**CHƯƠNG 5: HỆ THỐNG THANH TOÁN ĐIỆN TỬ**

1. **Tổng quan thanh toán trực tuyến**
   1. **Khái niệm thanh toán điện tử**

Thanh toán điện tử (electronic payment) là việc thanh toán dựa trên nền tảng công nghệ thông tin, trong đó sử dụng máy tính nối mạng để truyền các thông điệp điện tử, chứng từ điện tử giúp cho quá trình thanh toán nhanh chóng an toàn và hiệu quả. Thanh toán điện tử là việc thanh toán qua thông điệp điện tử thay việc thanh toán tiền mặt.

Quá trình thanh toán điện tử có sử dụng các phương tiện điện tử và công nghệ thanh toán tài chính (ví dụ như mã hoá số thẻ tín dụng, séc điện tử, hoặc ví điện tử) giữa ngân hàng, trung gian và các bên tham gia hợp pháp.

Việc thanh toán được thực hiện qua mạng máy tính kết nối với các đơn vị thành viên tham gia thanh toán. Việc sử dụng mạng để chuyển những chứng từ điện tử, dữ liệu tài chính điện tử giúp cho việc thực hiện thanh toán nhanh chóng, mở rộng khoảng cách và phạm vi thanh toán giữa các ngân hàng, doanh nghiệp và người tiêu dùng trên phạm vi quốc gia và toàn thế giới.

* 1. **Đặc điểm của thanh toán điện tử**

Hệ thống thanh toán điện tử được thực hiện trên cơ sở kỹ thuật số, chúng được xây dựng và phát triển để thực hiện các thanh toán trên mạng Internet. Về bản chất, các hệ thống thanh toán điện tử là phiên bản điện tử của các hệ thống thanh toán truyền thống như tiền mặt, séc và các loại thẻ thanh toán.

Tuy nhiên, so với thanh toán truyền thống, các hệ thống thanh toán điện tử có hai điểm khác biệt:

*Thứ nhất*, các hệ thống thanh toán điện tử được thiết kế để có thể thực thi việc mua - bán điện tử trên mạng Internet. Việc sử dụng công nghệ thông tin và các phương tiện điện tử với khai thác mạng cho phép quá trình giao dịch và công cụ giao dịch được số hoá và được ảo hoá bằng những chuỗi bit;

*Thứ hai*, trong thanh toán truyền thống*, chỉ ngân hàng mới có quyền phát hành tiền và các giấy tờ có giá trị khác.* Trong thanh toán điện tử, các công ty và các tập đoàn tài chính cũng được phép phát triển các phần mềm đóng vai trò là các công cụ thanh toán. Vì vậy, trong thanh toán điện tử, khách hàng có thể lựa chọn một trong nhiều cách thức thanh toán khác nhau trên cơ sở phần mềm của các công ty và các tập đoàn tài chính. Về hình thức, các cách thức thanh toán này cơ bản giống nhau, chúng chỉ khác về mặt lôgíc, về quy trình thanh toán và một số dịch vụ đi cùng.

* 1. **Ưu thế của thanh toán điện tử**

*a. Thanh toán điện tử không bị hạn chế về không gian*.

Đặc điểm thứ nhất của thanh toán điện tử cho phép các bên thanh toán vào bất kì thời điểm nào và trong điều kiện nào miễn là hoạt động thanh toán hợp pháp, có sử dụng các phương tiện thanh toán hợp pháp.

Một trong những thành quả mà chúng ta đang hưởng thụ là sự phát triển mạnh mẽ của khoa học, công nghệ thông tin và việc khai thác, ứng dụng trong các lĩnh vực khác nhau. Việc ứng dụng công nghệ thông tin trong lĩnh vực thanh toán cho phép các bên trong thanh toán thu hẹp khoảng cách địa lí, mở rộng phạm vi thanh toán trên toàn cầu. Đây cũng là một trong những điều kiện để đẩy mạnh sự phát triển của thương mại quốc tế, TMĐT. Thanh toán điện tử cũng là nhân tố cấu thành của nền kinh tế số hóa.

## *b. Thanh toán điện tử không hạn chế về thời gian*

Thanh toán điện tử là hệ thống thanh toán thông qua mạng máy tính và viễn thông đạt được tốc độ thanh toán với thời gian thực. Thông qua các mạng WAN, internet cho phép thực hiện thanh toán trên phạm vi toàn cầu, trong suốt 24/24 giờ trong ngày và 7 ngày/tuần.

### *c. Thanh toán điện tử là phương thức thanh toán có nhiều ưu việt*

Kỉ nguyên 21 là kỉ nguyên công nghệ thông tin và kinh tế tri thức. Các phương thức thanh toán điện tử ra đời đẩy mạnh xu thế phát triển các phương thức thanh toán không dùng tiền mặt, hạn chế sử dụng tiền mặt trong thanh toán truyền thống và sẽ chiếm ưu thế thể hiện xu hướng tất yếu của thời đại. Các quốc gia văn minh, các nền kinh tế phát triển luôn coi trọng vấn đề này.

Thanh toán điện tử mở rộng sang các lĩnh vực mới: trao đổi dữ liệu tài chính điện tử, tiền điện tử, ví tiền số hoá, sec điện tử, thẻ thông minh, các loại thẻ thanh toán

Các hệ thống thanh toán điện tử trong lĩnh vực ngân hàng được khai thác tối đa như: Hệ thống chuyển tiền điện tử trong cùng hệ thống ngân hàng, hệ thống thanh toán điện tử đa ngân hàng; hệ thống thanh toán liên ngân hàng quốc tế qua SWIFT.

Ngoài ra, các dịch vụ thanh toán điện tử mới được các ngân hàng đưa vào khai thác như: EBanking, Internet Banking, Phone Banking cũng đang phát triển rất nhanh.

* 1. **Các yêu cầu của hệ thống thanh toán điện tử**

*Tính độc lập (Independence).* Một số phương thức thanh toán điện tử đòi hỏi phần mềm hoặc thiết bị đặc biệt để thanh toán. Hầu như tất cả các phương thức thanh toán điện tử đòi hỏi người bán hàng phải trang bị (cài đặt phần mềm, phần cứng) để có thể thực hiện thanh toán. Yêu cầu là các hệ thống thanh toán mang tính độc lập, không phụ thuộc vào phần cứng và phần mềm chuyên dụng.

*Tính tương tác và dịch chuyển (*Interoperability and portability). Các hệ thống thương mại điện tử phải được liên kết với nhau và liên kết với các hệ thống thanh toán. Phương thức thanh toán điện tử phải phù hợp với hệ thống thương mại điện tử và hạ tầng công nghệ thông tin.

*Tính an toàn và bảo mật.* An toàn và bảo mật cho các giao dịch tài chính qua các mạng mở như Internet là hết sức qun trọng vì đây sẽ là mục tiêu tấn công của các loại tội phạm công nghệ cao, ăn cắp hoặc sử dụng thẻ tín dụng trái phép. Do các dịch vụ trên Internet hiện nay được cung cấp toàn cầu với mọi tiện ích phục vụ cho mọi khách hàng, mọi thành phần trong xã hội, vì vậy các hệ thống thanh toán điện tử phải đảm bảo tính khả dụng nhưng cũng chống lại được sự tấn công đe dọa tính bí mật thông tin cá nhân, thông tin tài chính của các chủ thể tham gia giao dịch.

*Tính ẩn danh.* Không giống với thẻ tín dụng và sec, nếu người mua dùng tiền mặt, rất khó truy tìm dấu tích người mua sau giao dịch. Các hệ thống thanh toán điện tử nếu yêu cầu cung cấp thông tin cá nhân, hình ảnh và những đặc điểm nhận dạng thì đặc điểm nhận dạng hoặc thông tin cá nhân của các chủ thể phải được giữ kín. Phải đảm bảo không làm lộ các thông tin cá nhân của khách hàng.

*Tính phân đoạn (divisibility).* Hầu như người bán chấp nhận thẻ tín dụng cho các giao dịch có giá trị giới hạn (Min-Max). Nếu giá trị giao dịch quá nhỏ (một vài $) hoặc quá lớn (giá một chiếc máy bay), thẻ tín dụng sẽ không là phương thức thanh toán khả thi. *Tính dễ sử dụng* cho bất kỳ ai và trong mọi doanh nghiệp, khách hàng có thể sử dụng

*Tính tiết kiệm/hiệu quả* (phí giao dịch). Chi phí cho mỗi giao dịch nên chỉ là một con số rất nhỏ (gần bằng 0), đặc biệt với những giao dịch giá trị thấp. Ví dụ với thẻ tín dụng có mức phí tối thiểu + 3% giá trị giao dịch, với giao dịch giá trị nhỏ, mức phí là bao nhiêu cho phù hợp.

*Tính thông dụng.* Khả năng sử dụng rộng rãi và tối thiểu hóa hàng rào luật pháp, cạnh tranh - cho phép – chấp nhận. Ví dụ: Paypal phải đấu tranh với những cáo buộc của hệ thống ngân hàng là minh họa về tính thông dụng.

*Tính hoán đổi, chuyển đổi* từ hình thức này sang hình thức khác. Ví dụ: Tiền số có thể chuyển thành các kiểu loại tiền khác. Có thể dễ dàng chuyển từ tiền điện tử sang tiền mặt hay chuyển tiền từ tiền điện tử sang tài khoản cá nhân. Từ tiền điện tử có thể phát hành séc điện tử, séc giấy. Tiền số bằng ngoại tệ này có thể dễ dàng chuyển sang ngoại tệ khác với tỷ giá tốt nhất.

*Tính linh hoạt.* Nên cung cấp nhiều phương thức thanh toán, tiện lợi cho mọi đối tượng.

*Tính hợp nhất.* Để hỗ trợ cho sự tồn tại của các ứng dụng này thì giao diện nên được tạo ra theo sự thống nhất của từng ứng dụng. Khi mua hàng trên bất cứ trang web nào cũng cần có những giao diện với những bước gần giống nhau.

*Tính co dãn.* Cho phép khách hàng và những nhà kinh doanh có thể tham gia vào hệ thống mà không làm hỏng cơ cấu hạ tầng, đảm bảo xử lý tốt dù khi nhu cầu thanh toán trong thương mại điện tử tăng.

1. **Thẻ thanh toán**

Khái niệm: Là loại thẻ được sử dụng phổ biến nhất, theo đó người chủ thẻ được sử dụng một hạn mức tín dụng tuần hoàn để mua sắm hàng hoá, dịch vụ tại những cơ sở chấp nhận loại thẻ này.

Về bản chất đây là một dịch vụ tín dụng thanh toán với hạn mức chi tiêu nhất định do ngân hàng cung cấp cho khách hàng căn cứ vào khả năng tài chính, số tiền ký quỹ hoặc tài sản thế chấp của khách hàng. Khoảng thời gian từ khi thẻ được dùng để thanh toán hàng hoá, dịch vụ tới lúc chủ thẻ phải trả tiền cho ngân hàng có độ dài phụ thuộc vào từng loại thẻ tín dụng của các tổ chức khác nhau. Nếu chủ thẻ thanh toán toàn bộ số dư nợ vào ngày đến hạn, thời gian này sẽ trở thành thời gian ân hạn và chủ thẻ hoàn toàn được miễn lãi đối với số dư nợ cuối kỳ. Tuy vậy, nếu hết thời gian này mà một phần hay toàn bộ số dư nợ cuối kỳ chưa được thanh toán cho ngân hàng thì chủ thẻ sẽ phải chịu một khoản lãi và phí chậm trả.

Khi toàn bộ số tiền phát sinh được hoàn trả cho ngân hàng, hạn mức tín dụng của chủ thẻ được khôi phục như ban đầu. Đây chính là tính chất “ tuần hoàn” revolving của thẻ tín dụng.

Visa International (Tổ chức thẻ quốc tế Visa): Thẻ Visa, tiền thân là Bank Americard do Bank of America phát hành vào năm 1960, hiện nay là loại thẻ có quy mô phát triển lớn nhất trên toàn cầu. Đến cuối năm 1990 có khoảng 257 triệu thẻ đang lưu hành với doanh thu khoảng 354 tỷ USD. Nhưng chỉ trong khoảng 3 năm, và cuối năm 1993 doanh thu của Visa tăng mạnh mẽ lên đến 542 tỷ USD. Visa hiện có khoảng 164.000 máy ATM (Automatic Teller Machine) ở 65 nước trên thế giới.

MasterCard International (Tổ chức thẻ quốc tế Mastercard): MasterCard ra đời vào năm 1966 với tên gọi là Master Charge do hiệp hội thẻ liên Ngân hàng ICA( Interbank Card Association) phát hành thông qua các Ngân hàng thành viên trên thế giới. Năm 1990, một hệ thống ATM lớn nhất thế giới được sử dụng phục vụ cho những người dùng thẻ MasterCard. Cũng năm này, MasterCard đã phát hành được hơn 178 triệu thẻ, có 5.000 thành viên phát hành và 9 triệu điểm tiếp nhận thẻ. Đến năm 1993, doanh thu của MasterCard lên đến 320, 6 tỷ USD và khoảng 216 triệu thẻ đang lưu hành tại hơn 220 nước trên thế giới. Cho tới nay, tham gia vào hiệp hội MasterCard lên đến 29.000 thành viên.

*- Quy trình thanh toán thẻ tín dụng:*

Bước 1: Chủ thẻ dùng thẻ để thanh toán tiền hàng hoá, dịch vụ hoặc rút tiền mặt. Khi nhận được thẻ từ khách hàng, Ngân hàng đại lý hoặc CSCNT phải kiểm tra tính hợp lệ của thẻ: Logo, biểu tượng của thẻ tín dụng quốc tế, băng chữ ký, ký hiệu đặc biệt, thời hạn hiệu lực, các yếu tố in nổi trên thẻ…

Sau khi kiểm tra tính hợp lệ của thẻ, CSCNT hoặc điểm ứng tiền mặt phải hoàn thành hoá đơn, đề ngày giao dịch, số tiền giao dịch, số cấp phép (nếu có), tên và số hiệu CSCNT, loại hàng hoá, dịch vụ cung ứng.

Tiếp đó, CSCNT sẽ phải yêu cầu khách hàng ký vào hoá đơn (chữ ký trên hoá đơn phải khớp đúng với chữ ký ở băng sau của thẻ).

Hoá đơn thanh toán thẻ gồm 3 liên: 1 liên giao cho khách hàng giữ, 2 liên còn lại CSCNT giữ lại.

Trong trường hợp CSCNT và chủ thẻ thoả thuận huỷ bỏ một phần hay toàn bộ giao dịch đã thực hiện, CSCNT không được hoàn lại cho chủ thẻ bằng tiền mặt mà phải thực hiện giao dịch hoàn trả. Đối với CSCNT có trang bị máy POS có hệ thống thu nhận tín hiệu điện từ EDC (Electronic Draft Capture - Máy thanh toán tự động) thì có thể điều chỉnh hay huỷ bỏ toàn bộ giao dịch trước khi truyền dữ liệu.

CSCNT phải liên hệ ngay với Ngân hàng để xin cấp phép khi: Số tiền giao dịch bằng hoặc lớn hơn hạn mức thanh toán và có nghi ngờ thẻ giả hay chủ thẻ có vấn đề.

Chỉ sau khi được Ngân hàng phát hành hoặc Tổ chức thẻ Quốc tế cho phép giao dịch bằng cách cung cấp số cấp phép thì CSCNT mới được thực hiện giao dịch.

Bước 2: CSCNT giao dịch với Ngân hàng.

Ở đây có sự phân biệt giữa CSCNT có sử dụng các máy POS có hệ thống thu nhận tín hiệu điện từ EDC và CSCNT không sử dụng máy này.

Đối với CSCNT có trang bị máy POS có thu nhận tín hiệu điện từ EDC: Việc đọc các dữ liệu trên thẻ và in ra hoá đơn thanh toán thẻ sẽ do máy thực hiện kể cả việc xin cấp phép. Dữ liệu về giao dịch sẽ được lưu giữ trên bộ nhớ của máy. Hàng ngày, CSCNT truyền dữ liệu thanh toán về Ngân hàng thanh toán. Còn hoá đơn thanh toán EDC sẽ được tập hợp và chuyển cho Ngân hàng thanh toán mỗi tuần.

Đối với CSCNT không trang bị máy có thiết bị thu nhận điện từ EDC: Việc đối chiếu danh sách thẻ cấm lưu hành, xin cấp phép đều do CSCNT thực hiện sau đó sẽ dùng máy cà tay để in ra hoá đơn thanh toán. Hàng ngày, CSCNT sẽ tổng hợp toàn bộ.

Bảng 4.1: So sánh thẻ tín dụng quốc tế ACB và VCB

|  |  |  |
| --- | --- | --- |
| Đặc điểm thẻ | Thẻ VCB | Thẻ ACB |
|  |  |  |
| Loại thẻ | Thẻ chuẩn-Thẻ vàng | Thẻ chuẩn-Thẻ vàng |
|  |  |  |
| Hạn mức tín dụng | Thẻ chuẩn 10-50 triệuVNĐ | Thẻchuẩn: 10-40triệu VNĐ |
|  | Thẻ vàng 50-90 triệu VNĐ | Thẻ vàng 40-50 triệu VNĐ |
|  |  |  |
| Số tiền ký quỹ | 125% hạn mức tín dụng | 110% hạn mức tín dụng |
|  |  |  |
| Lái suất tín dụng | 0, 8%/1tháng | 0, 85%/1 tháng |
|  |  |  |
| Phí thường niên | Thẻ chuẩn 100.000VNĐ | Thẻ chuẩn 200.000 VNĐ |
|  | Thẻ vàng 200.000 VNĐ | Thẻ vàng 300.000 VNĐ |
|  |  |  |
| Phí rút quá giới hạn | 8-15%/năm tuỳ thuộc vào thời | 27-35% hàng năm tối thiểu là |
|  | gian kể từ khi rút thấu chi | 20.000 đồng |
|  |  |  |
| Phí rút tiền mặt | 4% tối thiểu 50.000 VNĐ | 4% tối thiểu 60.000 VNĐ |
|  |  |  |
| Phí thông báo mất | 300.000 VNĐ/1 lần | 300.000 VNĐ/1 lần |
| cắp thẻ |  |  |
|  |  |  |

(Nguồn Điều kiện phát hành thẻ tại VCB và ACB)

Lợi dụng sự chưa hoàn hảo trong các hệ thống bảo mật, các dữ liệu về thẻ thanh toán có thể bị đánh cắp và sử dụng bất hợp pháp, gây ra những rủi ro cho nhiều bên liên quan như:

*Rủi ro đối với chủ thẻ:*

Do tính chất của thẻ tín dụng là không biết được người rút tiền có phải là chủ thẻ hay không mà chủ yếu dựa vào việc kiểm tra số PIN ở trên thẻ nên các chủ thẻ dễ bị lừa ăn cắp thẻ cùng với số PIN. Việc để lộ số PIN có thể là do chủ thẻ vô tình để lộ hoặc bị ăn cắp một cách tinh vi. Bên cạnh đó chủ thẻ còn gặp phải tình trạng làm giả thẻ tín dụng ngày càng tinh vi. Việc làm giả thẻ có thể tiến hành theo hai hình thức.

Đối tượng làm giả thẻ có thể mua chuộc nhân viên tại các cơ sở chấp nhận thẻ để các nhân viên này sau khi quét thẻ tính tiền sẽ bí mật quét thẻ thêm một lần vào một thiết bị đặc biệt có thể đọc được toàn bộ thông tin về thẻ. Sau khi có đầy đủ các thông tin đó chúng sẽ nhanh chóng làm một chiếc thẻ tương tự và tiến hành mua bán hàng hoá như bình thường. Hình thức thứ hai tinh vi hơn là chúng sẽ cài thẳng những con chip điện tử tinh vi vào trong máy tính tiền hoặc máy rút tiền tự động. Sau đó chúng sẽ quay trở lại các địa điểm trên để lấy các con chip đã chứa những thông tin về các thẻ đã giao dịch và tiến hành làm thẻ giả với những thông tin đã lấy cắp được.

*Rủi ro đối với ngân hàng phát hành:*

Rủi ro thứ nhất là việc chủ thẻ lừa dối sử dụng thẻ tại nhiều điểm thanh toán thẻ khác nhau với mức thanh toán thấp hơn hạn mức thanh toán nhưng tổng số tiền thanh toán lại cao hơn hạn mức thanh toán trong thẻ. Việc thanh toán quá mức chỉ được biết khi ngân hàng nhận được các hoá đơn thanh toán của các đơn vị chấp nhận thẻ. Và khi chủ thẻ không có khả năng thanh toán thì rủi ro này sẽ do ngân hàng tự chịu.

Một hình thức lừa dối khác từ phía chủ thẻ là do việc lợi dụng tính chất thanh toán quốc tế của thẻ để thông đồng với người khác chuyển thẻ ra nước khác để thanh toán ngoài quốc gia chủ thẻ cư trú.

Khi ngân hàng tiến hành đòi tiền từ chủ thẻ cho việc thanh toán ở quốc gia khác thì chủ thẻ căn cứ vào việc mình không có thị thực xuất nhập cảnh hoặc căn cứ vào xác nhận của cơ quan để từ chối thanh toán. Trong khi đó, các đơn vị chấp nhận thẻ cũng không phải chịu trách nhiệm do việc thanh toán bằng thẻ được tiến hành mà không cần biết chủ thẻ là ai. Bằng chứng duy nhất có thể so sánh là căn cứ vào chữ ký trên thẻ và trên hoá đơn nhưng do thông đồng từ trước nên việc giả mạo chữ ký trong các hoá đơn là điều rất dễ dàng.

*Rủi ro đối với ngân hàng thanh toán:*

Tuy chỉ là đơn vị trung gian trong hoạt động thanh toán thẻ song các ngân hàng thanh toán cũng có thể gặp rủi ro nếu họ có sai sót trong việc cấp phép cho các khoản thanh toán có giá trị lớn hơn hạn mức qui định. Bên cạnh đó, nếu không kịp thời cung cấp cho các đơn vị chấp nhận thẻ danh sách các thẻ bị mất hoặc bị vô hiệu mà trong thời gian đó các thẻ này vẫn được sử dụng thì các ngân hàng phát hành sẽ từ chối thanh toán cho những khoản này.

*Rủi ro cho các đơn vị chấp nhận thẻ:*

Rủi ro cho các đơn vị chấp nhận thẻ chủ yếu là bị từ chối thanh toán cho số hàng hoá cung ứng ra vì các lý do liên quan đến thẻ. Đó là việc thẻ bị hết hiệu lực nhưng các đơn vị chấp nhận thẻ không phát hiện ra mặc dù đã được thông báo. Tự ý sửa đổi các hoá đơn (vô tình hoặc cố ý) và bị các ngân hàng phát hiện ra thì cũng sẽ không được thanh toán.

1. **Tiền ảo**

*a Khái niệm*

Hệ thống thanh toán bằng thẻ tín dụng không hiệu quả trong các thanh toán nhỏ. Tiền mặt điện tử có ưu điểm trong các thanh toán nhỏ hơn 1USD. Tiền điện tử là một phần mềm của hệ thống thanh toán dựa trên việc sử dụng tiền số ẩn danh. Công ty Digicash đã phát triển phần mềm này để đảm bảo an toàn cho việc thanh toán qua e-mail hay internet.

Người sử dụng tiền điện tử phải có một tài khoản tại ngân hàng số trên internet (ví dụ như ngân hàng First Digital) để gửi hoặc rút tiền số.

Trước hết, người sử dụng phải tự đăng ký để có mật khẩu riêng, nhờ đó mới có thể tải xuống phần mềm cho khách hàng được phân phối bởi Digicash. Sau đó người sử dụng có thể mở tài khoản tại ngân hàng tiền điện tử của mình. Tiền số được thực hiện từ chữ ký số, dùng để tượng trưng cho một lượng tiền xác định.

Khi người sử dụng rút tiền, phần mềm cho khách hàng trong máy tính của họ sẽ tính toán lượng tiền cần thiết của mỗi loại cho phù hợp với yêu cầu cần rút. Sau đó, nó sẽ tạo ra một dãy số bất kỳ cho lượng tiền này rồi gửi tới ngân hàng số cùng với một

“nhân tố vô hình” (*nhân tố vô hình* là một thông số để tiến hành cơ cấu chữ ký vô hình nhằm bảo đảm bí mật cho người chi trả).

Ngân hàng sẽ sử dụng chìa khoá bí mật để mã hoá dãy số này, cùng lúc đó sẽ trừ bớt đi lượng tiền đã rút ra trong tài khoản của ngưởi sử dụng. Lượng tiền sẽ được gửi trở lại và sau khi nhận được “nhân tố vô hình” thì sẽ được lưu giữ trong máy tính cá nhân của người sử dụng.

Khi người sử dụng cần thanh toán, phần mềm của họ sẽ tính toán lượng tiền cần thiết có thể đáp ứng nhu cầu, lượng tiền thu thập được sẽ được gửi tới người được thanh toán, người đó sẽ gửi số tiền đó tới ngân hàng số để đảm bảo tính hợp lệ của chúng. Tài khoản của người này cũng sẽ được thêm vào một lượng tiền tương đương.

Việc xác định rõ mỗi lượng tiền chỉ được dùng một lần là rất quan trọng, nếu như người nhận muốn có một lượng tiền mới để tiêu dùng thì họ phải rút thêm lượng tiền cần thiết ra.

Việc bảo đảm an toàn cho tiền mặt điện tử dựa vào kỹ thuật chữ ký điện tử chìa khoá công cộng (RSA). Khi nó được thực hiện vào lần đầu tiên, phần mềm tiền điện tử sẽ sinh ra một cặp chìa khoá mã hoá RSA. Thêm vào đó, mỗi lượng tiền rút ra từ tài khoản đều được bảo vệ bởi một mật khẩu mà chỉ có người sở hữu tài khoản đó mới biết được.

Tiền mặt điện tử đảm bảo tính nặc danh cho người chi trả, những đặc điểm nhận diện của người chi trả không thể được phát hiện ra trong suốt quá trình thanh toán, trừ khi chính họ lựa chọn việc nhận diện chính mình.

Tuy nhiên, ngân hàng lại nhận diện được người được thanh toán khi họ hoàn thành giao dịch.

Tính bí mật được bảo đảm bởi kỹ thuật chữ ký vô hình, đó là cách để ngân hàng đảm bảo tính hợp pháp của tiền số mà không cần tới khả năng xem xét được dãy số ở bên trong. Để hiểu rõ hơn về cơ chế này, xem e là chìa khoá công cộng của ngân hàng, d là chìa khoá cá nhân và biểu thức: n=p\*q. Thông thường, ngân hàng sẽ ký thông báo m bằng cách tính toán m^d mod n.

Mẹo thường dùng để ngân hàng phải ký mà không biết được là ký cái gì là ẩn đi lượng tiền bằng một số k bất kỳ (1<=k<=n) gọi là "nhân tố vô hình". Người sử dụng sẽ gửi tới ngân hàng giá trị của r=(m\*k^e) mod n. Ngân hàng sẽ ký bằng cách tính toán

r^d= (m\*k^e)^d mod n. Ngân hàng sẽ giữ văn bản ghi chép giá trị của r, đồng thời cũng là văn bản lưu giữ tất cả các thông tin được ẩn đi bởi "nhân tố vô hình".

Khi người sử dụng nhận được giá trị r^d, họ sẽ thay đổi "nhân tố vô hình" bằng cách tính toán t=r^d k^-1 mod n=m^d mod n.

*b. Các phương pháp giữ tiền*

Trực tuyến: cá nhân không giữ tiền điện tử mà thông qua bên thứ ba (ngân hàng trực tuyến giữu tài khoản của khách hàng)

Ngoại tuyến: Khách hàng giữ tiền trong thẻ thông minh hay túi tiền điện tử, việc gian lận hay gửi lại tiền mặt điện tử cần chứng nhận mã hoá.

*c. Ưu nhược điểm của tiền mặt điện tử*

Ưu điểm:

* Hiệu quả hơn trong các giao dịch nhỏ
* Chi phí vận chuyển thấp hơn
* Tất cả mọi người đều có thể sủ dụng chúng, không giống như thẻ tín dụng và không yêu cầu chứng thực.
* Thay thế được tiền mặt vì lưu giữ được trong thẻ thông minh hay ví tiền điện tử.

Lợi ích mà tiền mặt điện tử mang lại cho khách hàng là sự tiên lợi bởi họ không cần phải mang tiền theo mình. Tiền mặt điện tử có trong cả tài khoản tiền điện tử cũng như có thể tải xuống thẻ tín dụng cỡ "thẻ thông minh".

Khách hàng khi mua bán trên internet có thể tìm thấy một số loại tiền điện tử có thể đảm bảo bí mật tốt hơn những thẻ tín dụng hiện nay. Đối với người kinh doanh, tiền mặt điện tử cho phép kết nối với thị trường toàn cầu mà không bị giới hạn hay ảnh hưởng bởi loại tiền của địa phương. Khác với tiền giấy, tiền điện tử có thể được lập trình để hạn chế hoặc giới hạn các hình thức mua bán. Những sự lựa chọn đặc biệt có thể được lập trình trong ngôn ngữ điện tử của lượng tiền nhỏ để có thể giới hạn sự mua bán một số sản phẩm hoặc dịch vụ đặc biệt. Cha mẹ cũng có thể gửi tới cho con cái đang học ở các trường đại học một lượng tiền điện tử chỉ được dùng vào việc thanh toán tiền học phí và tiền thuê mướn. Một lợi ích khác của tiền điện tử cho người kinh doanh là mọi hoạt động của thị trường có thể được mở rộng nếu như khách hàng và người kinh doanh có thể gửi tiền đi khắp thế giới chỉ bằng việc nhấn một phím trên máy tính cá nhân của họ.

Nhược điểm:

* Không có dấu hiệu về thuế như tiền thông thường
* Có khả năng bị giả mạo

Sự bất lợi của tiền điện tử là chỉ có những khách hàng với máy tính cá nhân mới có thể truy cập để sử dụng chúng, trong khi những khách hàng có thu nhập thấp và không có máy tính thì không thể. Tiền mặt điện tử có thể không an toàn bằng tiền gửi trong ngân hàng bởi lượng tiền được giữ trong ví tiền điện tử có thể bị mất vĩnh viễn khi thẻ bị hỏng.

Quan trọng hơn là chính phủ cần phải kiểm soát được lượng tiền lưu thông và phát hiện ra những hành vi phạm tội. Những vấn đề này cần phải được giải quyết để giành được niềm tin của khách hàng và nhà nước.

*d. Phát hành tiền điện tử*

Tiền mặt điện tử chỉ cho phép tiêu dùng một lần, phải được ẩn danh, giống như tiền thông thường, phải được cất giữ an toàn để tránh việc làm giả. Có khả năng chuyển đổi độc lập, không phụ thuộc vào vấn đề quốc gia hay cơ chế giữ.

*e. Hệ thống tiền mặt điện tử*

Tiền mặt điện tử không phổ biến ở Mỹ nhưng khá thông dụng ở Châu âu và Nhật bản. Tuy nhiên lý do cho sự không thành công của nó ở Mỹ không thực sự rõ ràng. Một mặt có thể là do thói quen tiêu dùng khá phức tạp, mặt khác cũng có thể do thiếu những phần mềm tiêu chuẩn có thể chạy dễ dàng trong một hệ thống phần cứng và phần mềm phong phú

Checkfree

Cho phép thanh toán với hệ thống Séc điện tử trực tuyến

Clickshare

Được tạo ra cho các nhà xuất bản báo hoặc tập chí Được dùng cho các thanh toán nhỏ.Việc mua bán sẽ được tính cho iSP của người sử dụng, người sẽ lần lượt làm hoá đơn cho khách hàng

Cybercash

Cybercash được Bill Melton phát minh ra vào tháng 8 năm 1994 và đã đưa đến thành công lớn cho giải pháp của quá trình cung cấp thẻ tín dụng. Để sử dụng được Cybercash, khách hàng phải tải phần mềm miễn phí Cybercash xuống từ dịch vụ internet của Cybercash.

Phần mềm này sẽ thiết lập mối liên kết điện tử giữa khách hàng, người kinh doanh và ngân hàng của họ cũng như mối liên hệ giữa những cá nhân với nhau. Khi giá cả đã được thoả thuận và khách hàng đã sẵn sàng cho việc mua bán thì khách hàng chỉ việc click vào nút "TRả Tiền".

Người bán hàng sẽ gửi cho khách hàng một danh đơn hàng gửi trực tuyến, bao gồm đầy đủ thông tin mua bán và tổng số tiền phải trả.

Khi thông báo này hiện ra trên màn hình, khách hàng sẽ thêm vào số thẻ tín dụng, tên của mình cũng như ngày hết hạn của thẻ. Khách hàng cũng có thể lựa chọn dịch vụ ghi nợ để mua hàng. Trong trường hợp này, khách hàng phải điền số chứng minh thư của mình vào danh đơn hàng gửi trực tuyến của người bán hàng.

Thông báo này sẽ được mã hoá và được gửi kèm với danh đơn hàng gửi tới người bán. Người này sẽ thêm vào những thông tin nhận diệnc cần thiết và gửi chuyển thiếp tới dịch vụ Cybercash. tại đó, dịch vụ Cybercash sẽ đề xướng một thẻ tín dụng tiêu chuẩn hay yêu cầu cho pháp vay nợ với ngân hàng của người bán hay với ngân hàng – trung tâm xử lý được chỉ định.

Khi yêu cầu cho phép vay nợ đã được hoàn thành, dịch vụ Cybercash sẽ gửi chuyển tiếp câu trả lời tới người bán hàng, sau đó, người bán hàng sẽ hoàn tất nốt quá trình giao dịch.

Cybercash chỉ cho phép nhìn thấy những thông tin cần thiết cho quá trình thanh toán, không giữ lại bất cứ thông tin nào liên quan tới hàng hoá mua bán. Đặc điểm này giúp bảo vệ bí mật của cá nhân cũng như đảm bảo an toàn cho quá trình giao dịch.

Các đặc điểm chung của Cybercash:

* Kết nối các đặc tính của tiền mặt và séc
* Đưa ra các dịch vụ thanh toán nhỏ, thanh toán séc và thẻ tín dụng
* Cho phép kết nối trực tiếp các nhà kinh doanh với bộ xử lý thẻ tín dụng để cung cấp sự giấy phép cho các giao dịch. Có thể cho phép quá trình ngăn chặn việc thanh toàn thiếu tiền trong giao dịch.

Cybercoins

Được giữ trong ví Cybercash, đó là một cơ cấu phần mềm được đặt ở máy tính của khách hàng Được dùng trong việc mua bán từ 25c đến 10$

Thanh toán tức thời: việc thanh toán được tiến hành trực tiếp từ tài khoản.

Coin. Net

Việc mua bán được tiến hành thông qua những đồng xu điện tử được giữ trong máy tính của khách hàng. Hoạt động dựa vào việc cài đặt một chốt đặc biệt trong trang web của người sử dụng. Các nhà kinh doanh không cần phải có một phần mềm đặc biệt để thích ứng với ecoins. Dịch vụ ecoin ngăn chặn được việc gửi lại tiền và theo dõi được quá trình giao dịch nhưng khách hàng vẫn có thể ẩn danh đối với người bán.

Milicent

Được phát triển bởi công ty Digital, hiện nay là một phần của Compaq. Là một hệ thống điện tử Những người tham gia kinh doanh tạo ra và bán chứng khoán tạm thời của mình cho người môi giới để giảm giá. Khách hàng thường đăng ký với người môi giới và mua một lượng chứng khoán nhất định, thường mua kèm với thẻ tín dụng. Việc mua bán này thường được tiến hành bằng cách chuyển chứng khoán của người môi giới sang một loại chứng khoán đặc biệt của người bán.

MiliCent cont'd

Khách hàng có thể mua hàng có giá trị rất thấp. Có hai lý do để cần có người môi giới, đó là những thanh toán nhỏ cần phải được kết hợp lại để đảm bảo thu được lợi nhuận giúp cho việc sử dụng hệ thống được dễ dàng, khách hàng chỉ cần liên hệ vời một nhà môi giới duy nhất cho tất cả các nhu cầu về chứng khoán.

*g. Ảnh hưởng của tiền mặt điện tử tới xã hội*

*Đối với cơ quan lập pháp và cơ quan điều chỉnh của chính phủ:*

Vấn đề chính là làm thế nào để tiền mặt điện tử phù hợp với cơ cấu ngân hàng và tiền tệ hiện tại thông qua hệ thống dự trữ của nhà nước? Những quy định hiện tại không được mở rộng tương ứng với tiền mặt điện tử. Ví dụ như chúng ta không có những quy định về việc những giao dịch tiền số sẽ phải đóng thuế ở đâu. Thêm vào đó, những quy định không rõ ràng hiện nay làm cho hệ thống ngân hàng không thể hoạt động hiệu quả trong vấn đề này (tiền mặt điện tử). Những cơ quan điều chỉnh cần phải tập trung vào việc xây dựng những cơ sở hạ tầng cần thiết cho thời đại của tiền điện tử.

*Đối với những cơ quan phát hành tiền mặt điện tử tiềm năng: Ngân hàng và phi ngân hàng*

Các tổ chức phi ngân hàng là những nhà tiên phong trong việc phát hành tiền điện tử, lĩnh vực mà họ tin rằng hệ thống các ngân hàng truyền thống không ưa thích. Tuy nhiên, họ nên sử dụng những kinh nghiệm của mình làm đòn bẩy trong việc cung cấp những dịch vụ giao dịch an toàn và giứp đặt ra những tiêu chuẩn cụ thể.

Theo quan điểm của các ngân hàng, những khách hàng dùng tiền điện tử sẽ mang lại tính kinh tế cho họ hơn là những khách hàng dùng séc, bởi như thế ngân hàng sẽ phải mất thời gian để theo dõi séc của khách hàng. Hệ thống ngân hàng cũng nhận thấy một ưu điểm nữa là họ được khách hàng tin tưởng. Hệ thống ngân hàng và phi ngân hàng nên tập trung vào việc hình thành một liên minh nhằm bổ sung những thiếu sót cho nhau.

*Đối với những nhà kinh doanh*

Tiền mặt điện tử sẽ mở ra khả năng cho việc thực hiện những giao dịch trực tuyến bởi thẻ tín dụng không thích hợp với những giao dịch nhỏ. trong một cuộc mua bán nhỏ, rất có thể phí thanh toán cho việc giao dịch thẻ tín dụng sẽ nhiều hơn số tiền thu được từ việc giao dịch đó. Và, tiền mặt điện tử đưa ra một phương thúc thanh toán hiệu quả hơn cho tất cả các bên tham gia.

*Đối với khách hàng*

Tiền mặt điện tử mang lại sự thuận tiện và đảm bảo bí mật cho khách hàng. Trong khi quá trình mua bán thẻ tín dụng được ghi lại trong những cơ sơ dữ liệu thì việc bảo mật lại trở thành vấn đề chính. uy nhiên, khách hàng cũng nên thúc đẩy các nhà cung cấp tiền điện tử đưa ra những cách thức bảo vệ khách hàng và xác định rõ ai là người phải chịu trách nhiệm trong vấn đề làm giả tiền điện tử.

Các ảnh hưởng của tiền điện tử tới xã hội có thể được tóm tắt bằng bảng sau:

Bảng 4.2: Ảnh hưởng của tiền điện tử

|  |  |  |  |
| --- | --- | --- | --- |
| NGƯỜI THAM GIA |  | ẢNH HƯỞNG TÍCH | ẢNH HƯỞNG TIÊU CỰC |
| CHÍNH |  | CỰC |  |
|  |  |  |  |
| Người điều hành |  | Mang lại hiệu quả cao cho | Không có khả năng theo dõi |
|  |  | việc chuyển đổi tiền | Thiếu sự điều chỉnh |
|  |  |  | Trốn thuế |
|  |  |  |  |
| Người phát hành |  | Có thêm những thị trường | Xuất hiện sự giả mạo |
|  |  | mới |  |
|  |  |  |  |
| Khách hàng |  | Đảm bảo tính kinh tế | Thiếu sự bảo vệ khách hàng |
|  |  | Đảm bảo bí mật cá nhân |  |
|  |  |  |  |
| Người kinh doanh |  | Có thể kết nối tới thị | Xuất hiện sự giả mạo |
|  |  | trường toàn cầu hoạt động hiệu quả |  |
|  |  |  |  |
|  |  |  |  |

*h. Dự đoán tương lai của tiền điện tử:*

Tiền mặt điện tử cùng với sự thanh toán điện tử sẽ phát triển rất nhanh vào thời gian tới bởi những hiệu quả hoạt động tiềm năng, sự tiện lợi, tính bảo mật cao, truy cập trực tiếp tới khách hàng mà không bị giới hạn bởi địa lý, và sự bảo đảm thành công với mỗi mặt hàng theo yêu cầu của khách hàng. Bên cạnh đó, tiền mặt điện tử cũng sẽ thúc đẩy sự ra đời của những quy định thích hợp dựa trên vấn đề thuế và sự bảo vệc cho khách hàng.

Chúng ta hãy hình dung về một tương lai chỉ còn tiền số, sẽ không còn tiền giấy trong túi của mọi người. Mọi sự lựa chọn sẽ là một hay hai "chip card", hay có thể là một túi tiền điện tử. Bên cạnh sự thay thế tiền và hối phiếu bằng giấy, tiền mặt điện tử sẽ thay đổi thói quen mua bán của chúng ta, tạo ra cuộc cách mạng trong lĩnh vực mua bán hàng hoá và dịch vụ. Ví dụ như thay vì việc phải trả tiền đặt mua báo dài hạn, chúng ta có thể chỉ việc trả tiền cho những cột báo cụ thể, hay những tài liệu nhất định.

Những ngân hàng truyền thống sẽ phải đối phó với xu hướng tiền mặt điện tử và sẽ phải đưa ra những dịch vụ tài chính trực tuyến. rong mọi quá trình giao dịch kinh doanh hay trao đổi tiền, hoạt động ngân hàng là thực sự cần thiết, nhưng ngân hàng thì lại không. Theo sự phác hoạ của Microsoft Network, ai có được sự tiếp cận với khách hàng, người đó sẽ trở thành "the king of the hill". Họ dự đoán rằng tất cả các ngân hàng chính trên thế giới sẽ có giao diện trên không gian Cyber và con số các chi nhánh địa phương sẽ giảm xuống nhanh chóng. Các cơ quan phát hành thẻ tín dụng cũng cần phải coi tiền mặt điện tử như một vật thay thế đầy tiềm năng. Chúng ta hy vọng rằng Visa international và Mastercard sẽ đưa ra những sản phẩm mới trong xu hướng trao đổi trực tuyến này.

Họ cho rằng tại thời điểm tiền mặt điện tử được sử dụng một cách rộng rãi, giá của một chiếc máy tính cá nhân là khá rẻ. Do đó, vấn đề truy cập hợp lý sẽ trở nên đơn giản. Tuy nhiên, chúng ta vẫn chưa thể hình dung tiền mặt điện tử sẽ được đưa ra như thế nào, liệu mọi người có thể truy cập nó với chiếc điện thoại hay không?

Tiền mặt điện tử sẽ được xem như sự tiếp nối trong xu hướng mở ra một thị trường thanh toán toàn cầu cho đa số. Khi mà những con số tượng trưng cho sự giàu có vượt qua số lượng những trái phiếu bằng giấy mà chúng ta có, khi mà những rào cản giữa các quốc gia đã bị xoá bỏ thì lúc đó nền kinh tế toàn cầu sẽ được hình thành, chính phủ sẽ không thể quản lý đươc vần đề cung cấp tiền. Xu hướng của một nền kinh tế không biên giới sẽ dẫn đến sự chia tách của nền kinh tế và quốc gia.

*i. Hệ thống hoạt động của tiền điện tử*

Tiền điện tử được xây dựng trên hệ thống mã hoá được gọi là chữ ký điện tử. Phương thức này sử dụng một đôi mã số cùng phối hợp hoạt động: một bộ cho mục đích khoá hay gọi là mã hoá và bộ còn lại sử dụng trong việc giải mã. Các thông tin được mã hoá bằng một bộ mã và chỉ giải mã được trong trường hợp sử dụng bộ mã thứ hai. Mật khẩu mã hệ được giữ riêng và mật khẩu giải mã sử dụng chung. Thông qua việc hỗ trợ khách hàng (bao gồm cả người mua và người bán) bằng mật khẩu chung, một ngân hàng có thể tạo điều kiện cho khách hàng giải mã bất cứ một thông tin nào đã được mã hoá với mật khẩu riêng của ngân hàng.

Nếu khách hàng giải mã ra một thông tin nhận diện, trong trường hợp đó khách hàng có thể yên tâm đó là do ngân hàng đã mã hoá thông tin đó. Trong hai thập kỷ vừa qua, các chữ ký điện tử đã được bảo vệ nhờ sự hỗ trợ của toán học và điều này đã chứng minh được rằng đây là mệt phương tiện chống chữ ký giả mạn tốt hơn so với chữ ký tay. Trước khi tiền điện tử được sử dụng để mua hàng hoá và dịch vụ, nó phải được một máy chủ về tiền tệ xác nhận trước thông qua các máy chủ tiền tệ.

Quá trình giao dịch mua bán tiền điện tử từ một máy tính bao gồm hai bước: tạo một tài khoản, tiến hành giữ cân đối tài khoản đó để có thể đáp ứng yêu cầu của bất cứ cuộc mua bán nào. Hiện tại, hầu hết các hệ thống tiền điện tử đều đòi hỏi các khách hàng phải có tài khoản tại ngân hàng trực tuyến trung tâm.

Yêu cầu này sẽ hạn chế được các số hoạt động quốc tế cũng như một loạt các giao dịch chồng chéo. Ngoài ra các khách hàng cần phải có khả năng tiếp xúc và để trả các dịch vụ trong và ngoài nước.

Để hỗ trợ khách hàng có thể truy nhập mạng toàn cầu, tiền điện tử cần phải có khả năng chuyển đổi ra rất nhiều loại tiền tệ khác nhau trên thế giới tại các ngân hàng khác nhau. Do đó nhà cung cấp dịch vụ tại mốt nước có thể chấp nhận thanh toán rất nhiều loài tiền khác nhau, thanh toán với họ bằng tiền của nước sở tại và chuyển khoản ngược lại cho các ngân hàng địa phương. Thiết lập một hiệp hội các ngân hàng trực tuyến như một hệ thống hối đoái là một trong những giải pháp được áp dụng.

Khi đã đăng ký tài khoản, các khách hàng sử dụng phần mềm tiền điện tử trên máy tính để tạo ra mốt con số bất kỳ để ghi nhớ. Trong quá trình ghi nợ tài khoản của khách hàng, ngân hàng sử dụng mật khẩu riêng để số hoá con số ghi nhớ khoản tiền chuyển khoản và chuyển thông tin số hoá đó ngược lại khách hàng. Trong thực tế, mạng của máy có thể xác nhận thanh toán có hiệu lực vì họ đều có mã chung của ngân hàng và qua đó họ có thể kiểm tra được kết quả. Do đó ngân hàng có thể chống được chữ ký giả, người được trả tiền được đảm bảo khoản nợ sẽ được thanh toán một cách hợp pháp và người sử dụng sẽ tránh được tình trạng giả mạo và xâm phạm thông tin cá nhân.

Trong thực tế, DIGITA/CASH là một ví dụ thực hiện hệ thống thanh toán bằng tiền điện tử. Tất cả người sử dụng đều có tài khoản tại một ngân hàng điện tử. Sử dụng tài khoản này, họ có thể ký quỹ hoặc rút tiền điện tử. Khi một giao dịch rút tiền điện tử diễn ra, máy tính của người sừ dụng tiền điện tử sẽ tính toán xem có bao nhiêu đồng tiền điện tử sẽ được rút để thanh toán cho việc mua hàng hoá và dịch vụ hoặc chuyển khoản. Kết quả tính toán cuối cùng được gửi đến cho ngân hàng điện tử. Ngân hàng ghi nợ cho tài khoản của người sử dụng với lượng tiền yêu cầu. Tiền được rút ra sẽ được gửi trở lại cho khách hàng. Và như vậy ngân hàng sẽ là nơi đảm bảo cho giá trị của tiền điện tử thanh toán thông qua phương thức mã số và chữ ký điện tử.

*k. Sử dụng tiền điện tử*

Khi một lượng tiền được mua, phần mềm tiền điện tử trên máy tính của khách hàng sẽ lưu giữ số lượng tiền đã được ngân hàng xác nhận.

Người sử dụng có thể tiêu tiền điện tử tại bất cứ cửa hàng nào chấp nhận thanh toán mà không cần phải mở một tài khoản hay chuyển số thẻ tín dụng cho người bán. Khi khách hàng muốn thanh toán cho người bán hàng, phần mềm máy tính của người sử

dụng sẽ tự động thu thập và chuyển khoản số lượng tiền cần thiết từ khoản tiền điện tử dự trữ.

Qui trình thanh toán có thể diễn ra giữa hai bên hoặc ba bên, tuy nhiên các giao dịch thường diễn ra giữa hái bên người mua và người bán. Trong giao dịch này người bán sẽ kiểm tra độ chính xác chữ ký điện tử của các ghi nhớ do ngân hàng phát hành thông qua việc sử dụng mã chung của ngân hàng, Nếu kết thúc trọn vẹn quá trình thanh toán, người mua có thể lưu giữ giá trị tiền điện tử trên phần mềm máy tính 'của họ, sau đó ký quỹ khoản đó với ngân hàng và nhận lại tiền mặt theo giá trị đã ký qũy bằng tiền điện tử.

Trong giao dịch giữa ba bên, ngoài người mua và người bán còn có sự tham gia của ngân hàng và phương tiện giao dịch không chỉ có tiền. Trong giao dịch này, khi người bán nhận được các ghi nhớ của ngân hàng, lập tức họ chuyển trực tiếp cho ngân hàng điện tử và ngân hàng có trách nhiệm xác nhận giá trị của các ghi nhớ này và đảm bảo chúng chưa từng được sử dụng lần nào. Sau đó ngân hàng sẽ ghi có vào tài khoản của người bán.

Trong rất nhiều ảnh huởng kinh doanh, giao dịch giữa hai bên không thể thực hiện được vì nguy cơ thanh toán hai lần với cùng một khoản tiền nhất định. Để có thể hạn chế được vấn đề phát sinh này, các ngân hàng sẽ so sánh các ghi nhớ nhận được từ người bán với số liệu thực tế về khoản tiền đã được ghi nhận lại. Cũng giống như tiền giấy, tiền điện tử được nhận diện thông qua dãy số xê-ri. Do đó để chống lại khả năng thanh toán hai lần, các ghi nhớ của ngân hàng đều được lưu giữ dưới một hình thức nhất định và có thể được nhận diện trên phạm vi toàn cầu.

Tuy nhiên các ghi nhớ của ngân hàng khó có thể trình duyệt tại một điểm trung tâm giao địch trực tuyến. Đối với các ngân hàng hàng ngày thực hiện một số lượng lớn giao dịch thanh toán, do đó việc nhân diện trở thành vấn đề khó khăn và tốn rất nhiều thời gian. Hơn thế nữa, việc kiểm soát các ghi nhớ sẽ phát sinh nhiều chi phí quản lý về phía ngân hàng.

1. **Ví điện tử**

*a. Khái niệm chung*

Giao dịch thương mại điện tử thường đòi hỏi người sử dụng phải thanh toán thông qua internet. Khách hàng nhập vào yêu cầu của mình trên internet bằng cách điền đầy đủ họ tên, địa chỉ, số thẻ tín dụng hay thẻ ghi nợ, ngày thẻ hết hạn và những thông tin cần thiết khác để hoàn thành giao dịch. Người bán hàng sẽ dựa vào những thông tin đó để tính tiền cho khách hàng, bao gồm cả tiền hàng và tiền vận chuyển.

Khi khách hàng mở rộng phạm vi mua bán của mình trên mạng, bao gồm rất nhiều site về thương mại điện tử, việc phải lặp lại quá trình điền những thông tin giống nhau (như tên, địa chỉ...) trở nên hết sức phiền toái. Ví tiền điện tử cung cấp một cơ cấu dùng để chứa những thông tin như thế mà khi nhập thông tin vào những giao dịch điện tử, khách hàng có thể kích hoạt nó. Ví tiền điện tử sẽ tự động điền vào những thông tin được yêu cầu, do đó có thể làm giảm bớt gánh nặng cho khách hàng.

Đặc điểm cơ bản của ví tiền điện tử là khả năng lưu giữ những thông tin sơ lược của khách hàng như đặc điểm nhận diện, địa chỉ, tên tuổi...Ngoài ra, nó còn dùng để chứa thẻ tín dụng, tiền điện tử.

*b. Ưu điểm*

Làm cho việc mua bán trở nên dễ dàng và hiệu quả hơn: không cần thiết phải lặp lại việc điền những thông tin nhận diện vào trong form mua bán. Amazon.com là một trong những nhà kinh doanh trực tuyến đầu tiên đã hạn chế sự lặp lại khi điền những thông tin vào form mua bán.

Có thể làm việc ở nhiều cửa hàng khác nhau nhằm tăng tốc độ thanh toán.

Có thể điều tiết các cơ cấu thanh toán phức tạp, theo dõi quá trình giao dịch của khách hàng. Những ví tiền điện tử đã được cải tiến có thể cung cấp những form an toàn cho thẻ tín dụng.

*c. Các loại ví tiền điện tử*

Gần đây đã xuất hiện rất nhiều loại ví tiền điện tử khác nhau. Sự khác nhau này phụ thuộc vào chức năng, khả năng di chuyển, tính tiện lợi hay những đặc điểm khác của chúng. Dưới đây sẽ đưa ra một số loại phổ biến nhất:

Agile Wallets

* + Được Cybercash phát triển
  + Cho phép khách hàng ghi thẻ tín dụng và các thông tin nhận diện vào,
  + được cất giữ ở dịch vụ trung tâm.
  + Cho phép thanh toán "one click"
  + Không dùng để chứa thẻ thông minh hay
  + Cybercash E-Wallets
  + Được Launchpad Technologies phát triển
  + Phần mềm ví tiền miễn phí này có thể dùng để đựng thẻ tín dụng và các thông tin cá nhân và được giữ trong máy tính của người sử dụng, không phải ở dịch vụ trung tâm, thông tin được đưa vào mẫu thanh toán từ eWallet
  + Thông tin được mã hoá và bảo vệ bằng Password Microsoft Wallets
  + Được cài đặt sẵn trong internet Explorer 4.0, nhưng không có ở trong Netscape
  + Mọi thông tin đều được mã hoá và được bảo vệ bằng Password
  + Chỉ dẫn Microsoft Wallet Merchant sẽ hướng dẫn cách cài đặt Microsoft Wallet.

*d. Ví tiền cá nhân*

Ví tiền cá nhân lưu giữ những thông tin sơ lược của người sử dụng. Trong quá trình cài đặt ban đầu cho ví tiền điện tử, người sử dụng sẽ đưa vào ví những thông tin cần thiết và bảo vệc chúng bằng một password tự chọn. Sau đó chiếc ví này sẽ chứa toàn bộ những thông tin này vào một file đã được mã hoá trong thông tin kèm theo của người sử dụng và sẽ giải mã khi người sử dụng nhập đúng password. Trong suốt quá trình này sự an toàn của những thông tin trong ví phụ thuộc vào độ dài của password mà người sử dụng lựa chọn để lưu giữ trong thông tin đính kèm. Độ dài của thuật toán mã hoá được dùng để mã hoá thông tin trong ví cũng có tính quan trọng sống còn, đặc biệt là khi có nhiều người sử dụng thông tin đính kèm này. Khi đưa ra những yêu cầu, người sử dụng có thể đưa vào form từng thành phần của ví để tự động điền những thông tin cần thiết. eWallet của Launchpad Technology và vWallet của Verifone là những ví dụ.

Với vWallet, người sử dụng có thể tạo ra rất nhiều ví tiền khác nhau, do đó với một chiếc máy tính cá nhân, những người sử dụng có thể có những ví tiền riêng biệt.

*e. Remote Wallets (ví tiền từ xa)*

Trong trường hợp này, thông tin cá nhân của người sủ dụng sẽ được bảo vệ bởi một tổ chức. Khi cần thông tin trong ví, khách hàng chỉ cần click đúng vào biểu tượng cần thiết, biểu tượng này sẽ cho phép người sử dụng điền vào password cho ví của họ.

Sau khi có được giấy phép, trình ứng dụng của người bán hàng sẽ tự động tìm kiếm những thông tin của người sử dụng để hoàn chỉnh yêu cầu của khách hàng. Việc làm này đòi hỏi khách hàng phải đăng ký trình ứng dụng remote wallet bằng cách nhập vào thông tin cần thiết của họ và bảo vệ chúng bằng password.

Người sử dụng có thể dùng chiếc ví này tại những site cung cấp chúng. Cybercash là một tổ chức cung cấp cho khách hàng trình ứng dụng ví instaBuy. Một loại ví phổ biến khác là CitiWallet của Citibank. CitiWallet có những đặc điểm như có thể chứa thẻ tín dụng, theo dõi được quá trình giao dịch thông qua tất cả các thẻ tín dụng, khuyến khích các nhà kinh doanh.

Chi với một lần click, người sử dụng có thể dùng ví của họ để điền đầy đủ thông tin vào form mua bán hay để trả tiền. uy nhiên, nhược điểm của loại ví này là khách hàng phải mở ví của mình trong suốt thời gian họ vào những site khác nhau, còn ví tiền cá nhân thì lại luôn được mở trong máy tính cá nhân của người sử dụng trong suốt thời gian giao dịch của người sử dụng.

*f. Các tiêu chuẩn cho ví tiền điện tử*

Tiêu chuẩn được đề ra bởi W3C (World wide web consortium). W3C đang nỗ lực để tạo ra phương pháp có thể mở rộng thông tin về các thanh toán nhỏ được ghi vào các trang web: hệ thống mở rộng này sẽ cho phép việc cải thiện hệ thống mà không cần phải bỏ đi những việc đã làm trước đó. Những nhà kinh doanh phải chấp nhận một số phương pháp thanh toán khác nhau để đảm bảo số lượng độc giả lớn nhất có thể có:

Các nhà kinh doanh phải ghi vào trong trang web của họ những thông tin cụ thể của các phương pháp thanh toán nhất định. Phải hoạt động nhanh hơn để làm cho các phương pháp hiện thời không trở nên lạc hậu.

1. **Thẻ lưu giá trị**

Là thẻ có giá trị tiền tệ dùng để mua hàng và thường được nạp thêm tiền khi cần. Bao gồm các loại thẻ: Thẻ mua hàng sử dụng với một mục đích: thẻ mua hàng tại siêu thị, thẻ điện thoại, thẻ Internet...; Thẻ mua hàng sử dụng nhiều mục đích: dùng để mua hàng, rút tiền mặt, thanh toán tiền điện thoại, điện, nước...

1. **E-banking**



Ngân hàng điện tử được hiểu là các nghiệp vụ, các sản phẩm dịch vụ ngân hàng truyền thống trước đây được phân phối trên các kênh mới như Internet, điện thoại, mạng không dây… Hiện nay, ngân hàng điện tử tồn tại dưới hai hình thức: hình thức ngân hàng trực tuyến, chỉ tồn tại dựa trên môi trường mạng Internet, cung cấp dịch vụ 100% thông qua môi trường mạng; và mô hình kết hợp giữa hệ thống ngân hàng thương mại truyền thống và điện tử hoá các dịch vụ truyền thống, tức là phân phối những sản phẩm dịch vụ cũ trên những kênh phân phối mới. Ngân hàng điện tử tại Việt Nam chủ yếu phát triển theo mô hình này. hiện nay dịch vụ ngân hàng điện tử được các ngân hàng thương mại Việt Nam cung cấp qua các kênh chính sau đây: ngân hàng tại nhà (home-banking, Internet-banking); ngân hàng tự động qua điện thoại (Phone-banking, mobile banking); ngân hàng qua mạng không dây (Wireless-banking)…

**CHƯƠNG 6: AN NINH TRONG TMĐT**

1. **Vấn đề an ninh trực tuyến**

Vấn đề bảo mật, an ninh trên mạng là một trong những vấn đề nóng hổi trong hoạt động thực tiễn của Thương mại điện tử. Liệu khách hàng có tin tưởng khi thực hiện các giao dịch trên mạng không? Và liệu những nhà cung cấp dịch vụ giao dịch trực tuyến cũng như các ISP có bảo đảm đuợc những thông tin của khách hàng giao dịch trên mạng được an toàn không? Chúng ta sẽ làm sáng tỏ một số vấn đề sau để trả lời cho các câu hỏi trên

**Các loại tội phạm trên mạng**

Trên mạng máy tính internet hiện nay hàng ngày có rất nhiều vấn đề tội phạm tin học đã và đang xảy ra. Có một số loại tội phạm chính sau:

**Gian lận trên mạng** là hành vi gian lận, làm giả để thu nhập bất chính. Ví dụ sử dụngsố thẻ VISA giả để mua bán trên mạng.

**Tấn công Cyber** là một cuộc tấn công điện tử để xâm nhập trái phép trên internet vàomạng mục tiêu để làm hỏng dữ liệu, chương trình, và phần cứng của các website hoặc máy trạm.

**Hackers** (tin tặc): Hackers nguyên thuỷ là tiện ích trong hệ điều hành Unix giúp xâydựng Usenet, và Word Wide Web… Nhưng, dần dần thuật ngữ hacker để chỉ người lập trình tìm cách xâm nhập trái phép vào các máy tính và mạng máy tính

**Crackers**: Là người tìm cách bẻ khoá để xâm nhập trái phép vào máy tính hay cácchương trình

Các loại tấn công trên mạng:

1> Tấn công kỹ thuật là tấn công bằng phần mềm do các chuyên gia có kiến thức hệ thống giỏi thực hiện

2> Tấn công không kỹ thuật là việc tìm cách lừa để lấy được thông tin nhạy cảm

3> Tấn công làm từ chối phục vụ (Denial-of-service (DoS) attack) là sử dụng phải đặc biệt liên tục gửi đến máy tính mục tiêu làm nó bị quá tải, không thể phục vụ được

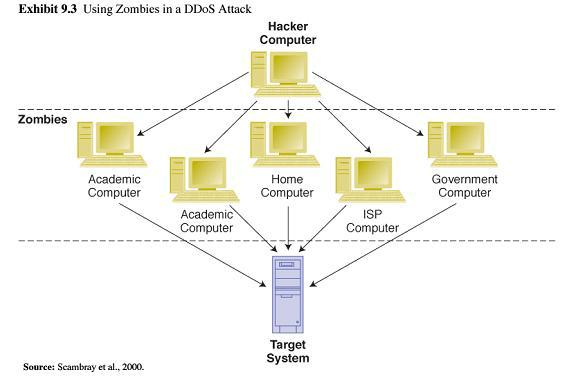
4> Phân tán cuộc tấn công làm từ chối phục vụ (Distributed denial of service (DDoS) attack) là sự tấn công làm từ chối phục vụ trong đó kẻ tấn công có quyền truy cập bất hợp pháp vào vào nhiều máy trên mạng để gửi số liệu giả đến mục tiêu

5>Virus là đoạn mã chương trình chèn vào máy chủ sau đó lây lan. Nó không chạy độc lập

6> Sâu Worm là một chương trình chạy độc lập. Sử dụng tài nguyên của máy chủ để lan truyền thông tin đi các máy khác

Các cuộc tấn công tin tặc trên mạng ngày càng tăng trên mạng Internet và ngày càng đa dạng vì trên mạng hiện giờ là thông tin và tiền. Các nhân tố tác động đến sự ra tăng tin tặc là sự phát triển mạnh TMĐT và nhiều lỗ hổng công nghệ của các website.

Mô hình tin tặc phân tán cuộc tấn công làm từ chối phục vụ



1. **An ninh trên máy trạm**

Làm sao biết được Web server được sở hữu bởi một doanhnghiệp hợp pháp? Làm sao biết được trang web này không chứa đựng những nội dung bảo cho người có quyền này được truy tặc là sự phát triển mạnh của TMĐT và nhiều lỗ hổng công nghệ của các website hay mã chương trình nguy hiểm? Làm sao biết được Web server không lấy thông tin của mình cung cấp cho bên thứ 3

1. **An ninh trên máy chủ:**

Làm sao biết được người sử dụng không có ý định phá hoạihoặc làm thay đổi nội dung của trang web hoặc website? Làm sao biết được làm gián đoạn hoạt động của server.

1. **An ninh trên kênh truyền**

Làm sao biết được không bị nghe trộm trên mạng? Làm sao biết đượcthông tin từ máy chủ đến user không bị thay đổi?

Một số khái niệm về an toàn bảo mật hay dùng trong TMĐT

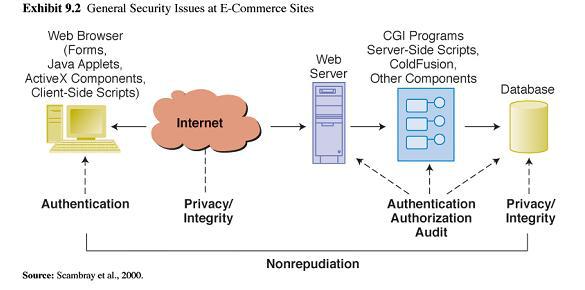
*Quyền được phép (Authorization):* Quá trình đảm bảo cho người có quyền này được truycập vào một số tài nguyên của mạng

*Xác thực(Authentication):* Quá trình xác thực một thực thể xem họ khai báo với cơ quanxác thực họ là ai

*Auditing*: Quá trình thu thập thông tin về các ý đồ muốn truy cập vào một tài nguyênnào đó trong mạng bằng cách sử dụng quyền ưu tiên và các hành động ATBM khác

*Sự riêng tư: (Confidentiality/privacy)* là bảo vệ thông tin mua bán của người tiêu dùng

Tính toàn vẹn (Integrity): Khả năng bảo vệ dữ liệu không bị thay đổi Không thoái thác (Nonrepudiation): Khả năng không thể từ chối các giao dịch đã thực hiện



Các vấn đề an toàn bảo mật của một website TMĐT

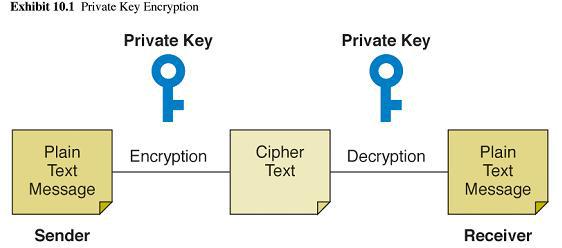
Có rất nhiều giải pháp công nghệ và không công nghệ để đảm bảo an toàn bảo mật trên mạng. Một trong những giải pháp quan trọng ứng dụng trong TMĐT là sử dụng kỹ thuật mật mã và các giao thức bảo mật

**Cơ chế mã hóa**

Để đảm bảo an toàn bảo mật cho các giao dịch, người ta dùng hệ thống khoá mã và kỹ thuật mã hoá cho các giao dịch TMĐT. Mã hoá là quá trình trộn văn bản với khoá mã tạo thành văn bản không thể đọc được truyền trên mạng. Khi nhận được bản mã, phải dùng khóa mã để giải thành bản rõ. Mã hoá và giải mã gồm 4 thành phần cơ bản: 1> Văn bản rõ – plaintext 2> Văn bản đã mã – Ciphertext 3> Thuật toán mã hoá - Encryption algorithm 4> Khoá mã – Key — là khoá bí mật dùng nó để giải mã thông thường. Mã hoá là tiền đề cho sự thiết lập các vấn đề liên quan đến bảo mật và an ninh trên mạng.

Có hai phương pháp mã hóa phổ biến nhất: *phương pháp mã đối xứng (*khóa riêng):

dùng để mã và giải mã điện rõ, các người gửi và người nhận đều sử dụng văn bản



Mã hóa dùng khóa riêng

Mã không đối xứng (mã công cộng): sử dụng một cặp khoá: công cộng và riêng, khoá công cộng để mã hoá và khoá riêng để giải mã. Khi mã hoá người ta dùng hai khoá mã hoá riêng rẽ được sử dụng. Khoá đầu tiên được sử dụng để trộn các thông điệp sao cho nó không thể đọc được gọi là khoá công cộng. Khi giải mã các thông điệp cần một mã khoá thứ hai, mã này chỉ có người có quyền giải mã giữ hoặc nó được sử dụng chỉ bởi người nhận bức thông điệp này, khoá này gọi là khoá riêng.

Ðể thực hiện các công việc mã hoá và giải mã, cần một cơ quan trung gian giữ các khoá riêng, đề phòng trường hợp khoá này bị mất hoặc trong trường hợp cần xác định người

gửi hoặc người nhận. Các công ty đưa ra các khoá mã riêng sẽ quản lý và bảo vệ các khoá này và đóng vai trò như một cơ quan xác định thẩm quyền cho các mã khoá bảo mật.

**Chứng thực số hóa**

Chứng thực số để xác nhận rằng người giữ các khoá công cộng và khoá riêng là ai đã đăng ký. Cần có cơ quan trung gian để làm công việc xác thực. Chứng thực có các cấp độ khác nhau.

Không phải tất cả các mã khoá riêng hay các chứng chỉ số hoá đều được xây dựng như nhau. Loại đơn giản nhất của giấy chứng chỉ hoá được gọi là chứng nhận Class 1, loại này có thể dễ dàng nhận khi bất kỳ người mua nào truy nhập vào WEB site của VeriSign[www.verisign.com](http://www.verisign.com/)) . Tất cả những cái mà doanh nghiệp phải làm là cung cấp tên, địa chỉ và địa chỉ e-mail, sau khi địa chỉ e-mail được kiểm tra, sẽ nhận được một giấy chứng nhận số hoá. Về mặt nào đó nó cũng giống như một thẻ đọc thư viện.

Các chứng nhận Class 2 yêu cầu một sự kiểm chứng về địa chỉ vật lý của doanh nghiệp, Ðể thực hiện điều này các công ty cung cấp chứng nhận sẽ tham khảo cơ sở dữ liệu của Equifax hoặc Experian trong trường hợp đó là một người dùng cuối và Dun&Bradstreet trong trường hợp đó là một doanh nghiệp. Quá trình này giống như là một thẻ tín dụng. Mức cao nhất của một giấy chứng nhận số hoá được gọi là chứng nhận Class 3. Có thể xem nó như là một giấy phép lái xe. Ðể nhận được nó doanh nghiệp phải chứng minh chính xác mình là ai và phải là người chịu trách nhiệm. Các giấy phép lái xe thật có ảnh của người sở hữu và được in với các công nghệ đặc biệt để tránh bị làm giả.

Các giấy chứng nhận Class 3 hiện chưa được chào hàng, tuy nhiên các công ty hoạt động trong lĩnh vực an toàn và bảo mật đã mường tượng ra việc sử dụng nó trong tương lai gần cho các vấn đề quan trọng như việc đàm phán thuê bất động sản qua WEB hoặc vay vốn trực tuyến. Nó cũng có thể được sử dụng như là các chứng nhận định danh hợp pháp hỗ trợ việc phân phát các bản ghi tín dụng hoặc chuyển các tài liệu của toà án. Hiện tại các biểu mẫu thu nhận thông tin thanh toán trên WEB thường đạt chứng nhận an toàn và bảo mật Classs 1, nhưng hiện tại một số cửa hàng trên WEB cũng đã đạt mức an toàn và bảo mật Class 2 và khách hàng cũng đã bắt đầu nhận được chúng thông qua một công nghệ được gọi là SET.

**Một số giao thức bảo mật thông dụng**

**Cơ chế bảo mật SSL (Secure Socket Layer)**

Về mặt lý thuyết rất nhiều công ty có thể đóng vai trò như một cơ quan chứng thực thẩm quyền. VeriSign Inc (www.verisign.com), là công ty cung cấp dịch vụ về chứng thực số dẫn đầu tại Mỹ. Công ty này sử dụng bản quyền về công nghệ từ RSA Inc. (www.rsa.com). RSA giữ đăng ký sáng chế về công nghệ mã khoá riêng/công cộng được

giới thiệu vào năm 1976 củaWhitfield Diffie và Martin Hellman và nó được chuyển giao cho VeriSign vào năm 1995 cho dù các công ty khác cũng giữ quyền sử dụng nó. Để bảo mật, doanh nghiệp phải mua một khoá riêng từ VeriSign thu phí 349 USD/ năm cho một WEB site thương mại với một khoá bảo mật như vậy và phí để bảo dưỡng hàng năm là 249 USD, doanh nghiệp có thể mua thêm khoá bảo mật với mức giá tương đương.

Sau khi máy chủ nhận được một khoá mã bảo mật, việc tiếp nhận một đơn đặt hàng trở nên đơn giản. "Ðiểm nổi bật của SSL ta có thể ngay lập tức tạo một trang HTML với các biểu mẫu để khách hàng cung cấp thông tin về họ trong lúc giao dịch, và đảm bảo rằng các thông tin này được bảo mật và mã hoá khi được gửi đi trên Internet" .

Sau khi các thông tin mà khách hàng nhập vào các biểu mẫu trên trang WEB hiển thị trên trình duyệt của họ được mã hoá với SSL nó được gửi đi trên Internet một cách an toàn. Trong thực tế khi người sử dụng truy nhập vào các trang WEB được hỗ trợ bởi SSL, họ sẽ thấy một biểu tượng như một chiếc khoá ở thanh công cụ bên dưới chương trình

**Cơ chế bảo mật SET**

Tiêu chuẩn bảo mật mới nhất trong thương mại điện tử là SET viết tắt của Secure Electronic Transaction-Giao dịch điện tử an toàn, được phát triển bởi một tập đoàn các

công ty thẻ tín dụng lớn như Visa, MasterCard và American Express, cũng như các nhà băng, các công ty bán hàng trên mạng và các công ty thương mại khác. SET có liên quan với SSL do nó cũng sử dụng các khoá công cộng và khoá riêng với khoá riêng được giữ bởi một cơ quan chứng nhận thẩm quyền. Không giống như SSL, SET đặt các khoá riêng trong tay của cả người mua và người bán trong một giao dịch. Ðiều đó có nghĩa là một người sử dụng thông thường cần các khoá riêng của họ và cần phải đăng ký các khoá này cũng giống như các máy chủ phải làm. Dưới đây là cách mà hệ thống này làm việc. Khi một giao dịch SET được xác nhận quyền sử dụng, mã khoá riêng của người sử dụng sẽ thực hiện chức năng giống như một chữ ký số, để chứng minh cho người bán về tính xác thực của yêu cầu giao dịch từ phía người mua và các mạng thanh toán công cộng. Trong thực tế nó giống như là việc ký vào tờ giấy thanh toán trong nhà hàng. Chữ ký số chứng minh là ta đã ăn thịt trong món chính và chấp nhận hoá đơn.

Do người mua không thể thoát ra khỏi một giao dịch SET, để khiếu nại về việc họ không mua hàng nên các giao dịch SET theo lý thuyết sẽ chạy qua các hệ thống thanh toán giống như ta mua hàng ở thiết bị đầu cuối tại các cửa hàng bách hóa thực.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CHƯƠNG 7: QUY ĐỊNH PHÁP LUẬT VỀ TMĐT**   1. **Quy định pháp luật về TMĐT**    1. Khái niệm về pháp luật thương mại điện tử   Khái niệm về pháp luật thương mại điện tử như sau:  *“Pháp luật thương mại điện tử là tổng hợp các nguyên tắc, quy phạm pháp luật do Nhà nước ban hành điều chỉnh các quan hệ xã hội phát sinh trong quá trình các chủ thể là các cá nhân, tổ chức thực hiện các hoạt động thương mại được thực hiện một phần hay toàn bộ quy trình thương mại bằng các phương tiện điện tử có kết nối với mạng internet, mạng viễn thông di động hay các mạng mở khác”.*  Như vậy, với khái niệm như trên, các quan hệ xã hội phát sinh trong hoạt động thương mại điện tử đều được pháp luật điều chỉnh và đảm bảo được lợi ích nhà nước, quyền và lợi ích hợp pháp của các chủ thể tham gia hoạt động thương mại điện tử.  **1.2 Pháp luật về thương mại điện tử trên thế giới**  **\* Các tổ chức Quốc tế**   * UNCITRAL - Ủy ban của LHQ về Luật Thương mại Quốc tế: đưa ra Luật mẫu về Thương mại điện tử vào năm 1996 làm khung hướng dẫn cho các nước xây dựng các đạo luật về thương mại điện tử. * OECD - Tổ chức Hợp tác và Phát triển Kinh tế: nghiên cứu, điều tra một số lĩnh vực của Thương mại điện tử như thuế, bảo vệ người tiêu dùng và riêng tư cá nhân, tác động của ICT đến tăng trưởng kinh tế * WIPO - Tổ chức Bảo vệ Sở hữu trí tuệ: về các lĩnh vực bản quyền, nhãn hiệu thương mại và các vấn đề liên quan đến tên miền * ICANN - giải quyết các tranh chấp về tên miền quốc tế * WTO - giải quyết các vấn đề liên quan đến rào cản thương mại điện tử quốc tế   **\* Các nước trên thế giới và khu vực**   * EU: Năm 2000 đưa ra hướng dẫn chung về thương mại điện tử “Directive on electronic commerce” * US: UETA - Luật giao dịch điện tử thống nhất (Uniform Electronic Transactions Act) * Canada: Luật giao dịch điện tử * Australia: Luật giao dịch điện tử các bang * Singapore: Luật giao dịch điện tử, năm 1998   **1.2.1 Luật mẫu của UNCITRAL về thương mại điện tử**  Nhằm tạo khung pháp lý cho phát triển thương mại điện tử, năm 1996 Uỷ ban Luật Thương mại quốc tế của Liên hợp quốc (UNCITRAL) đã soạn thảo một luật mẫu về thương mại điện tử, hình thành những quy định mẫu về thừa nhận giá trị pháp lý của các thông điệp dữ liệu nhằm bảo vệ về mặt pháp lý cho những tổ chức, cá nhân mong muốn tham gia thương mại điện tử. Luật mẫu có thể được sử dụng như một tài liệu tham khảo cho các nước trong quá trình xây dựng pháp luật về thương mại điện tử của mình. Tinh thần của Luật mẫu là bảo đảm những giao dịch thương mại điện tử được thừa nhận giá trị pháp lý và nếu cần thiết thì sẽ có những hành động thích hợp để tăng cường khả năng thi hành cho những giao dịch bằng phương tiện điện tử. Luật mẫu được soạn thảo dựa trên những nguyên tắc cơ bản sau:   * Tài liệu điện tử có thể được coi là có giá trị pháp lý như tài liệu ở dạng văn bản nếu thoả mãn các yêu cầu kỹ thuật nhất định; * Tự do thoả thuận hợp đồng; * Tôn trọng việc sử dụng tự nguyện phương thức truyền thông điện tử; * Giá trị pháp lý của hợp đồng và tính ưu việt của những quy định pháp lý về hình thức hợp đồng; những đòi hỏi đối với hợp đồng để có giá trị pháp lý và khả năng được thi hành phải được tôn trọng; * Áp dụng về mặt hình thức hơn là quan tâm tới nội dung : luật chỉ áp dụng đối với hình thức hợp đồng mà không đề cập nội dung, trên cơ sở phải thoả mãn những đòi hỏi pháp lý nhất định; * Pháp luật về bảo vệ người tiêu dùng phải đi trước. Nhiều quốc gia đã thể hiện các nguyên tắc và nội dung của luật mẫu UNCITRAL vào hệ thống pháp luật quốc gia của nước mình.   **1.2.2. Luật thương mại điện tử của một số nước trên thế giới**  Xây dựng khung pháp lý cho TMĐT là việc rất cấp thiết. Để hỗ trợ các hoạt động TMĐT, nhiều nước trên thế giới đều đã xây dựng khung pháp lý riêng, dựa trên những khái niệm và những nguyên tắc cơ bản của bộ luật mẫu về Thương mại điện tử của Uỷ Ban Pháp luật thương mại quốc tế - Liên hợp quốc (UN Commision on International Trade Law - UNCITRAL) soạn thảo năm 1996. Bộ luật mẫu này cung cấp các nguyên tắc có tính quốc tế, giải quyết một số trở ngại, nhằm tạo ra môi trường an toàn về pháp lý cho các hoạt động thương mại điện tử.  Biểu 2.  **Khung pháp lý cho các hoạt động TMĐT của một số nước trên thế giới**   |  |  | | --- | --- | | **Nước**  Australia | **Một số văn bản pháp lý**  Luật giao dịch điện tử năm 1999 (căn cứ trên luật mẫu về TMĐT của UNCITRAL) quy định các nghĩa vụ pháp lý với việc phát hành đối với phương tiện điện tử | | Nhật Bản | Hàng loạt luật liên quan đến công nghệ thông tin ban hành trong năm 2000 công nhận tính hiệu lực của việc chuyển các văn bản bằng phương tiện điện tử. Luật về chữ ký điện tử và tổ chức chứng thực điện tử của Nhật Bản cũng được ban hành ngày 25/5/2000. | | Trung Quốc | Luật hợp đồng thừa nhận tính hiệu lực của các hợp đồng điện tử | | Đặc khu Hongkong | Ngày 7/1/2000, Hồng Kông đã ban hành pháp lệnh giao dịch điện tử. Văn bản này có quy định về chữ ký điện tử, bản ghi điện tử và được áp dụng rộng rãi cho mọi hoạt động truyền thông, công nhận tính pháp lý của các giao dịch điện tử. | | Hàn Quốc | Hàn Quốc có Luật Chữ ký điện tử vào năm 1999 và sửa đổi vào năm 2001 | | Mehico | Nghị định về TMĐT được thông qua năm 2000 | | New Zealand | Luật Giao dịch điện tử (căn cứ vào luật mẫu về TMĐT của UNCITRAL) ban hành năm 1998, xác định quyền và nghĩa vụ của các bên tham gia vào một giao dịch điện tử. Luật cũng quy định việc cấp phép qua thiết bị điện tử đối với khu vực công cộng và trách nhiệm của các nhà cung cấp dịch vụ thuộc bên thứ ba. Cơ chế giải quyết tranh chấp điện tử qua Internet được sử dụng để giải quyết tranh chấp | | Thái Lan | Luật Giao dịch điện tử của Thái Lan được thông qua vào tháng 10/2000 đã bao quát cả chữ ký điện tử. | | Mỹ | Áp dụng Luật thương mại chung  Áp dụng Luật Chuyển tiền điện tử đối với các sản phẩm lưu trữ giá trị dưới sự kiểm soát của Cục Dự trữ Liên bang.  Luật Giao dịch điện tử thống nhất thông qua năm 1999 thừa nhận tính bình đẳng của chữ ký điện tử và chữ ký viết tay. Các bang ban hành luật riêng dựa trên luật giao dịch điện tử thống nhất. | | Malaysia | Ngày 1/10/1998, Luật về chữ ký điện tử của Malaysia đã có hiệu lực. | | Singapore | Ngày 29/6/1998, Luật giao dịch điện tử của Singapore đã ra đời quy định về chữ ký điện tử, chữ ký số cũng như bản ghi điện tử. | | Philipines | Luật Thương mại điện tử của Philipines ban hành ngày 14/6/2000 đã điều chỉnh về chữ ký điện tử, giao dịch điện tử và tội phạm liên quan tới thương mại điện tử. | | Brunei | Luật Giao dịch điện tử của Brunei được ban hành tháng 11/2000 bao quát đến vấn đề hợp đồng điện tử cũng như chữ ký điện tử và chữ ký số. | | Ấn Độ | Luật về công nghệ thông tin của Ấn Độ được thi hành từ tháng 10/2000 quy định về chữ ký số và bản ghi điện tử. |   **1.3 Khuôn khổ pháp lý cho thương mại điện tử ở Việt Nam**  Cùng với hệ thống pháp luật chung, các văn bản pháp luật liên quan đến thương mại điện tử cũng bước đầu được hình thành và dần hoàn thiện.  **1.3.1. Luật giao dịch điện tử**  Luật Giao dịch điện tử được Quốc hội khoá XI, kỳ họp thứ 8 thông qua ngày 29/11/2005 và có hiệu lực từ ngày 1/03/2006. Luật gồm 8 chương, 54 điều quy định về thông điệp dữ liệu, chữ ký điện tử và chứng thực chữ ký điện tử, giao kết và thực hiện hợp đồng điện tử, giao dịch điện tử của cơ quan nhà nước, an ninh, an toàn, bảo vệ, bảo mật trong giao dịch điện tử, giải quyết tranh chấp và xử lý vi phạm trong giao dịch điện tử. Phạm vi điều chỉnh chủ yếu của Luật là giao dịch điện tử trong hoạt động của các cơ quan nhà nước, trong lĩnh vực dân sự, kinh doanh, thương mại.  Luật Giao dịch điện tử nhấn mạnh nguyên tắc tiến hành giao dịch điện tử là tự nguyện, được tự thoả thuận về việc lựa chọn công nghệ để thực hiện giao dịch, trung lập về công nghệ, bảo đảm sự bình đẳng và an toàn.  Chữ ký điện tử là một nội dung được đề cập đến trong Luật Giao dịch điện tử. Luật công nhận giá trị pháp lý của chữ ký điện tử, nêu lên nghĩa vụ của bên ký, bên chấp nhận chữ ký và tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử và dành hẳn một chương đề cập đến giao dịch điện tử của cơ quan Nhà nước.  **1.3.2 Luật thương mại**  Luật Thương mại (sửa đổi) được Quốc hội khoá XI, kỳ họp thứ 7 thông qua ngày 14/06/2005 và có hiệu lực từ ngày 1/01/2006 là văn bản pháp lý làm nền tảng cho các hoạt động thương mại, trong đó có thương mại điện tử. Điều 15 của Luật quy định “Trong hoạt động thương mại, các thông điệp dữ liệu đáp ứng các điều kiện, tiêu chuẩn kỹ thuật theo quy định của pháp luật thừa nhận có giá trị pháp lý tương đương văn bản”. Ngoài ra, tại khoản 4, Điều 120 (các hình thức trưng bày, giới thiệu hàng hoá, dịch vụ), trong đó coi “Trưng bày, giới thiệu hàng hoá, dịch vụ trên Internet” là một hình thức trưng bày, giới thiệu hàng hoá, dịch vụ.  **1.3.3 Bộ luật dân sự**  Tại khoản 1, điều 124 “Hình thức giao dịch dân sự” của Bộ luật dân sự (Quốc hội khoá XI, kỳ họp thứ 7 thông qua ngày 14/06/2005 và có hiệu lực từ ngày 1/01/2006) quy định “Giao dịch dân sự thông qua phương tiện điện tử dưới hình thức thông điệp dữ liệu được coi là giao dịch bằng văn bản”. Bộ luật Dân sự đưa ra quy định cụ thể về các trường hợp giao kết, sửa đổi, thực hiện, huỷ bỏ hợp đồng. Theo đó, thời điểm giao kết hợp đồng là thời điểm bên đề nghị nhận được trả lời chấp nhận giao kết. Địa điểm giao kết hợp đồng dân sự do các bên thoả thuận, nếu không có thoả thuận thì địa điểm giao kết hợp đồng dân sự là nơi cư trú của cá nhân hoặc trụ sở của pháp nhân đã đưa ra đề nghị giao kết hợp đồng. Đây là những khái niệm quan trọng cần tính đến khi xây dựng các văn bản pháp luật liên quan đến giao kết và thực hiện hợp đồng trong môi trường điện tử  **1.3.4. Luật Hải quan**  Luật Hải quan (sửa đổi) được Quốc hội khoá XI, kỳ họp thứ 7 thông qua ngày 14/06/2005 và có hiệu lực từ ngày 1/01/2006 có bổ sung một số quy định về trình tự khai hải quan điện tử, địa điểm khai, hồ sơ hải quan điện tử, thủ tục hải quan đối với hàng hoá xuất nhập khẩu bằng Thương mại điện tử.  **1.3.5. Luật sở hữu trí tuệ**  Luật sở hữu trí tuệ được Quốc hội khoá XI, kỳ họp thứ 8 thông qua ngày 29/11/2005 và có hiệu lực từ ngày 1/07/2006 thể hiện một bước tiến trong việc hoàn thiện hệ thống văn bản pháp luật bảo hộ quyền sở hữu trí tuệ. Luật Sở hữu trí tuệ có một số điều khoản liên quan đến thương mại điện tử như quy định về các hành vi bị xem là xâm phạm quyền tác giả, quyền liên quan trong môi trường điện tử như cố ý huỷ bỏ, thay đổi thông tin quản lý quyền dưới hình thức điện tử có trong tác phẩm, dỡ bỏ hoặc thay đổi thông tin quản lý quyền dưới hình thức điện tử mà không được phép của chủ sở hữu quyền liên quan. Tuy không có quy định cụ thể liên quan đến lĩnh vực thương mại điện tử, nhưng các nguyên tắc trong Luật Sở hữu trí tuệ có thể áp dụng đối với lĩnh vực này.  **1.3.6 Một số văn bản pháp luật khác**  Bên cạnh Luật Thương mại, Luật Giao dịch điện tử và Bộ luật Dân sự, có một số văn bản khác cũng đề cập đến thương mại điện tử như :   * Quyết định số 27/2005/QĐ-BBCVT do Bộ trưởng Bộ Bưu chính – Viễn thông ký và ban hành ngày 11/08/2005 quy định về quản lý và sử dụng tài nguyên Internet. * Thông tư liên tịch số 02/2005/TTLT-BCVT-VHTT-CA-KHĐT ngày 14/07/2006 về quản lý đại lý Internet * Ngoài ra, Luật Công nghệ thông tin và Nghị định về thương mại điện tử cũng đang khẩn trương được xây dựng, tạo cơ sở pháp lý cho thương mại điện tử phát triển  |  |  | | --- | --- | | **Các yêu cầu pháp lý cho việc phát triển thương mại điện tử** | | | 370_ | **Sự phát triển của Thương mại điện tử trên thế giới đã làm thay đổi cách thức kinh doanh, giao dịch truyền thống và đem lại những lợi ích to lớn cho xã hội.** | | |  | | --- | | Tuy nhiên bên cạnh đó cũng phải thừa nhận rằng những rủi ro gặp phải trong quá trình giao dịch, kinh doanh trên mạng là hiện thực và việc này đòi hỏi phải có các giải pháp không chỉ về mặt kỹ thuật mà còn cần phải hình thành được một cơ sở pháp lý đầy đủ. | | |  1. **Sở hữu trí tuệ**   Theo Tổ chức trí tuệ thế giới (WIPO – World Intellectual Property Organization), sở hữu trí tuệ thuộc về “các sáng tạo của trí tuệ: phát minh, các tác phẩm văn hóa và nghệ thuật, các biểu tượng, tên, hình ảnh và thiết kế được sử dụng trong thương mại.” Trong khi bảo vệ bí mật cá nhân là mối quan tâm lớn đối với các cá nhân, thì bảo vệ sở hữu trí tuệ là mối quan tâm trước hết đối với những ai có tài sản trí tuệ. Quyền sở hữu trí tuệ là một trong các nền tảng của xã hội hiện đại. Thiếu các quyền này, thì các ngành công nghiệp phim ảnh, âm nhạc, phần mềm, xuất bản, dược và các ngành công nghiệp sinh học sẽ trì trệ không phát triển được. Có bốn loại sở hữu trí tuệ chính trong TMĐT: Bản quyền, nhãn hiệu thương mại, tên miền và bằng phát minh.  a, Bản quyền (Copyrights)  Một bản quyền là một văn bản công nhận duy nhất của nhà nước cấp cho chủ nhân của nó có độc quyền đối với việc: (1), sao chép sản phẩm, một phần hoặc toàn bộ; (2), phân phối, thể hiện, trình diễn sản phẩm ở dạng thức công chúng hoặc bất kỳ dạng thức nào, kể cả trên Internet. Nói chung, chủ sở hữu cũng có quyền xuất khẩu tác phẩm đến các quốc gia khác.  Các loại công trình sau đây thường có bản quyền:   * Các tác phẩm văn học (ví dụ sách và phần mềm máy tính); * Các tác phẩm âm nhạc (ví dụ bản nhạc) * Các tác phẩm sân khấu (ví dụ vở kịch) * Các tác phẩm nghệ thuật (ví dụ bản vẽ, tranh…) * Các bản ghi âm, cuốn phim, chương trình phát thanh, truyền hình, chương trình truyền hính cap.   Trên Web, bản quyền cũng có thể được sử dụng để bảo vệ hình ảnh, logo, văn bản, HTML, JavaScript và các tài liệu khác.  Nguy cơ lớn nhất đối với sở hữu trí tuệ là nạn ăn cắp cá nhân với quy mô lớn. Hàng chục triệu người sử dụng Internet để tải bất hợp pháp nhạc, video, trò chơi, phần mềm, phim và các sản phẩm số khác.  Có nhiều hiệp định quốc tế bảo vệ bản quyền toàn cầu. Trong số này, Hiệp ước Becnơ (Bern Convention) là một trong số các thỏa thuận quan trọng nhất. Hiệp ước Becnơ được ký từ năm 1886. Hiện nay Hiệp ước được quản lý bởi WIPO và được hỗ trợ bởi 90% các quốc gia trên thế giới.  Người sở hữu bản quyền có thể tìm kiếm được lệnh của tòa án nhằm ngăn cản hoặc làm dừng lại sự xâm phạm hoặc tuyên bố thiệt hại. Một số loại xâm phạm bản quyền có thể kéo theo trách nhiệm hình sự. Ví dụ: Sản xuất mang tính thương mại công trình xâm phạm, bán các tác phẩm xâm phạm, đưa các tác phẩm xâm phạm vào mua bán, kinh doanh, sản xuất và bán công nghệ phá hủy các hệ thống bảo vệ bản quyền.  Bản quyền không kéo dài mãi mãi, nó có hiệu lực trong một số thời gian nhất định sau khi chủ sở hữu qua đời (ở Anh là 50 năm, ở Mỹ là 70 năm). Sau khi kết thúc thời hạn đó, tác phẩm trở thành sở hữu công cộng. *\* Sao chụp bất hợp pháp phần mềm, bản nhạc và các tư liệu số khác*  Nạn sao chụp bất hợp pháp các tư liệu số hóa đang đe dọa các ngành công nghiệp phần mềm, âm nhạc và phim ảnh. Theo Weis (2004), thiệt hại dosao chụp bất hợp pháp phần mềm trên thế giới lên tới 29 tỷ đôla năm 2003 (chiếm tới 36% doanh thu phần mềm).  Ở Mỹ, sao chụp bất hợp pháp phần mềm chiếm tới 22% tổng doanh thu phần mềm, trong khi đó ở Trung Quốc và Việt Nam là 92%.  Các quốc gia đã có nhiều hoạt động pháp lý và hành động thực tế để giải quyết vấn đề nói trên. Tuy nhiên, cho đến nay các hành động trên còn tỏ ra thiếu hiệu quả. *\* Một số cách tiếp cận trong bảo vệ bản quyền*  Có thể sử dụng phần mềm để sản xuất nội dung số không sao chép được. Các cách tiếp cận sau đây có thể được sử dụng để thiết kế hệ thống quản lý bản quyền điện tử một cách có hiệu quả:   * Sử dụng mã hóa để ngăn cản xâm phạm bản quyền; * Theo dõi sự xâm phạm bản quyền; * Sử dụng phương pháp “ngấn nước”, hay “hình mờ” (watermark).  *\* Quản trị bản quyền số*  Quản trị bản quyền số là một thuật ngữ chung, muốn nói đến các sắp xếp cho phép một người bán nội dung ở hình thái điện tử có thể kiểm soát tư liệu và ngăn cấm việc sử dụng chúng với các cách thức khác nhau, và có thể xác định được việc sử dụng đó. Thông thường, nội dung là một tác phẩm số hóa có bản quyền mà người bán là người chủ sở hữu quyền. Các sắp xếp đó được gọi là các biện pháp kỹ thuật.  Trong quá khứ, khi nội dung về bản chất là một *vật tương tự (analog)*, và việc mua một bản sao mới của tác phẩm bản quyền là dễ hơn so với sản xuất bản sao đó một cách độc lập. Chất lượng của phần lớn bản sao thường thấp, điều này làm cho quá trình sao chép ít hấp dẫn, và trong phần lớn trường hợp là ít hiệu quả. Tình hình đã thay đổi với sự xuất hiện của công nghệ số. Công nghệ này tạo ra khả năng tạo ra các bản sao chất lượng cao với chi phí không lớn. Internet gần như loại bỏ sự cần thiết phải có môi trường vật lý trung gian để truyền tải tác phẩm. Do vậy, các hệ thống Quản trị bản quyền số cần phải giới hạn các cá nhân sử dụng hợp lý, minh bạch (fair use) tài liệu số (sử dụng cho các mục đích phi thương mại). ***b, Nhãn hiệu thương mại (Trademarks)***  Nhãn hiệu thương mại là biểu tượng được doanh nghiệp sử dụng để phân biệt hàng hóa và dịch vụ của họ với hàng hóa và dịch vụ của doanh nghiệp khác.  Biểu tượng có thể được cấu trúc từ các từ, các hình vẽ. các chữ cái, các hình mẫu, một sự kết hợp màu sắc, và các yếu tố có thể phân định khác.  Nhãn hiệu thương mại cần được đăng ký tại một quốc gia để được luật pháp bảo vệ. Để được dăng ký, nhãn hiệu thương mại cần khác biệt (distinctive), nguyên bản và không gây nhầm lẫn. Một khi đã được đăng ký, nhãn hiệu thương mại có thể tồn tại mãi mãi, đồng thời với việc phí đăng ký được trả.  Chủ nhân của một nhãn hiệu thương mạicó độc quyền:   * Sử dụng nhãn hiệu thương mại đối với các hàng hóa và dịch vụ mà nhãn hiệu được đăng ký đối với chúng. * Tiến hành các hoạt động hợp pháp nhằm ngăn ngừa bất kỳ người nào đó sử dụng nhãn hiệu cho các hàng hóa và dịch vụ giống hoặc tương tự với hàng hóa và dịch vụ mà nhãn hiệu đã được đăng ký mà không có sự đồng ý của chủ nhân nhãn hiệu.   Trên Internet, hàng hóa và sản phẩm thương hiệu giả có thể được bán và đấu giá từ bất kỳ đâu. Việc xâm phạm nhãn hiệu thương mại có thể kèm theo trách nhiệm hình sự. Đặc biệt, được coi là tội phạm một ai đó sử dụng bất hợp pháp nhãn hiệu thương mại đã được đăng ký, bao gồm việc bán và nhập khẩu hàng hóa mang nhãn hiệu đánh cắp, hoặc sử dụng, hoặc có thiết bị làm giả nhãn hiệu.  ***c, Tên miền (Domain names)*** Một biến dạng của nhãn hiệu là tên miền. Tên miền là phần bậc cao của địa chỉ Internet (URL). Có hai tranh luận xung quanh tên miền. Thứ nhất, liệu có cần thêm vào tên miền bậc cao nhất (như .com, .org, .gov…) hay không. Thứ hai là việc sử dụng tên nhãn hiệu đã thuộc về các công ty khác làm tên miền hay không. Trong năm 2003 và 2004, tổ chức quản lý tên miền đã thông qua các tên miền bậc cao như sau: .biz, .name, .pro,.museum, .acro, .coop. Tên miền bậc quốc gia tồn tại ở phần lớn các nước (uk, ca, vn…). *Tranh chấp tên miền*  Tranh chấp về tên miền liên quan tới những tên miền cấp hai, chúng đề cập tới tên liền kề phía bên trái của tên miền cấp cao nhất trong địa chỉ Internet. Ví dụ, trong tên miền “www.microsoft.com”, tên miền cấp hai là Microsoft.  Hai tên miền cấp hai giống hệt nhau không thể cùng tồn tại dưới cùng một tên miền cấp một.  Ví dụ, mặc dù Công ty Delta Faucet và Delta Airlines đều muốn đặt tên miền là “delta.com”, nhưng chỉ có một công ty có thể có tên miền delta. Không may cho cả Công ty Delta Faucet và Delta Airlines, Công ty đã đặt tên miền là delta.com là Công ty tài chính Delta của Woodbury, có trụ sở tại Newyork. (Delta Airlines sử dụng tên miền deltaairlines.com trong khi công ty Delta Faucet sử dụng tên miền là Deltafaucet.com). *Một số ví dụ điển hình về tranh chấp về tên miền*  *Mcdonalds.com:* tên miền này đã bị đăng ký bởi một cá nhân viết bài cho tạp chí Wired, người này đã viết một câu chuyện về giá trị tên miền. Trong bài báo của mình, tác giả đã yêu cầu liên lạc với mình tại địa chỉ ronald@mcdonalds.com với đề nghị liên quan tới tên miền đó. Để dành lại tên miền MacDonalds, tác giả đã yêu cầu Công ty Mcdonalds phải có một khoản đóng góp từ thiện.  *Micros0ft.com:* Công ty Zero Micro Software, đã đăng ký tên miền micros0ft.com (với số không thay thế chữ o), nhưng việc đăng ký này đã bị đình chỉ sau khi Microsoft kiện công ty này. *Mtv.com:* tên miền MTV trước tiên đã bị đăng ký bởi Công ty Adam Curry cho trò chơi video MTV. MTV đầu tiên đã không quan tâm tới tên miền này trên Internet. Nhưng khi Adam Curry từ bỏ MTV, Công ty đã muốn kiểm soát tên miền. Sau khi vụ kiện ở liên bang được tiến hành, tranh chấp đã được giải quyết.  *Taiwan.com:* Tổ chức thông tin Trung Quốc ở lục địa Xinhua đã được phép đăng ký tên miền taiwan.com, trong sự bất bình của chính phủ Đài loan. *\* Đầu cơ tên miền (Cybersquatting)*  Đầu cơ tên miền là hoạt động đăng ký tên miền nhằm mục đích bán lại với giá cao hơn. Đạo luật bảo vệ người tiêu dùng năm 1999 đã nhằm tới những kẻ đầu cơ tên miền tiến hành đăng ký tên miền Internet của các công ty và người nổi tiếng rồi lấy đó làm con tin đòi tiền “chuộc” đối với cá nhân hoặc công ty. Các công ty như Christian Dior, Nike, Deutsche Bank, và ngay cả Microsoft cũng đã phải đấu tranh hoặc trả tiền để lấy lại tên miền tương ứng với tên của công ty mình.  Đầu cơ tên miền bị phán xét trên cả phương diện đạo đức và pháp lý. Trong quá khứ, nhiều cá nhân được hưởng quyền đăng ký tên miền liên quan đến các nhãn hiệu nổi tiếng.  Năm 1999, tại Mỹ đã đưa vào áp dụng Đạo luật Bảo vệ người tiên dùng chống đầu cơ tên miền (Anticybersquatting Consumer Protection Act). Đạo luật này cho phép chủ sở hữu của nhãn hiệu thương mại được kiện ra tòa vì các thiệt hại theo luật định. d, Bằng phát minh sáng chế (Patents) Bằng phát minh sáng chế là một văn bản cho phép chủ sở hữu độc quyền đối với phát minh trong một thời gian nhất định (ví dụ, ở Mỹ là 17 năm, ở Anh là 20 năm). Bằng phát minh sáng chế nhằm bảo vệ các phát minh công nghệ hữu hình, đặc biệt là trong các ngành công nghiệp truyền thống. Bằng phát minh sáng chế không giành cho sáng tạo văn học và nghệ thuật. Bằng phát minh sáng chế tạo nên độc quyền đối với một ý tưởng hoặc một phát minh, không phụ thuộc vào việc nó được thể hiện như thế nào. Một phát minh có thể là một thiết bị vật lý, một phương pháp hoặc một quá trình làm ra thiết bị vật lý.  Hàng ngàn bằng phát minh sáng chế liên quan đến IT đã được cấp bằng phát minh sáng chế trong những năm qua. Một số ví dụ về bằng phát minh sáng chế TMĐT đã được cấp cho Công ty Open Market Corp: bằng phát minh sáng chế Kiểm tra và Kiểm soát truy cập Internet (số 5708780); bằng phát minh sáng chế Các hệ thống bán hàng trên mạng (số 5715314), Hệ thống Quảng cáo tích cực số hóa (số 5724424). Google có bằng phát minh sáng chế 6296361 về phương pháp quảng cáo GoTo.com. Trên cơ sở các bằng phát minh sáng chế đã được cấp, nhiều công ty đã tiến hành kiện các công ty khác sử dụng các công nghệ hoặc ý tưởng của mình.  e, Các site hâm mộ (fan) và thù ghét (hate)  Các site hâm mộ (fan), hay thù ghét là một phần của hiện tượng tự xuất bản trên Internet, bao gồm việc tạo blog. Các site hâm mộ cố thể gây rắc rối đối với sở hữu trí tuệ. Ví dụ, một số người kiếm trước được bản sao các bộ phim hoặc chương trình TV mới và lập ra các site cạnh tranh với các site chính thức của nhà sản xuất phim hoặc chương trình TV. Mặc dù các nhà sản xuất có thể nhận được lệnh của tòa án đóng của các site như vậy, nhưng lập tức các site tương tự sẽ xuất hiện vào ngày hôm sau. Mặc dù ý định của các fan là tốt, nhưng họ có thể gây ra thiệt hại đối với các nhà sáng tạo tài sản trí tuệ.  Các site thù ghét cũng tạo nên những vấn đề đối với các công ty. Nhiều site thù ghét đã nhằm tới các công ty lớn (như Wal-Mart, Microsoft, Nike...). Liên kết với các site thù ghét là sự công kích (cybersbashing), đó là việc đăng ký một tên miền chuyên phê phán mọt tổ chức hoặc một cá nhân (ví dụ, walmartblows.com). Cho đến khi các site này chỉ chứa các lời công kích, không mang tính chất phỉ báng và bôi nhọ, chúng vẫn được phép hoạt động.  Các tư liệu được công bố ở các site hâm mộ hoặc thù ghét và các site nhóm tin tức  (newsgroups) có thể vi phạm bản quyền của các nhà sáng chế hoặc các nhà phân phối tài sản trí tuệ.  Điều này cho thấy sự gắn kết tiềm tàng giữa vấn đề bảo vệ sở hữu trí tuệ và vấn đề tự do ngôn luận.   1. **Tội phạm trong TMĐT**   Khi người mua và người bán không thể nhìn thấy nhau, và hơn nữa lại có thể ở các quốc gia khác nhau, có nhiều khả năng là những người không trung thực sẽ tiến hành nhiều kiểu gian lận và các hành vi tội phạm khác qua Internet. Theo FTC (Ủy ban thương mại liên bang, Mỹ - Federal Trade Commission),(ftc.gov), hơn 50% các đơn kiện về sự gian lận là liên quan đến Internet. Một báo cáo của sMarketer cho thấy trong năm 2004, các thương nhân kinh doanh trên Internet đã mất 2,6 tỷ USD (1,8% tổng doanh thu) do lừa đảo thanh toán trực tuyến. Nguy cơ tội phạm trực tuyến đã được cảnh báo tới khách hàng. Trong những năm đầu tiên của TMĐT, nhiều loại tội phạm đã xuất hiện, từ các mánh khóe liên quan đến giá cổ phiếu cho đến thành lập ngân hàng ảo biến mất cùng với tiền đầu tư của khách hàng.  Chúng ta xem xét vấn đề trên ba góc độ: sự gian lận trong TMĐT, bảo vệ người tiêu dùng và người bán hàng.  ***3.1 Sự gian lận trong TMĐT*** - *Sự gian lận trong đấu giá trực tuyến*  Theo số liệu của eMarketer, gian lận trong đấu giá trực tuyến chiếm tới khoảng 87% các sự kiện tội phạm trực tuyến *- Gian lận trong thị trường chứng khoán*  Trong phần lớn các trường hợp, các nhà xúc tiến cổ phiếu truyền các tin không đúng sự thật, mang tính phóng đại về tương lai của công ty mà chúng chào hàng. Trong các trường hợp khác, thông tin được cung cấp có thể là chính xác, nhưng các nhà xúc tiến lại che giấu họ đã được trả những gì để ca ngợi các công ty. *- Gian lận tài chính khác*  Chứng khoán chỉ là một trong số lĩnh vực mà ở đó những kẻ gian lận hoạt động tích cực. Các lĩnh vực khác bao gồm bán các đầu tư giả mạo, các cơ hội kinh doanh ma và nhiều kiểu khác. Bằng cách sử dụng Internet, các tội phạm tài chính có thể tiếp cận với rất nhiều người, chủ yếu qua thư điện tử. Hơn nữa, các mưu đồ bất lương liên quan đến trao đổi ngoại tệ trên Internet ngày càng tăng vì phần lớn các cửa hàng trao đổi ngoại tệ trực tuyến không được cấp giấy phép. *- Ăn cắp danh tính và phishing*  Trong một vài năm qua, vấn đề ăn cắp danh tính đã tăng tên. Ăn cắp danh tính thường được thực hiện nhờ thông tin không mong đợi từ các nạn nhân qua Internet. Ăn cắp danh tính là một hoạt động tội phạm, trong đó một người nào đó tự giới thiệu mình như một người khác, sử dụng số bảo hiểm xã hội cá nhân, số tài khoản ngân hàng và các thông tin định danh cá nhân khác để vay tiền, mua hàng, bán cổ phiếu…  Những kẻ tội phạm kiếm được thông tin bằng nhiều cách khác nhau. Ví dụ, chúng có thể sử dụng phần mềm gián điệp, hoặc *kỹ thuật phishing*. Một phương pháp phổ biến sử dụng phishing là thu thập thông tin qua các Website giả mạo. Ví dụ, một kẻ nào đó, tự nhận là đại diện của một ngân hàng hoặc công ty điện thoại, qua thư điện tử yêu cầu một người nào đó cập nhật thông tin cá nhân trên Website giả mạo giống hệt Website thực, rồi nhận được thư điện tử từ cá nhân đó. URL của Website giả mạo được cung cấp trong thư điện tử. Thư điện tử có thể cảnh báo rằng người nhận thư cần nhập thông tin, nếu không dịch vụ đối với họ có thể bị dừng lại. Để bảo vệ khỏi kiểu lừa đảo này, người dùng cần phải luôn luôn truy cập trực tiếp tới Website thực, không nên qua đường liên kết.  Microsoft và Amazon.com đã từng làm hồ sơ kiện lên tòa đối với một công ty Canada liên quan đến vụ việc công ty này đã gửi thư điện tử giả, mang danh đại diện của Microsoft và Amazon.com. Vào tháng 7 năm 2004, Đạo luật về Nâng cao sự trừng phạt đối với nạn ăn cắp danh tính (Identity Theft Penalty Enhancement Act) của Mỹ có hiệu lực, đưa ra các trừng phạt nặng đối với tội ăn cắp danh tính kết hợp với thực hiện các tội phạm khác (ví dụ ăn cắp tiến). Các nhà phê phán cho rằng luật chưa đầy đủ, vì không coi bản thân hoạt động phishing là một tội và không tạo ra các bảo vệ mới đối với các giao dịch trực tuyến.  Nhiều dạng gian lận phi tài chính cũng tồn tại trên mạng. Ví dụ, khách hàng có thể nhận được hàng hóa hoặc dịch vụ kém chất lượng, có thể nhận được hàng hóa không kịp thời, có thể phải thanh toán những khoản đáng ra người bán hàng phải trả….  ***3.2 Bảo vệ người tiêu dùng*** Bảo vệ người tiêu dùng là một trong các yếu tố quyết định thành công của bất kỳ loại hình thương mại nào, đặc biệt là TMĐT, nơi người mua không nhìn thấy người bán.  Về phía người tiêu dùng, để tự bảo vệ mình, khi tiến hành giao dịch điện tử cần lưu ý đến các vấn đề sau đây: - Người dùng cần tin tưởng rằng họ đang truy cập vào Website thực của các công ty nổi tiếng, kiểu như Wal-Mart, Disney, Amazon.com, bằng cách truy cập trực tiếp vào site, không nên qua đường liên kết, và mua hàng có thương hiệu tại các site này;   * Kiểm tra các site không quen biết qua địa chỉ và qua số điện thoại, fax; * Kiểm tra người bán qua thông tin của phòng thương mại địa phương hoặc các tổ chức nghề nghiệp; * Nghiên cứu xem site của người bán an toàn như thế nào và được tổ chức tốt ra sao; * Kiểm tra các chính sách về hoàn tiền, bảo hành, các cam kết về dịch vụ của người bán trước khi mua hàng; * So sánh giá cả trực tuyến với giá cả trong các cửa hàng truyền thống; * Hỏi bạn bè về các site. Tìm các chứng nhận, xác nhận về site; * Nghiên cứu xem có những đền bù gì trong các trường hợp tranh cãi; * Tư vấn với các cơ quan hoặc hiệp hội bảo vệ người tiêu dùng;   Trên góc độ các tổ chức và doanh nghiệp, tháng 12/1999, OECD đã ban hành Bản hướng dẫn về bảo vệ người tiêu dùng trong bối cảnh thương mại điện tử để giúp bảo vệ người tiêu dùng khi tiến hành mua bán trên mạng. Mục đích của ban hành Bản hướng dẫn bảo vệ người tiêu dùng là khuyến khích 1) Kinh doanh trung thực; tiến hành quảng cáo và tiến hành nghiên cứu thị trường; 2) Có thông tin rõ ràng về nhận dạng của một doanh nghiệp trực tuyến, hàng hoá và dịch vụ được chào và điều khoản của giao dịch; 3) Quá trình minh bạch cho việc xác định các giao dịch; 4) Cơ chế thanh toán an toàn; 5) Cơ chế giải quyết tranh chấp và đền bù phù hợp, đúng hạn và hợp lý; 5) Bảo vệ bí mật cá nhân; và giáo dục người tiêu dùng và doanh nghiệp.  Bảng 8.1. Hướng dẫn của OECD về bảo vệ người tiêu dùng  có ý nghĩa tới việc giải quyết tranh chấp và đền bù đúng thời gian mà không chịu chi phí quá đáng.   * *Bảo vệ bí mật:* TMĐT B2C cần được tiến hành phù hợp với những nguyên tắc bảo vệ bí mật được thừa nhận như được đưa ra trong Hướng dẫn của OECD điều chỉnh bảo vệ bí mật riêng tư và việc trao đổi qua biên giới của dữ liệu cá nhân (1980). Cũng tính tới tuyên bố hội nghị bộ trưởng của OECD về bảo vệ bí mật cá nhân trên mạng toàn cầu (1998), để cung cấp khả năng bảo vệ người tiêu dùng một cách phù hợp và hiệu quả. * *Giáo dục và nâng cao nhận thức:* Chính phủ, doanh nghiệp và đại diện người tiêu dùng cần phối hợp với nhau để tuyền truyền cho người tiêu dùng về TMĐT, hỗ trợ việc ra quyết định với đầy đủ thông tin bở người tiêu dùng khi tham gia vào TMĐT, và tăng cường nhận thức của doanh nghiệp và người tiêu dùng về cơ chế bảo vệ người tiêu dùng được áp dụng cho hoạt động trực tuyến của họ.   *Nguồn:* Tổ chức phát triển và hợp tác kinh tế, Hướng dẫn về Bảo vệ người tiêu dùng trong bối cảnh TMĐT (2000); http://www1.oecd.org//publications/e-book/9300023E.PDF  Hướng dẫn của OECD được thiết kế như một công cụ trung lập để giúp các chính phủ, doanh nghiệp và người tiêu dùng bằng cách đưa ra những hướng dẫn thực tế để giúp hình thành và duy trì niềm tin của khách hàng vào TMĐT. Hướng dẫn này đưa ra những khía cạnh cơ bản của TMĐT B2C và phản ánh những quy định pháp luật đang hiện hành đối với khách hàng trong những hình thức truyền thống hơn của thương mại. Họ nhấn mạnh tầm quan trọng của việc minh bạch hoá và tiết lộ thông tin và sự cần thiết có sự hợp tác giữa các chính phủ, doanh nghiệp và người tiêu dùng ở mức quốc gia và quốc tế. Hướng dẫn nhằm cung cấp những nguyên tắc để giúp :   * + Chính phủ xem xét, và (nếu cần thiết) tạo sự phù hợp, hình thành khuôn mẫu và thi hành chính sách và sáng kiến khách hàng trong TMĐT.   + Doanh nghiệp, người tiêu dùng và những tổ chức tự quản khác, bằng việc đưa ra hướng dẫn về những đặc điểm cơ bản của việc bảo vệ khách hàng mà có thể được cân nhắc trong quá trình phát triển và thi hành những cơ chế tự quản.   + Tổ chức kinh doanh và người tiêu dùng, bằng việc đưa ra những sự tiết lộ thông tin cơ bản và những thực tiễn kinh doanh điển hình mà họ có thể cung cấp hoặc mong chờ ở trên mạng.   Hướng dẫn của OECD đã đề cập theo chiều sâu những vấn đề liên quan tới thẩm quyền xét xử, những luật được áp dụng và khả năng tiếp cận tới việc bồi thường. Vì bản chất rộng và sâu của những vấn đề trên, những câu hỏi làm sao chúng có thể được đưa ra một cách tốt nhất trong bối cạnh TMĐT không phải chỉ duy nhất đối với việc bảo vệ người tiêu dùng. Tuy nhiên, tiềm năng của Internet làm tăng số lượng giao dịch B2C qua biên giới, lợi ích của khách hàng giao dịch B2C cũng được đảm bảo một cách đầy đủ.  Hướng dẫn trên của OECD cho thấy tính phức tạp của vấn đề và thực tế vẫn còn thiếu sự đồng thuận quốc tế về những vấn đề này. Hướng dẫn thừa nhận rằng mọi giao dịch qua biên giới giữa doanh nghiệp và người tiêu dùng nằm trong khung khổ pháp lý về quyền xét xử và luật áp dụng, nhưng TMĐT đặt ra những thách thức mới cho khung khổ pháp lý đó. Hướng dẫn đòi hỏi cần phải làm nhiều việc hơn nữa để đưa ra những vấn đề này và đảm bảo rằng lợi ích của người tiêu dùng được bảo vệ khi hình thành những quy định mới.  Hướng dẫn trên cũng đề cập tới tầm quan trọng của việc tạo khả năng tiếp cận của khách hàng đối với những thủ tục bồi thường hợp lý, đúng thời gian và tiện lợi và khuyến khích xây dựng những cơ chế giải quyết tranh chấp thay thế hiệu quả. Việc khởi kiện để giải quyết một tranh chấp thường rất tốn phí, khó khăn và mất nhiều thời gian. Những vấn đề như vậy có thể càng phức tạp hơn đối với những tranh chấp mạng tính quốc tế. Trong những hình thức thương mại khác, sự phát triển của những cơ chế giải quyết tranh chấp thay thế hiệu quả có thể giúp tránh được những thủ tục phức tạp hiện hành, để giải quyết những khiếu nại của người tiêu dùng một cách nhanh chóng, dễ dàng và hợp lý, và thiết lập những cơ chế giải quyết tranh chấp trực tuyến hiệu quả nhằm tạo dựng niềm tin cho người tiêu dùng.  Cuối cùng, vấn đề bảo vệ người tiêu dùng và bí mật cá nhân là vấn đề của cả khu vực chính phủ và khu vực tư nhân. Chính phủ phải đảm bảo rằng có đủ luật cho phép bảo vệ người tiêu dùng; khu vực tư nhân phải thi hành chế độ bảo vệ bí mật cá nhân có ý nghĩ, thân thiện và tự điều chỉnh. Cho tới khi người sử dụng tin tưởng rằng việc truyền thông và dữ liệu của họ là an toàn khỏi việc bị ngăn chặn và việc sự dụng trái phép, có vậy mới khuyến khích họ sử dụng Internt vì mục đích thương mại. Chỉ với niềm tin của khách hàng mới có thể giúp TMĐT phát triển.  ***3.3 Bảo vệ người bán hàng*** Internet làm cho việc người tiêu dùng và những người khác gian lận đễ dàng hơn do tính dễ ẩn danh. Người bán phải được bảo vệ khỏi:   * Khách hàng từ chối là đã đặt mua hàng * Khách hàng tải các phần mềm có bản quyền/ hoặc nội dung về rồi bán cho những người khác * Khách hàng cung cấp thông tin thanh toán giả (thẻ tín dụng hoặc séc) khi trả tiền cho sản phẩm và dịch vụ được cung ứng. * Tên của mình bị những người khác sử dụng (người bán mạo danh) * Những từ ngữ, câu, tên, khẩu hiệu và địa chỉ Web của mình bị người khác sử dụng.   Để bảo vệ người bán hàng có thể sử dụng nhiều biện pháp khác nhau. Một số Website (ví dụ cardcops.com) cung cấp sơ sở dữ liệu về các số thẻ tín dụng bị từ chối thanh toán cho các đơn hàng.  Người bán hàng truy cập vào cơ sở dữ liệu này có thể sử dụng các thông tin để quyết định việc xử lý bán hàng ra sao. Trong tương lai, ngành công nghiệp thẻ tín dụng dự định sử dụng sinh trắc học để giải quyết vấn đề ăn cắp hàng hóa. Đồng thời, người bán có thể sử dụng hạ tầng mã khóa công cộng (PKI) và các chứng nhận số hóa, đặc biệt là giao thức SET, để ngăn ngừa gian lận.  Một số giải pháp khác bao gồm:   * Sử dụng phần mềm thông minh để xác định các khách hàng có vấn đề (hoặc xác định một cách thủ công trong các công ty nhỏ). Một kỹ thuật là so sánh địa chỉ khi khai thẻ tín dụng với địa chỉ yêu cầu chuyển hàng tới. * Xác định các dấu hiệu cảnh báo đối với các giao dịch giả mạo. Sau khi đã mất 4,1 tr. đôla do không thu được tiền bán hàng tháng 5 năm 2000, Expedia đã xây dựng một danh sách các dấu hiệu cảnh báo như vậy để sử dụng trong công ty. * Yêu cầu những khách hàng mà địa chỉ khi khai thẻ tín dụng khác với địa chỉ yêu cầu chuyển hàng tới gọi đến ngân hàng của họ và bổ sung địa chỉ luân phiên vào tài khoản ngân hàng của họ. Người bán chỉ đồng ý vận chuyển hàng đến địa chỉ luân phiên khi yêu cầu trên được thực hiện.   Việc sử dụng thỏa thuận với bên thứ ba hoặc các công ty ủy thác là một cách thức giúp ngăn ngừa gian lận của người mua và người bán. Trên thị trường cũng có bán các công cụ phần mềm quản trị gian lận.   1. **Các vấn đề đạo đức trong TMĐT**   Có nhiều vấn đề đạo đức liên quan đến Internet và TMĐT. Các vấn đề đạo đức liên quan đến TMĐT có thể là các vấn đề đặc thù như xung đột kênh, xung đột giá, phi trung gian hóa… Ở đây đề cập đến hai vấn đề chung là sử dụng Internet không liên quan đến công việc và Bộ luật đạo đức. *4.1 Sử dụng Internet không vì mục đích công việc*  Các nhân viên thường sử dụng thư điện tử và Web cho các mục đích không liên quan đến công việc. Trong một số công ty, việc sử dụng này chiếm một tỷ lệ quá lớn so với sử dụng cho mục đích công việc. Vấn đề này có một số góc độ. Ví dụ, thư điện tử có thể được sử dụng để quấy rầy các nhân viên khác, đặt ra mối đe dọa đạo đức đối với công ty. Thư điện tử cũng có thể được sử dụng cho hoạt động cờ bạc (ví dụ cá cược bóng đá). Một số nhân viên có thể sử dụng thư điện tử của công ty để quảng cáo cho các hoạt động kinh doanh của riêng mình. Sử dụng các thiết bị CNTT khác của công ty cho các mục đích cá nhân cũng có thể đặt ra một số vấn đề. Ví dụ, trong một số trường đại học 50-70% thời lượng dùng Internet là cho giải trí, nhiều khi làm nghẽn tắc mạng. Hơn nữa, mất nhiều thời gian của nhân viên chi lãng phí cho các hoạt động lướt mạng. 4.2 Bộ luật đạo đức (Codes of Ethics) Một cách tiếp cận thực tế nhằm hạn chế việc sử dụng Internet cho các mục đích không liên quan đến công việc là phát triển chính sách sử dụng Internet và phổ biến cho mọi nhân viên đều biết. Thiếu một chính sách chính thức sẽ khó khăn hơn nhiều trong việc áp đặt hành vi theo mong muốn và xử lý các vi phạm. Một số công ty hàng tháng gửi bản nhắc nhở về chính sánh sử dụng mạng của công ty trên mạng nội bộ. Một số công ty khác cảnh báo với nhân viên rằng các hoạt động trên mạng của nhân viên được công ty theo dõi và thư điện tử của họ có thể bị đọc. Các thông báo như vậy có thể là một phần của bộ luật đạo đức.  Bộ luật đạo đức công ty thể hiện sự chính thức hóa các quy định, các hành vi và hành động mong đợi. Đặc biệt, bộ luật đạo đức cần chú ý tới các nội dung và hình ảnh mang tính công kích, cũng như thông tin cá nhân.  Bộ luật đạo đức cần động viên cán bộ nhân viên của công ty suy nghĩ về việc ai sẽ và ai không sẽ truy cập vào thông tin trước khi họ đưa thông tin lên Website. Bộ luật cũng cần xác định công ty có cho phép cán bộ nhân viên của họ được phép xây dựng các trang Web riêng trên mạng nội bộ (Intranet) của công ty hay không, cũng như việc sử dụng thư điện tử cá nhân và việc truy cập Internet vì các mục đích không liên quan đến công việc trong giờ làm việc. Công ty cần phải tạo lập một ý tưởng tổng quát về vai trò của Website tại nơi làm việc. Điều này sẽ định hướng công ty trong việc phát triển chính sách và đảm bảo cán bộ nhân viên của công ty có thái độ hợp lý đối với chính sách.  Dưới đây là một số chỉ dẫn hữu ích đối với chính sách Web của công ty:   * Công bố ở dạng văn bản các quy định chính sách của công ty về việc sử dụng Internet của cán bộ nhân viên công ty; * Làm cán bộ nhân viên của công ty hiểu rõ rằng họ không được phép sử dụng các tài liệu có đăng ký bản quyền khi chưa được phép; * Đưa lên Website nội dung hoạt động trên mạng mà công ty không ủng hộ * Làm cho tin tưởng rằng chính sách nội dung và hoạt động của Website là phù hợp với luật pháp của các quốc gia khác. * Làm cho tin tưởng rằng nội dung của Website là phù hợp với các chính sách khác của công ty. * Cử người theo dõi các vấn đề pháp lý và nghĩa vụ pháp lý. * Xem xét đánh giá về pháp lý đối với nội dung Website để tin rằng không có gì là phi luân lý và không hợp pháp trên Website của công ty. |