Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

Phan Thái Dũng
dungpt@sbv.gov.vn

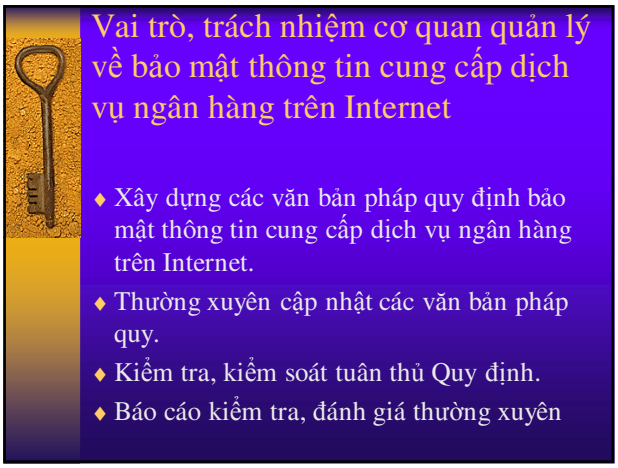
Cục Công nghệ tin học – Ngân hàng Nhà nước Việt Nam

NỘI DUNG

- Nguy cơ mất an toàn bảo mật thông tin việc cung cấp dịch vụ ngân hàng trên Internet
- Vai trò, trách nhiệm cơ quan quản lý về bảo mật thông tin cung cấp dịch vụ ngân hàng trên Internet
- Một số Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet
- Tổ chức, triển khai các Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

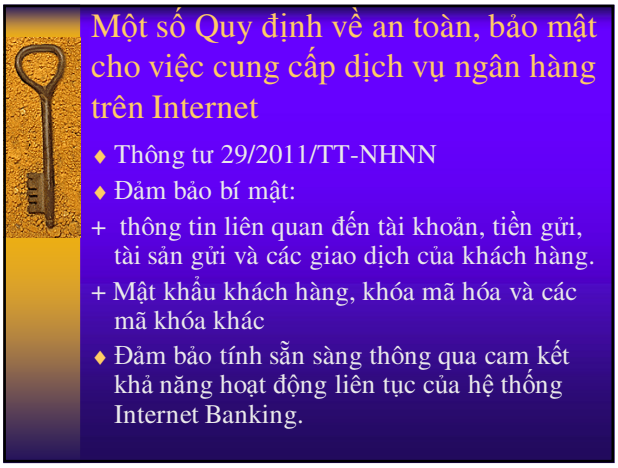
Nguy cơ mất an toàn cung cấp dịch vụ ngân hàng trên Internet

- Bị tấn công: Tội phạm quốc tế, nước ngoài..
- Cán bộ, nhân viên: đạo đức nghề nghiệp..
- Bên thứ ba: quản lý bên thứ 3.
- Người sử dụng: chưa nhận thức attt.
- Kỹ thuật: trang bị, ứng dụng các tính năng.
- Môi trường: môi trường internet.
- Quy trình kỹ thuật, vận hành: đầy đủ, chặt chẽ, chống gian lận.



Vai trò, trách nhiệm cơ quan quản lý về bảo mật thông tin cung cấp dịch vụ ngân hàng trên Internet

- Xây dựng các văn bản pháp quy định bảo mật thông tin cung cấp dịch vụ ngân hàng trên Internet.
- Thường xuyên cập nhật các văn bản pháp quy.
- Kiểm tra, kiểm soát tuân thủ Quy định.
- Báo cáo kiểm tra, đánh giá thường xuyên

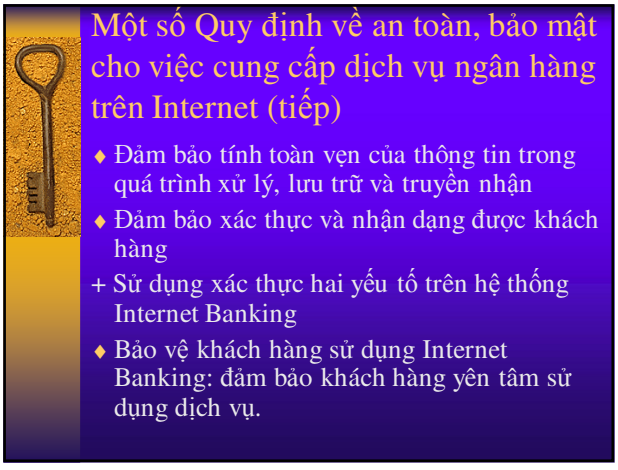


Một số Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet

- Thông tư 29/2011/TT-NHNN
- Đảm bảo bí mật:

+ thông tin liên quan đến tài khoản, tiền gửi, tài sản gửi và các giao dịch của khách hàng.
+ Mật khẩu khách hàng, khóa mã hóa và các mã khóa khác

- Đảm bảo tính sẵn sàng thông qua cam kết khả năng hoạt động liên tục của hệ thống Internet Banking.

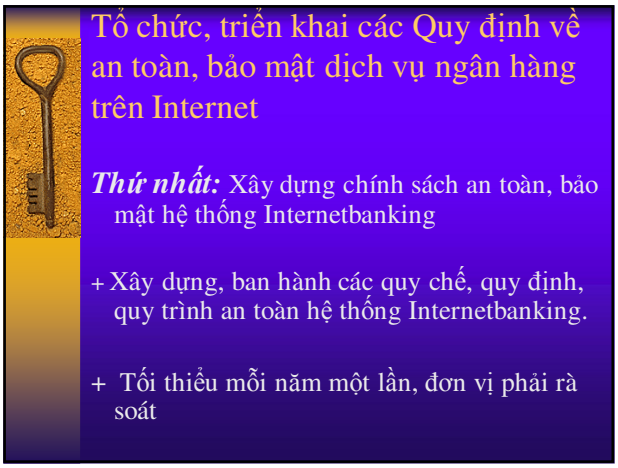


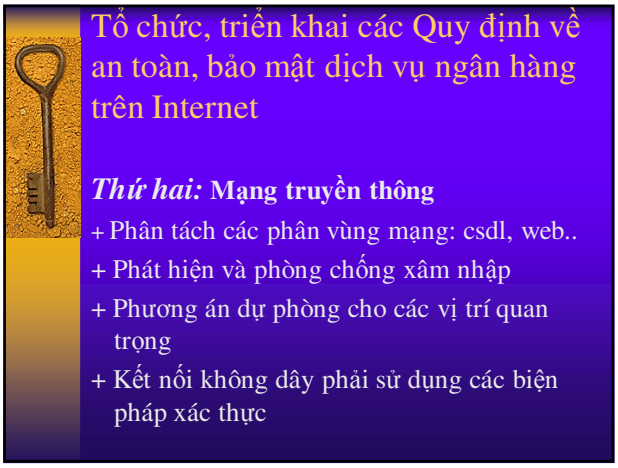
Một số Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet (tiếp)

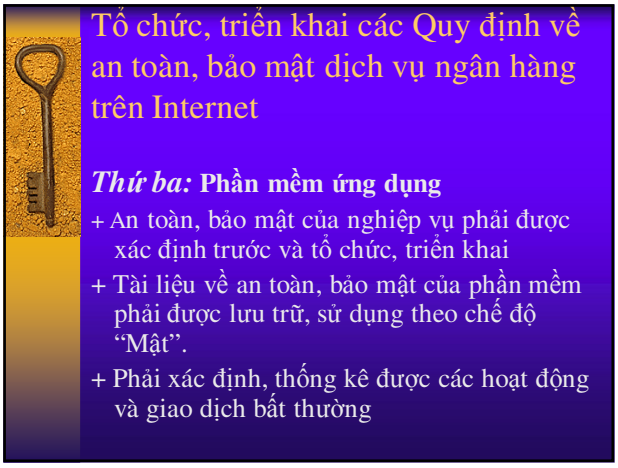
- Đảm bảo tính toàn vẹn của thông tin trong quá trình xử lý, lưu trữ và truyền nhận
- Đảm bảo xác thực và nhận dạng được khách hàng

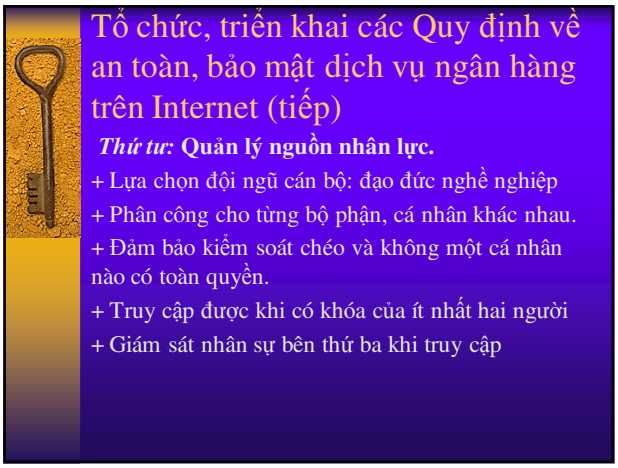
+ Sử dụng xác thực hai yếu tố trên hệ thống Internet Banking

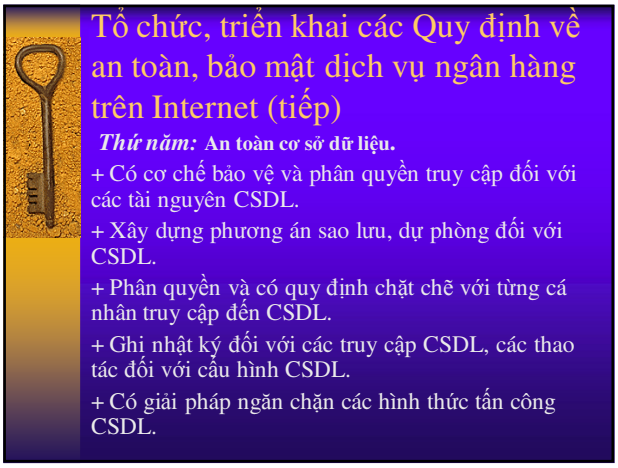
- Bảo vệ khách hàng sử dụng Internet Banking: đảm bảo khách hàng yên tâm sử dụng dịch vụ.

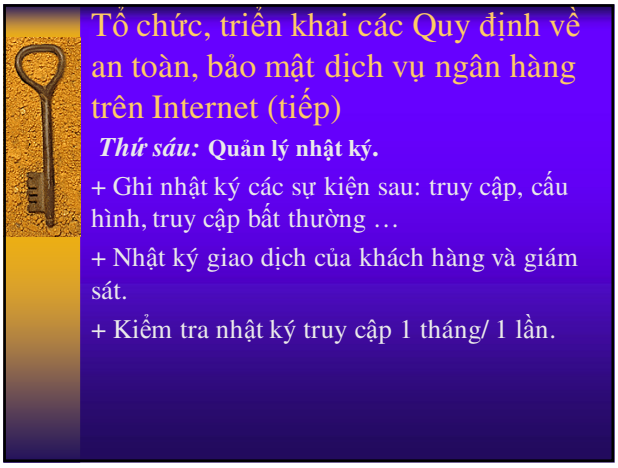

Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet
Thứ nhất: Xây dựng chính sách an toàn, bảo mật hệ thống Internetbanking
+ Xây dựng, ban hành các quy chế, quy định, quy trình an toàn hệ thống Internetbanking.
+ Tối thiểu mỗi năm một lần, đơn vị phải rà soát

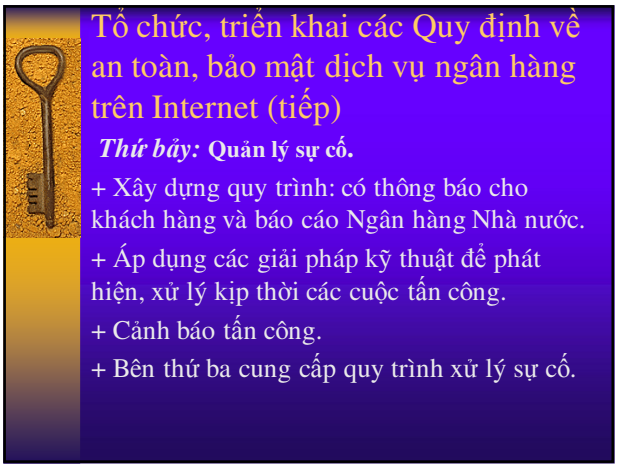

Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet
Thứ hai: **Mạng truyền thông**
+ Phân tách các phân vùng mạng: csdl, web..
+ Phát hiện và phòng chống xâm nhập
+ Phương án dự phòng cho các vị trí quan trọng
+ Kết nối không dây phải sử dụng các biện pháp xác thực

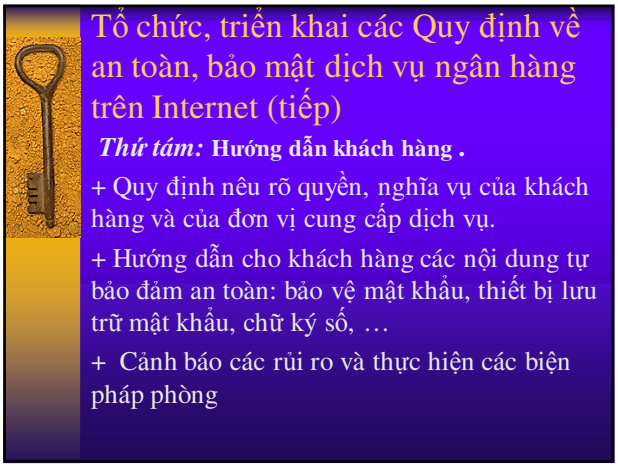

Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet
Thứ ba: **Phần mềm ứng dụng**
+ An toàn, bảo mật của nghiệp vụ phải được xác định trước và tổ chức, triển khai
+ Tài liệu về an toàn, bảo mật của phần mềm phải được lưu trữ, sử dụng theo chế độ "Mật".
+ Phải xác định, thống kê được các hoạt động và giao dịch bất thường

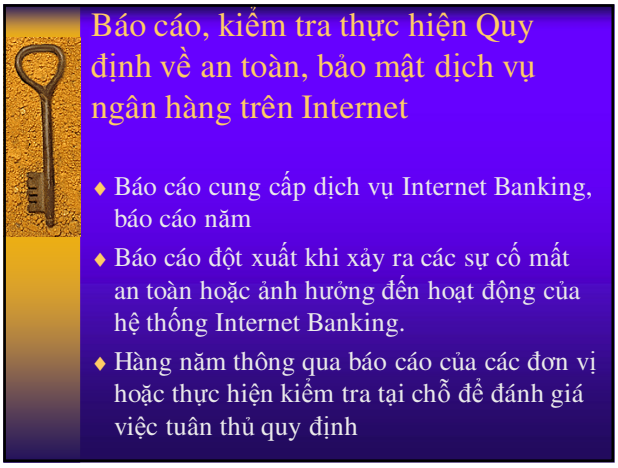

Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet (tiếp)
Thứ tư: **Quản lý nguồn nhân lực.**
+ Lựa chọn đội ngũ cán bộ: đạo đức nghề nghiệp
+ Phân công cho từng bộ phận, cá nhân khác nhau.
+ Đảm bảo kiểm soát chéo và không một cá nhân nào có toàn quyền.
+ Truy cập được khi có khóa của ít nhất hai người
+ Giám sát nhân sự bên thứ ba khi truy cập


Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet (tiếp)
Thứ năm: **An toàn cơ sở dữ liệu.**
+ Có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên CSDL.
+ Xây dựng phương án sao lưu, dự phòng đối với CSDL.
+ Phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến CSDL.
+ Ghi nhật ký đối với các truy cập CSDL, các thao tác đối với cấu hình CSDL.
+ Có giải pháp ngăn chặn các hình thức tấn công CSDL.


Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet (tiếp)
Thứ sáu: **Quản lý nhật ký.**
+ Ghi nhật ký các sự kiện sau: truy cập, cấu hình, truy cập bất thường …
+ Nhật ký giao dịch của khách hàng và giám sát.
+ Kiểm tra nhật ký truy cập 1 tháng/ 1 lần.


Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet (tiếp)
Thứ bảy: **Quản lý sự cố.**
+ Xây dựng quy trình: có thông báo cho khách hàng và báo cáo Ngân hàng Nhà nước.
+ Áp dụng các giải pháp kỹ thuật để phát hiện, xử lý kịp thời các cuộc tấn công.
+ Cảnh báo tấn công.
+ Bên thứ ba cung cấp quy trình xử lý sự cố.


Tổ chức, triển khai các Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet (tiếp)
Thứ tám: **Hướng dẫn khách hàng .**
+ Quy định nêu rõ quyền, nghĩa vụ của khách hàng và của đơn vị cung cấp dịch vụ.
+ Hướng dẫn cho khách hàng các nội dung tự bảo đảm an toàn: bảo vệ mật khẩu, thiết bị lưu trữ mật khẩu, chữ ký số, …
+ Cảnh báo các rủi ro và thực hiện các biện pháp phòng


Báo cáo, kiểm tra thực hiện Quy định về an toàn, bảo mật dịch vụ ngân hàng trên Internet
♦ Báo cáo cung cấp dịch vụ Internet Banking, báo cáo năm
♦ Báo cáo đột xuất khi xảy ra các sự cố mất an toàn hoặc ảnh hưởng đến hoạt động của hệ thống Internet Banking.
♦ Hàng năm thông qua báo cáo của các đơn vị hoặc thực hiện kiểm tra tại chỗ để đánh giá việc tuân thủ quy định


Trân trọng cảm ơn.
Phan Thái Dũng
dungpt@sbv.gov.vn
Cục Công nghệ tin học – Ngân hàng Nhà nước Việt Nam