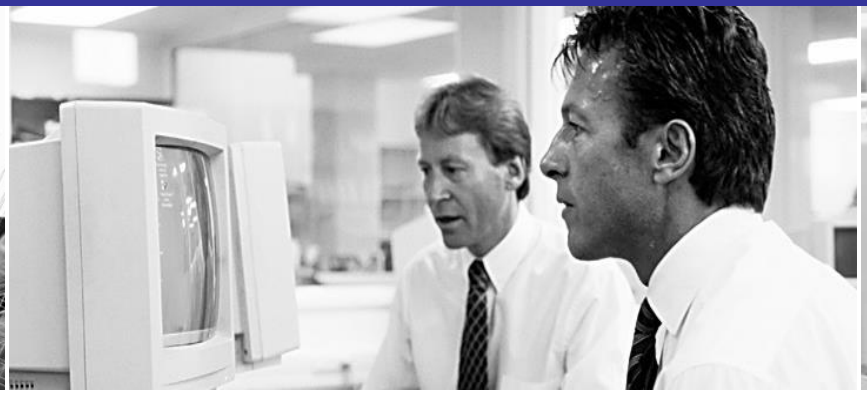
Chương 7
An toàn trong TMĐT

Môn: THƯƠNG MẠI ĐIỆN TỬ



STU
Trần Quang
Khoa Công Nghệ Thông Tin

Vấn đề trong an toàn TMĐT

- Cần tìm ra được sự cân bằng hợp lý giữa 2 yêu cầu quan trọng là sự an toàn và sự tiện dụng (các chức năng và đặc tính dễ thao tác trên hệ thống)
- Hệ thống càng an toàn thì thường mắc phải nhược điểm thao tác xử lý phức tạp
- Ngược lại thao tác tiện dụng lại dễ dẫn đến khó đảm bảo an toàn

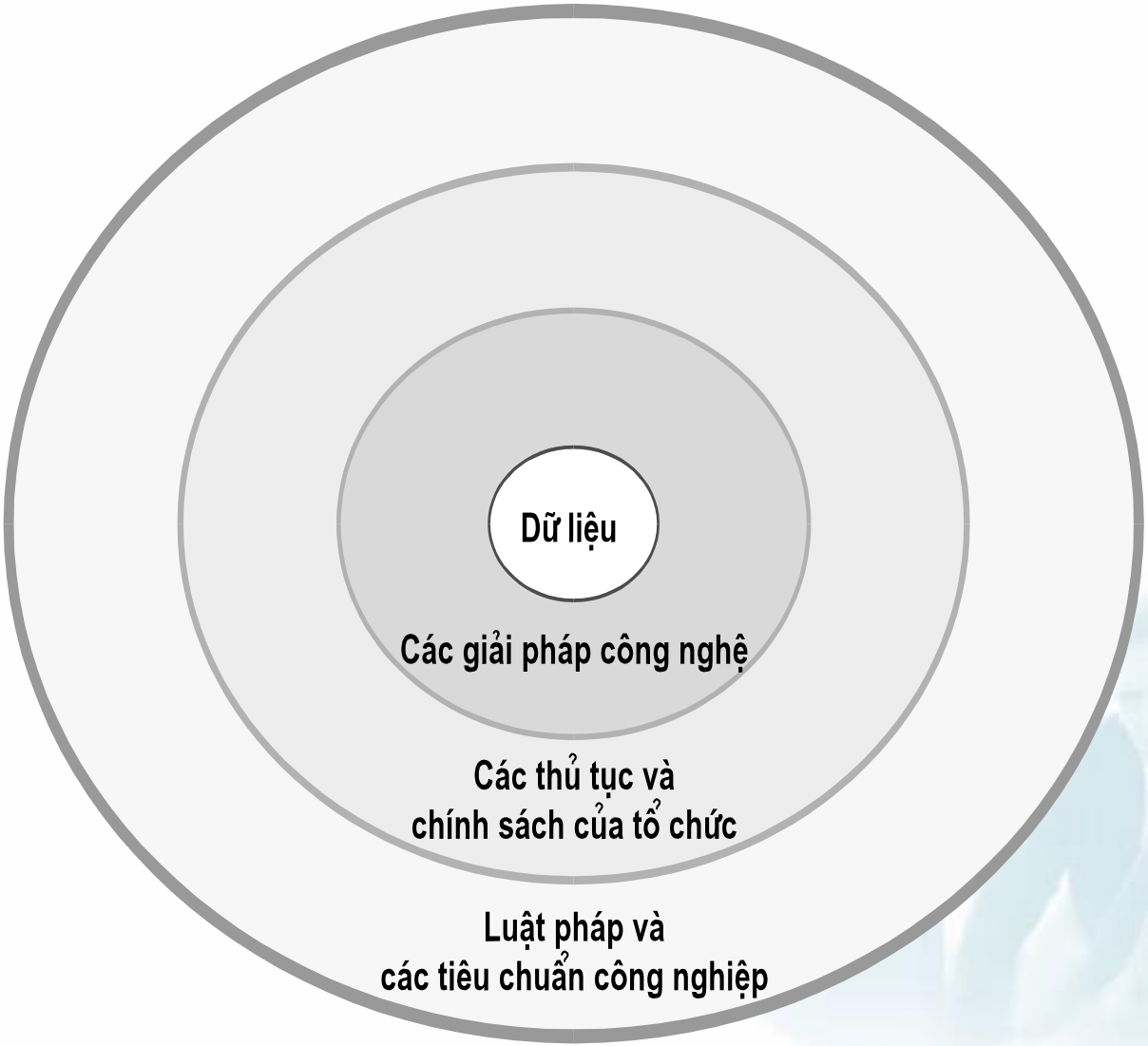
Rủi ro trong TMĐT

- Người mua có thể gặp rủi ro là không nhận được hàng mà mình đã đặt và thanh toán.
- Người mua có thể bị đánh cắp tiền trong lúc mua sắm
- Người bán có thể không nhận được tiền thanh toán
- Người bán có thể bị lấy trộm hàng hóa, hoặc nhận thanh toán bằng thẻ tín dụng giả → các rắc rối về pháp lý

Rủi ro trong TMĐT

- Việc giảm rủi ro trong TMĐT là quá trình phức tạp liên quan đến nhiều yếu tố: công nghệ mới, các thủ tục và chính sách của công ty, các quy định của pháp luật.
- Cần chú ý bản thân công nghệ mới chưa thể giải quyết tất cả các vấn đề về an toàn
- Cần có các thủ tục, chính sách của tổ chức
- Ở phạm vi lớn hơn cần các văn bản luật, các quy định chế tài của nhà nước

Môi trường an toàn trong TMĐT



Các lưu ý về an toàn trong TMĐT

- An toàn luôn mang tính tương đối.
- Bất cứ hệ thống nào cũng có thể phá vỡ nếu không đủ sức chống lại tấn công
- Sự an toàn vĩnh viễn cũng không cần thiết trong thời đại thông tin. Nhiều thông tin chỉ có giá trị trong một khoảng thời gian nào đó, nên chỉ cần an toàn trong khoảng đó là đủ
- An toàn gắn liền với chi phí → cân nhắc
- An toàn là cả một chuỗi liên kết và nó sẽ đứt ở khâu yếu nhất

Các tính chất trong an toàn TMĐT

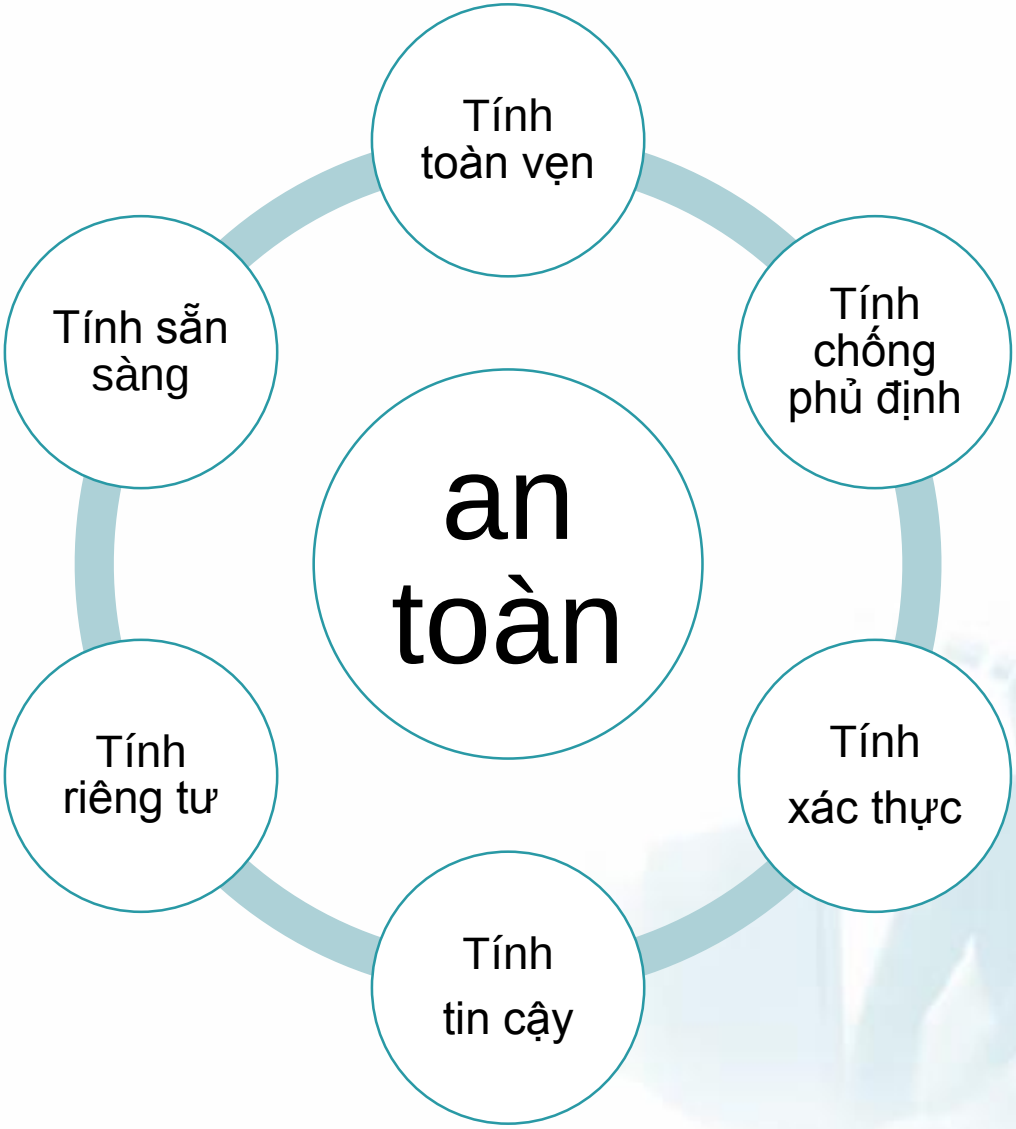


TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Tội phạm mạng

- Số lượng ngày càng tăng, mức độ ngày càng nghiêm trọng
- Symantec: tội phạm mạng nổi lên từ 2007
- IC3 (Internet Crime Compliant Center): đã xử lý trên 200,000 tội phạm trên Internet
- Tháng 4/2014: phát hiện lỗi bảo mật trong phần mềm Open SSL, có tên Heartbleed. Cảnh báo e-banking của 15 ngân hàng và cổng thanh toán tại Việt Nam bị tấn công và có nguy cơ lộ thông tin giao dịch online

Tội phạm mạng

- Năm 2016 là năm đặc biệt nóng về tội phạm công nghệ cao trên mạng Internet
- Ngày 29/7/2016, màn hình các quầy làm thủ tục của Vietjet ở sân bay Tân Sơn Nhất và Vietnam Airlines ở Nội Bài xuất hiện các dòng chữ xuyên tạc. Đồng thời, trang web vietnamairlines.com cũng bị tấn công và hơn 400.000 thông tin khách hàng thuộc chương trình Bông Sen Vàng của Vietnam Airlines bị hacker phát tán trên Internet.

Tội phạm mạng

- Trong tháng 5/2016, TPBank suýt bị hacker quốc tế lừa đảo, lấy 1,13 triệu USD. Rất may TPBank phát hiện kịp thời và lập tức liên lạc với các bên liên quan để ngăn chặn.
- Ngày 5/8/2016, một khách của Vietcombank phát hiện tài khoản của mình tự động có giao dịch chuyển đi 500 triệu đồng. Đại diện Vietcombank cho biết có thể khách hàng này đã bị hacker tấn công và lấy trộm mật khẩu Internet Banking để chuyển tiền…

Các loại tội phạm mạng

Các loại hành vi tội phạm mạng thường gặp:

- Hacking
- Identity theft
- Fraud
- Predator

Hacking (xâm nhập)

- Sử dụng khả năng của mình để xâm nhập vào hệ thống máy tính, hệ thống dữ liệu và truy cập thông tin cá nhân của người dùng.
- Mục tiêu có thể đơn giản chỉ đánh cắp thông tin và bán cho người khác, hay thực hiện hoạt động gián điệp, xâm nhập vào hệ thống của doanh nghiệp và ăn cắp kế hoạch chiến lược kinh doanh, bản quyền sản phẩm; cũng có thể là dùng để đe dọa hoặc đánh sập hệ thống đó

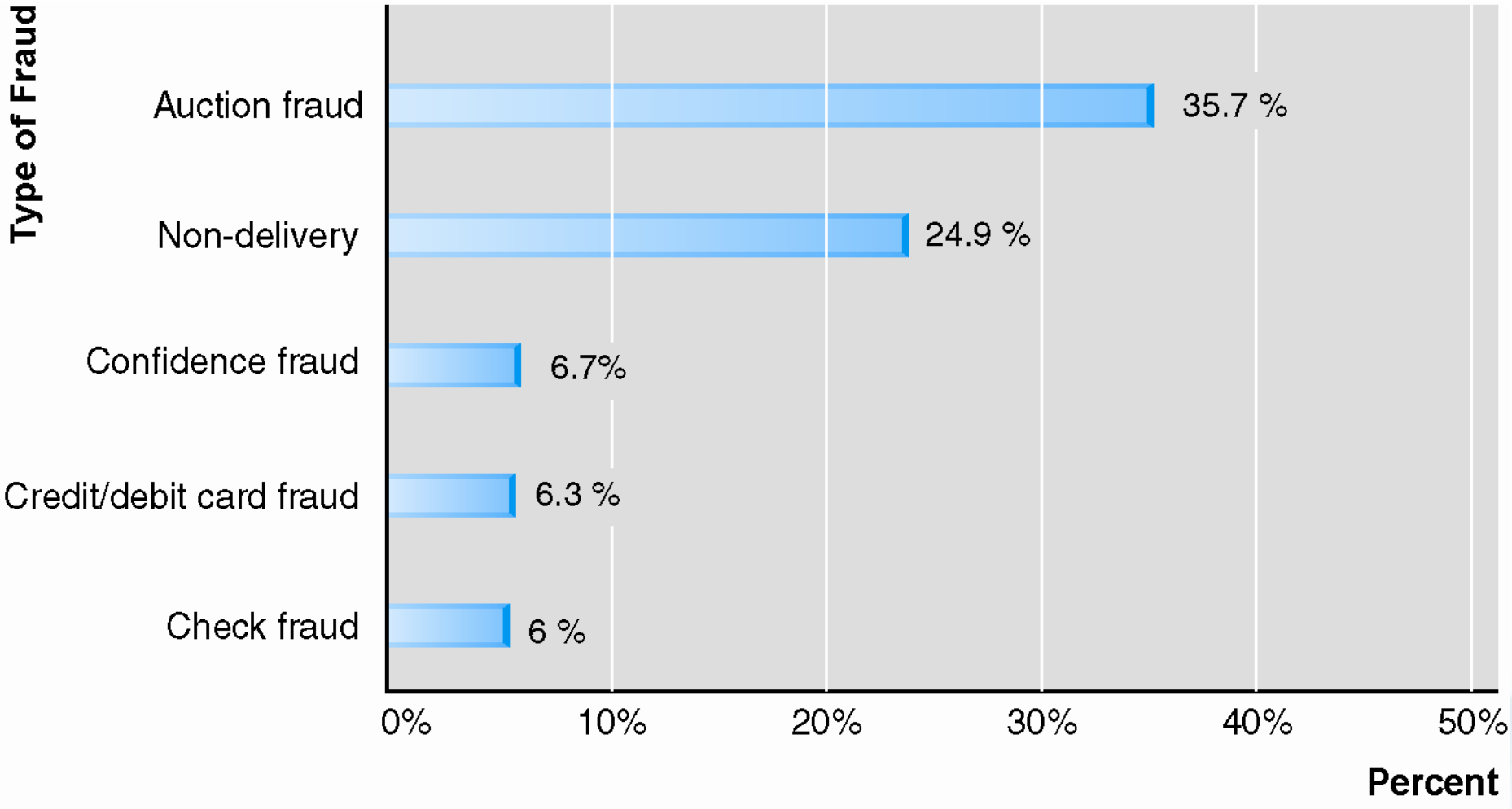
Identity Theft (mạo danh)

- Loại này thường đánh cắp thông tin cá nhân của người khac, rồi sử dụng cho chính mình hay đem rao bán trên mạng.
- Thông tin bị đánh cắp này có thể được dùng để rút tiền từ tài khoản trực tuyến, mua hàng qua mạng hay trao đổi cho những hoạt động khác trên internet

Fraud (lừa đảo)

- Không cần phải đột nhập vào máy chủ để có được thông tin cá nhân. Họ lừa để người dùng tự cung cấp thông tin cho tội phạm
- Ví dụ tội phạm có thể mở một cửa hàng hoặc dịch vụ giả mạo, gửi lời mời qua email cho nạn nhân về một dịch vụ giá rẻ hoặc miễn phí và yêu cầu nạn nhân tạo một tài khoản với các thông tin cá nhân để có thể sử dụng sản phẩm hay dịch vụ đó.

Thống kê của IC3



Predators (săn bắt)

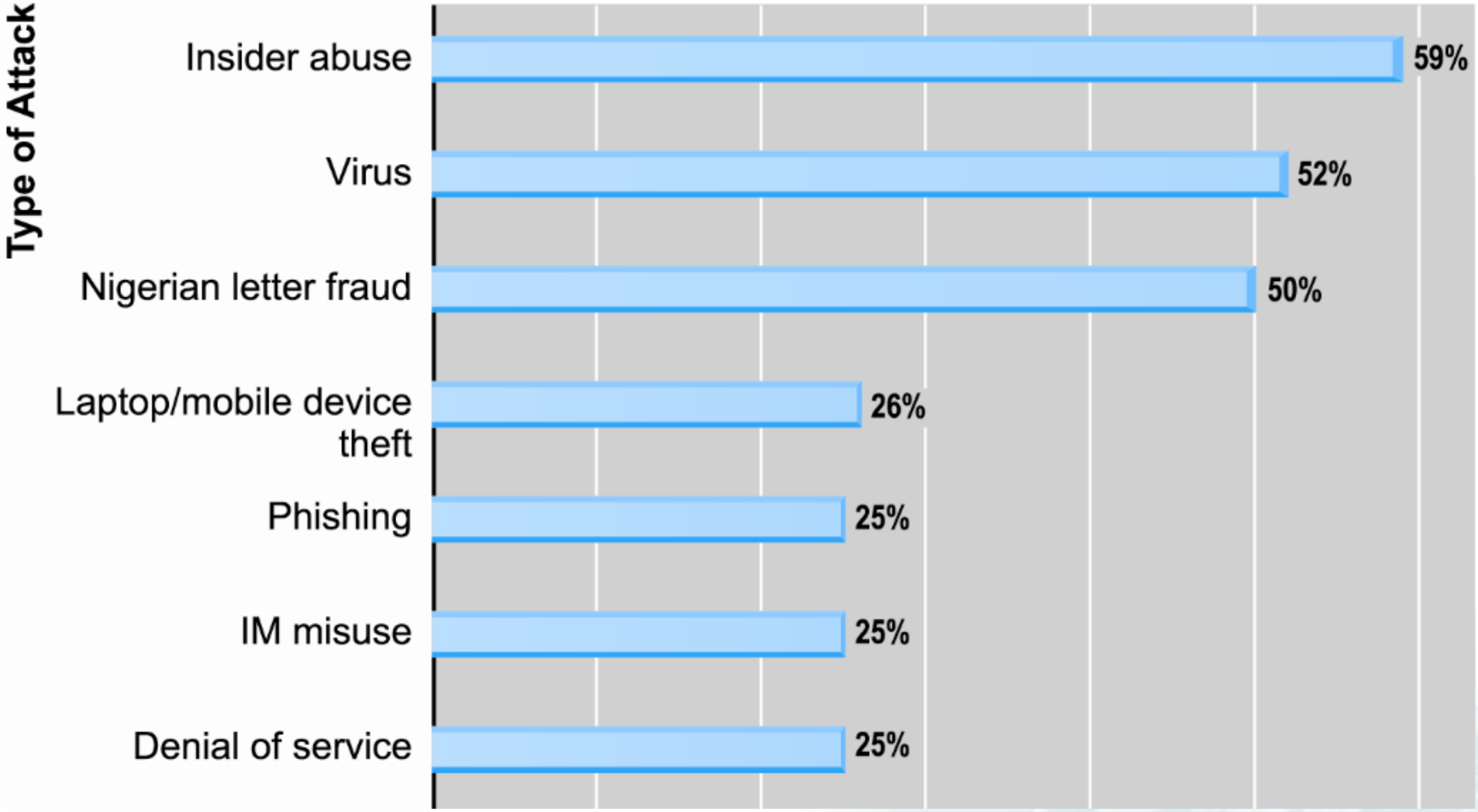
- Đây là dạng tội phạm mạng chuyên sử dụng mạng xã hội để tìm kiếm nạn nhân và thu thập thông tin.
- Qua giao tiếp trực tuyến như nói chuyện, đưa ra tình huống lựa chọn, họ tạo dựng kịch bản lừa đảo dựa trên những thông tin mà nạn nhân vô tình cung cấp (chẳng hạn như thường vắng nhà khi nào, tìm hiểu thói quen hàng ngày) và chờ thời cơ ra tay.

Tấn công hệ thống máy tính

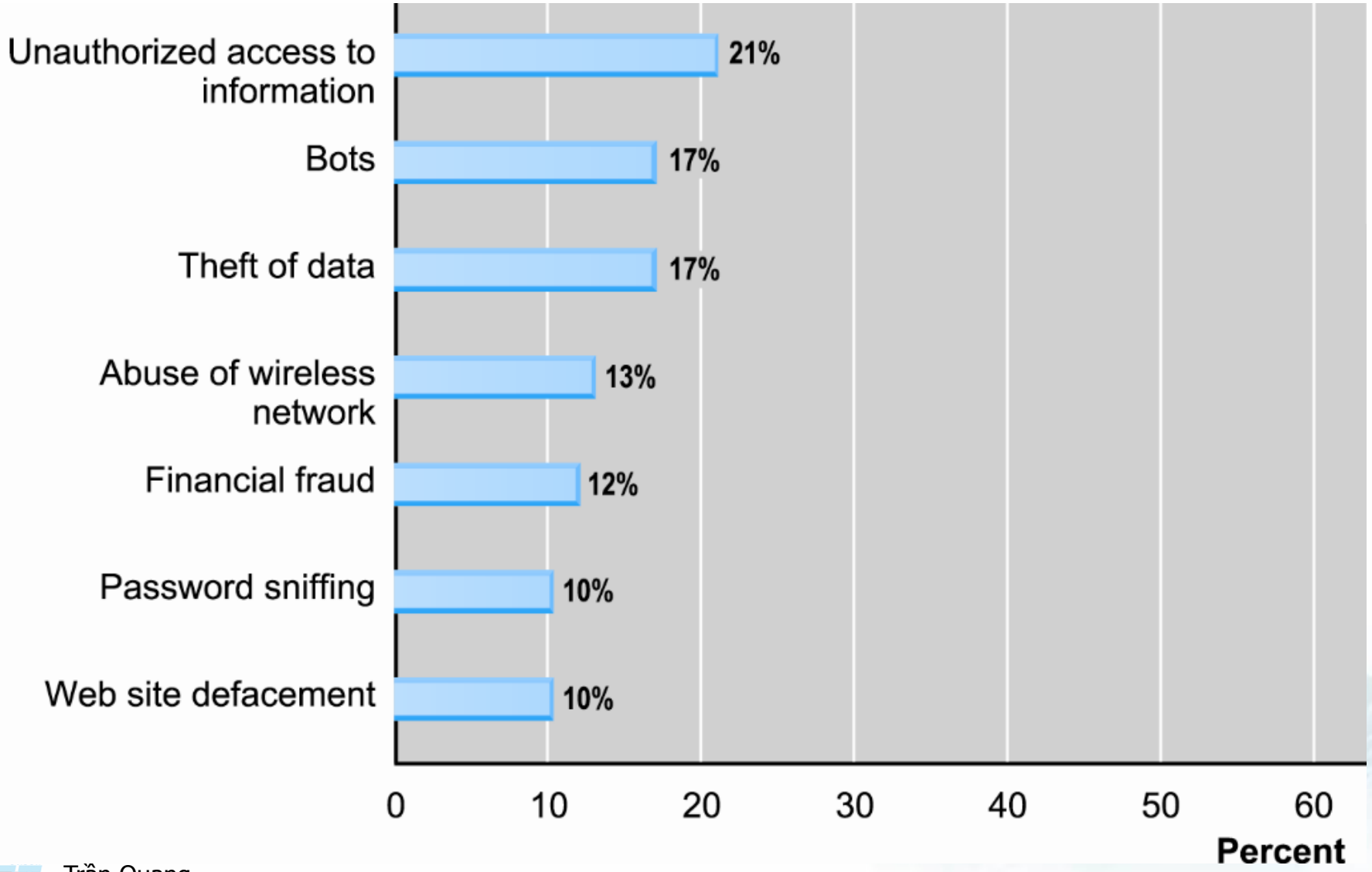
Năm 2016, tại Việt Nam VNCERT đã ghi nhận hơn 130.000 lượt tấn công, tăng rất nhiều so với 2015

- Tấn công Phishing (lừa đảo) hơn 10.000 lượt
- Tấn công Malware (mã độc) 46.000 lượt
- Tấn công Deface (tấn công thay đổi giao diện) hơn 77.000 lượt

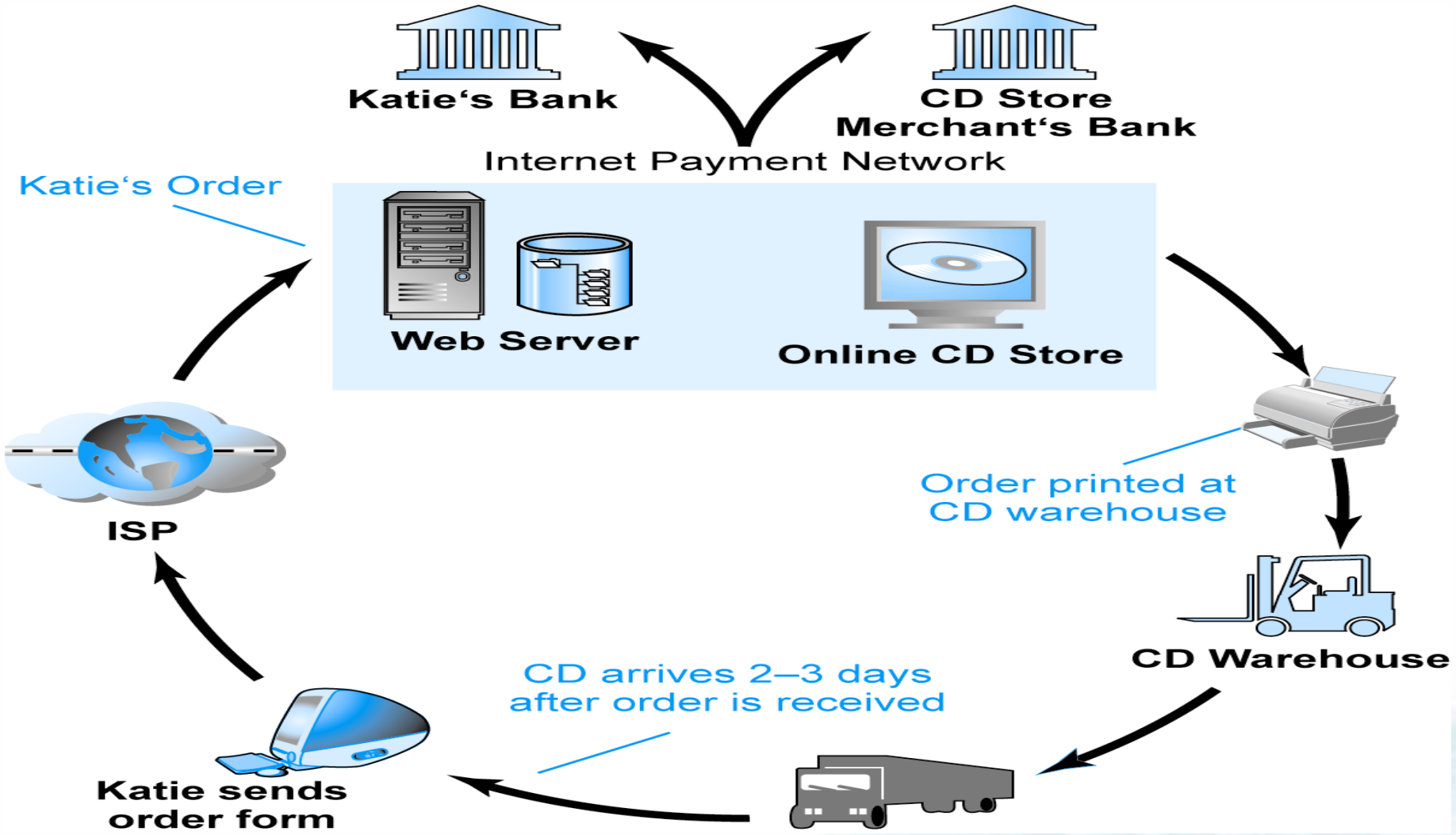
Các kiểu tấn công hệ thống máy tính



Các kiểu tấn công hệ thống máy tính



Một giao dịch điển hình trong TMĐT



Các đe dọa trong môi trường TMĐT

3 điểm chính đe dọa làm tổn hại trong môi trường TMĐT

- Client
- Server
- Đường truyền

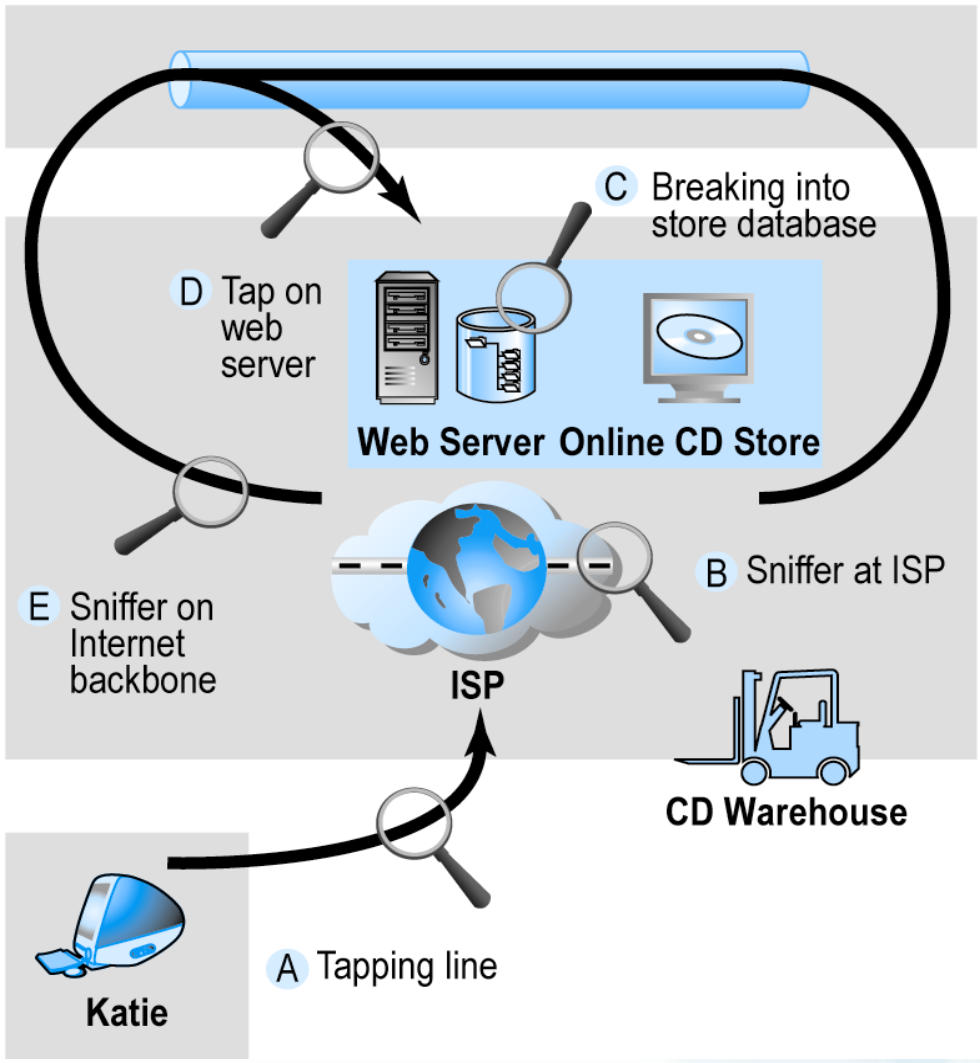
Các điểm dễ tổn thương

Security Risks

Internet communications

Servers
- ISP
- Merchant
- Banks

Clients
- Business
- Home



Tapping and sniffing
Alteration of messages
Theft and fraud

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Malicious code attack
Line taps
Physical loss of computer

Các mối đe dọa thường gặp

- Malicious code (viruses, worms, trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- Hacking and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- DoS and DDoS attacks
- Sniffing
- Insider attacks
- Poorly designed server and client software

Mã code độc

- Virus
  - Macro virus, file-infecting virus, script virus, …
- Worms
- Trojan horse
- Bots
  - Lén lút cài đặt trên máy tính, chờ thực hiện các lệnh từ ngoài do attacker gởi đến
- …

Các chương trình không mong muốn

Cài đặt không có sự đồng ý của người dùng:

- Browser parasites
  - Có thể theo dõi và thay đổi các settings của browser
- Adware
  - Gọi các pop-up quảng cáo không mong muốn
- Spyware
  - Có thể dùng để thu thập các thông tin, như các cú gõ phím của user, email, …

Phishing

- Kỹ thuật lừa đảo được mô tả chi tiết vào năm 1987. Thuật ngữ Phising là kết hợp giữa 2 từ Fishing và Phreaking.
- Là dạng tấn công Social Engineering sử dụng để lừa đảo người dùng và khai thác lỗ hổng của việc sử dụng công nghệ kém an ninh ở các website hiện hành.

Phishing

- Thường diễn ra ở các trang mạng xã hội, các website đấu giá, mua bán online, …
- Sử dụng email hoặc tin nhắn gởi đến người dùng, yêu cầu cung cấp thông tin cần thiết.
- Người dùng chủ quan đã cung cấp thông tin cho trang web trông có vẻ hợp pháp, nhưng lại là trang web giả mạo của các hacker.
- IP spoofing, ARP spoofing, …

Phishing

- Một hình thức lừa đảo quốc tế thường gặp là "lừa đảo lệ phí trả trước". Đây hình thức lừa đảo nhằm chiếm dụng khoản tiền của nạn nhân với hy vọng sẽ nhận được một khoản tiền khác lớn hơn. Loại tội phạm này còn có nhiều tên gọi khác, ví dụ “Lá thư Nigeria”, “Trò lừa 419”, “Tù nhân Tây Ban Nha”, “Trò lừa món tiền đen”, “Trò lừa Nga/Ukraina”.
- http://itlaw.wikia.com/wiki/Nigerian_4-1-9_fraud

Hacking và Cybervandalism

- Hacker
- Cracker
- Chương trình phá hoại (Cybervandalism)
- Các loại hackers
  - White hats
  - Black hats
  - Grey hats

Thẻ tín dụng gian lận

- Nổi lo thông tin thẻ tín dụng bị đánh cắp đã ngăn cản việc mua bán online
- Hacker nhắm vào các thông tin khách hàng và thẻ tín dụng trên server người bán, sử dụng các dữ liệu này để thực hiện các giao dịch gian lận
- Các công ty online chịu rủi ro cao hơn các công ty offline

Spoofing (Pharming)
Spam (Junk) Web Sites

- Spoofing (Pharming)
  - Sử dụng các địa chỉ e-mail giả dạng như một người nào khác
  - Đe dọa sự toàn vẹn của site
- Spam (Junk) Web sites
  - Dùng tên miền tương tự một site hợp pháp, để hướng các giao dịch đến

Tấn công DoS và DDoS

- Denial of service (DoS)
- Tấn công từ chối dịch vụ là kiểu tấn công mà một người làm cho hệ thống không thể sử dụng, hoặc làm hệ thống chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

Tấn công DoS và DDoS

- Distributed denial of service (DDoS)
  - Sử dụng nhiều máy tính tấn công mạng cùng lúc từ nhiều điểm khác nhau
- Botnets là các mạng tự trị, liên kết các máy tính đã bị lây nhiễm; các máy này sẽ thực hiện các hoạt động phá hoại như tấn công từ chối dịch vụ, spam, …

Nghe trộm trên mạng (Sniffing)

- KJỹ thuật này không tấn công trực tiếp vào máy client hay server, mà nhắm vào không gian truyền dữ liệu giữa các máy.
- Sniffing ban đầu được các quản trị viên dùng theo dõi, chẩn đoán, phát hiện sự cố nhằm giúp cải thiện hoạt động hệ thống mạng.
- Tuy nhiên, về sau trở thành công cụ của hacker phục vụ mục đích thu thập trái phép các thông tin nhạy cảm, tên tài khoản, mật khẩu, credit card,… của người dùng

Các giải pháp kỹ thuật

- Bảo vệ đường truyền Internet (mã hóa)
- Bảo vệ các kênh truyền thông (SSL, S-HTTP, VPNs)
- Bảo vệ mạng (firewalls)
- Bảo vệ servers và clients
- Mã hóa