# Bug Types – Summary

Lỗi (Bug) là gì, chúng ta phân biệt các loại lỗi nào và làm thế nào để xác định đúng loại lỗi cho lỗi của bạn?

Lỗi là một vấn đề liên quan đến phần mềm. Nếu một thứ gì đó trên trang web hoặc ứng dụng không hoạt động như dự định, "lỗi" này được gọi là lỗi (bug). Tại test IO, chúng tôi phân biệt giữa các loại lỗi sau:

* Lỗi chức năng (Functional bugs)
* Lỗi nội dung (Content bugs)
* Lỗi hiển thị (Visual bugs)
* Đề xuất khả năng sử dụng (Usability suggestions)

## Lỗi chức năng (Functional Bugs)

Lỗi chức năng liên quan đến chức năng của một phần mềm. Ví dụ: một nút không gửi được biểu mẫu, thanh tìm kiếm không phản hồi đầu vào của người dùng, ứng dụng bị treo, v.v. Bất cứ khi nào bạn thực hiện một hành động mà trang web/ứng dụng không phản hồi như mong đợi, đó có thể là một vấn đề chức năng.

## Làm thế nào để xác định hành vi của ứng dụng có phải là lỗi chức năng:

* Cố gắng tìm hiểu xem một tính năng có được thiết kế theo một cách cụ thể hay nó thực sự bị hỏng. Hãy kiểm tra riêng nó và kết hợp với các tính năng khác để phát hiện sự khác biệt tiềm ẩn.
* Hãy suy nghĩ về ý định của khách hàng và xem xét rằng sản phẩm có thể chỉ hoạt động theo cách nó đã được triển khai.
* Tìm bằng chứng cho thấy một cái gì đó không hoạt động như lẽ ra nó phải hoạt động và hỗ trợ cho tuyên bố của bạn.
  + Ví dụ: Một chức năng cửa hàng trực tuyến hoạt động khác với các cửa hàng trực tuyến khác mà bạn biết. Điều đó không có nghĩa là chức năng đó bị hỏng. Khách hàng có thể triển khai sản phẩm của họ theo bất kỳ cách nào họ muốn.
  + Ví dụ: Nếu bạn cho rằng một trường biểu mẫu không được xác thực và đó là một lỗi, vui lòng đảm bảo có bất kỳ dấu hiệu nào cho thấy trường đó có ý định được xác thực. Bạn có thể cung cấp bằng chứng này bằng cách cho thấy trường đó được xác thực trong một số trường hợp nhưng không phải trong các trường hợp khác. Nếu bạn không cung cấp bất kỳ bằng chứng nào, đó là một tuyên bố chưa được chứng minh.
* Một vấn đề về hiển thị hoặc nội dung trở thành vấn đề chức năng khi nó cản trở một chức năng và do đó nên được báo cáo là lỗi chức năng.
* Nếu một phần chức năng hoạt động nhất quán theo cùng một cách trong các tình huống khác nhau và không có vấn đề rõ ràng, thì có thể nó được thiết kế như vậy (không phải là lỗi).

## Đánh giá mức độ nghiêm trọng (Severity Assessment)

Mức độ nghiêm trọng phù hợp cho một lỗi chức năng phụ thuộc vào một số yếu tố: tác động chức năng của vấn đề, mức độ của vấn đề, liệu có tồn tại giải pháp khắc phục hay nó là một lỗi "chặn đứng" (showstopper), liệu có thể có tổn thất doanh số tiềm năng và đáng kể hay không, và liệu bạn có thể so sánh lỗi này với các lỗi khác có cùng mức độ nghiêm trọng hay không. Do đó, tại test IO, chúng tôi phân biệt ba mức độ nghiêm trọng cho lỗi chức năng:

**Thấp (Low):**

* Tác động tối thiểu đến việc sử dụng sản phẩm.
* Sản phẩm hiển thị hành vi không mong muốn, nhưng việc sử dụng chung không bị ảnh hưởng.
* Ít người dùng, sản phẩm hoặc mặt hàng bị ảnh hưởng.
* Một tính năng/chức năng bị hỏng hoặc không khả dụng, nhưng một giải pháp khắc phục dễ dàng sẽ giải quyết vấn đề.

**Cao (High):**

* Tác động nghiêm trọng đến việc sử dụng sản phẩm, nhưng chức năng chính vẫn nguyên vẹn.
* Một số lượng lớn người dùng, sản phẩm hoặc mặt hàng bị ảnh hưởng.
* Chức năng không đơn giản bị hỏng hoặc không khả dụng, và không có giải pháp khắc phục.
* Chức năng quan trọng bị hỏng hoặc không khả dụng, nhưng có giải pháp khắc phục (do đó không phải là lỗi "chặn đứng").

**Nghiêm trọng (Critical):**

* Lỗi ngăn cản chức năng cốt lõi của ứng dụng/trang web.
* Lỗi "chặn đứng" ngăn người dùng tiếp tục quá trình chính, ví dụ: thanh toán.
* Lỗi gây ra tổn thất doanh số tiềm năng và đáng kể cho khách hàng.

## Lỗi nội dung (Content Bugs)

Lỗi nội dung liên quan đến nội dung thực tế của trang web hoặc ứng dụng: văn bản, nhãn, hình ảnh, video, biểu tượng, liên kết, dữ liệu, v.v. Do đó, các lỗi nội dung điển hình là:

* Liên kết hoặc hình ảnh bị hỏng (lỗi 404) (trừ khi nằm trong menu điều hướng, tiêu đề, chân trang hoặc điều hướng breadcrumb, đó là các lỗi chức năng thấp)
* Chuyển hướng bị lỗi, nói chung
* Văn bản bị thiếu, ví dụ: trong một chú giải công cụ trống
* Nội dung bị thiếu, ví dụ: vùng nội dung trống
* Nội dung bị thiếu, ví dụ: nếu 4 trong số 5 biểu tượng có chú giải công cụ, 1 cái không có
* Bản dịch bị thiếu, ví dụ: một số nút trên trang web tiếng Anh có nhãn tiếng Pháp
* Một số sản phẩm bị thiếu trong kết quả tìm kiếm, nhưng chức năng tìm kiếm vẫn hoạt động
* Dữ liệu bị thiếu

Xin lưu ý rằng lỗi chính tả không được coi là lỗi nội dung trên nền tảng của chúng tôi và không thể gửi dưới dạng lỗi đó.

## Lỗi hiển thị (Visual Bugs)

Lỗi hiển thị liên quan đến giao diện người dùng đồ họa của trang web hoặc ứng dụng, ví dụ:

* Các vấn đề về khung bố cục như văn bản/phần tử bị lệch
* Sự cố về Thiết kế đáp ứng (Responsive Design), ví dụ: một phần tử được hiển thị trên một thiết bị di động nhưng không hiển thị trên thiết bị khác
* Văn bản/phần tử vô tình chồng lên nhau
* Văn bản/phần tử bị cắt xén

## Nâng cấp lỗi nội dung hoặc lỗi hiển thị thành lỗi chức năng

Ngay khi một lỗi nội dung hoặc hiển thị ngăn cản một chức năng, nó nên được báo cáo là lỗi chức năng, ngay cả khi thực tế chức năng đó không bị lỗi.

Một trường hợp quan trọng khi lỗi nội dung nên được gửi dưới dạng lỗi chức năng là khi nó xảy ra trong một thành phần chức năng của sản phẩm – cụ thể là các vấn đề liên kết trong menu điều hướng, tiêu đề, chân trang hoặc điều hướng breadcrumb. Các vấn đề như vậy thường là các lỗi chức năng thấp (Low).

## Các vấn đề lặp lại (Repetitive problems)

Khi một vấn đề về nội dung hoặc hiển thị xảy ra lặp lại, nó chỉ có thể được gửi một lần, mặc dù mỗi lần xuất hiện có thể có URL, liên kết, hình ảnh, v.v. khác nhau. Điều này cũng đúng nếu các lần xuất hiện ở trên cùng một trang hoặc các trang khác nhau. Báo cáo lỗi duy nhất này nên nêu rõ rằng các URL, liên kết, hình ảnh, v.v. khác cũng bị ảnh hưởng.

Không được gửi các báo cáo lỗi riêng lẻ cho mỗi lần xuất hiện của vấn đề và sẽ bị từ chối. Ví dụ, chỉ nên gửi một báo cáo cho các vấn đề nội dung sau: Một số hình ảnh sản phẩm trên nhiều trang chi tiết sản phẩm của một cửa hàng trực tuyến bị hỏng, một số liên kết tải xuống hướng dẫn sử dụng PDF trên nhiều trang chi tiết sản phẩm dẫn đến các trang 404, một số mô tả sản phẩm bằng ngôn ngữ khác với phần còn lại của cửa hàng trực tuyến, một số chú giải công cụ không chứa bất kỳ thông tin nào, một số liên kết thuộc cùng một nhóm bị hỏng, v.v.

Các vấn đề hiển thị sau đây chỉ nên được gửi một lần: Một số văn bản hoặc hình ảnh lớn hơn các ô của chúng, nhiều trường nhập liệu không đủ lớn để chứa văn bản mặc định của chúng mà không hiển thị hoàn toàn, nhiều đoạn giới thiệu vô tình chồng lên các phần tử khác, v.v.

# Lỗi chức năng - Tóm tắt

Lỗi chức năng là gì, cách đánh giá mức độ nghiêm trọng của chúng và cách phân biệt chúng với các đề xuất về khả năng sử dụng?

Lỗi chức năng liên quan đến chức năng của phần mềm, chẳng hạn như một nút không gửi được biểu mẫu, tìm kiếm không phản hồi hoặc ứng dụng bị treo. Nếu trang web/ứng dụng không phản hồi như mong đợi, đó có thể là dấu hiệu của một vấn đề chức năng. Việc xác định xem đó là hành vi có chủ ý hay một lỗi có thể khó khăn do thông tin hạn chế về sản phẩm của khách hàng. Tuy nhiên, phân tích hành vi sản phẩm và đưa ra các phỏng đoán hợp lý dựa trên kinh nghiệm có thể hữu ích.

## Cách xác định xem một hành vi có phải là lỗi chức năng:

Khi kiểm thử, hãy kiểm tra xem hành vi đó là được thiết kế hay bị hỏng bằng cách kiểm tra các tính năng riêng lẻ và kết hợp. Hãy xem xét ý định của khách hàng và cung cấp bằng chứng khi tuyên bố điều gì đó không hoạt động chính xác. Một cửa hàng trực tuyến hoạt động khác với các cửa hàng khác không nhất thiết có nghĩa là nó bị hỏng. Hãy báo cáo các vấn đề hiển thị hoặc nội dung cản trở chức năng dưới dạng lỗi chức năng.

## Đánh giá mức độ nghiêm trọng

Các yếu tố cần xem xét khi đánh giá mức độ nghiêm trọng của lỗi phải bao gồm tác động chức năng của lỗi, mức độ của vấn đề, sự có sẵn của các giải pháp khắc phục, khả năng mất doanh số tiềm năng và so sánh với các lỗi có mức độ nghiêm trọng tương tự. Mức độ nghiêm trọng có thể được xác định bằng cách đánh giá mức độ liên quan của chức năng trong bối cảnh toàn bộ sản phẩm, số lượng người dùng bị ảnh hưởng, mức độ dễ dàng tìm thấy giải pháp khắc phục và khả năng mất doanh số. So sánh lỗi với các lỗi đã được phê duyệt trước đó cũng có thể giúp xác định mức độ nghiêm trọng của nó.

## Chúng tôi có ba mức độ nghiêm trọng cho lỗi chức năng:

* THẤP (LOW)
* CAO (HIGH)
* NGHIÊM TRỌNG (CRITICAL)

## Các đánh giá phổ biến

Có một danh sách các trường hợp với các mức độ nghiêm trọng cố định mà sơ đồ đánh giá ở trên không áp dụng. Danh sách có thể thay đổi theo thời gian, vì vậy cần được kiểm tra thường xuyên.

## Lỗi trường hợp đặc biệt (Edge case bugs)

Lỗi trường hợp đặc biệt xảy ra khi một tính năng được sử dụng một cách bất thường. Những lỗi có liên quan sẽ được chuyển tiếp dưới dạng lỗi Thấp (Low), trong khi hầu hết những lỗi không liên quan sẽ bị từ chối.

## Lỗi cố ý gây ra (Forced bugs)

Lỗi cố ý gây ra do hành vi không điển hình hoặc các điều kiện đặc biệt thường không liên quan đến khách hàng và nằm ngoài phạm vi. Hành vi như vậy có thể kích hoạt cảnh báo nghiêm trọng từ phía chúng tôi. Do đó, chúng tôi khuyên bạn nên hạn chế gửi các lỗi cố ý gây ra.

# Device and Data Protection

## Social Engineering Techniques

Trong bài viết này, bạn sẽ khám phá một số rủi ro về kỹ thuật xã hội và cách nhận biết cũng như tránh chúng.

## Rủi ro an ninh mạng

Rủi ro an ninh mạng đã nổi lên như một mối quan tâm cấp thiết đối với các công ty công nghệ thông tin. Chúng có thể liên quan đến việc mất tính bảo mật, toàn vẹn hoặc khả dụng của thông tin, dữ liệu hoặc hệ thống thông tin (hoặc kiểm soát) và có khả năng tác động tiêu cực đến hoạt động của một tổ chức (tức là nhiệm vụ, chức năng, hình ảnh hoặc danh tiếng của tổ chức đó).

Vì vậy, việc hiểu và quản lý rủi ro an ninh mạng đã trở thành một khía cạnh cơ bản trong chiến lược quản lý rủi ro an ninh mạng mạnh mẽ của Test IO.

Quản lý rủi ro an ninh mạng bao gồm việc xác định và giảm thiểu các mối đe dọa và lỗ hổng tiềm ẩn trong các hệ thống và mạng kỹ thuật số của công ty.

## Lỗ hổng

Lỗ hổng là những điểm yếu trong một máy tính hoặc mạng khiến nó dễ bị khai thác tiềm năng, chẳng hạn như sử dụng hoặc truy cập trái phép.

Các lỗ hổng bao gồm nhưng không giới hạn ở các điểm yếu trong quy trình bảo mật, kiểm soát hành chính hoặc nội bộ, hoặc cấu hình vật lý, cũng như các tính năng hoặc lỗi cho phép kẻ tấn công vượt qua các biện pháp bảo mật.

## Các mối đe dọa lỗ hổng

Mối đe dọa là bất cứ thứ gì có khả năng gây hại cho tài sản và/hoặc tổ chức.

Các mối đe dọa có thể là đối đầu (từ một cá nhân, nhóm hoặc tổ chức), ngẫu nhiên (từ người dùng hoặc quản trị viên), cấu trúc (từ thiết bị CNTT, phần mềm hoặc thiết bị điều khiển), hoặc môi trường (thảm họa tự nhiên hoặc do con người gây ra hoặc sự cố/ngừng hoạt động của cơ sở hạ tầng).

## Kỹ thuật xã hội

Kỹ thuật xã hội là một loại xâm nhập phi kỹ thuật phụ thuộc nhiều vào tương tác của con người. Nó thường liên quan đến việc lừa người khác không tuân thủ các quy trình bảo mật thông thường. Kẻ tấn công sử dụng các kỹ năng xã hội và tương tác của con người để lấy thông tin về một tổ chức hoặc hệ thống thông tin của họ.

Hầu hết các chuyên gia đều đồng ý rằng kỹ thuật xã hội thường liên quan đến việc lợi dụng xu hướng tự nhiên của con người là tin tưởng ai đó và tin lời họ. Đây chính xác là điều khiến mọi người dễ bị tấn công!

Để vượt qua các biện pháp kiểm soát bảo mật, kẻ tấn công có thể sử dụng các kênh liên lạc khác nhau (tin nhắn tức thời, email, cuộc gọi điện thoại, v.v.) và kỹ thuật (phương pháp). Dưới đây là một số kỹ thuật:

### Yêu cầu trực tiếp đơn giản

Trong một số trường hợp, kẻ tấn công sẽ yêu cầu trực tiếp thông tin hoặc dữ liệu - chỉ đơn giản bằng cách hỏi. Đây là phương pháp đầu tiên và rõ ràng nhất. Nó không phải là thành công nhất, nhưng nó được sử dụng.

### 🗑️ Bới rác

Điều này liên quan đến việc bới rác (hoặc thùng rác) để lấy thông tin có thể được sử dụng để đánh cắp danh tính của một người. Thật đáng kinh ngạc khi những gì mọi người vứt bỏ có thể giúp những kẻ xấu tìm thêm thông tin về họ. Bới rác không hoàn toàn là "kỹ thuật xã hội", nhưng đôi khi nó có thể được sử dụng như một bước để có được thông tin hữu ích.

### 📬 Đột nhập hộp thư

Khi một người đã chọn nạn nhân, việc đột nhập hộp thư của người đó thường có thể cung cấp thêm thông tin để sử dụng chống lại họ. Đột nhập hộp thư đề cập đến hành vi mở và đánh cắp trái phép nội dung từ hộp thư bưu điện của người khác. Bạn càng biết nhiều về một người, các phương tiện thay thế để lấy dữ liệu càng hiệu quả.

### 🎣 Lừa đảo (Phishing)

Lừa đảo (Phishing) là một loại lừa đảo trực tuyến trong đó tội phạm gửi một email có vẻ như đến từ một công ty hợp pháp và yêu cầu bạn cung cấp thông tin nhạy cảm như mật khẩu, số thẻ tín dụng hoặc số An sinh xã hội của bạn. Bạn sẽ tìm hiểu kỹ thuật kỹ thuật xã hội này trong bài viết "Lừa đảo là gì".

### 🎭 Mạo danh

Đây là một phương pháp mà kẻ tấn công giả vờ là một người có thẩm quyền. Một số phương pháp được sử dụng trong các cuộc tấn công mạo danh bao gồm giả làm nhân viên hỗ trợ CNTT hoặc dịch vụ hỗ trợ khác, thợ sửa chữa, người giám sát hoặc quản lý, hoặc nhà cung cấp bên thứ ba đáng tin cậy.

### 🌐 Lướt web công ty

Rất nhiều thông tin của công ty có thể được thu thập trước khi nói chuyện với bất kỳ ai chỉ bằng cách lướt các trang web của công ty - ví dụ, địa chỉ email và số điện thoại của nhân viên, sơ đồ tổ chức, chức danh điều hành, thông tin tài chính, v.v.

Các phương pháp được mô tả ở trên là những chiến thuật phổ biến nhất được sử dụng hiện nay.

Tuy nhiên, hãy nhớ rằng kỹ thuật xã hội đang phát triển nhanh chóng trong thời đại công nghệ và những kẻ tấn công không ngừng phát minh ra các kỹ thuật mới để thực hiện các cuộc tấn công của chúng. Do đó, bạn nên luôn cảnh giác để tránh trở thành nạn nhân.

## Bộ công cụ của kẻ xâm nhập

Bạn đã bao giờ tự hỏi việc tấn công dễ dàng đến mức nào chưa?

Theo Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), tin tặc đăng nhiều công cụ mới lên các trang web tấn công mạng mỗi tháng.

Kẻ tấn công có thể khai thác hệ thống của bạn khá dễ dàng bằng các công cụ này nếu bạn được kết nối trực tiếp với mạng (tức là không sử dụng bộ định tuyến) và kẻ tấn công biết địa chỉ IP của bạn.

Kỹ thuật xã hội sử dụng thao túng để hỗ trợ tin tặc trong các cuộc khai thác của chúng. Ví dụ, một email lừa đảo được chuẩn bị kỹ lưỡng có thể lừa người dùng mở một tệp đính kèm độc hại kích hoạt một con sâu.

Nhận thức về bộ công cụ của tin tặc cho phép bạn thực hiện các biện pháp phòng ngừa tốt hơn, nhận biết các nỗ lực tấn công và góp phần vào một tư thế an ninh mạng mạnh mẽ hơn.

### 🔍 Quét lỗ hổng

Tin tặc internet liên tục quét mạng để xác định nơi các hệ thống dễ bị tấn công. Loại quét này còn được gọi là "khảo sát trước tấn công".

### 🔑 Công cụ bẻ khóa mật khẩu

Những kẻ xâm nhập sử dụng một chương trình tự động cố gắng đăng nhập vào một hệ thống bằng một loạt mật khẩu có thể dễ dàng đoán hoặc sử dụng từ điển làm nguồn từ.

### 🕵️‍♂️ Giả mạo mạng

Những kẻ xâm nhập thiết lập một chương trình mạo danh quy trình đăng nhập của một hệ thống khác. Khi bạn cố gắng đăng nhập vào hệ thống, chương trình của kẻ xâm nhập sẽ thu thập mật khẩu của bạn và sau đó trả về thông báo rằng hệ thống không khả dụng. Các chương trình này có thể thu thập hàng trăm mật khẩu hợp lệ.

### 🦠 Virus

Virus là một chương trình "lây nhiễm" các tệp được lưu trữ, thường là các chương trình thực thi, bằng cách chèn một bản sao của chính nó vào tệp. Các bản sao thường được thực thi khi tệp "bị nhiễm" được tải vào bộ nhớ, cho phép virus lây nhiễm các tệp khác.

### 🪱 Sâu (Worms)

Sâu (Worm) là một chương trình độc lập tự tái tạo bằng cách sao chép chính nó từ hệ thống này sang hệ thống khác qua mạng. Thường được kích hoạt khi ai đó mở một tệp đính kèm email bị nhiễm, chương trình sâu có thể gửi các bản sao đến mọi người trong danh bạ thư của người đó.

### 💣 Bom logic

Bom logic là một đoạn mã được cố ý chèn vào một hệ thống phần mềm sẽ kích hoạt một chức năng độc hại khi các điều kiện cụ thể được đáp ứng. Ví dụ, một lập trình viên có thể ẩn một đoạn mã bắt đầu xóa các tệp (chẳng hạn như cơ sở dữ liệu lương) nếu họ rời công ty.

### 🦂 Ransomware

Ransomware là một loại phần mềm độc hại mã hóa các tệp của nạn nhân. Kẻ tấn công sau đó yêu cầu nạn nhân trả tiền chuộc để khôi phục quyền truy cập vào dữ liệu khi thanh toán. Người dùng được hiển thị hướng dẫn cách trả phí để lấy khóa giải mã. Chi phí có thể dao động từ vài trăm đến hàng nghìn đô la, được trả cho tội phạm mạng bằng Bitcoin.

### ⛔ Tấn công từ chối dịch vụ (Denial of Service Attacks)

Tấn công từ chối dịch vụ (DoS) là một cuộc tấn công mạng trong đó kẻ tấn công tìm cách làm cho một máy hoặc tài nguyên mạng không khả dụng đối với người dùng dự định bằng cách tạm thời hoặc vô thời hạn làm gián đoạn các dịch vụ của một máy chủ được kết nối với Internet. Điều này thường được thực hiện bằng cách làm ngập máy hoặc tài nguyên mục tiêu bằng các yêu cầu dư thừa nhằm cố gắng làm quá tải hệ thống và ngăn một số hoặc tất cả các yêu cầu hợp pháp được thực hiện.

### 🛡️ Phòng thủ kỹ thuật xã hội

Bạn có biết rằng trong lịch sử, mắt xích yếu nhất trong chuỗi bảo mật là yếu tố con người không? Cho dù hệ thống bảo mật có mạnh mẽ đến đâu, nó có thể bị xâm phạm nếu người dùng không tuân thủ các giao thức và thực hành bảo mật. Điều này có thể bao gồm việc mắc lừa các trò lừa đảo, sử dụng mật khẩu yếu, bỏ qua các bản cập nhật phần mềm hoặc vô tình tải xuống phần mềm độc hại.

Bạn là tuyến phòng thủ đầu tiên và kiểm soát an ninh đầu tiên. Bạn phải biết cách không trở thành nạn nhân của kỹ thuật xã hội, từ đó bảo vệ an ninh thông tin của Test IO và khách hàng.

Khi thử nghiệm, bạn phải đảm bảo không gây rủi ro cho mạng và hệ thống của công ty khi sử dụng internet. Với tư cách là người kiểm thử của Test IO, bạn có trách nhiệm về an toàn internet.

Khi kết nối với internet, tất cả các thiết bị và mạng đều dễ bị tấn công, sử dụng hoặc truy cập trái phép. Một thiết bị bị xâm phạm có thể ảnh hưởng đến mọi thiết bị khác chia sẻ kết nối.

Để bảo vệ tài sản của mình khỏi các mối đe dọa từ internet, Test IO yêu cầu bạn liên tục cảnh giác bằng cách thực hiện những điều sau:

* Duy trì các biện pháp kiểm soát bảo mật mạnh mẽ trên máy chủ mạng (giữ an toàn thông tin đăng nhập proxy) và máy tính để bàn.
* Sử dụng tường lửa để lọc lưu lượng truy cập từ internet.
* Bảo vệ và cập nhật các tài nguyên CNTT bằng các bản vá và nâng cấp mới nhất.

## What Is Phishing?

Một trong những hình thức tấn công phi kỹ thuật mới hơn, lừa đảo trực tuyến (phishing), liên quan đến việc tạo và sử dụng email, tin nhắn và trang web được thiết kế trông giống như các doanh nghiệp hợp pháp, tổ chức tài chính và cơ quan chính phủ nổi tiếng nhằm đánh lừa người dùng internet tiết lộ dữ liệu hoặc thông tin cá nhân.

Các vụ lừa đảo trực tuyến thường vận hành các trang web giả mạo lừa người tiêu dùng tiết lộ dữ liệu cá nhân và tài chính của họ, bao gồm số an sinh xã hội, thông tin tài khoản ngân hàng và thẻ tín dụng, cũng như chi tiết về tài khoản trực tuyến và mật khẩu.

Các cuộc tấn công qua email và tin nhắn, chẳng hạn như giả mạo (spoofing), lừa đảo trực tuyến, v.v., có thể gây hại cho nhiều người dùng. Một tệp đính kèm có thể chứa "shellcode kết nối ngược" ở dạng mã hóa để các công cụ chống vi-rút/EDR không thể xác định nó là mối đe dọa. Tuy nhiên, khi bạn nhấp vào nó, shellcode sẽ "kết nối ngược" về máy tính của kẻ tấn công, từ đó tạo ra một phiên hợp lệ.

Xin lưu ý rằng tường lửa của bạn — ngay cả một cơ chế bảo mật được áp dụng trong mạng — cũng có thể cho phép kết nối được thiết lập.

Hãy suy nghĩ trước khi bạn nhấp hoặc mở tệp đính kèm email!

### 👮 Phải làm gì khi bạn nhận được email đáng ngờ

Hãy thận trọng khi xem qua các email của bạn. Test IO phụ thuộc vào nhận thức về bảo mật của bạn.

Nếu bạn nhận được một email đáng ngờ, hãy kiểm tra các điều sau:

* Bạn có biết người gửi không?
* Bạn đã nhận được email từ người gửi này trước đây chưa?
* Bạn có mong đợi một tin nhắn (đặc biệt là tin nhắn có tệp đính kèm) từ người gửi này không?
* Tiêu đề email (người gửi, dòng chủ đề, tên tệp đính kèm) có hợp lý không? Nó có chứa bất kỳ ký tự lạ nào không?
* Nó có liên quan đến công việc không, hay bạn đã chủ động thực hiện hành động đó?
* Tên của tệp đính kèm có vẻ khớp với người gửi và dòng chủ đề không? Nó có chứa lỗi chính tả và ngữ pháp không?
* Email này có chứa vi-rút không? Phần mềm chống vi-rút/EDR của bạn sẽ cho bạn biết điều này nếu nó được cài đặt, đang chạy và được cập nhật.

Sau khi trả lời các câu hỏi trên, nếu bạn cho rằng một email không mong muốn là đáng ngờ, bạn phải biết chính xác nên làm gì và không nên làm gì.

**❌ KHÔNG NÊN**

* Bạn có thể nhận được email ngay cả từ người dùng ngân hàng của mình yêu cầu bạn cập nhật tài khoản bằng cách nhấp vào một liên kết. Liên kết trong các email như vậy có khả năng đưa bạn đến một trang web độc hại. Không nhấp vào các liên kết đó!
* Không mở tệp đính kèm hoặc chạy macro nếu bạn đã mở email từ một người gửi không xác định.
* Không trả lời các email đáng ngờ.
* Không chuyển tiếp các email đáng ngờ.
* Không nhập thông tin đăng nhập của bạn sau khi nhấp vào các liên kết.
* Không chia sẻ thông tin ID chính phủ của bạn (số hộ chiếu, số giấy phép lái xe, v.v.) với người khác.
* Không nhấp vào các liên kết được nhúng trong email rác, ngay cả khi chúng có vẻ an toàn hoặc chính xác.

✅ **NÊN**

* Cách tốt nhất để xử lý một email đáng ngờ hoặc không mong muốn là báo cáo nó bằng cách nhấp vào nút "Kiểm tra SPAM/Độc hại" trong Outlook hoặc nút "Báo cáo lừa đảo" trong Outlook dành cho Windows/Mac/iOS/Android và Outlook Web Access.

Bạn có thể xóa email độc hại sau khi hoàn tất hành động Báo cáo lừa đảo.

Top 7 dấu hiệu của một email lừa đảo

1. Địa chỉ không quen thuộc/không hợp pháp: Kiểm tra tên hiển thị không khớp hoặc tên miền bất thường (ví dụ: "securitybank@yahoo.com" thay vì "securitybank.com").
2. Cảm giác khẩn cấp: Cẩn thận với các email có thuật ngữ khẩn cấp như "Khẩn cấp!" hoặc "Yêu cầu hành động!"
3. Lời chào chung chung: Cẩn thận với các lời chào thiếu cá nhân như "Kính gửi Khách hàng" thay vì tên của bạn.
4. Lỗi chính tả/ngữ pháp: Lỗi trong các email gửi hàng loạt thường là một dấu hiệu đáng ngờ.
5. Yêu cầu bất thường: Cẩn thận với các yêu cầu không mong muốn về việc chuyển tiền hoặc chia sẻ thông tin nhạy cảm.
6. Liên kết đáng ngờ: Di chuột qua các liên kết để xác minh đích đến của chúng; tránh nhấp nếu chúng có vẻ không đáng tin cậy.
7. Tệp đính kèm đáng ngờ: Tránh mở các tệp đính kèm không mong muốn, đặc biệt là các tệp .exe hoặc các loại tệp bất thường khác.

## Data Privacy

### 🔒🛡️ Tầm quan trọng của Bảo mật Dữ liệu

Trong các hoạt động internet hàng ngày, bạn có thể đối mặt với nhiều loại rủi ro an ninh mạng khác nhau – những mối đe dọa có thể làm tổn hại đến tính toàn vẹn, bảo mật và khả dụng của dữ liệu và hệ thống trong một tổ chức. Mọi người tại Test IO phải học cách nhận biết các mối đe dọa này để bảo vệ bản thân và tổ chức khỏi các cuộc tấn công có thể xảy ra.

### 🌐⚠️ Các Mối đe dọa Bên ngoài

Các mối đe dọa bên ngoài thường liên quan đến các rủi ro và lỗ hổng tiềm ẩn có nguồn gốc bên ngoài tổ chức. Khi được kết nối với internet, tất cả các máy tính và mạng – bao gồm cả mạng của Test IO – đều dễ bị tấn công bên ngoài và bị sử dụng hoặc truy cập trái phép bởi những kẻ xâm nhập (tin tặc). Chúng nhằm mục đích đánh cắp, làm hỏng hoặc làm gián đoạn tài nguyên của chúng ta, thường sử dụng các kỹ thuật như lừa đảo trực tuyến (phishing), phần mềm độc hại (malware), mã độc tống tiền (ransomware), tấn công SQL injection và tấn công từ chối dịch vụ phân tán (DDoS).

Một máy tính bị xâm nhập có thể ảnh hưởng đến mọi máy tính khác trên mạng.

### 👤⚠️ Các Mối đe dọa Nội bộ

Các mối đe dọa nội bộ thường đề cập đến các rủi ro và lỗ hổng tiềm ẩn có nguồn gốc từ bên trong tổ chức:

* Lỗi vô ý của nhân viên
* Lạm dụng cố ý (ví dụ: truy cập của nhân viên có ý đồ xấu ngoài phạm vi nhiệm vụ của họ)
* Lỗi trong các tập lệnh kiểm thử tự động khi dữ liệu kiểm thử là bản sao của dữ liệu sản xuất

Những mối đe dọa này có thể đến từ nhân viên, nhà thầu hoặc bất kỳ ai có quyền truy cập nội bộ vào hệ thống hoặc dữ liệu. Những mối đe dọa này, dù cố ý hay vô ý, đều có thể dẫn đến truy cập trái phép, rò rỉ dữ liệu, lạm dụng dữ liệu, sửa đổi hoặc thậm chí xóa dữ liệu.

### 📂🗂️ Các danh mục và phân loại dữ liệu

**Các danh mục dữ liệu theo nguồn gốc:**

* Dữ liệu cá nhân — Dữ liệu liên quan đến các cá nhân đang sống có thể được xác định từ dữ liệu đó, hoặc từ dữ liệu đó và các thông tin khác, mà người kiểm soát dữ liệu đang sở hữu hoặc có khả năng sẽ sở hữu.
* Dữ liệu khách hàng — Dữ liệu thuộc về khách hàng.
* Dữ liệu dự án/chương trình/tài khoản — Thông tin được tạo ra trong vòng đời dự án/chương trình/tài khoản.
* Dữ liệu công ty — Thông tin thuộc sở hữu của Test IO.

Nghiêm cấm việc sử dụng và chia sẻ các dữ liệu đã đề cập.

**Các phân loại bảo mật:**

* Công khai — Thông tin được chia sẻ tự do.
* Mật — Bất kỳ dữ liệu không công khai và không phải là dữ liệu tuyệt mật nào mà nếu bị rò rỉ, mất mát hoặc hư hỏng, có thể gây hại cho người tạo dữ liệu, chủ sở hữu, công ty hoặc khách hàng. Lớp này bao gồm hầu hết thông tin tại Test IO.
* Tuyệt mật — Bất kỳ dữ liệu nào mà nếu bị rò rỉ, mất mát hoặc hư hỏng, có thể gây hại đáng kể cho người tạo dữ liệu, chủ sở hữu, công ty hoặc khách hàng. Lớp thông tin này phải được bảo vệ và truy cập với sự cẩn trọng tối đa.

### 📁🔒 Dữ liệu Cá nhân

Nguyên tắc cơ bản của quyền riêng tư dữ liệu là bảo vệ thông tin cá nhân khỏi việc truy cập và lạm dụng trái phép hoặc bất hợp pháp.

Vì vậy, việc hiểu rõ thông tin cá nhân là gì sẽ giúp bạn nhận biết tốt hơn và áp dụng các biện pháp bảo vệ thích hợp khi xử lý dữ liệu đó, đảm bảo rằng dữ liệu được lưu trữ, sử dụng và chia sẻ một cách an toàn và tuân thủ các luật riêng tư liên quan cũng như chính sách của công ty.

*Tại Test IO, dữ liệu cá nhân, còn được gọi là thông tin nhận dạng cá nhân (PII), là bất kỳ dữ liệu nào có khả năng xác định một cá nhân cụ thể. Đó là bất kỳ thông tin nào có thể được sử dụng để phân biệt người này với người khác và có thể được sử dụng để giải mã dữ liệu ẩn danh.*

*Tại Test IO, PII được chia thành hai cấp độ khác nhau, với các quy trình và kiểm soát nội bộ khác nhau liên quan đến việc sử dụng chúng.*

**Dữ liệu cá nhân mật**

Là bất kỳ dữ liệu cá nhân nào không thuộc dữ liệu cá nhân tuyệt mật.

Dữ liệu cá nhân mật bao gồm:

* Tên
* Địa chỉ email
* Địa chỉ cá nhân
* Thông tin vị trí
* Đánh giá hiệu suất
* Ngày sinh
* Tình trạng hôn nhân
* Ảnh chụp
* Bất kỳ loại dữ liệu cá nhân nào khác không phải là tuyệt mật

**Dữ liệu cá nhân tuyệt mật**

Theo bất kỳ luật riêng tư dữ liệu nào, dữ liệu cá nhân tuyệt mật (PII tuyệt mật, PII nhạy cảm) yêu cầu các tiêu chuẩn bảo mật cao hơn nữa; nếu dữ liệu đó bị mất, bị xâm phạm hoặc bị tiết lộ mà không được phép, có thể dẫn đến tổn hại đáng kể, sự xấu hổ, bất tiện hoặc sự bất công đối với một cá nhân.

Dữ liệu cá nhân tuyệt mật bao gồm:

* Chủng tộc hoặc nguồn gốc dân tộc
* Quan điểm chính trị
* Niềm tin tôn giáo hoặc triết học
* Tư cách thành viên công đoàn
* Dữ liệu sinh trắc học
* Dữ liệu di truyền
* Hoạt động tình dục hoặc xu hướng tình dục
* Sức khỏe (thông tin y tế)
* Các thủ tục và biện pháp trừng phạt hành chính hoặc hình sự
* Dữ liệu tài chính
* Chi tiết thanh toán/công cụ tài chính
* Thông tin đăng nhập
* Hồ sơ cá nhân
* ID chính phủ
* Các biện pháp An sinh xã hội

### 🔒🚫 Thông tin Tuyệt mật

Các danh mục dữ liệu đặc biệt, chẳng hạn như thông tin sức khỏe cá nhân (PHI), thông tin thẻ thanh toán (PCI) và sở hữu trí tuệ của khách hàng, bao gồm thông tin cực kỳ nhạy cảm mà nếu bị mất, bị xâm phạm hoặc bị tiết lộ mà không được phép, có thể gây ra thiệt hại đáng kể.

Do tính chất nhạy cảm của dữ liệu này, nó phải tuân thủ các biện pháp bảo vệ pháp lý và quy định cụ thể. Xử lý không đúng cách có thể dẫn đến các hình phạt đáng kể và thiệt hại danh tiếng cho công ty. Do đó, các danh mục dữ liệu này thường được phân loại là tuyệt mật và yêu cầu mức độ bảo vệ cao từ tất cả các bên liên quan.

**Thông tin sức khỏe cá nhân (PHI)**

Bao gồm bất kỳ thông tin nào được tạo và sử dụng liên quan đến:

* Tình trạng sức khỏe thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân
* Thông tin cung cấp và thanh toán cho việc cung cấp dịch vụ chăm sóc sức khỏe cho cá nhân liên quan đến chẩn đoán, điều trị hoặc dịch vụ, bao gồm thông tin cá nhân nhận dạng cá nhân hoặc có thể là cơ sở hợp lý để tin rằng thông tin có thể được sử dụng để nhận dạng cá nhân

Thông tin về tình trạng sức khỏe của một cá nhân và các khoản thanh toán chăm sóc sức khỏe liên quan là dữ liệu nhạy cảm có thể liên kết với một người cụ thể và có thể gây hại cho họ nếu bị lạm dụng. Đây là lý do tại sao việc bảo vệ PHI lại rất quan trọng. Hơn nữa, việc không tuân thủ các quy định về xử lý PHI đúng cách có thể dẫn đến các hậu quả tài chính.

**Thông tin Thẻ Cá nhân (PCI)**

Trong khi cung cấp dịch vụ phát triển phần mềm và hỗ trợ cho khách hàng, các nhà phát triển của Test IO kết nối với các hệ thống của khách hàng có thể chứa và xử lý dữ liệu chủ thẻ (CHD).

Khách hàng yêu cầu Test IO thực hiện các hoạt động phát triển và hỗ trợ từ xa theo cách tuân thủ PCI DSS.

Các nhà phát triển có thể truy cập môi trường dữ liệu chủ thẻ của khách hàng từ xa thông qua kết nối VPN dựa trên các quyền được khách hàng cấp. Trong những trường hợp như vậy, các biện pháp kiểm soát chặt chẽ được quy định trong hợp đồng.

*Test IO không lưu trữ, xử lý hoặc truyền dữ liệu chủ thẻ và không có ý định di chuyển dữ liệu từ hệ thống của khách hàng sang hệ thống của Test IO.*

**Sở hữu Trí tuệ của Khách hàng**

Đề cập đến những điều sau:

* Thông tin tài chính (ví dụ: kế hoạch kinh doanh, kế toán, giải quyết nợ, nhà đầu tư, tài sản, định giá, chào thầu)
* Thông tin pháp lý (ví dụ: hợp đồng, kiện tụng, đàm phán, sở hữu trí tuệ, tổ chức nội bộ)
* Thông tin công nghiệp (ví dụ: quy trình công nghệ, giải pháp kỹ thuật, quy trình sản xuất, phương pháp hậu cần)
* Công nghệ và phương pháp phần mềm (bao gồm nhưng không giới hạn ở mã đối tượng phần mềm của bên thứ ba, dù có nằm trong phạm vi dự án hay không; mã nguồn; tệp cấu hình và hướng dẫn kỹ thuật và hướng dẫn sử dụng; các phiên bản alpha và beta của sản phẩm phần mềm của khách hàng hoặc bên thứ ba; phương pháp lập trình; kỹ thuật thiết kế; phương pháp tối ưu hóa phần mềm)
* Các sáng chế đã được cấp bằng sáng chế và đang chờ cấp bằng sáng chế, bản quyền và tài liệu viết
* Thông tin tiếp thị (ví dụ: thông tin khách hàng, chiến lược, kế hoạch quảng cáo)
* Các loại thông tin khác được coi là sở hữu trí tuệ của khách hàng
* Ảnh chụp có thể chứa thông tin tuyệt mật (nhạy cảm), đặc biệt là bằng cách tiết lộ tình trạng sức khỏe/tình trạng y tế hoặc nguồn gốc chủng tộc/dân tộc của một người, trong khi một số tình huống chỉ làm tăng khả năng liên kết như vậy.
  + Ví dụ, một bức ảnh cho thấy ai đó đang ngồi trên xe lăn có thể được coi là tuyệt mật vì nó có thể tiết lộ tình trạng sức khỏe của cá nhân. Tính nhạy cảm của thông tin đó là rõ ràng nếu ảnh được đi kèm với các dữ liệu cá nhân khác như tên của họ, v.v.

*Để ngăn chặn hiểu lầm hoặc vi phạm bảo mật, Test IO xử lý các ảnh chụp là thông tin cá nhân tuyệt mật.*

### 📊🔍 Cách Dữ liệu Cá nhân Có thể được Thu thập

Tương tác dưới đây là một ví dụ về cách dữ liệu cá nhân có thể được thu thập. Nếu bạn không chắc chắn cách xử lý một loại dữ liệu cụ thể, hãy tìm lời khuyên từ những người chịu trách nhiệm về bảo mật và quyền riêng tư ở cấp dự án (Quản lý Cộng đồng, Điều phối viên Dự án Cộng đồng và CSM) để được làm rõ.

## How to keep your device safe for Testing

Bảo vệ thiết bị của bạn rất quan trọng, không chỉ đối với bạn mà còn đối với khách hàng của chúng tôi. Trong bài viết này, chúng tôi sẽ cung cấp cho bạn một số mẹo về cách bảo vệ thiết bị của bạn khỏi vi-rút, rò rỉ dữ liệu, v.v. Việc giữ an toàn cho thiết bị của bạn cũng mang lại một lợi ích nữa cho bạn vì thiết bị sẽ luôn sẵn sàng để kiểm thử, vì vậy hãy giữ an toàn cho thiết bị của bạn!

### Bảo vệ chống rò rỉ dữ liệu

#### Bảo mật Trình duyệt

* Luôn giữ phiên bản trình duyệt của bạn được cập nhật.
* Không lưu mật khẩu/thông tin đăng nhập trong trình duyệt của bạn.

#### Mật khẩu mạnh

* Sử dụng mật khẩu mạnh, độc đáo cho tất cả các tài khoản của bạn.
* Tránh sử dụng thông tin dễ đoán như tên hoặc ngày sinh.
* Bật xác thực hai yếu tố (2FA) bất cứ khi nào có thể.
* Nếu bạn ở nơi công cộng, hãy che chắn thiết bị khi nhập mật khẩu. Bạn không bao giờ biết ai đang theo dõi hoặc ghi lại hoạt động của bạn.

#### Kết nối Wi-Fi an toàn

* Sử dụng mã hóa mạnh (WPA3) cho mạng Wi-Fi của bạn.
* Tránh Wi-Fi công cộng cho các hoạt động nhạy cảm; sử dụng mạng riêng ảo (VPN) nếu cần.

#### Mã hóa thiết bị của bạn

* Bật mã hóa thiết bị trên thiết bị di động và máy tính để bàn của bạn để bảo vệ dữ liệu được lưu trữ.

#### Bảo vệ thiết bị vật lý của bạn

* Thiết lập mật khẩu màn hình khóa hoặc xác thực sinh trắc học trên thiết bị di động.
* Khóa máy tính của bạn khi không sử dụng và sử dụng mật khẩu đăng nhập mạnh.
* Khi đi du lịch, hãy đảm bảo rằng bạn không để thiết bị của mình mà không được giám sát. Sử dụng két an toàn bất cứ khi nào có thể. Đừng bao giờ để thiết bị của bạn trên bàn cà phê ngay cả khi không có ai xung quanh trong quán cà phê.

#### Sao lưu dữ liệu thường xuyên

* Sao lưu các tệp quan trọng thường xuyên vào ổ đĩa ngoài hoặc dịch vụ đám mây an toàn.
* Đảm bảo đã bật sao lưu tự động và xác minh tính toàn vẹn của các bản sao lưu của bạn.

### Bảo vệ chống vi-rút

#### Cài đặt phần mềm chống vi-rút

* Sử dụng phần mềm chống vi-rút uy tín trên máy tính để bàn của bạn và giữ nó được cập nhật.
* Quét thiết bị của bạn thường xuyên để tìm phần mềm độc hại và vi-rút.

#### Luôn cập nhật phần mềm

* Thường xuyên cập nhật hệ điều hành, ứng dụng và chương trình chống vi-rút của bạn.

### Bảo vệ chống tin nhắn và email rác

#### Hãy nghi ngờ các tin nhắn và email

* Tránh nhấp vào các liên kết hoặc tải xuống tệp đính kèm từ các nguồn không xác định hoặc đáng ngờ.
* Xác minh tính hợp pháp của các tin nhắn hoặc email không mong muốn trước khi thực hiện bất kỳ hành động nào.

#### Sử dụng bộ lọc thư rác

* Bật bộ lọc thư rác trên tài khoản email của bạn để lọc các tin nhắn có khả năng gây hại.

#### Tránh các liên kết hủy đăng ký

* Hãy thận trọng khi nhấp vào các liên kết "hủy đăng ký" trong các email đáng ngờ, vì chúng có thể được sử dụng để xác nhận địa chỉ email của bạn với những kẻ gửi thư rác.

#### Quản lý cài đặt thông báo

* Tùy chỉnh cài đặt thông báo trên thiết bị di động của bạn để giảm khả năng tiếp xúc với tin nhắn rác.

#### Tự giáo dục bản thân

* Luôn cập nhật thông tin về các kỹ thuật lừa đảo và các trò lừa đảo phổ biến để nhận biết và tránh chúng.

### Các mẹo bổ sung

#### Xem lại quyền ứng dụng

* Thường xuyên xem xét và quản lý quyền ứng dụng trên thiết bị di động của bạn để hạn chế quyền truy cập không cần thiết vào dữ liệu của bạn.

#### Sử dụng ứng dụng nhắn tin an toàn

* Chọn các ứng dụng nhắn tin được mã hóa cho các cuộc trò chuyện bí mật.

#### Giám sát hoạt động tài khoản

Thường xuyên kiểm tra hoạt động và sao kê tài khoản của bạn để tìm bất kỳ giao dịch đáng ngờ hoặc trái phép nào.

### Kiểm tra thiết bị của bạn!

Nếu bạn không chắc chắn về thiết bị của mình, vui lòng chạy quét phần mềm độc hại trên (các) thiết bị kiểm thử của bạn.

## DOs and DON'Ts in Protecting Your Testing Devices

Với vai trò là một kiểm thử viên phần mềm, việc bảo vệ thiết bị của bạn là vô cùng quan trọng để đảm bảo tính toàn vẹn và bảo mật của các dự án bạn đang thực hiện. Vai trò của bạn thường liên quan đến việc xử lý dữ liệu nhạy cảm, truy cập vào các hệ thống khác nhau và đảm bảo phần mềm đáp ứng các tiêu chuẩn bảo mật.

Bài viết này cung cấp các mẹo thực tế cho kiểm thử viên phần mềm, giúp bạn bảo mật thiết bị, bảo vệ dữ liệu và duy trì sự tin cậy. Bằng cách tuân thủ các hướng dẫn này, bạn có thể giảm thiểu rủi ro bảo mật và tập trung vào việc cung cấp phần mềm chất lượng cao.

### 🛡️ Cách bảo vệ thiết bị của bạn

Để thiết bị của bạn an toàn khi kiểm thử môi trường khách hàng, bạn cần đảm bảo cả an toàn vật lý và an toàn kỹ thuật số cho thiết bị.

Các bước để bảo vệ dữ liệu của bạn:

* Giữ thiết bị của bạn an toàn: Cẩn thận với nơi bạn lưu trữ các thiết bị của mình, như USB và máy tính xách tay.
* Khóa máy tính của bạn: Luôn khóa máy tính khi bạn rời đi, dù chỉ trong thời gian ngắn.
* Sử dụng mật khẩu mạnh: Cân nhắc sử dụng mật khẩu dài, phức tạp để tăng cường bảo mật.
* Mã hóa tệp của bạn: Nếu bạn có các tệp bí mật, hãy nghĩ đến việc mã hóa chúng.
* Bảo vệ máy tính xách tay khi đi du lịch: Đừng để thiết bị của bạn mà không được giám sát, đặc biệt là trong ô tô hoặc trong hành lý của bạn.
* Báo cáo thiết bị bị mất hoặc bị đánh cắp: Nếu bạn mất một thiết bị di động hoặc phương tiện lưu trữ di động, hãy báo cáo cho Bộ phận Hỗ trợ Test IO và thay đổi mật khẩu đăng nhập của bạn.

Nếu bạn nghĩ máy tính của mình bị nhiễm vi-rút:

* Đóng tất cả các chương trình, tắt hệ thống và mang máy tính của bạn đến văn phòng bảo trì được chứng nhận.

**✅ NÊN làm:**

* Đặt mật khẩu mạnh.
* Khóa thiết bị khi không sử dụng.
* Cập nhật phần mềm thường xuyên, bao gồm hệ điều hành và trình duyệt của bạn.
* Hạn chế quyền truy cập vào máy tính của bạn khi bạn không sử dụng nó.
* Thận trọng khi trực tuyến: Cẩn thận với những gì bạn nhận được và người bạn nói chuyện.

**❌ KHÔNG NÊN làm:**

* Không chia sẻ mật khẩu hoặc bất kỳ thông tin nhạy cảm nào.
* Không để thiết bị của bạn không được giám sát.
* Không sử dụng phần mềm lỗi thời/không được hỗ trợ.
* Không cho phép người khác truy cập máy tính của bạn khi bạn không sử dụng.
* Không mở email đáng ngờ hoặc nhấp vào tệp đính kèm hoặc liên kết lạ.

### ⛔ Các Hoạt động Bị cấm

Bạn không được phép sử dụng, lưu trữ hoặc truyền tải bất kỳ điều nào sau đây:

* Phần mềm ngang hàng (P2P), như các ứng dụng torrent, trừ khi được ủy quyền.
* Phần mềm chia sẻ tài liệu có bản quyền, như nhạc hoặc phim, mà không có sự cho phép.
* Phần mềm khiêu dâm hoặc truy cập các trang web khiêu dâm.
* Các trình tạo khóa và phần mềm bẻ khóa, bao gồm các công cụ hack Wi-Fi.
* Các công cụ ẩn danh hóa và phần mềm bỏ qua hệ thống giám sát hoặc theo dõi mạng.
* Phần mềm lỗi thời hoặc không được hỗ trợ mà dễ bị tấn công.
* Các công cụ mã hóa không chuẩn.
* Phần mềm khai thác tiền điện tử hoặc sử dụng tài nguyên của công ty cho mục đích cá nhân.
* Phần mềm hack để tấn công cơ sở hạ tầng hoặc ứng dụng.