào tạo và cung cấp đội ngũ nhân lực IT chuyên nghiệp cho các doanh nghiệp, VnPro còn chú trọng vào việc xây dựng đội ngũ giảng viên có năng lực cùng chung tay thực hiện công tác kế thừa. Vừa qua ngày 18/03/2017, VnPro đã khai giảng lớp đào tạo nghiệp vụ sư phạm cho đội ngũ giảng viên.

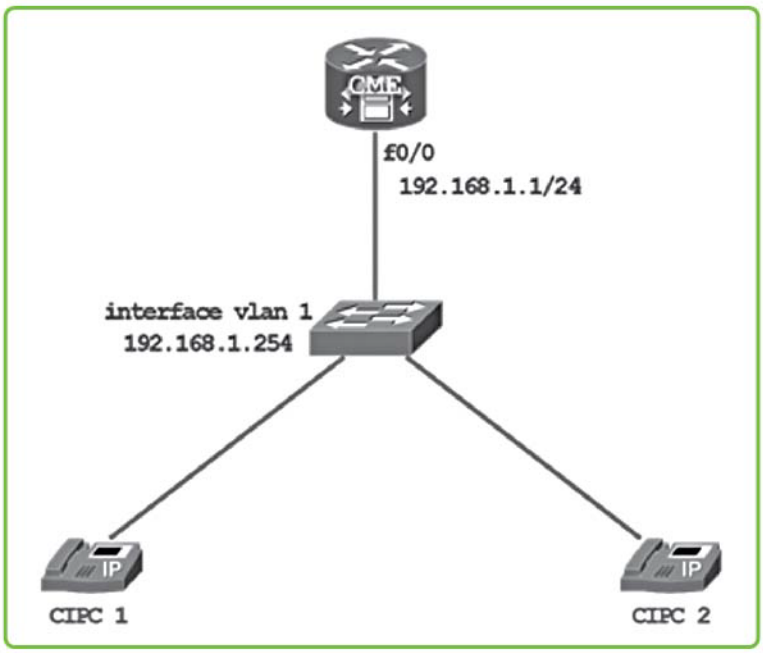
Buổi đào tạo này nhằm mục đích nâng cao chất lượng giảng viên vừa có kiến thức chuyên sâu về chuyên môn, vừa có kỹ năng sư phạm tốt. Tiêu chí của lớp giảng viên nâng cao chất lượng dịch vụ, cũng như là tìm kiếm những người có đam mê về quản trị mạng với mong muốn chia sẻ với cộng đồng. Đồng thời tìm kiếm nguồn lực nhân sự nhằm mở rộng và phát triển VnPro trong tương lai. Lớp giảng viên có sự góp mặt của các chuyên viên, chuyên gia trong lĩnh vực quản trị mạng đã và đang làm việc tại các công ty tập đoàn lớn ở Tp. Hồ Chí Minh.

Lớp đào tạo nghiệp vụ sư phạm tại VnPro vừa qua

Đội ngũ giảng viên mới ngoài việc tham gia các lớp hướng dẫn nhằm nâng cao kỹ năng trình bày và sư phạm, còn phải thường xuyên tham gia tại các lớp với vai trò trợ giảng nhằm tích lũy kinh nghiệm thật kỹ trước khi chính thức giảng dạy tại VnPro.

Bộ phận Marketing – Phòng Kinh Doanh

Cấu hình Auto Registration và Auto Assign



Yêu cầu:

1. Cấu hình cơ bản trên các thiết bị.
2. Cấu hình tính năng Auto Registration trên CME cấp số DN một cách tự động cho các SoftPhone hoặc HardPhone.

Thực hiện:

Yêu cầu 1. Cấu hình cơ bản trên các thiết bị.

Cấu hình cơ bản trên CME.

```
hostname R1
interface f0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit
no ip domain-lookup
```

```
ip dhcp excluded-address 192.168.1.254
ip dhcp excluded-address 192.168.1.1
ip dhcp pool Voice
 network 192.168.1.0 255.255.255.0
 default-route 192.168.1.1
 option 150 ip 192.168.1.1
 dns-server 8.8.8.8
 exit
```

Cấu hình cơ bản trên Switch.

```
hostname Sw1
interface vlan 1
 ip address 192.168.1.254 255.255.255.0
 no shutdown
 exit
```

```
ip default-gateway 192.168.1.1
line vty 0 4
 privilege level 15
 no login
 exit
line console 0
 logging synchronous
 exit
no ip domain-lookup

interface range f1/0/1-48
 switchport mode access
 switchport access vlan 1
 spanning-tree portfast
 exit
```

Yêu cầu 2. Cấu hình tính năng Auto Registration trên CME cấp số DN một cách tự động cho các SoftPhone hoặc HardPhone.

Auto-Registration được kích hoạt mặc định trên CME.

- Các Phone thực hiện tiến trình autoregistration method thường kết nối tới CME để lấy XMLDefault.cnf.xml file về.

```
telephony-service
 ip source-address 192.168.1.1 port 2000
 auto-reg-ephone
 max-ephone 42
 max-dn 144
 auto assign 1 to 2
 restart all
 exit

ephone-dn 1
 number 1001
 label BQK(1001)
 name BQK1001
 exit

ephone-dn 2
 number 1002
 label BQK(1002)
 name BQK1002
 exit
```

Sau khi các CiscoPhone đã register tới CME, ta tiến hành khảo sát file cấu hình **running-config** sẽ thấy 2 cấu hình **ephone** sau tự động được tạo ra.

```
ephone  1
 device-security-mode none
 mac-address 782B.CBDC.9205
 type CIPC
 button  1:1
!
ephone  2
 device-security-mode none
 mac-address 0000.AAAA.1001
 type CIPC
 button  1:2
```

Kiểm tra các phone đang tiến hành đăng ký với CME.

```
R1# show ephone attempted-registrations
```

7 vấn đề bảo mật cần lưu tâm trong năm 2017

Năm 2016 dậy sóng bởi những vụ tấn công DDoS lớn chưa từng có từ "đội quân ma" IoT, lỗ hổng bảo mật trên WordPress đe dọa hàng triệu blogger đối mặt với rủi ro khó lường, mã độc ransomware bùng phát tống tiền khắp nơi, những cáo buộc về việc cá nhân sử dụng email riêng trong công việc gây mất anh ninh quốc gia, và tấn công mạng làm sai lệch kết quả bầu cử tổng thống Mỹ mới đây. Không có biểu hiện gì cho thấy bức tranh bảo mật 2017 sẽ sáng lên.

Thậm chí, theo nhiều chuyên gia bảo mật, tình hình năm nay còn tồi tệ hơn với nhiều diễn biến an ninh mạng phức tạp, từ những mánh lới phi kỹ thuật (social engineering) được hacker khai thác triệt để cho tới những cách thức tiêm nhiễm malware mới tinh vi hơn, khai thác lỗ hổng truy cập cơ sở dữ liệu dễ bị tổn thương, lợi dụng công nghệ di động xâm nhập vào hệ thống của các tổ chức, doanh nghiệp và người dùng mục tiêu.

Dưới đây là 7 điểm nhấn trong bức tranh bảo mật 2017 theo nhận định của các chuyên gia.

Tăng cường quản lý mật khẩu

Mật khẩu từ lâu đã được xem là không thể thiếu để xác thực quyền truy cập hệ thống thông tin nhạy cảm, dù vậy trên thực tế nhận thức về điều này nhiều khi còn quá lơ là.

Thói quen sử dụng mật khẩu đơn giản, dễ đoán hoặc duy trì quá lâu, thậm chí để nguyên mật khẩu mặc định truy cập thiết bị vẫn khá phổ biến. Theo khảo sát hiện trạng an ninh các camera IP tại Việt Nam trong quý III/2016 của công ty an ninh mạng Bkav, có tới 76% thiết bị vẫn đang dùng tài khoản và mật khẩu mặc định của nhà sản xuất, tạo điều kiện cho kẻ xấu dễ dàng truy cập, chiếm quyền điều khiển thiết bị.

Tạp chí công nghệ Computerworld dẫn lời CEO Matt Dircks của công ty bảo mật Bomgar & Scott Millis, cho rằng các doanh nghiệp đã nhận thức được họ dễ bị tổn thương ra sao nên ngày càng quan tâm hơn đến các dịch vụ quản lý mật khẩu. Đây sẽ là xu hướng của năm nay.

Cuộc tấn công DDoS diễn ra cuối tháng 10/2016 nhắm vào nhà cung cấp dịch vụ tên miền Dyn gây ảnh hưởng hàng loạt dịch vụ Internet tại Mỹ là lời cảnh báo về nguy cơ mất an toàn thông tin (ATTT) từ những thiết bị IoT (Internet of Things) chỉ được bảo vệ bằng mật khẩu mặc định. Cuộc tấn công được cho là do mã độc Mirai lây nhiễm rất nhiều thiết bị IoT và tạo ra mạng botnet rộng lớn. Trước đó, vào tháng 9, cuộc tấn công tương tự vào công ty cung cấp dịch vụ hosting OVH của Pháp đạt mức băng thông kỷ lục lên tới 1 Terabit/giây.

Không chỉ camera IP mà router gia đình và thiết bị kết nối Internet khác để nguyên mật khẩu mặc định không phải là chuyện hiếm. Nhiều chuyên gia bảo mật cảnh báo, thói quen dùng mật khẩu yếu cũng đặt các cơ sở hạ tầng trọng yếu được vận hành bởi các hệ thống CNTT (như ICS/Scada) thành mục tiêu dễ bị hacker hạ gục từ xa.

Sử dụng bộ quản lý mật khẩu đáng tin cậy là cách tốt nhất để tạo ra mật khẩu mạnh ngẫu nhiên, lưu trữ an toàn, tiện dùng và định kỳ đổi mật khẩu sẽ khiến hacker nản lòng trong việc dò tìm, bẻ khóa.

Giám sát chặt đặc quyền

Chuyên gia bảo mật Matt Dircks cho biết, hacker luôn muốn dành quyền truy cập cấp cao thông qua mục tiêu chiếm đoạt tài khoản người dùng đặc quyền như quản trị viên, chuyên viên IT cao cấp, CEO và nhà cung cấp. Vì thế, việc các tổ chức chỉ chú trọng triển khai các giải pháp công nghệ bảo mật cho hệ thống, ứng dụng và dữ liệu quan trọng của họ là chưa đủ.

Tại buổi hội thảo Ngày ATTT Việt Nam 2016 diễn ra hôm 17/11 tại TP.HCM, các chuyên gia cảnh báo công tác phòng thủ chỉ dựa vào công nghệ chưa đủ để đối phó với các mối đe dọa ngày nay, khi mà hacker thông minh hơn, tấn công có chủ đích và đeo bám dai dẳng hơn với những mã độc tinh vi, phương thức tấn công liên tục được cải tiến.

"Nhiều cuộc tấn công mạng nhắm vào yếu tố con người vì dễ thành công hơn, lại có chi phí thấp, thậm chí có thể thuê dịch vụ tấn công giá thấp", Stefanus Natahusada, chuyên gia tư vấn bảo mật của Kaspersky cho biết.

Ông Vũ Trọng Đường - Giám đốc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT cũng nhìn nhận, nhiều lãnh đạo có quyền truy cập cao nhưng lại hành xử thiếu chuyên nghiệp là cơ hội để hacker lợi dụng khai thác tấn công.

Theo ông Dircks, trong năm 2017 này, các tổ chức sẽ phải nhận thức là bảo vệ hệ thống không đủ mà còn phải kiểm soát chặt chẽ những người dùng đặc quyền, không cho phép họ truy cập tới những gì không cần thiết, và có những cảnh báo kịp thời khi họ truy cập vượt ra ngoài khu vực được phép.

Con người vốn được xem là mắt xích yếu nhất trong hệ thống phòng thủ an ninh mạng, và các chuyên gia vẫn thường nhấn mạnh tầm quan trọng của công tác đào tạo kiến thức bảo mật, nâng cao nhận thức của người dùng.

Đặc biệt trong kỷ nguyên di động lấy ứng dụng (app) làm trung tâm, rất nhiều ứng dụng đòi quyền truy cập dữ liệu quan trọng và thông tin cá nhân nhạy cảm, và vì muốn nâng cao trải nghiệm khi sử dụng thiết bị cá nhân nên người dùng dễ chấp thuận, tạo cơ hội cho mã độc lây nhiễm và trao quyền lớn cho kẻ tấn công.

Thêm nữa, người dùng thường tin tưởng vào các nhà cung cấp dịch vụ và yên tâm được bảo vệ bởi các chương trình phòng chống mã độc cài trên thiết bị. Niềm tin đó theo nhiều chuyên gia là hết sức nguy hiểm trong bối cảnh thiếu hụt chuyên viên bảo mật, nhân lực trong lĩnh di động thiếu kỹ năng về an ninh mạng và hacker thì ngày càng thông minh, mã độc ngày càng độc hơn.

Tình trạng đổ lỗi cho nhau về trách nhiệm bảo mật

Gia tăng nhanh chóng đủ loại thiết bị IoT cũng chính là cơ hội để các loại malware phát tác khó kiểm soát. Điều đáng lo ngại là nhiều thiết bị IoT thiếu tính năng bảo mật, thậm chí có thể chỉ được bảo vệ bằng tên và mật khẩu mặc định, như phát hiện gần đây với rất nhiều camera IP. Trong khi đó, bộ phận CNTT thường chỉ có trách nhiệm với máy tính và hệ thống mạng nội bộ, những thiết bị IoT mới nhiều khi không rõ thuộc phạm vi trách nhiệm của ai, nghĩa là tiềm ẩn mất an ninh, ATTT rất lớn.

Ai chịu trách nhiệm bảo đảm an ninh ATTT, vá các lỗ hổng bảo mật cho thiết bị IoT? Tệ hơn nữa, nếu có sản phẩm kết nối mạng nội bộ mà chưa được vá lỗ hổng thì sao? Dữ liệu tự động đồng bộ lên mây thì ai sẽ chịu trách nhiệm về ATTT cho các thiết bị đồng bộ khác: nhà sản xuất thiết bị IoT, nhà cung cấp dịch vụ bảo mật, bộ phận CNTT, hay người dùng cuối? Rất nhiều câu hỏi đặt ra mà không dễ có câu trả lời rõ ràng. Nghĩa là khó qui trách nhiệm khi sự cố bảo mật xảy ra, cũng không rõ ai sẽ là người giải quyết? Những phản ứng tiêu cực sẽ là hậu quả từ cơ chế phân quyền không rõ ràng.

Ông Dircks cho rằng các CSO, CISO hay thậm chí là CIO đều đang ngồi trên ghế nóng vô hình với trách nhiệm nặng nề về bảo mật. Họ phải có trách nhiệm góp phần xây dựng chính sách ATTT với các qui định và biện pháp bảo đảm ATTT cho tổ chức. Thực thi thì thuộc về bộ phận CNTT. Vấn đề đặt ra với các đơn vị là truyền thông phải thông suốt giữa bộ phận CNTT và các lãnh đạo để họ hiểu rõ những nguy cơ tiềm ẩn, nhu cầu và kinh phí đầu tư, lựa chọn giải pháp bảo mật, và những khó khăn, thách thức mà tổ chức phải đối mặt.

Ransomware sẽ vượt tầm kiểm soát

Tấn công tống tiền bằng mã độc ransomware đã thành xu hướng chủ đạo tạo ra hoạt động kinh doanh béo bở cho giới tội phạm mạng. Báo cáo tình hình an ninh mạng năm 2016 của Symantec cho biết, năm qua trung bình mỗi ngày có hơn 4.000 cuộc tấn công của mã độc ransomware, tăng 300% so với năm trước.

Chia sẻ tại Ngày ATTT Việt Nam 2016, ông Võ Đỗ Thắng - Giám đốc Trung tâm Đào tạo Quản trị và An ninh mạng Athena, cho hay, số lượng ransomware mới không những tăng nhanh mà sinh ra rất nhiều biến thể, cực kỳ khó đối phó. Điều đáng sợ là rất dễ để tạo ra ransomware từ mã nguồn ban đầu tải về từ Internet.

Theo Scott Millis – Giám đốc công nghệ của công ty bảo mật thiết bị và di động Cyber adAPT, hầu hết các kỹ thuật phòng vệ hiện nay như tường lửa, chương trình antivirus hay ngăn chặn xâm nhập để giảm thiểu các mối nguy hại là không đủ để chống lại các cuộc tấn công mạng kiểu mới. Thực tế, từ những vụ rò rỉ dữ liệu vừa qua, như 1 tỷ tài khoản Yahoo bị đánh cắp thông tin, cho thấy việc phát hiện và đối phó phải được cải thiện.

Và khi hacker tăng cường dùng mánh lới phi kỹ thuật (social engineering), cũng như lợi dụng môi trường mạng xã hội để đánh cắp dữ liệu nhạy cảm của những người có vai trò quan trọng với tổ chức doanh nghiệp, thì việc tăng cường huấn luyện về bảo mật một cách toàn diện cho người dùng càng phải được đề cao.

Các chuyên gia bảo mật cảnh báo rằng, doanh nghiệp sẽ phải đối mặt với tình trạng tấn công ransomware ngày càng gia tăng, rủi ro khó lường có thể xảy ra bất cứ lúc nào nếu chính sách cũng như công nghệ về bảo mật không được cải thiện. Nhất là có nhiều loại ransomware có thể nằm phục sẵn rất lâu trong hệ thống trước khi hacker phát động tấn công nên càng khó phát hiện. Thêm nữa, theo ông Millis, những giải pháp như IaaS, SaaS và thiết bị IoT mới triển khai ngày càng nhiều khiến công cuộc bảo vệ hệ thống thông tin của doanh nghiệp càng gặp khó.

Thời gian phát hiện không mấy cải thiện

Thời gian phát hiện một cuộc tấn công thành công sẽ không mấy cải thiện trong năm nay. Có những trường hợp nạn nhân có thể mất tới hàng năm mới biết mình đã bị tấn công, gánh chịu thiệt hại rất lớn.

Theo ông Millis, thời gian nhận biết lâu như vậy là do công tác phát hiện hoạt động tấn công chưa được quan tâm đúng mức. Các công ty, nhà sản xuất và người dùng cá nhân đều tìm cách tránh xa những nguồn lây nhiễm malware trên mạng, các công nghệ phòng thủ tập trung vào ngăn chặn sự xâm nhập từ ngoài vào, và nhận diện malware theo kiểu như một cuộc chạy đua vũ trang mà hacker luôn dẫn trước.

Các công nghệ phản ứng và khả năng khắc phục sự cố được cải thiện, nạn nhân có thể cô lập và sửa chữa hư hỏng nhanh chóng. Nhưng, vấn đề là những công nghệ này không giúp giảm thiểu thời gian nhận biết, trừ khi mã độc được khám phá tình cờ, theo nhận định của ông Millis. Ông cũng cho rằng việc sử dụng các tập tin log của thiết bị kết nối mạng có thể giúp phát hiện sớm manh mối liệu một cuộc tấn công đã tiến hành thử hay thành công rồi, nhưng vấn đề là dữ liệu lưu trữ quá lớn và nhiều thể loại là một trở ngại không hề nhỏ cho phương thức này.

Hệ thống phát hiện sớm và quản lý theo sự kiện (Security Incident and Event Management - SIEM) đem đến khả năng phát hiện tấn công theo hành vi, những kết nối đáng ngờ từ trong hệ thống ra bên ngoài, biểu hiện bất thường của những sự kiện… Tuy nhiên, việc xây dựng SIEM ngày càng tốn kém, hơn nữa lưu lượng truyền trên mạng ngày càng "khủng", phần lớn còn được mã hóa nên khả năng phát hiện sớm các cuộc tấn công mạng vẫn còn xa so với mong đợi, theo báo cáo của Chi hội ATTT phía Nam tại Ngày ATTT Việt Nam 2016.

Gia tăng tấn công qua ngõ di động

Theo một báo cáo mới đây của Ponemon Institute, thiệt hại kinh tế do xâm phạm dữ liệu di động gây ra cho một doanh nghiệp lớn có thể lên đến 26 triệu USD, và 67% tổ chức tham gia khảo sát trả lời đã bị xâm phạm dữ liệu do nhân viên sử dụng thiết bị di động cá nhân truy cập thông tin nhạy cảm và bí mật của công ty.

Thực tế là người dùng thời nay thường xuyên di chuyển với thiết bị di động luôn bên mình, gây "khó" cho các giải pháp bảo mật thông thường. Thêm nữa, việc người dùng chủ động lựa chọn thiết bị cho mục đích cá nhân lẫn công việc cũng là cơ hội để hacker tận dụng khai thác nhiều kẽ hở. Với thiết bị di động, người dùng thường ưu tiên tăng cường trải nghiệm hơn là quan tâm nhiều cho việc giữ gìn ATTT. Các tổ chức, doanh nghiệp sẽ phải đối mặt với thách thức ngày càng phức tạp cho việc thực thi các chiến lược bảo mật của họ.

Thanh toán di động được chấp nhận khắp nơi cũng sẽ là mục tiêu của hacker. Các giải pháp mới mẻ như selfie để thanh toán của MasterCard và True Key của Intel để đăng nhập nhanh dịch vụ trực tuyến đòi hỏi người dùng cần hiểu rằng việc bảo vệ dữ liệu sinh trắc học của bản thân cũng phải hết sức cẩn trọng như với dữ liệu cá nhân và tài chính khác.

Truy cập các mạng Wi-Fi công cộng không hề an toàn, và các chuyên gia bảo mật thường khuyến nghị người dùng không nên thực hiện các giao dịch ngân hàng trực tuyến với mạng Wi-Fi công cộng. Vì thế, các nhà cung cấp dịch vụ Wi-Fi công cộng lẽ ra nên có thêm cảnh báo người dùng, kiểu như: truy cập mạng công cộng là không an toàn và thông tin truyền trên mạng có thể bị kẻ xấu đọc lén, thu thập và chuyển cho bên thứ ba khai thác trục lợi từ việc đánh cắp tài sản, danh tính hay thông tin cá nhân của người dùng, ông Millis gợi ý.

IoT cũng là Internet của các mối đe dọa

Các lỗ hổng và tấn công thông qua thiết bị IoT sẽ gia tăng và làm tăng nhu cầu chuẩn hóa cho một loạt biện pháp bảo mật. Tại hội nghị hacker Def Con năm nay đã công bố 47 lỗ hổng bảo mật mới ảnh hưởng tới 23 thiết bị của 21 nhà sản xuất.

Những đợt tấn công DDoS trên diện rộng mới đây bởi mạng botnet Mirai tạo ra từ các thiết bị IoT không an toàn là lời cảnh tỉnh cho bất kỳ tổ chức, doanh nghiệp nào.

Thiết bị IoT đang lan tỏa nhanh trong đời sống với khả năng kết nối mạnh mẽ và ngày càng thông minh hơn, trong đó có nhiều loại thiết bị điện tử tiêu dùng, nhà và xe hơi kết nối. Tuy nhiên, không phải thiết bị kết nối Internet nào cũng thông minh. Thực tế, nhiều thiết bị IoT thiếu khả năng bảo mật, hoặc có nhưng lại thường bị bỏ qua không được kích hoạt khi sử dụng, và số thiết bị như vậy trên Internet không phải là ít. Chúng dễ bị hacker lợi dụng làm cầu nối tấn công có chủ đích vào các hệ thống, đặc biệt nguy hiểm nếu đó là những hệ thống điều khiển cơ sở hạ tầng trọng yếu, như lưới điện, hệ thống đường sắt, giao thông công cộng. Thậm chí có những hệ thống điều khiển như vậy còn chứa rất nhiều thiết bị với công nghệ từ những năm 1950 – 1960, hầu như không còn đảm bảo an toàn.

Cũng như smartphone trước đây, thiết bị IoT mới ở giai đoạn khởi đầu và đang có xu hướng bùng phát, lại chưa nhận được sự quan tâm đúng mức về bảo mật, chủ yếu đang được tập trung khai thác những chức năng phong phú của chúng. Những vấn đề phức tạp về bảo mật mà thiết bị di động cá nhân đang đối mặt cũng là tương lai đối với IoT – chúng hầu như rất dễ bị tổn thương. Đó là điều các tổ chức, doanh nghiệp và mọi cá nhân cần ghi nhớ trong kỷ nguyên Internet vạn vật.

PC World VN 01/2017

Liên từ và cách sử dụng

1. Liên từ kết hợp (coordinating conjunctions)

- Dùng loại liên từ này để nối những các từ loại hoặc cụm từ/ nhóm từ cùng một loại, hoặc những mệnh đề ngang hàng nhau (tính từ với tính từ, danh từ với danh từ ...)
- Gồm có: for, and, nor, but, or, yet
- Ví dụ:

She is a good and loyal wife.

Use your credit cards frequently and you'll soon find yourself deep in debt.

He is intelligent but very lazy.

She says she does not love me, yet I still love her.

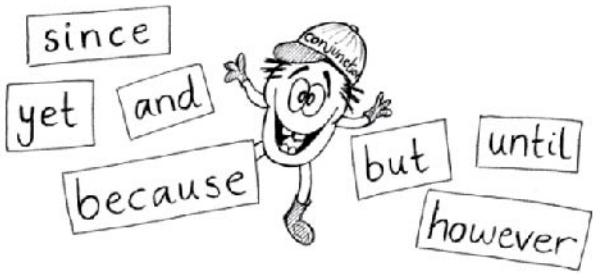
We have to work hard, or we will fail the exam.

He will surely succeed, for (because) he works hard.

That is not what I meant to say, nor should you interpret my statement as an admission of guilt.

- **Chú ý:** khi dùng liên từ kết hợp để nối hai mệnh đề, chúng ta thêm dấu phẩy sau mệnh đề thứ nhất trước liên từ

Ulysses wants to play for UConn, but he has had trouble meeting the academic requirements.



2. Tương liên từ (correlative conjunctions)

- Một vài liên từ thường kết hợp với các từ khác để tạo thành các tương liên từ. Chúng thường được sử dụng theo cặp để liên kết các cụm từ hoặc mệnh đề có chức năng tương đương nhau về mặt ngữ pháp
- Gồm có: both . . . and…(vừa….vừa…), not only . . . but also… (không chỉ…mà còn…), not . . . but, either . . . or (hoặc ..hoặc..), neither . . . nor (không….cũng không…), whether . . . or , as . . . as, no sooner…. than…(vừa mới….thì…)
- Ví dụ:

They learn both English and French.
He drinks neither wine nor beer.
I like playing not only tennis but also football.
I don't have either books or notebooks.
I can't make up my mind whether to buy some new summer clothes now or wait until the prices go down.

3. Liên từ phụ thuộc (subordinating conjunctions)

- Loại liên từ phụ thuộc nối kết các nhóm từ, cụm từ hoặc mệnh đề có chức năng khác nhau - mệnh đề phụ với mệnh đề chính trong câu.
- Ví dụ như các liên từ sau và nghĩa kèm theo của chúng:

As
1. Bởi vì: As he is my friend, I will help him.
2. Khi: We watched as the plane took off.
After: sau khi
After the train left, we went home.
Although/ though: mặc dù
Although it was after midnight, we did not feel tired.
Before: trước khi
I arrived before the stores were open.
Because: bởi vì
We had to wait, because we arrived early.
For: bởi vì
He is happy, for he enjoys his work.
If: nếu, giá như
If she is here, we will see her.
Lest: sợ rằng
I watched closely, lest he make a mistake.
Chú ý: sử dụng động từ nguyên thể trong mệnh đề "lest"
Providing/ provided: miễn là
All will be well, providing you are careful.
Since
1. Từ khi: I have been here since the sun rose.
2. Bởi vì: Since you are here, you can help me.
So/ so that
1. Bởi vậy: It was raining, so we did not go out.
2. Để (= in order that): I am saving money so I can buy a bicycle.
Supposing (= if)
Supposing that happens, what will you do?
Than: so với
He is taller than you are.
Unless: trừ khi
Unless he helps us, we cannot succeed.
Until/ till: cho đến khi
I will wait until I hear from you.
Whereas
1. Bởi vì: Whereas this is a public building, it is open to everyone.
2. Trong khi (ngược lại): He is short, whereas you are tall.
Whether: hay không
I do not know whether she was invited.
While
1. Khi: While it was snowing, we played cards.
2. Trong khi (ngược lại): He is rich, while his friend is poor.
3. Mặc dù: While I am not an expert, I will do my best.
As if = in a similar way
She talks as if she knows everything.
As long as
1. Nếu: As long as we cooperate, we can finish the work easily.
2. Khi: He has lived there as long as I have known him.
As soon as: ngay khi
Write to me as soon as you can.
As though = in a similar way
It looks as though there will be a storm.
In case: Trong trường hợp...
Take a sweater in case it gets cold.
Or else = otherwise: nếu không thì
Please be careful, or else you may have an accident.
So as to = in order to: để
I hurried so as to be on time.
Chú ý: Ngoài liên từ, chúng ta có thể sử dụng các trạng từ liên kết như therefore, otherwise, nevertheless, thus, hence, furthermore, consequently…
Ví dụ:
We wanted to arrive on time; however, we were delayed by traffic.
I was nervous; therefore, I could not do my best.
We should consult them; otherwise, they may be upset.

4. Phân biệt cách sử dụng của một số liên từ và giới từ có cùng nghĩa.

Liên từ	Giới từ
because	because of
although	despite
while	during

– Sự khác biệt giữa chúng là: liên từ + một mệnh đề, trong khi đó giới từ + một danh từ hoặc ngữ danh từ
– Ví dụ:
They were upset because of the delay
They were upset because they were delayed.

Despite the rain, we enjoyed ourselves.
Although it rained, we enjoyed ourselves.

We stayed indoors during the storm.
We stayed indoors while the storm raged.

9 bí quyết ĐẮC NHÂN TÂM ở công sở

1. Thân thiện

Mỉm cười chào tất cả các đồng nghiệp khi gặp nhau sẽ tạo cho bạn cây cầu thiện cảm đầu tiên. Hình ảnh thân thiện dễ mến của bạn sẽ ghi dấu trong những lần giữ cửa thang máy chờ khi đồng nghiệp đang hối hả chạy đến, nhặt dùm tập tài liệu đánh rơi hay đưa một cái kẹp tóc khi cần...

2. Thật lòng khen ngợi, động viên đúng lúc

Ông bà mình thường nói "lời nói không mất tiền mua" nhưng lời nói có thể "mua" cho bạn sự ủng hộ và sự thăng tiến và hơn cả là những người bạn nơi làm việc. Ai cũng có những năng lực nổi trội ngoài công việc của họ. Nếu bạn biết cô A ca vọng cổ hay và đề nghị cô hát trong Tiệc cuối năm công ty, cô B nấu ăn ngon để nhờ làm bánh kem sinh nhật công ty hay cô C vẽ đẹp để nhờ trang trí Noel văn phòng ...thì bạn đã giúp họ toả sáng. Họ sẽ nhớ mãi điều đó và sẽ tìm dịp để khen ngợi lại bạn.

Công việc không phải lúc nào cũng xuôi chèo mát mái. Nếu một ngày đồng nghiệp bị khiển trách, hãy chia sẻ bằng một cái siết chặt tay hoặc ngồi lắng nghe thật chia sẻ. Bạn đang là người bạn đồng hành đáng yêu nhất trong những giây phút buồn bực nhất của họ đó.

3. Không nề hà việc khó

Một khách hàng xuất hiện đột ngột và sừng sộ tại sảnh chờ công ty nơi bạn làm đòi gặp Sếp? Tất cả nhân viên đều hết sức e ngại nếu công ty bạn không có phòng chăm sóc khách hàng? Hãy dùng kiến thức và kinh nghiệm xử lý than phiền khiếu nại và "xung phong" tiến ra sảnh trước để tỏ rõ thiện chí. Chắc chắn đây là thử thách vô cùng khó khăn nhưng cũng là cơ hội cho bạn rèn luyện kỹ năng giao tiếp. Mọi người sẽ đánh giá cao việc bạn đã đảm nhận những việc khó về mình.

4. Hăng hái giúp đỡ

Ở Công ty Đầu tư Xây dựng B., anh Kiên luôn nhiệt tình giúp mọi người in sao các file bản vẽ đến mức nhiều đối tác còn nghĩ anh là nhân viên IT mà không biết anh là kỹ sư giám sát công trình. Anh đã được đồng nghiệp mến tặng chức danh trợ lý IT và cũng nhanh chóng thăng tiến lên phụ trách một toà tháp trong dự án vì năng lực làm việc nhóm và giành được thiện cảm của các sếp khi cân nhắc vị trí thăng tiến cho các kỹ sư đang ở vị trí ngang bằng. Hãy luôn chìa cánh tay ra khi có thể, bạn sẽ nhận được nhiều cánh tay vào lúc mình cần sự trợ giúp để lên đỉnh thành công.

5. Chào đón đồng nghiệp mới

Ngày đầu tiên đi làm việc ở chỗ mới, ai cũng cần một sự chào đón và sự hướng dẫn tận tình của đồng nghiệp. Cô giáo lớp một in dấu đậm trong tâm trí ta như thế nào thì người bạn đầu tiên ở nơi mới cũng khiến ta ấm áp như thế. Vậy ta cũng hãy luôn là người bạn thân ái đầu tiên của những đồng nghiệp mới. Bạn hãy nói lời chào mừng và nói rằng bạn sẵn lòng hướng dẫn nếu họ có thắc mắc ban đầu. Hãy giúp họ biết chỗ ăn trưa gần nhất, giúp họ nhận biết các đồng nghiệp khác cũng như cách sử dụng các trang thiết bị trong văn phòng, bạn sẽ có chỗ đứng chắc chắn trong lòng họ.

6. Uy tín, lịch thiệp

Nếu bạn mượn đồ dùng của đồng nghiệp như kim bấm, kéo cắt giấy, tài liệu tham khảo...hãy trả đúng hẹn bởi khi họ cần mà không có thì bạn vô tình đã quạt cho than trong lò giận dữ của họ bùng cháy. Bạn hứa giúp họ tìm nơi cung cấp dịch vụ nhưng không làm thì lần sau họ sẽ không dám giao trứng cho ác nữa.

Văn phòng là một xã hội thu nhỏ nên bạn hãy ứng xử chừng mực lịch thiệp như ở nơi công cộng. Những tư thế ngả ngớn, nói chuyện điện thoại ồn ào, hỉ mũi ầm ĩ hay hát to khi nghe Ipod ..sẽ khiến đồng nghiệp khó chịu tránh xa người thiếu tôn trọng không gian chung.

7. Tích cực lắng nghe

Một trong những bí quyết trong nghệ thuật giao tiếp là kỹ năng lắng nghe. Những người bán hàng giỏi nhất là những người biết lắng nghe để hiểu nhu cầu cầu và đáp ứng nhu cầu khách hàng được hiệu quả nhất. Lúc bạn nghe là lúc bạn hiểu được đồng nghiệp được tốt nhất. Nếu gặp rắc rối, bạn hãy nghe từ người đối thoại, nhiều khi chỉ là chuyện hiểu lầm và ta không mất thời gian để giải quyết hay giận dữ cho những chuyện không hề tồn tại.

8. Êm dịu nhưng hiệu quả trong cách góp ý đồng nghiệp

Trong công việc, những chuyện bất đồng ý kiến hay ứng xử là điều luôn tồn tại. Vấn đề là chúng ta ứng xử trên tinh thần tôn trọng lẫn nhau. Hãy dùng chiếc bánh Sandwich trong giao tiếp để phát biểu ý kiến để xây dựng đồng nghiệp nhé. Làm sao để bước ra từ sau cuộc nói chuyện, người đồng nghiệp của chúng ta rút kinh nghiệm từ những sai lầm mà không mất đi thiện cảm dành cho ta.

9. 9999

Vâng, im lặng là vàng đối với những câu chuyện riêng tư mà đồng nghiệp chia sẻ cho ta. Nhiều khi "bản năng bà Tám" thúc đẩy ta mạnh mẽ nói ra nhưng hãy nghĩ đến nguyên tắc số 9 này để giữ lại mối quan hệ bằng vàng của ta với đồng nghiệp.

ƯU ĐÃI

-20% Học Viên Cũ

-30% Sinh Viên

Doanh Nghiệp

LỊCH KHAI GIẢNG THÁNG 04/2017

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNA						
AK4	CCNAX (200-125)	03/04	2 – 4 – 6	8:30 – 11:30AM	3.700.000	152 giờ
AK6				2:00 – 5:00PM	3.700.000	
AK8		11/04	3 – 5 - 7	8:30 – 11:30AM	3.700.000	
AK10				2:00 – 5:00PM	3.700.000	
A5				6:30 – 9:30PM	7.400.000	
A7		15/04	Thứ 7	Sáng + Chiều	7.400.000	
AK9		18/04	3 – 5 - 7	8:30 – 11:30AM	3.700.000	
AK11				2:00 – 5:00PM	3.700.000	
A9				6:30 – 9:30PM	7.400.000	
AK12		21/04	2 – 4 – 6	8:30 – 11:30AM	3.700.000	
A8				6:30 – 9:30PM	7.400.000	
AK13		27/04	3 – 5 - 7	8:30 – 11:30AM	3.700.000	
A11				6:30 – 9:30PM	7.400.000	
AO3	CCNAX Online	11/04	3 – 5 - 7	6:30 – 9:30PM	2.900.000	72 giờ
AO5		22/04	Thứ 7	Sáng + Chiều	2.900.000	
AO4		28/04	2 – 4 – 6	6:30 – 9:30PM	2.900.000	
AS3	CCNA Security (640-554)	18/04	3 – 5 – 7	6:30 – 9:30PM	5.900.000	72 giờ
AV3	CCNA Voice	18/04	3 – 5 – 7	6:30 – 9:30PM	7.400.000	100 giờ
CHƯƠNG TRÌNH CCNP						
P1-4	ROUTE (300 - 101)	05/04	2 – 4 – 6	6:30 – 9:30PM	8.900.000	120 giờ
P1-K1		18/04	3 – 5 – 7	8:30 – 11:30AM	5.900.000	
P1-5				6:30 – 9:30PM	8.900.000	
P1-7		15/04	Thứ 7	Sáng +Chiều	8.900.000	
P1-K3		27/04	3 – 5 – 7	8:30 – 11:30AM	5.900.000	
P1-7				6:30 – 9:30PM	8.900.000	
PO-1	ROUTE Online	21/04	2 – 4 – 6	2:00 – 5:00PM	5,500,000	72 giờ
P2-K1	SWITCH (300 - 115)	04/04	3 – 5 – 7	8:30 – 11:30AM	5.900.000	120 giờ
P2-3				6:30 – 9:30PM	8.900.000	
P2-K3		18/04	3 – 5 – 7	8:30 – 11:30AM	5.900.000	
P2-5				6:30 – 9:30PM	8.900.000	
SO-1		22/04	Thứ 7	Sáng +Chiều	8.900.000	
P3-3	TSHOOT (300 - 135)	18/04	3 – 5 – 7	6:30 – 9:30PM	8.900.000	120 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW3	CCIE WRITTEN (Version 5)	18/04	3 – 5 – 7	6:30 – 9:30PM	12.500.000	120 giờ
KHÓA HỌC CHUYÊN ĐỀ						
PS1-3	FIREWALL	15/04	Thứ 7	Sáng + Chiều	5.900.000	54 giờ

Lê Uyên Email: tranleuyen@vnpro.org Mobile: 0903 834 636

Thanh Trâm Email: thanhtram@vnpro.org Mobile: 0949 246 829

Hồng Nhung Email: hongnhung@vnpro.org Mobile: 0978 624 293

Mỹ Trang Email: mytrang@vnpro.org Mobile: 0964 464 377

LIÊN HỆ DỰ ÁN - TƯ VẤN HỆ THỐNG MẠNG - THUÊ THIẾT BỊ PHÒNG HỌC - MUA SÁCH

Website: www.vnpro.vn Email: vnpro@vnpro.org Điện thoại: (08) 35124257

Bản tin Dân Cisco - Được phát hành bởi **Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt**

Chịu trách nhiệm xuất bản: **Nguyễn Cảnh Hoàng**

Giấy phép xuất bản số: **69/QĐ - STTTT** Ngày ĐK: **26/10/2011**

Công ty in: **Sao Băng Design**

Số lượng in: **2.000 cuốn/kỳ**

Kỳ hạn xuất bản: **1 kỳ/tháng**