# 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?

## Data Privacy

## How to keep your device safe for Testing

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