HƯỚNG DẪN AN TOÀN, BẢO MẬT TRONG GIAO DỊCH NGÂN HÀNG ĐIỆN TỬ (INTERNET BANKING) VÀ NGÂN HÀNG DI ĐỘNG (MOBILE BANKING)

I Nguyên tắc về bảo mật thông tin

1. KHÔNG tiết lộ tên đăng nhập (username), mật khẩu truy cập, mã PIN của bất kỳ dịch vụ Ngân hàng điện tử, mã OTP, số thẻ, số tài khoản cho bất cứ ai qua bất kỳ kênh nào như điện thoại, email, mạng xã hội, ứng dụng, website, đường link lạ...
2. KHÔNG đặt mật khẩu đơn giản hoặc trùng với các thông tin dễ nhớ như (ngày sinh, số CMND,....).
3. KHÔNG dùng máy tính công cộng để truy cập, thực hiện giao dịch Internet Banking.
4. KHÔNG lưu lại tên đăng nhập và mật khẩu truy cập trên các trình duyệt web.
5. KHÔNG mở những tập tin hoặc bấm vào đường link nào được gởi từ những email lạ.
6. KHÔNG làm theo hướng dẫn những tin nhắn SMS trên di động có nguồn gốc không rõ ràng.
7. KHÔNG sử dụng các thiết bị di động đã bị phá khóa để tải và sử dụng phần mềm ứng dụng Internet Banking, phần mềm tạo OTP.
8. KHÔNG cài đặt ứng dụng Mplus trên các điện thoại đã bị bẻ khóa (jailbreak, rootkit,...).
9. KHÔNG mở tài khoản và đăng ký dịch vụ Ngân hàng điện tử cho người khác sử dụng.
10. VIETBANK không bao giờ chủ động yêu cầu Quý khách hàng khai báo tên đăng nhập và mật khẩu truy cập của dịch vụ Ngân hàng điện tử qua điện thoại hoặc email.
11. KHÔNG chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng. VIETBANK không bao giờ yêu cầu khách hàng chuyển tiền, nạp tiền vào số điện thoại để nhận thưởng bất kỳ chương trình khuyến mại nào của VIETBANK.
12. Thường xuyên thay đổi mật khẩu đăng nhập tối thiểu định kỳ 3 tháng/lần. Mật khẩu phải có độ dài tối thiểu sáu ký tự, bao gồm các ký tự chữ và số, có chứa chữ hoa và chữ thường.
13. Thay đổi mã khóa bí mật ngay lần đăng nhập đầu tiên.
14. Tránh viết mật khẩu ra giấy hoặc ghi chép dưới hình thức khác.
15. Thay đổi mật khẩu truy cập dịch vụ Internet banking, Mobile Banking ngay lập tức và thông báo cho VIETBANK sau khi phát hiện ra mình vừa click vào các đường link nghi ngờ giả mạo hoặc vô tình trả lời thông tin cho người lạ gọi tới.
16. Luôn luôn "đăng xuất" xuất khỏi màn hình dịch vụ khi không tiếp tục sử dụng dịch vụ nữa.
17. Chỉ đăng nhập vào chương trình Internet Banking theo đường dẫn của website chính thức của VIETBANK tại địa chỉ https://online.vietbank.com.vn
18. Chỉ tải (download) ứng dụng của VIETBANK Mobile Banking từ kho ứng dụng của Apple/Google/Window Phones.

19. Cài đặt, sử dụng phần mềm diệt vi rút trên thiết bị cá nhân sử dụng để giao dịch Internet Banking.
20. Thông báo ngay cho VIETBANK các trường hợp: mất, thất lạc, hư hỏng thiết bị tạo OTP, số điện thoại nhận tin nhắn SMS, thiết bị lưu trữ khoá bảo mật tạo chữ ký số; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công.
21. Nếu phát hiện những nội dung email hoặc tin nhắn SMS bất thường mà có liên quan đến VIETBANK, Quý khách vui lòng liên hệ với điểm giao dịch VIETBANK gần nhất hoặc đường dây nóng Trung tâm Dịch vụ Khách hàng để được hỗ trợ.
22. Kiểm tra cẩn thận các liệt kê giao dịch trên tài khoản vừa thực hiện giao dịch chuyển khoản, các thông báo số dư về tài khoản và thông báo ngay cho ngân hàng nếu phát hiện có bất kỳ sự bất thường nào.

II Cảnh báo các loại hình tấn công trực tuyến

Một số loại hình tấn công trực tuyến mà tội phạm thường sử dụng hiện nay:

1. **Lừa đảo tài chính quốc tế:** Trò lừa thường bắt đầu bằng một bức thư hoặc email có hình thức như được gửi trực tiếp tới người nhận thông báo trúng thưởng hoặc hợp tác đầu tư, theo đó người nhận sẽ nhận được một khoản tiền lớn khi thực hiện một số hình thức chuyển tiền trực tuyến hỗ trợ quá trình nhận tiền.
2. **Trộm danh tính:** là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính, chủ yếu là trộm thông tin thẻ tín dụng, tạo ra một món nợ lớn cho khách hàng.
3. **Virus:** là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó vào các đối tượng lây nhiễm khác. Virus thường phá hoại máy tính của nạn nhân bị lây nhiễm để lấy cắp các thông tin cá nhân nhạy cảm, mở cửa sau cho tin tặc đột nhập chiếm quyền điều khiển nhằm có lợi cho người phát tán virus. Gần đây, hình thức virus qua email khá phổ biến, xâm nhập vào các thư điện tử và thường xuyên nhân bản để phát tán virus đến những người trong danh bạ của khách hàng.
4. **Phishing (lừa đảo trên mạng):** sử dụng như một tên website giả mạo để đánh lừa khách hàng đăng nhập vào để từ đó lợi dụng, xâm phạm tài chính và thông tin của khách hàng.
5. **Hacking (Phá khóa):** truy cập bất hợp pháp vào máy tính khách hàng bằng đường Internet.
6. **Lừa gạt qua mạng xã hội (facebook, twitter, zalo…):** hiện tượng kẻ gian giả mạo hoặc chiếm tài khoản mạng xã hội của người quen, bạn bè và trò chuyện, dụ khách hàng nạp tiền thẻ điện thoại, mua thẻ cào, thẻ game… hoặc tiết lộ các thông tin cá nhân, thông tin bảo mật các dịch vụ thẻ, ngân hàng điện tử (tên đăng nhập, mật khẩu truy cập, mã OTP). Sau đó kẻ gian lợi dụng, xâm phạm tài khoản dịch vụ của khác hàng và chiếm đoạt tiền bằng nhiều hình thức.

III Liên lạc với VIETBANK theo số tổng đài Trung tâm Dịch vụ Khách hàng: 1800 1122

1. Khi gặp bất kỳ lỗi, khó khăn hay vướng mắc trong quá trình sử dụng dịch vụ.
2. Trong mọi trường hợp, số điện thoại duy nhất của Trung tâm Dịch vụ Khách hàng VIETBANK gọi đến điện thoại của Quý khách đều hiển thị là số 1800 1122.