***Bài tập***

***Tình huống 1:***

**Mối đe dọa thứ nhất**: Thông tin đăng kí thăm khám chuyển tiền viện phí/nạp tiền bị lộ ra ngoài.

**Nhận dạng: tấn công bằng social engineerin**g.

**Mục đích**: Tin tặc tạo ra các email, ứng dụng giả mạo để dụ người dùng cung cấp thông tin cá nhân hoặc chuyển tiền viên phí,…Chúng đánh cắp để những kẻ xấu lợi dụng sẽ cố gắng ép nạn nhân cung cấp thông tin thẻ tín dụng hoặc dữ liệu cá nhân của bệnh nhân như số điện thoại, số CMND,CCCD, mã OTP, mã bệnh nhân ,.. email lừa đảo được gửi để lấy thông tin đăng nhập , thực hiện các lệnh chuyển tiền, vay, quảng cáo thuốc, quảng cáo phòng khám kém chất lượng,... để trục lợi cho mình.

**Hậu quả**: sẽ bị thất thoát dữ liệu. Thông tin cá nhân bị rao bán lộ ra ngoài, phát tán trên mạng xã hội. Ảnh hưởng đến quá trình điều trị và khám bệnh không đúng quy trình,gây mất tiền lúc đóng viện phí. Nghiêm trọng hơn, chúng có thể quay lại tống tiền chúng ta. Lúc này, hậu quả không chỉ nằm ở việc điều trị bệnh mà còn là thiệt hại tài chính nặng nề

**Mối đe dọa thứ 2**: Thông tin cá nhân của bác sĩ và bệnh nhân bị đánh cắp

**Nhận dạng**: **tấn công bằng social engineering.**

**Mục đích**: kẻ xấu lợi dụng để trục lợi mục đích cá nhân, dùng thông tin khách hàng và bác sĩ để gây rối, những thông tin như số điện thoại, email,…có thể sẽ bị kẻ xấu dùng để cung cấp cho những doanh nghiệp như bất động sản, các cá nhân trong nghề sale,..để làm khách hàng cho mình

**Hậu quả:** Thông tin cá nhân bị rao bán lộ ra ngoài, gây ảnh hưởng đến cuộc sống , bác sĩ có thể bị người nhà bệnh nhân gây rối, tấn công nếu quá trình chữa bệnh và chuẩn đoán thiếu nhiệt tình hoặc không chính xác,…

**Mối đe dọa thứ 3**: Hồ sơ bệnh án của bệnh nhân bị lộ.

**Nhận dạng: tấn công bằng mã độc**

**Mục đích**: kẻ xấu dùng email chứa mã độc để gửi cho khách hàng, khi mã độc pháp tán sẽ kẻ xấu sẽ lấy cắp hồ sơ bệnh án, chúng lợi dụng để gây hoang mang cho khách hàng từ đó quảng cáo các loại thuốc, phòng khám kém chất lượng gây ảnh hưởng đến sức khỏe của bệnh nhân.

**Hậu quả**: Ảnh hưởng đến cuộc sống. Gây thiệt hại về kinh tế cho khách hàng, ảnh hưởng đến sức khỏe bệnh nhân, nguy hiểm hơn có thể ảnh hưởng đến tính mạng,…

***Tính huống 2***

**Mối đe dọa thứ nhấ**t: thông tin cá nhân tài khoản(mật khẩu, email,số điện thoại,.. bị lộ,)

**Nhận dạng :**cuộc tấn công bằng mã độc

**Mục đích**: những kẻ tấn công sẽ giả danh ngân hàng gài mã độc vào email, người dùng tải xuống, mã độc sẽ bị phát tán, nó sẽ cung cấp thông tin dữ liệu cá nhân như số điện thoại, mật khẩu, mã OTP.. ., cho kẻ xấu từ đó chúng thực hiện các lệnh chuyển tiền, rút tiền, vay,…

**Hậu quả**: sẽ bị thất thoát dữ liệu. Tin tặc có thể rút tiền,chuyển khoản, vay lãi,..hoặc rao bán khối dữ liệu đó phát tán trên mạng xã hội,. Nghiêm trọng hơn, chúng có thể quay lại tống tiền chúng ta. Lúc này, hậu quả không chỉ nằm ở việc mất dữ liệu mà còn là thiệt hại tài chính nặng nề.

**Ví dụ**: kẻ xấu gởi cho khách hàng A 1 email giả danh ngân hàng, khách hàng tải xuống mã độc từ đó phát tán, khi đăng nhập vào ví tiền online(banking) thông tin cá nhân bị lộ ra ngoài từ đó chúng lợi dụng để lấy tiền hoặc phát tán ra bên ngoài,..

**Mối đe dọa thứ 2**: Thông tin giao dịch bị đánh cắp.

**Nhận dạng: tấn công bằng social engineering và tần công bằng mã độc**

**Mục đích:** chúng cũng sẽ mạo danh ngân hàng tạo ra các ứng dụng website để khách hàng đăng nhập vào gây lộ thông tin số điện thoại, ví điện tử,..hoặc chúng có thể cài mã độc để để lấy thông tin giao dịch.

**Hậu quả**: Khi khách hàng giao dịch kẻ xấu nhận biết được từ đó chúng giả danh ngân hàng , ép khách hàng đóng tiền, chuyển khoản, khai báo thông tin cá nhân,.. từ đó kẻ xấu phát tán thông tin ra ngoài. Nghiêm trọng hơn, chúng có thể quay lại tống tiền chúng ta. Lúc này, hậu quả không chỉ nằm ở việc mất thông tin mà còn là thiệt hại nặng nề về tài chính

**Ví dụ**: kẻ xấu mạo danh tạo ra ứng dụng ngân hàng. khi đăng nhập và liên kết với ví tiền online(banking) thông tin bị đánh cắp từ đó chúng lợi dụng để ép khách hàng đóng tiền phí, hoăc chúng rao bán cung cấp số điện thoại cho những doanh nghiệp như bất động sản, các cá nhân trong nghề sale,..để làm khách hàng cho mình

**Mối đe dọa thứ 3**: chức năng chuyển khoản/rút tiền bị xâm phạm

**Nhận dạng: tấn công bằng mã độc**

**Mục đích**: Chúng sẽ cài mã độc vào khách hàng bằng email, khi giao dịch mã độc sẽ điều khiển lệnh chuyển tiền của khách hàng qua tài khoản của chúng mà khách hàng không thể phát hiện.

**Hậu quả**: Tiền bị kẻ xấu đánh cắp, nếu số tiền chuyển khoản lớn sẽ bị ảnh hưởng nặng nề về tài chính

**Ví dụ**: kẻ xấu gởi cho khách hàng B một email giả danh ngân hàng, khách hàng tải xuống mã độc từ đó phát tán, khi đăng nhập vào ví tiền online(banking) mã độc sẽ điều khiển lệnh chuyển tiền . Khi khách hàng B chuyển tiền cho người C. thì số tiền đó lại chuyển qua cho kẻ xấu từ đó ảnh hưởng đến tài chính của mình