8 LỜI KHUYÊN ĐỂ THỰC HIỆN GIAO DỊCH NGÂN HÀNG TRỰC TUYẾN AN TOÀN

1 Theo dõi tài khoản của bạn thường xuyên.

Đảm bảo rằng tất cả các giao dịch được ghi sổ là những giao dịch bạn đã ủy quyền. Báo cáo ngay lập tức mọi hoạt động hoặc gian lận đáng ngờ cho ngân hàng của bạn.

2 Hãy cảnh giác với những email lạ!

Không trả lời các email tự xưng là từ ngân hàng của bạn (hoặc bất kỳ công ty nào khác) yêu cầu thông tin chi tiết tài khoản hoặc mật khẩu của bạn. **Các ngân hàng sẽ không liên hệ với bạn qua email để hỏi các thông tin chi tiết tài khoản của bạn.**

3 Tránh nhấp vào liên kết trong email.

Thông thường, việc đăng nhập vào trang web ngân hàng theo phương thức thủ công sẽ an toàn hơn nhiều để đảm bảo bạn đang truy cập một trang web an toàn.

4 Thay đổi mật khẩu ngân hàng của bạn thường xuyên.

Tránh sử dụng cùng một mật khẩu cho nhiều trang web và đảm bảo rằng bạn đang chọn một mật khẩu mạnh kết hợp giữa các chữ hoa và chữ thường, số và ký tự đặc biệt. Tránh sử dụng các từ hoặc cụm từ có chứa tên, tên viết tắt hoặc ngày sinh của bạn.

5 Kích hoạt xác thực hai yếu tố.

Nhiều tổ chức tài chính đã bổ sung vào một lớp bảo mật cho chủ tài khoản. Xác thực hai yếu tố yêu cầu bạn nhập thông tin xác thực bổ sung trước khi bạn có thể truy cập vào tài khoản của mình.

6 Tắt đăng nhập tự động.

Không cho phép trình duyệt web lưu trữ thông tin tên người dùng và mật khẩu riêng tư đối với các trang web ngân hàng trực tuyến của bạn.

7 Khi khả dụng, chỉ sử dụng các ứng dụng di động chính thức của ngân hàng của bạn.

Và đảm bảo rằng bạn tải xuống ứng dụng từ các nguồn uy tín như Apple Store hoặc Google Play Store.

8 Bạn không chắc liệu điều gì đó có hợp pháp hay không?

Bạn có thắc mắc về công nghệ ngân hàng của bạn không? Hãy gọi cho họ—họ sẽ sẵn sàng trợ giúp!

Mang đến cho bạn sự cộng tác của:

THE STATE OF TEXAS DEPARTMENT OF BANKING

TexasBankers Association

8 LỜI KHUYÊN ĐỂ AN TOÀN HƠN TRÊN MẠNG

1 Lừa đảo qua email

Nếu có điều gì đó có vẻ quá tốt để có thể là sự thật thì đó có thể là lừa đảo. Đừng bao giờ tin rằng nhân viên giải thưởng xổ số hoặc các hoàng tử nước ngoài sẽ liên hệ với bạn qua email!

2 Lừa Đảo Thanh Toán

Luôn đề phòng các séc, séc thủ quỹ, phiếu chuyển tiền hoặc chuyển khoản điện tử lừa đảo được gửi cùng yêu cầu bạn chuyển lại một phần tiền.

3 Lời Đề Nghị Chủ Động

Luôn cảnh giác với những lời đề nghị chủ động yêu cầu bạn phải "HÀNH ĐỘNG NHANH CHÓNG."

4 Luôn Cập Nhật

Đảm bảo thiết bị được cập nhật với các bản cập nhật bảo mật mới nhất cho hệ điều hành của bạn — Windows, Apple IOS, điện thoại di động iOS (Apple, Android, v.v.).

5 Cảnh Báo và Lỗi

Không tin tưởng các trang web có cảnh báo hoặc lỗi chứng chỉ.

6 Cảnh Giác với Các Tệp Đính Kèm trong Email

Việc nhấp vào tệp đính kèm email hoặc phần mềm miễn phí từ các nguồn không xác định không bao giờ là một ý tưởng hay. Bạn có thể khiến hệ thống của mình gặp phải lừa đảo và trộm cắp trực tuyến.

7 Chia Sẻ Trực Tuyến

Xem mức độ bạn chia sẻ trực tuyến. Bạn càng đăng tải nhiều thông tin về bản thân trên các trang mạng xã hội thì càng dễ dàng bị ai đó sử dụng các thông tin đó để truy cập vào tài khoản của bạn, đánh cắp danh tính của bạn và các thông tin khác nữa. Phải bảo vệ thông tin cá nhân của bạn bằng cách tối đa hóa cài đặt quyền riêng tư của bạn.

8 Lừa Đảo Tài Chính

Hãy luôn cảnh giác với những trò lừa đảo tài chính liên quan đến thảm họa. Những kẻ lừa đảo lợi dụng mọi người sau những sự kiện thảm khốc bằng cách tự xưng là thành viên của các tổ chức từ thiện hợp pháp trong khi trên thực tế, họ đang cố gắng đánh cắp tiền hoặc các thông tin cá nhân có giá trị.

Các nguồn tài liệu bổ sung về an toàn trực tuyến:
Sở Ngân Hàng Texas – www.dob.texas.gov
Hiệp Hội Ngân Hàng Texas – www.texasbankers.com/BankingSafely
Better Business Bureau – www.bbb.org/council/for-businesses/cybersecurity/