|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**BÁO CÁO MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**PHISHING**

SINH VIÊN THỰC HIỆN: **LƯU TRƯỜNG NGHĨA**

MSSV: 1811061958 LỚP: 18DTHB3

**VÕ XUÂN THỊNH**

MSSV: 1811062007 LỚP: 18DTHB3

**LÊ TUẤN KIỆT**

MSSV: 1811062164 LỚP: 18DTHB3

TP. HỒ CHÍ MINH, 4/2021

|  |  |
| --- | --- |
| logomobile.png | BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM** |

**BÁO CÁO MÔN HỌC**

**BẢO MẬT THÔNG TIN**

**PHISHING**

NGÀNH: **CÔNG NGHỆ THÔNG TIN**

MÔN HỌC: **BẢO MẬT THÔNG TIN**

SINH VIÊN THỰC HIỆN: **LƯU TRƯỜNG NGHĨA**

MSSV: 1811061958 LỚP: 18DTHB3

**VÕ XUÂN THỊNH**

MSSV: 1811062007 LỚP: 18DTHB3

**LÊ TUẤN KIỆT**

MSSV: 1811062164 LỚP: 18DTHB3

GVHD: **THS. TỐNG THANH VĂN**

TP. Hồ Chí Minh, 4/2021

**Mục Lục**

[Lời Mở Đầu 1](#_Toc70541512)

[CHƯƠNG 1. TỔNG QUAN NỘI DUNG BÁO CÁO 2](#_Toc70541513)

[1.1. GIỚI THIỆU VỀ CÔNG CỤ THỰC HIỆN ĐỀ TÀI 2](#_Toc70541514)

[1.1.1. Tổng quan về Visual Code 2](#_Toc70541515)

[1.1.1.1. Một số tính năng của Visual Code 2](#_Toc70541516)

[1.1.2. Tổng quan về nhà cung cấp hosting miễn phí 000webhost 5](#_Toc70541517)

[1.1.2.1. Khái niệm 000webhost 5](#_Toc70541518)

[1.1.2.2. Cách sử dụng 000webhost 7](#_Toc70541519)

[1.1.2.3. Tính năng và hiệu suất của 000webhost 8](#_Toc70541520)

[1.1.2.4. Ưu điểm của 000webhost 15](#_Toc70541521)

[1.2. Giới thiệu về ngôn ngữ lập trình PHP 18](#_Toc70541522)

[1.2.1. Vì sao nên sử dụng ngôn ngữ PHP trong lập trình Web 20](#_Toc70541523)

[CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG 22](#_Toc70541524)

[2.1. Giới thiệu về tấn công giả mạo Phishing 22](#_Toc70541525)

[2.1.1. Các phương thức tấn công của Phishing 23](#_Toc70541526)

[2.1.1.1. Giả mạo email 23](#_Toc70541527)

[2.1.1.2. Giả mạo Website 24](#_Toc70541528)

[2.1.1.3. Vượt qua các bộ lọc Phishing 24](#_Toc70541529)

[2.1.2. Hình thức tấn công Phishing 24](#_Toc70541530)

[2.1.2.1. Tấn công Phishing kết hợp nhiều phương tiện 24](#_Toc70541531)

[2.1.2.2. Tấn công Phishing lợi dụng các tin tức nóng 25](#_Toc70541532)

[2.1.2.3. Tấn công lừa đảo vì tiền 26](#_Toc70541533)

[2.1.3. Cách phòng chống Phishing 27](#_Toc70541534)

[2.1.3.1. Đối với cá nhân 27](#_Toc70541535)

[2.1.3.2. Đối với các tổ chức, doanh nghiệp 27](#_Toc70541536)

[2.1.3.3. Phòng chống bằng các phần mềm khác 28](#_Toc70541537)

[2.1.4. Cách nhận biết Phishing lừa đảo qua Email và trang Website giả mạo 29](#_Toc70541538)

[2.1.4.1. Cách xác định một Email lừa đảo 29](#_Toc70541539)

[CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM 36](#_Toc70541540)

[3.1. Giao diện sản phẩm 36](#_Toc70541541)

[3.1.1. Giao diện trang chủ đăng nhập 36](#_Toc70541542)

[3.1.2. Form lưu trữ dữ liệu 37](#_Toc70541543)

[3.1.3. Source code giao diện sản phẩm 38](#_Toc70541544)

[3.1.4. Source code giao diện để lấy cắp dữ liệu 38](#_Toc70541545)

[3.2. Cách sản phẩm đánh cắp dữ liệu 39](#_Toc70541546)

[3.3. Kết luận 40](#_Toc70541547)

# Lời Mở Đầu

Đồ án môn học với những ngôn ngữ lập trình khá phổ biến với sinh viên khoa Công Nghệ Thông Tin như ngôn ngữ Java để tự thống kê kiến thức và lên ý tưởng cho những đồ án của mình. Đó là yêu cầu và cũng như thách thức đối với sinh viên khi làm quen với thực hành từ những lý thuyết sách vở.

Trong môi trường mạng máy tính, một lượng tin hay một khối dữ liệu khi được gửi từ người gửi đến người nhận thường phải đi qua nhiều trạm với nhiều người sử dụng khác nhau, không ai đảm bảo rằng thông tin dữ liệu ấy sẽ được an toàn tuyệt đối trước khi đến với người nhận.

Chúng ta đã nghe nhiều về những mối đe dọa từ Internet đối với sự riêng tư của chúng ta hay những kẻ chuyên đánh cắp mật khẩu, những kẻ săn tin chuyên nghiệp và cả những kẻ quấy rối, chúng sẽ không bao giờ để yên cho chúng ta.

Chính vì vậy hôm nay với sự hướng dẫn của thầy Tống Thanh Văn nhóm chúng em sẽ trình bày về phương thức PHISHING (tấn công giả mạo) bao gồm các hình thức tấn công PHISHING cũng như những cách phòng tránh bản thân bị tấn công PHISHING.

Xuất phát từ những lý do trên, cùng với sự hướng dẫn của Giảng viên Tống Thanh Văn, chúng em thực hiện 1 số chức năng như mã hóa mật khẩu, phân quyền account, theo dõi người dùng… để vận dụng những kiến thức đã được học vào thực tiễn, xây dựng một hệ thống bảo mật cho người dùng.

Chúng em xin chân thành cảm ơn!

Sinh viên thực hiện

**Lưu Trường Nghĩa**

**Võ Xuân Thịnh**

**Lê Tuấn Kiệt**

# CHƯƠNG 1. TỔNG QUAN NỘI DUNG BÁO CÁO

## 1.1. GIỚI THIỆU VỀ CÔNG CỤ THỰC HIỆN ĐỀ TÀI

### 1.1.1. Tổng quan về Visual Code



Visual Studio Code (VS Code hay VSC) là một trong những trình soạn thảo mã nguồn phổ biến nhất được sử dụng bởi các lập trình viên. Nhanh, nhẹ, hỗ trợ đa nền tảng, nhiều tính năng và là mã nguồn mở chính là những ưu điểm vượt trội khiến VS Code ngày càng được ứng dụng rộng rãi.

Là một trình biên tập lập trình code miễn phí dành cho Windows, Linux và macOS, Visual Studio Code được phát triển bởi Microsoft. Nó được xem là một sự kết hợp hoàn hảo giữa IDE và Code Editor.

Visual Studio Code hỗ trợ chức năng debug, đi kèm với Git, có syntax highlighting, tự hoàn thành mã thông minh, snippets, và cải tiến mã nguồn. Nhờ tính năng tùy chỉnh, Visual Studio Code cũng cho phép người dùng thay đổi theme, phím tắt, và các tùy chọn khác.

#### 1.1.1.1. Một số tính năng của Visual Code

**Hỗ trợ nhiều ngôn ngữ lập trình**

Visual Studio Code hỗ trợ nhiều ngôn ngữ lập trình như C/C++, C#, F#, Visual Basic, HTML, CSS, JavaScript, … Vì vậy, nó dễ dàng phát hiện và đưa ra thông báo nếu chương chương trình có lỗi.

**Hỗ trợ đa nền tảng**

Các trình viết code thông thường chỉ được sử dụng hoặc cho Windows hoặc Linux hoặc Mac Systems. Nhưng Visual Studio Code có thể hoạt động tốt trên cả ba nền tảng trên.

**Cung cấp kho tiện ích mở rộng**

Trong trường hợp lập trình viên muốn sử dụng một ngôn ngữ lập trình không nằm trong số các ngôn ngữ Visual Studio hỗ trợ, họ có thể tải xuống tiện ích mở rộng. Điều này vẫn sẽ không làm giảm hiệu năng của phần mềm, bởi vì phần mở rộng này hoạt động như một chương trình độc lập

**Kho lưu trữ an toàn**

Đi kèm với sự phát triển của lập trình là nhu cầu về lưu trữ an toàn. Với Visual Studio Code, người dùng có thể hoàn toàn yên tâm vì nó dễ dàng kết nối với Git hoặc bất kỳ kho lưu trữ hiện có nào.

**Hỗ trợ web**

Visual Studio Code hỗ trợ nhiều ứng dụng web. Ngoài ra, nó cũng có một trình soạn thảo và thiết kế website.

**Lưu trữ dữ liệu dạng phân cấp**

Phần lớn tệp lưu trữ đoạn mã đều được đặt trong các thư mục tương tự nhau. Ngoài ra, Visual Studio Code còn cung cấp các thư mục cho một số tệp đặc biệt quan trọng.

**Hỗ trợ viết Code**

Một số đoạn code có thể thay đổi chút ít để thuận tiện cho người dùng. Visual Studio Code sẽ đề xuất cho lập trình viên các tùy chọn thay thế nếu có.

**Hỗ trợ thiết bị đầu cuối**

Visual Studio Code có tích hợp thiết bị đầu cuối, giúp người dùng khỏi phải chuyển đổi giữa hai màn hình hoặc trở về thư mục gốc khi thực hiện các thao tác.

**Màn hình đa nhiệm**

Người dùng Visual Studio Code có thể mở cùng lúc nhiều tệp tin và thư mục – mặc dù chúng không hề liên quan với nhau

**Intellisense**

Hầu hết các trình viết mã đều có tính năng nhắc mã Intellisense, nhưng ít chương trình nào chuyên nghiệp bằng Visual Studio Code. Nó có thể phát hiện nếu bất kỳ đoạn mã nào không đầy đủ. Thậm chí, khi lập trình viên quên không khai báo biến, Intellisense sẽ tự động giúp họ bổ sung các cú pháp còn thiếu.

**Hỗ trợ Git**

Visual Studio Code hỗ trợ kéo hoặc sao chép mã trực tiếp từ GitHub. Mã này sau đó có thể được thay đổi và lưu lại trên phần mềm.

**Vì sao nên dùng Visual Code**

- Hỗ trợ đa nền tảng: Windows, Linux, Mac

- Hỗ trợ đa ngôn ngữ: C/C++, C#, F#, Visual Basic, HTML, CSS, JavaScript, JSON

- Ít dung lượng

- Tính năng mạnh mẽ

- Intellisense chuyên nghiệp

- Giao diện thân thiện

- Và trên hết, **Visual Studio Code** là phần mềm miễn phí, được đông đảo lập trình viên trên thế giới sử dụng.

### 1.1.2. Tổng quan về nhà cung cấp hosting miễn phí 000webhost

#### 1.1.2.1. Khái niệm 000webhost



000webhost là một trong nhiều các nhà cung cấp dịch vụ hosting trên thế giới. Điều khiến người ta nhớ đến họ gắn liền với gói dịch vụ hosting miễn phí. Trải qua nhiều năm, gói dịch vụ hosting miễn phí đó vẫn duy trì và giải quyết được nhiều nhu cầu cá nhân của mọi người.

Hôm nay, chúng ta sẽ thử “mổ xẻ” để xem bên trong cái mác nhà cung cấp hosting miễn phí này có gì đặc biệt nhé.

**000webhost thuộc sở hữu của Hostinger**

Có thể các bạn đã biết, đứng đằng sau nhà cung cấp hosting miễn phí này là [Hostinger](https://viettelidc.com.vn/tin-tuc/ban-da-tung-nghe-noi-ve-hostinger-la-gi-hay-chua). Đây cung là một trong nhiều nhà cung cấp các dịch vụ hosting hiện nay. Và có lẽ, với 000webhost, đây là chiến lược sử dụng các gói hosting miễn phí của Hostinger để thu hút khách hàng tiềm năng.

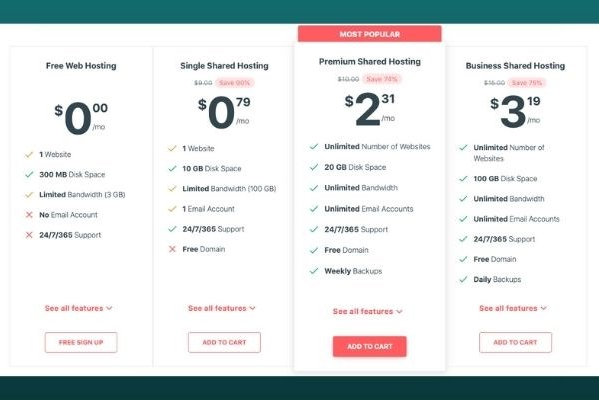
Về bản thân Hostinger, họ cũng có khá nhiều dịch vụ khác “cao cấp” hơn so với 000webhost. Ở Hostinger dường như không hoặc ít có khái niệm hosting miễn phí. Thay vào đó, nếu bạn muốn sử dụng dịch vụ này, hãy tìm đến 000webhost. Điều này tránh việc khách hàng sẽ đánh giá Hostinger là một website chuyên cung cấp các dịch vụ hosting miễn phí. Như vậy có thể sẽ làm ảnh hưởng đến thương hiệu của họ.

**Ngoài hosting miễn phí ra còn có các gói trả phí**

Đặc sản ở 000webhost là hosting miễn phí. Nhưng cũng không khó để tìm cho mình một dịch vụ hosting trả phí ở đây. Điều đáng ngạc nhiên là cho dù gắn mác hosting trả phí nhưng về bản chất, giá của nó cũng không khác hosting miễn phí là mấy.

Chỉ với chưa tới 1 USD là bạn đã có thể sở hữu cho mình một gói hosting ở đây rồi. Đương nhiên, giới hạn dung lượng là điều chắc chắn. Về cơ bản, gói trả phí thấp nhất này cũng tương đương với gói hosting miễn phí. Chỉ khác là bạn sẽ nhận được thêm hỗ trợ từ 000webhost mà thôi.

Tính đến thời điểm hiện tại, gói hosting trả phí cao nhất tại 000webhost chỉ dừng lại ở 3.19 USD/tháng. Rõ ràng nó chỉ phù hợp cho những nhu cầu cá nhân hơn là kinh doanh. Nếu như vậy thì xem ra, hosting miễn phí vẫn tiết kiệm hơn nhiều đúng không nào?



*Hosting miễn phí là một trong nhiều lựa chọn tại 000webhost*

#### 1.1.2.2. Cách sử dụng 000webhost

Mục đích của việc cung cấp hosting miễn phí tại 000webhost theo chúng tôi đánh giá là “miếng mồi câu” để giúp họ tiếp cận khách hàng. Nghĩa là họ sẽ cung cấp các gói hosting miễn phí, thu hút nhiều người dùng. Sau đó khi hệ thống của khách hàng phình to dần lên thì việc sử dụng hosting trả phí là điều đương nhiên.

Chính vì thế mà việc đăng ký hosting miễn phí tại 000webhost dễ hơn bao giờ hết. Chỉ với một địa chỉ email, trong vòng chưa đến một phút là bạn đã đăng ký thành không gói hosting miễn phí của họ rồi.

Hosting miễn phí sẽ được khởi tạo gần như mặc định ngay sau đó. Bạn cũng sẽ không cần phải mất thời gian yêu cầu hay đề xuất gì với 000webhost cả. Đáng tiếc là với gói hosting miễn phí, nếu như bạn không có chuyên môn về công nghệ, khi gặp vấn đề thì sẽ không có ai hỗ trợ bạn cả. Trong thoả thuận dịch vụ trước khi đồng ý sử dụng hosting miễn phí, họ cũng đã nếu rất rõ vấn đề này rồi.

Nhưng bạn cũng đừng quá lo, không phải vì là gói hosting miễn phí mà họ gây khó dễ cho việc triển khai cài đặt đâu. Nó cũng khá cơ bản và dễ dàng như các gói hosting khác mà thôi.

#### 1.1.2.3. Tính năng và hiệu suất của 000webhost

Nhìn chung, 000webhost cung cấp ít tài nguyên hơn so với nhiều đối thủ cạnh tranh – ví dụ: băng thông, dung lượng ổ đĩa, miền và miền phụ đều bị giới hạn.

Nếu tất cả những gì bạn cần là một thiết lập dịch vụ lưu trữ đơn giản, nó sẽ làm tốt công việc. Nếu bạn muốn có thể tùy chỉnh các thiết lập của mình, bạn sẽ cần phải tìm ở nơi khác.

000webhost có trình tạo website riêng. Mặc dù đôi khi nó có thể hơi rườm rà, nhưng nó không tệ đối với một dịch vụ miễn phí. Nó cũng cung cấp hàng trăm mẫu miễn phí, cũng như các khóa học miễn phí về mọi thứ từ phát triển web và SEO cho đến tiếp thị kỹ thuật số và phát triển trò chơi.

**Nó miễn phí!**

Mọi người đều thích quà tặng. Và với 000webhost, bạn có thể nhận được gói dịch vụ lưu trữ “miễn phí vĩnh viễn”. Không giống như những nhà lưu trữ miễn phí khác, 000webhost sẽ không đặt quảng cáo trên website của bạn. Tuy nhiên, ngay cả công ty cũng thừa nhận rằng dịch vụ lưu trữ này đi kèm với những hạn chế nhất định.

Điều đó có thể không quan trọng với bạn tại thời điểm này. Có thể bạn đang học cách xây dựng website và bạn chỉ muốn nghịch một chút. Hoặc có thể bạn đang làm việc trên một website lớn và bạn cần kiểm thử nó trực tuyến, nhưng bạn không muốn bắt đầu trả tiền cho dịch vụ lưu trữ thực sự trước khi nó sẵn sàng.

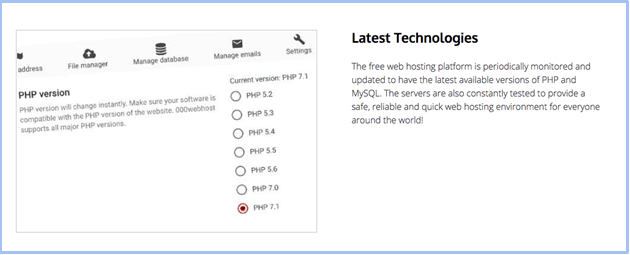
Nhưng hãy chắc chắn bạn có nghiên cứu tìm hiểu. Cần lưu ý 000webhost đã bị rò rỉ dữ liệu nghiêm trọng vào năm 2015. Tuy nhiên, công ty đã xin lỗi và giải quyết tất cả các vấn đề, đưa nó trở thành một nhà lưu trữ an toàn hơn rất nhiều so với trước khi bị tấn công.

**Tường lửa tích hợp và bảo vệ chống DDoS**

Dịch vụ lưu trữ của 000webhost bao gồm một tường lửa và bảo vệ chống DDoS được tích hợp sẵn, và công ty có một đội ngũ quản trị tận tâm luôn theo dõi các máy chủ của mình 24/24. Điều này đồng nghĩa: mặc dù dịch vụ lưu trữ của bạn là miễn phí, nhưng bạn vẫn có thể yên tâm vì luôn có người giám sát trên máy chủ.

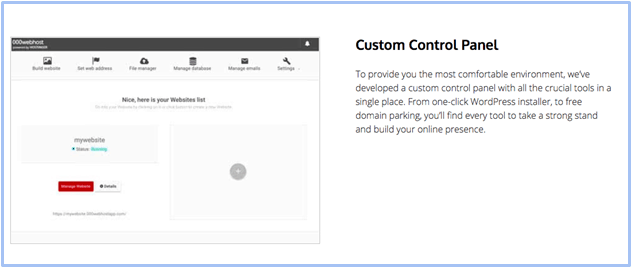
**Các tính năng tiên tiến**

Một vài trong số những “tính năng tiên tiến” mà 000webhost cung cấp sẽ được xếp là tiêu chuẩn bởi các nhà lưu trữ web khác, nhưng chúng vẫn đáng chú ý. Các tính năng này bao gồm hỗ trợ cho PHP, MySQL, Curl, GD2, Zend, VML, fopen (), các PHP socket, Ioncube Loader và các tệp .htaccess.



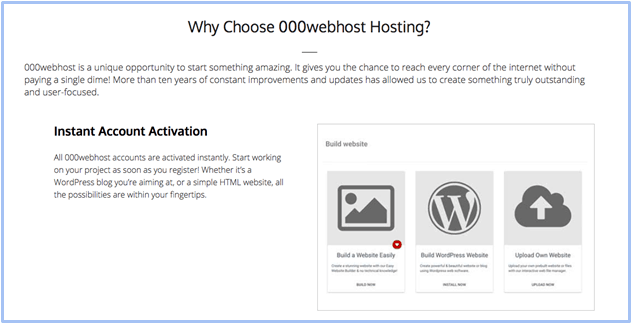
**Bảng điều khiển tùy chỉnh**

Ngoài cPanel, 000webhost còn có một bảng điều khiển tùy chỉnh với một loạt các công cụ quản trị bổ sung, bao gồm nhiều trình cài đặt bằng một cú nhấp để bạn có thể bắt đầu website mới của mình. Bạn cũng sẽ có thể lưu trú miền, quản lý tên miền và thực hiện các tác vụ quản trị cơ bản khác.



**Kích hoạt tài khoản tức thì**

Tất cả tài khoản mới đều được kích hoạt ngay lập tức và các nâng cấp cũng được xử lý tức thì.Điều đó đồng nghĩa bạn có thể bắt đầu ngay lập tức, ngay cả khi bạn đang dùng gói miễn phí.



**DỄ SỬ DỤNG**

**Dịch vụ lưu trữ web dành cho những tay mơ**

Một trong những điểm cộng lớn nhất của 000webhost là độ dễ dàng để bắt đầu của nó. Quy trình nhập môn khá suôn sẻ và bạn có thể cài đặt một CMS hoặc sử dụng trình tạo web trực quan mà không phải chờ đợi tài khoản của bạn được cấu hình và cài đặt.

Bảng quản trị độc quyền có thể hơi gây lúng túng lúc đầu, nhưng rồi bạn cũng sẽ hiểu nó thôi và ngoài chuyện này ra thì tất cả đều khá đơn giản.

**Tạo một tài khoản**

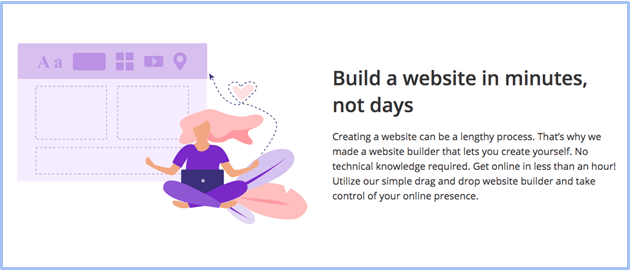
Như mọi khi, tôi nghĩ rằng rất đáng thử nghiệm quy trình bằng cách đăng ký và tạo một tài khoản. Việc bắt đầu khá dễ dàng, nhưng nền tảng sẽ cố gắng bán thêm các tính năng như sao lưu hàng ngày và bảo vệ Cloudflare trong suốt quá trình. Nếu bạn không cẩn thận, bạn có thể phải trả một hóa đơn khá lớn, nhưng ít nhất có thể sẽ đáng để xem xét một số tiện ích bổ trợ.

**Kết nối một miền và cài đặt WordPress**

Tôi cũng đã thử kết nối một tên miền và cài đặt WordPress bằng cách sử dụng một trong những trình cài đặt bằng một cú nhấp. Toàn bộ quy trình dễ dàng và rõ ràng đến đáng ngạc nhiên. Tôi thậm chí còn nhận được các hướng dẫn trên màn hình về cách kết nối miền, bao gồm cả các địa chỉ của các máy chủ tên miền.

**Nhiều công cụ tạo website khác nhau**

Với tư cách là một khách hàng của 000webhost, bạn có thể lựa chọn sử dụng trình cài đặt bằng một cú nhấp cho các hệ thống quản lý nội dung phổ biến hoặc chuyển sang trình tạo website kéo thả. Nếu cả hai cách này đều không phù hợp với bạn, bạn cũng có thể kết nối thông qua FTP và tải lên trình cài đặt của riêng mình.



**Miền phụ miễn phí**

Rất có thể bạn sẽ muốn đăng ký một tên miền riêng và trỏ nó vào máy chủ 000webhost của bạn. Nếu không, bạn có thể tận dụng các miền phụ miễn phí bằng cách lưu trữ website của bạn tại [YOURNAME].000webhostapp.com.

Việc này có thể hữu ích như một cách để bạn truy cập website của mình trong khi bạn đang phát triển nó, trước khi thông qua URL mà bạn dự định sử dụng.

**Dễ dàng nâng cấp**

000webhost giúp bạn dễ dàng nâng cấp gói dịch vụ lưu trữ của mình nếu bạn cần thêm không gian máy chủ hoặc tài nguyên. Việc chuyển diễn ra nhanh, dễ dàng và liền mạch, đồng thời việc nâng cấp sẽ mở khóa các đặc quyền bổ sung như quyền tiếp cận với hỗ trợ trực tiếp.

**HIỆU SUẤT**

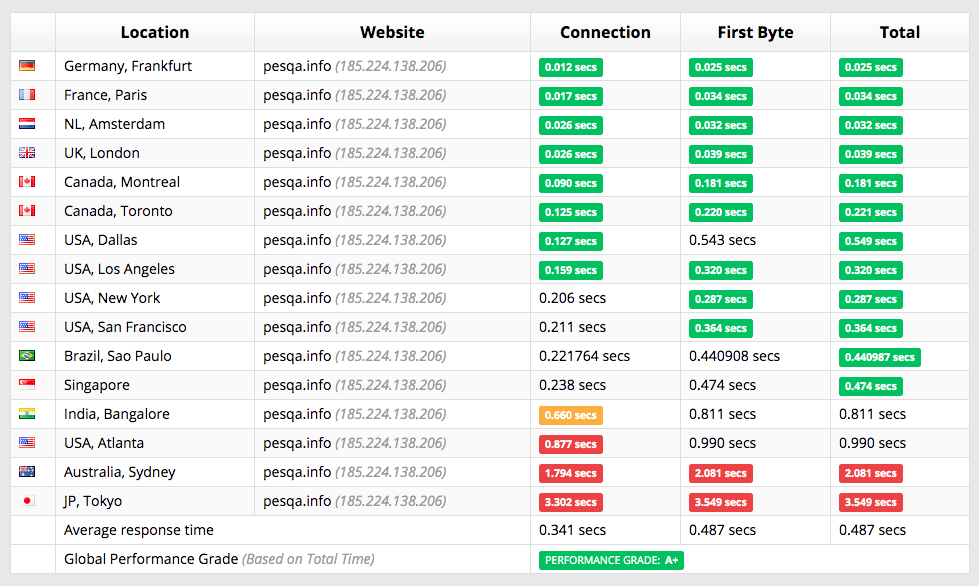
**Phần lớn là ổn, nhưng không phải tốt nhất**

000webhost tuyên bố một cách rất thuyết phục rằng sẽ cung cấp “các máy chủ lưu trữ web miễn phí có thời gian hoạt động 99,9% với độ tin cậy vô song”. Mặc dù có vẻ như nhà lưu trữ web nào cũng đều tuyên bố như vậy, nhưng một số lại tốt hơn những công ty khác.

Nếu bạn kiểm tra các đánh giá của 000webhost, hầu hết khách hàng có vẻ khá hài lòng với hiệu suất. Dịch vụ hỗ trợ khách hàng là thứ mà họ không yêu thích, nhưng tôi sẽ nói về nó sau.

Để kiểm tra hiệu suất, tôi đã chạy một vài bài kiểm thử riêng. Tôi khá ấn tượng bởi các tốc độ tải trên phần lớn Hoa Kỳ và châu Âu, nhưng các tốc độ siêu chậm ở Sydney và Tokyo đã kéo mức trung bình xuống. Vì một số lý do, các máy chủ cũng tải chậm ở Atlanta.

Nhìn chung, xét đến việc đây là một nhà cung cấp miễn phí thì các kết quả này là rất tốt.



**HỖ TRỢ**

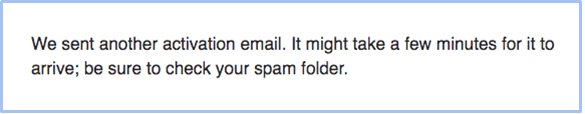
**Hỗ trợ bị giới hạn đối với người dùng miễn phí**

Nếu bạn chọn gói miễn phí của 000webhost, bạn sẽ phải tự xoay sở, đây là một lý do khác khiến bạn sẽ muốn xem xét việc nâng cấp.

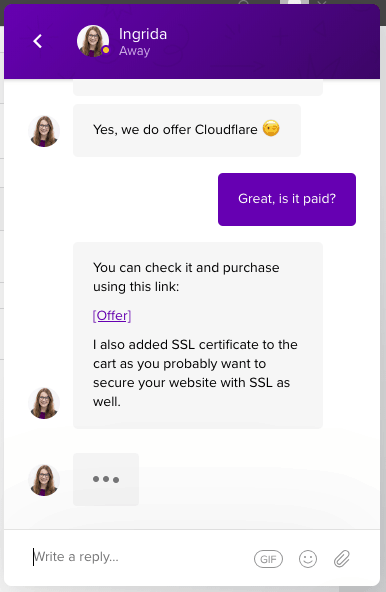
Tin tốt là có một diễn đàn thảo luận nơi bạn có thể liên lạc với các khách hàng khác và các khách hàng trả phí để có quyền tiếp cận đội hỗ trợ 24/7hoạt động mọi ngày trong năm.

Tôi quyết định liên hệ với đội hỗ trợ để kiểm thử và trải nghiệm không được suôn sẻ như nó đã có thể.

Trò chuyện trực tiếp bị vô hiệu hóa đối với những người không phải là khách hàng và theo kinh nghiệm của tôi, đội ngũ không phản hồi các truy vấn trên các trang mạng xã hội. Thêm vào đó, mặc dù tôi đã cố gắng đăng ký vào các diễn đàn thảo luận, nhưng tôi chưa bao giờ nhận được email xác nhận.



Tuy nhiên, các nhân viên rất thân thiện và hết sức giúp đỡ khi tôi liên hệ với họ với tư cách một khách hàng có trả phí. Mỗi lần tôi nhảy vào trò chuyện trực tiếp với tư cách là một khách hàng trả phí, nhân viên đều tiếp nhận ngay lập tức và giải quyết vấn đề của tôi một cách nhanh chóng.



#### 1.1.2.4. Ưu điểm của 000webhost

**KHAI THÁC. Đăng ký dễ dàng với đăng ký 1-click**

Đăng ký 000webhost là một trải nghiệm nhanh chóng và không gây ngạc nhiên. Định dạng thông thường là phải trải qua quá trình đăng ký, trong đó bạn phải điền rất nhiều chi tiết và cung cấp cho họ tất cả các loại thông tin, sau đó xác nhận địa chỉ email của bạn.

Với 000webhost, bạn có thể thực hiện các thao tác trên hoặc tận dụng đăng ký nhấp chuột 1 của chúng nơi bạn có thể đăng nhập bằng tài khoản Google hoặc Facebook của mình. Tôi đã thử đăng ký Google và nó rất nhanh, không đau và hoạt động tốt.

**KHAI THÁC. Hướng dẫn xây dựng trang web**

*Bắt đầu một trang web mới với 000webhost dễ dàng như một chuyến tham quan có hướng dẫn*

Điều đầu tiên sẽ xảy ra khi bạn đăng nhập vào tài khoản mới được tạo là hệ thống 000webhost sẽ cung cấp cho bạn một loạt các câu hỏi. Tôi đã thấy điều này trước đây trên các nhà xây dựng trang web khác như Shopify và nó rất hữu ích, đặc biệt là trong trường hợp 000webhost.

Như tôi đã đề cập trước đó trong phần giới thiệu của mình, 000webhost dành cho những người [mới xây dựng trang web](https://www.webhostingsecretrevealed.net/vi/blog/web-hosting-guides/make-a-website/) và điều này có thể là một trợ giúp lớn. Thay vì buộc họ phải xem xét các chi tiết kỹ thuật về một bản dựng, 000webhost giúp trình bày một chuỗi các câu hỏi suy nghĩ sẽ hướng dẫn việc xây dựng.

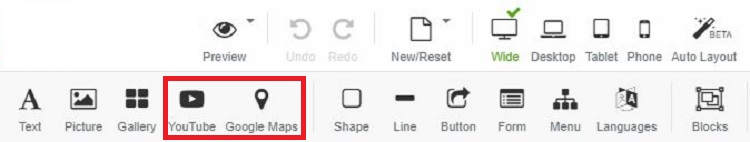
**KHAI THÁC. Bốn tùy chọn tạo trang web**

Đối với những người có thể không hoàn toàn mới đối với quy trình xây dựng trang web, bạn có thể bỏ qua các câu hỏi được hướng dẫn và bỏ qua bảng điều khiển chính. Điều này cung cấp cho bạn các tùy chọn 4 - để sử dụng trình tạo trang web 000webhost gốc, cài đặt WordPress, sử dụng Wix hoặc tải lên trang web của riêng bạn.

Trong số bốn, việc chọn Wix thực sự đưa bạn ra khỏi môi trường 000webhost và chuyển bạn đến trang Wix thay vào đó, nằm ngoài phạm vi của đánh giá này (bạn có thể [đọc bài đánh giá Wix của tôi](https://www.webhostingsecretrevealed.net/vi/sitebuilder-review/wix-review/) thay thế). Vì tôi không có vỏ sẵn sàng của một trang web, tôi quyết định thử các tùy chọn xây dựng trang web WordPress và bản địa của họ.

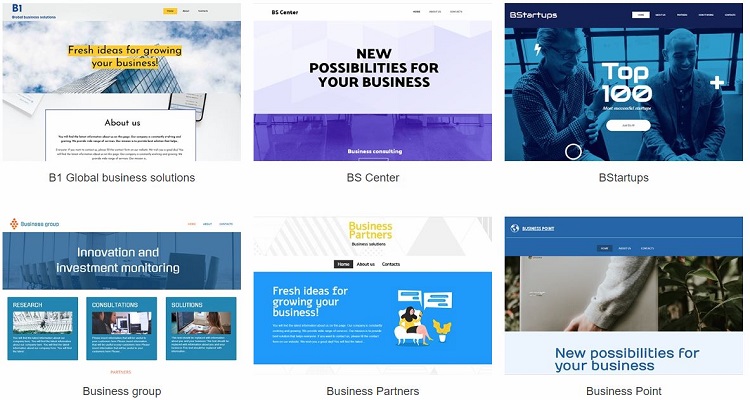
Chọn WordPress cho phép bạn tạo một trang web WordPress cơ bản với công cụ tự động của họ. Tất cả những gì bạn cần làm là nhập tên người dùng và mật khẩu mong muốn cho cơ sở dữ liệu. Nếu bạn quyết định dùng thử công cụ xây dựng trang gốc - tốt, nó cũng hoạt động giống như nhiều người khác.

**KHAI THÁC. Dễ dàng sử dụng Trình tạo trang web gốc**

*Công cụ tiện dụng trong giao diện dễ sử dụng*

Sử dụng trình tạo trang web gốc tương đối không gây đau đớn và đó là trải nghiệm chỉnh sửa hình ảnh điển hình của bạn. Tôi đã làm như thế họ có một số công cụ kéo và thả tiện lợi như Google Maps và YouTube. Thật thú vị cho một dịch vụ miễn phí, cũng có một số công cụ thương mại điện tử bạn có thể sử dụng.

**KHAI THÁC. Rất nhiều mẫu miễn phí**

*Trình tạo trang web gốc 000webhost đi kèm với rất nhiều mẫu miễn phí*

Một điều tôi phải chấp nhận là đối với người xây dựng trang web gốc của họ, 000webhost đã chuẩn bị rất nhiều mẫu miễn phí. Đây có lẽ là một điều tốt vì chủ sở hữu trang web mới có thể sẽ không có ý tưởng rõ ràng về những gì họ có thể muốn hoặc cần, và các mẫu này đóng vai trò là một hướng dẫn tốt cho họ.

## 1.2. Giới thiệu về ngôn ngữ lập trình PHP

Như đã đề cập, PHP là ngôn ngữ script được tạo cho các giao tiếp phía server. Do đó, nó có thể xử lý các chức năng phía server như thu thập dữ liệu biểu mẫu, quản lý file trên server, sửa đổi cơ sở dữ liệu và nhiều hơn nữa.

Ngôn ngữ này ban đầu được tạo ra bởi [Rasmus Lerdorf](https://en.wikipedia.org/wiki/Rasmus_Lerdorf) để theo dõi khách truy cập vào trang chủ cá nhân của anh ấy. Khi đã trở nên phổ biến hơn, Lerdorf phát hành nó thành dự án nguồn mở. Quyết định này đã khuyến khích các nhà phát triển sử dụng, sửa chữa, cải thiện code và cuối cùng biến nó thành ngôn ngữ script mà chúng ta sử dụng ngày nay.

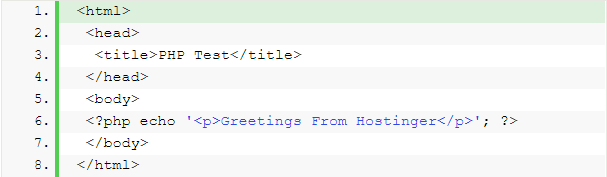
Mặc dù PHP được coi là ngôn ngữ script vì mục đích chung, nhưng nó được sử dụng rộng rãi nhất để [phát triển web](https://www.hostinger.vn/huong-dan/hoc-gi-truoc-de-tro-thanh-web-developer/). Điều này do một trong những tính năng nổi bật của nó – khả năng nhúng vào file HTML.

Nếu không muốn người khác xem mã nguồn của mình, bạn có thể ẩn bằng ngôn ngữ script này. Đơn giản chỉ cần bạn viết code vào file PHP, nhúng nó vào HTML thì mọi người sẽ không bao giờ biết được nội dung gốc.

Lợi ích khác của tính năng đặc biệt này là khi phải sử dụng cùng một lần đánh dấu HTML. Thay vì viết đi viết lại nhiều lần, chỉ cần viết code vào file PHP. Bất cứ khi nào cần sử dụng HTML, bạn hãy chèn file PHP và bạn có thể chạy rất tốt.

Ví dụ về trang PHP xem trên Facebook. Mở trang chủ, bạn có thể thấy URL kết thúc bằng PHP (facebook.com/home.php). Nói cách khác, trang này được xây dựng với file PHP (home.php) có chứa hypertext preprocessor code và tags HTML.

Nếu muốn tìm hiểu thêm về cách viết file PHP, bạn có thể xem ví dụ đơn giản dưới đây:



Nếu bạn đặt file PHP bằng văn bản này vào thư mục gốc của trang web, bạn sẽ tìm thấy nó bằng cách truy cập yoursite.com/greetings.php

Output của file PHP này trong HTML sẽ như thế này:



Đây là ví dụ cơ bản nhất vì bạn không cần phải chạy script này dưới bất kỳ hình dạng hay hình thức nào. Chúng tôi chỉ đơn giản sử dụng câu lệnh **echo** với trang để hiển thị **Greetings From Hostinger (Lời chào từ Hostinger)**. Tuy nhiên, ví dụ này cho thấy cách trang web có thể diễn giải code PHP thành HTML.

### 1.2.1. Vì sao nên sử dụng ngôn ngữ PHP trong lập trình Web

PHP không phải là ngôn ngữ script phía server duy nhất có sẵn – vẫn còn nhiều ngôn ngữ khác nữa. Tuy nhiên, nó lợi thế hơn các đối thủ cạnh tranh nếu như bạn đang chạy trang web [WordPress](https://www.hostinger.vn/huong-dan/wordpress-la-gi-toan-tap-ve-cms-pho-bien-nhat-gioi/).

Như chúng tôi đã đề cập trước đó, WordPress được xây dựng dựa trên việc sử dụng PHP. Vì vậy sử dụng ngôn ngữ này giúp cải thiện đáng kể số lượng tùy chỉnh có thể có trên trang web. Bạn có thể sử dụng nó để sửa đổi [plugins](https://www.hostinger.vn/huong-dan/plugin-hay-cho-wordpress-nam-2018/) và [themes](https://www.hostinger.vn/huong-dan/theme-wordpress-free) có sẵn hoặc tự tạo plugin! Nếu bạn muốn trở thành nhà phát triển [WordPress](http://hostinger.vn/huong-dan/wordpress/), bạn bắt buộc phải học PHP.

Nếu vẫn chưa bị thuyết phục, đây là một số lý do khác khiến PHP là ngôn ngữ script tuyệt vời để sử dụng:

**- Dễ học** – bạn có thể học dễ dàng vì nó có [tài liệu tuyệt vời](https://www.php.net/docs.php) về các chức năng cùng các ví dụ.

**- Được sử dụng rộng rãi** – nó được sử dụng để tạo ra các loại nền tảng như thương mại điện tử, blogs, phương tiện truyền thông xã hội, v.v. Thống kê cho thấy [79% tất cả các trang web](https://w3techs.com/technologies/details/pl-php) đều sử dụng PHP!

**- Chi phí thấp** – nó là nguồn mở để bạn có thể sử dụng miễn phí.

**- Cộng đồng lớn** – nếu gặp phải bất kỳ vấn đề nào với nó, bạn không phải lo lắng vì có rất nhiều blog PHP trên internet.

**- Tích hợp với cơ sở dữ liệu** – một số ví dụ như [MySQL](https://www.hostinger.vn/huong-dan/mysql-la-gi/), [Oracle](https://www.oracle.com/index.html), [Sybase](https://en.wikipedia.org/wiki/Sybase), [DB2](https://www.ibm.com/analytics/us/en/db2/), v.v.

# CHƯƠNG 2. CƠ CHẾ HOẠT ĐỘNG

## 2.1. Giới thiệu về tấn công giả mạo Phishing

**Phishing (Tấn công giả mạo)**là hình thức tấn công mạng mà kẻ tấn công giả mạo thành một đơn vị uy tín để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng.

Thông thường, tin tặc sẽ giả mạo thành ngân hàng, trang web giao dịch trực tuyến, ví điện tử, các công ty thẻ tín dụng để lừa người dùng chia sẻ các thông tin nhạy cảm như: tài khoản & mật khẩu đăng nhập, mật khẩu giao dịch, thẻ tín dụng và các thông tin quý giá khác.

Phương thức tấn công này thường được tin tặc thực hiện thông qua email và tin nhắn. Người dùng khi mở email và click vào đường link giả mạo sẽ được yêu cầu đăng nhập. Nếu “mắc câu”, tin tặc sẽ có được thông tin ngay tức khắc.

Phương thức phishing được biết đến lần đầu tiên vào năm 1987. Nguồn gốc của từ Phishing là sự kết hợp của 2 từ: fishing for information (câu thông tin) và phreaking (trò lừa đảo sử dụng điện thoại của người khác không trả phí). Do sự giống nhau giữa việc “câu cá” và “câu thông tin người dùng”, nên thuật ngữ Phishing ra đời.

Hầu hết mọi người gặp lừa đảo trực tuyến với email lừa đảo hoặc giả danh ngân hàng, công ty tín dụng hoặc các doanh nghiệp như Amazon và eBay. Những email này trông rất giống thật và cố gắng thuyết phục mọi nạn nhân tiết lộ thông tin cá nhân. Tuy nhiên, thông báo dạng email chỉ là một phần nhỏ của lừa đảo trực tuyến.

### 2.1.1. Các phương thức tấn công của Phishing

#### 2.1.1.1. Giả mạo email



Một trong những kỹ thuật cơ bản trong tấn công Phishing là **giả mạo email**. Tin tặc sẽ gửi email cho người dùng dưới danh nghĩa một đơn vị/tổ chức uy tín, dụ người dùng click vào đường link dẫn tới một website giả mạo và “mắc câu”.

Những email giả mạo thường rất giống với email chính chủ, chỉ khác một vài chi tiết nhỏ, khiến cho nhiều người dùng nhầm lẫn và trở thành nạn nhân của cuộc tấn công.

Để làm cho nội dung email giống thật nhất có thể, kẻ tấn công luôn cố gắng “ngụy trang” bằng nhiều yếu tố:

- Địa chỉ người gửi (VD: địa chỉ đúng là sales.congtyA@gmail.com thì địa chỉ giả mạo có thể là sale.congtyA@gmail.com)

- Chèn Logo chính thức của tổ chức để tăng độ tin cậy

- Thiết kế các cửa sổ pop-up giống y hệt bản gốc (cả về màu sắc, font chữ,…)

- Sử dụng kĩ thuật giả mạo đường dẫn (link) để lừa người dùng (VD: text là vietcombank.com.vn nhưng khi click vào lại điều hướng tới vietconbank.com.vn)

- Sử dụng hình ảnh thương hiệu của các tổ chức trong email giả mạo để tăng độ tin cậy.

Mánh khóe tinh vi của kẻ tấn công Phishing khiến nạn nhân dễ dàng tin tưởng và đăng nhập.

#### 2.1.1.2. Giả mạo Website

Thực chất, việc **giả mạo website** trong tấn công Phishing chỉ là làm giả một Landing page chứ không phải toàn bộ website. Trang được làm giả thường là trang đăng nhập để cướp thông tin của nạn nhân. Kỹ thuật làm giả website có một số đặc điểm sau:

- Thiết kế giống tới 99% so với website gốc

- Đường link (url) chỉ khác 1 ký tự duy nhất. VD: reddit.com (thật) với redit.com (giả); google.com với gugle.com, microsoft.com với mircosoft.com.

- Luôn có những thông điệp khuyến khích người dùng nhập thông tin cá nhân vào website (call-to-action).

#### 2.1.1.3. Vượt qua các bộ lọc Phishing

Hiện nay, các nhà cung cấp dịch vụ email như Google hay Microsoft đều có nhữngbộ lọc email spam/phishing để bảo vệ người dùng. Tuy nhiên những bộ lọc này hoạt động dựa trên việc kiểm tra văn bản (text) trong email để phát hiện xem email đó có phải phishing hay không. Hiểu được điều này, những kẻ tấn công đã cải tiến các chiến dịch tấn công Phishinglên một tầm cao mới. Chúng thường sử dụng ảnh hoặc videođể truyền tải thông điệp lừa đảo thay vì dùng text như trước đây. Người dùng cần tuyệt đối cảnh giác với những nội dung này.

### 2.1.2. Hình thức tấn công Phishing

#### 2.1.2.1. **Tấn công Phishing kết hợp nhiều phương tiện**

Các kịch bản tấn công Phishing lừa đảo đang trở nên phong phú hơn. Mục đích chính vẫn là đánh cắp thông tin đăng nhập bằng cách giả dạng một đơn vị có thẩm quyền.

Ngoài các kiểu tấn công lừa đảo thông qua Website, những kẻ lừa đảo còn kết hợp sử dụng các chiêu trò, mánh khóe lừa đảo bằng điện thoại di động, hoặc gửi các tin nhắn, email kèm theo nội dung lừa đảo hoặc các phần mềm độc hại.

Đặc biệt, các hình thức tấn công mạng có chủ đích được thực hiện nhiều hơn. Mặc dù gặp khó khăn trong quá trình tìm hiểu mục tiêu trước khi tấn công, nhưng các hacker vẫn kiên trì thực hiện để đạt được thành công. Spear phishing chính là tên gọi của hình thức tấn công lừa đảo có chủ đích này.

Các cuộc tấn công được thiết kế riêng thường đòi hỏi hacker phải xây dựng nhiều trang web hơn so với các cuộc tấn công lừa đảo thông thường. Và nó đang có dấu hiệu gia tăng nhiều hơn.

#### 2.1.2.2. **Tấn công Phishing lợi dụng các tin tức nóng**

Các cuộc tấn công lừa đảo chủ yếu nhắm vào các dịch vụ liên quan đến mua sắm, thanh toán trực tuyến và “cyber holidays”.

Nhiều trang web giả mạo doanh nghiệp Apple đã gia tăng gấp 4 lần trong sự kiện phát hành sản phẩm mới vào tháng 3-2020 vừa qua.

Và tất nhiên, những tin tức thời sự nóng cũng luôn được các hacker tận dụng để tạo ra sự hoảng loạn trong cộng đồng, từ đó khiến họ mất đi sự cảnh giác trước các nguy cơ bị tấn công bởi tội phạm mạng.

Trong suốt thời gian bùng phát dịch bệnh do COVID-19, các chuyên gia an ninh mạng đã theo dõi và nhận thấy hàng loạt các vụ tấn công lừa đảo ở Ý với nội dung lừa đảo liên quan tới việc hỗ trợ kiểm tra tình trạng sức khỏe nếu người dùng nhấp vào liên kết của họ.

Các tin tức về thiên tai cũng là xu hướng phổ biến giúp cho các loại tấn công lừa đảo được thực hiện dễ dàng hơn.

Các trang web hỗ trợ rút ngắn URL cũng là một trong số những giải pháp hỗ trợ đắc lực cho các hacker khi chúng muốn che giấu phần URL giả mạo, tránh sự kiểm soát của người dùng.

Đồng thời các URL được rút ngắn này cũng dễ dàng xuất hiện hợp pháp khắp nơi trên các trang mạng xã hội, các diễn đàn trực tuyến, hoặc các trang tin tức hợp pháp mà không gặp bất cứ trở ngại nào về việc kiểm tra nếu URL đó là độc hại.

Điều này có nghĩa là người dùng phải thật sự cảnh giác nhiều hơn với các URL được rút ngắn, và chỉ click vào liên kết khi bạn biết rõ nguồn gốc của chúng.

#### 2.1.2.3. **Tấn công lừa đảo vì tiền**

Đúng vậy, tiền chính là động lực lớn nhất thúc đẩy mọi kế hoạch tấn công mạng lừa đảo hiện nay.

Các dịch vụ lưu trữ dữ liệu trên đám mây (cloud storage) hỗ trợ doanh nghiệp upload và chia sẻ tài nguyên với nhiều người dùng. Đây là xu hướng mới nhận được sự quan tâm lớn của nhiều doanh nghiệp hiện nay, một cơ hội lớn cho các hacker chuyên thực hiện các tấn công mạng mã hóa dữ liệu và yêu cầu tiền chuộc.

Cụ thể, một tài khoản Google Drive của một công ty bị hack với khối lượng data lưu trữ có giá trị tương xứng với số tiền chuộc lên đến hàng trăm ngàn USD, Nếu họ không thỏa hiệp với các Hacker để thu hồi dữ liệu, họ cũng phải đối mặt với số tiền bồi thường lớn vì không bảo vệ thông tin khách hàng đúng cách, đảm bảo quyền riêng tư cho khách hàng.

Trước đây, tấn công mạng thường nhắm vào các doanh nghiệp tài chính như PayPal và Chase. Tuy nhiên, giờ đây các hacker lại mở rộng mục tiêu tấn công tới các trang web như Facebook, Google, Microsoft và Apple. Vì đây là những đơn vị cung cấp dịch vụ lưu trữ đám mây phổ biến nhất, hỗ trợ lưu trữ dữ liệu khổng lồ cho mọi doanh nghiệp và cá nhân.

Đối với cá nhân, nếu thông tin bị đánh cắp có thể được rao bán để mở thẻ tín dụng hoặc lấy cắp danh tính cho các mục đích kiếm tiền khác.

Ngoài ra, Hacker cũng sẽ tham chiếu các thông tin tài khoản đánh cắp này trên các trang web khác để mở rộng quyền truy cập tài khoản.

### 2.1.3. Cách phòng chống Phishing

#### 2.1.3.1. Đối với cá nhân

Để tránh bị hacker sử dụng **tấn công Phishing** để lừa đảo trên Internet, thu thập dữ liệu cá nhân, thông tin nhạy cảm của bạn. Hãy lưu ý những điểm sau:

- Cảnh giác với các email có xu hướng thúc giục bạn nhập thông tin nhạy cảm. Cho dù lời kêu gọi có hấp dẫn thế nào đi chăng nữa thì vẫn nên kiểm tra kỹ càng. VD: bạn mới mua sắm online, đột nhiên có email từ ngân hàng tới đề nghị hoàn tiền cho bạn, chỉ cần nhập thông tin thẻ đã dùng để thanh toán. Có tin được không?!

- Không click vào bất kỳ đường link nào được gửi qua email nếu bạn không chắc chắn 100% an toàn.

- Không bao giờ gửi thông tin bí mật qua email.

- Không trả lời những thư lừa đảo. Những kẻ gian lận thường gửi cho bạn số điện thoại để bạn gọi cho họ vì mục đích kinh doanh. Họ sử dụng công nghệ Voice over Internet Protocol. Với công nghệ này, các cuộc gọi của họ không bao giờ có thể được truy tìm.

- Sử dụng Tường lửa và phần mềm diệt virus. Hãy nhớ luôn cập nhật phiên bản mới nhất của các phần mềm này.

- Hãy chuyển tiếp các thư rác đến spam@uce.gov. Bạn cũng có thể gửi email tới reportphishing@antiphishing.org Tổ chức này giúp chống lại các phishing khác.

#### 2.1.3.2. Đối với các tổ chức, doanh nghiệp

- Training cho nhân viên để tăng kiến thức sử dụng internet an toàn. Thường xuyên tổ chức các buổi tập huấn, diễn tập các tình huống giả mạo

- Sử dụng dịch vụ G-suite dành cho doanh nghiệp, không nên sử dụng dịch vụ Gmail miễn phí vì dễ bị giả mạo.

- Triển khai bộ lọc SPAM để phòng tránh thư rác, lừa đảo

- Luôn cập nhật các phần mềm, ứng dụng để tránh các lỗ hổng bảo mật có thể bị kẻ tấn công lợi dụng.

- Chủ động bảo mật các thông tin nhạy cảm, quan trọng.

#### 2.1.3.3. Phòng chống bằng các phần mềm khác

SpoofGuard: là một plug trình duyệt tương thích với Microsoft Internet Explore. SpoofGuard đặt một “cảnh báo” trên thanh công cụ của trình duyệt. Nó sẽ chuyển từ màu xanh sang màu đỏ nếu bạn vô tình vào trang web giả mạo Phishing. Nếu bạn cố nhập các thông tin nhạy cảm vào một mẫu từ trang giả mạo, SpoofGuard sẽ lưu dữ liệu của bạn và cảnh báo bạn. Mức độ cảnh báo có thể được thiết lập qua các thông số.

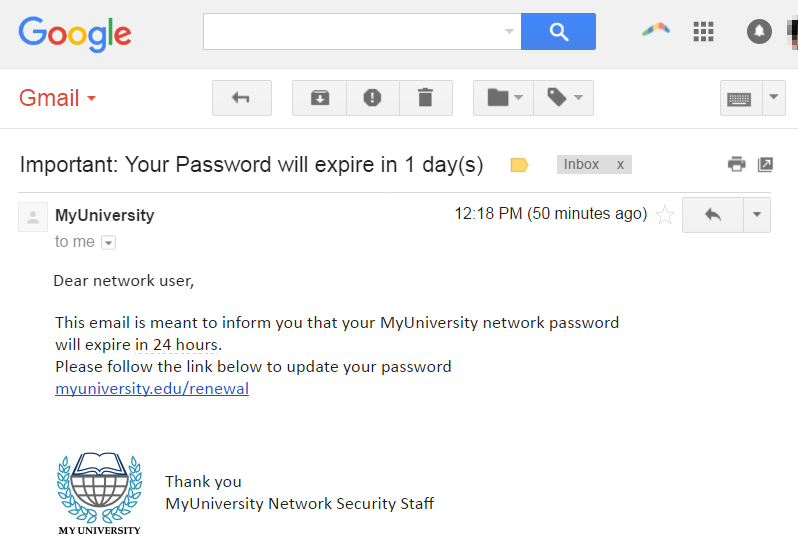


Anti-phishing Domain Advisor:  giúp bạn phát hiện, cảnh báo và ngăn chặn từ các trang web lừa đảo, chèn mã độc thông qua dữ liệu nhận dạng của hệ thống Panda Security. Nó là một công cụ tốt để bảo vệ bạn khi lướt web.

Netcraft Tool: Netcraft cung cấp các dịch vụ bảo mật internet bao gồm các dịch vụ chống gian lận và **chống Phishing**, thử nghiệm ứng dụng và quét PCI. Nó cũng giúp cũng phân tích nhiều khía cạnh của Internet, bao gồm thị phần của máy chủ web, hệ điều hành, nhà cung cấp dịch vụ lưu trữ và cơ quan cấp giấy chứng nhận SSL.

### 2.1.4. Cách nhận biết Phishing lừa đảo qua Email và trang Website giả mạo

#### 2.1.4.1. Cách xác định một Email lừa đảo



Thoạt nhìn, email giả mạo trông không khác gì “chính chủ”

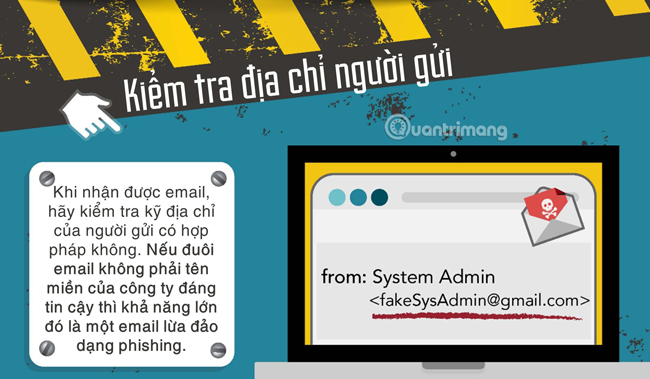
Đây là một số cụm từ thường gặp nếu bạn nhận được một email hay tin nhắn là lừa đảo

**“Xác thực tài khoản của bạn” / “Verify your account”** – Các website hợp pháp sẽ không bao giớ bắt bạn gửi password, tên tài khoản hay bất cứ thông tin cá nhân nào của bạn qua email.

**“Nếu bạn không phản hồi trong vòng 48h, tài khoản của bạn sẽ bị ngừng hoạt động” / “If you don’t respond within 48 hours, your account will be closed.”** – Đây là một tin nhắn truyền tải một thông điệp cấp bách để bạn trả lời ngay mà không cần suy nghĩ

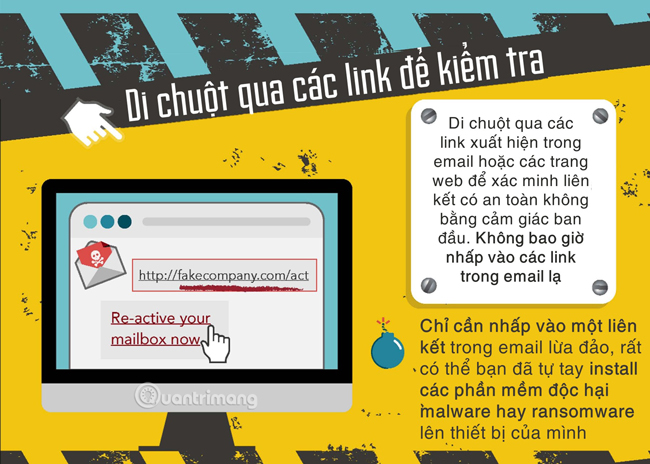
**“Dear Valued Customer.” / “Kinh thưa quí khách hàng”** – Những tin nhắn từ các email lừa đảo thường xuyên gửi đi với số lượng lớn và thường sẽ không chứa first name và last name của bạn.

**“Nhấp chuột vào link bên dưới để truy cập đến tài khoản của bạn” / “Click the link below to gain access to your account.” –**Các thông điệp HTML có thể chứa các liên kết hay các form nhập liệu mà bạn có thể điền các thông tin vào giống như khi các form trên một website. Những đường dẫn đó có thể chứa tất cả hoặc một phần thông tin của các công ty thực sự và thường “đeo mặt nạ”, có nghĩa là các đường dẫn mà bạn thấy không đưa bạn đến website mà bạn nghĩ, ngược lại nó sẽ đưa bạn đến những website lừa đảo.

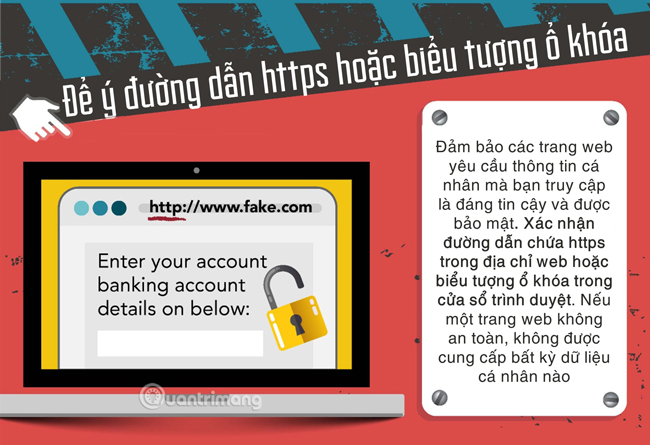












**1. Kiểm tra địa chỉ người gửi**

Khi nhận được email, hãy kiểm tra kỹ địa chỉ của người gửi có hợp pháp không. Nếu đuôi email không phải tên miền của công ty đáng tin cậy thì khả năng lớn đó là một email lừa đảo dạng phishing.

**2. Lưu ý với những email không đề cập đến người nhận cụ thể**

Luôn cảnh giác với những email không chỉ định một người nhận cụ thể. Hãy chắc chắn rằng email này được gửi cho bạn, theo đúng tên bạn đăng ký.

**3.Zoom kĩ vào cách sử dụng từ ngữ, lỗi chính tả, lỗi cú pháp**

Email có lỗi chính tả và ngữ pháp kém thường là những cuộc tấn công lừa đảo.

**4. Luôn di chuột qua các link để kiểm tra**

Di chuột qua các link xuất hiện trong email hoặc các trang web để xác minh liên kết có an toàn không bằng cảm giác ban đầu. Không bao giờ nhấp vào các link trong email lạ.

Chỉ cần nhấp vào một liên kết trong email lừa đảo, rất có thể bạn đã tự tay install các phần mềm độc hại malware hay ransomware lên thiết bị của mình.

**5. Cẩn thận với email mang tính thúc ép**

Không bao giờ trả lời các email lạ yêu cầu thông tin cá nhân hay sử dụng các cụm từ giật gân như "KHẨN CẤP", "THÔNG BÁO CUỐI CÙNG".

Loại email lừa đảo phổ biến nhất là yêu cầu người dùng cập nhật mật khẩu.

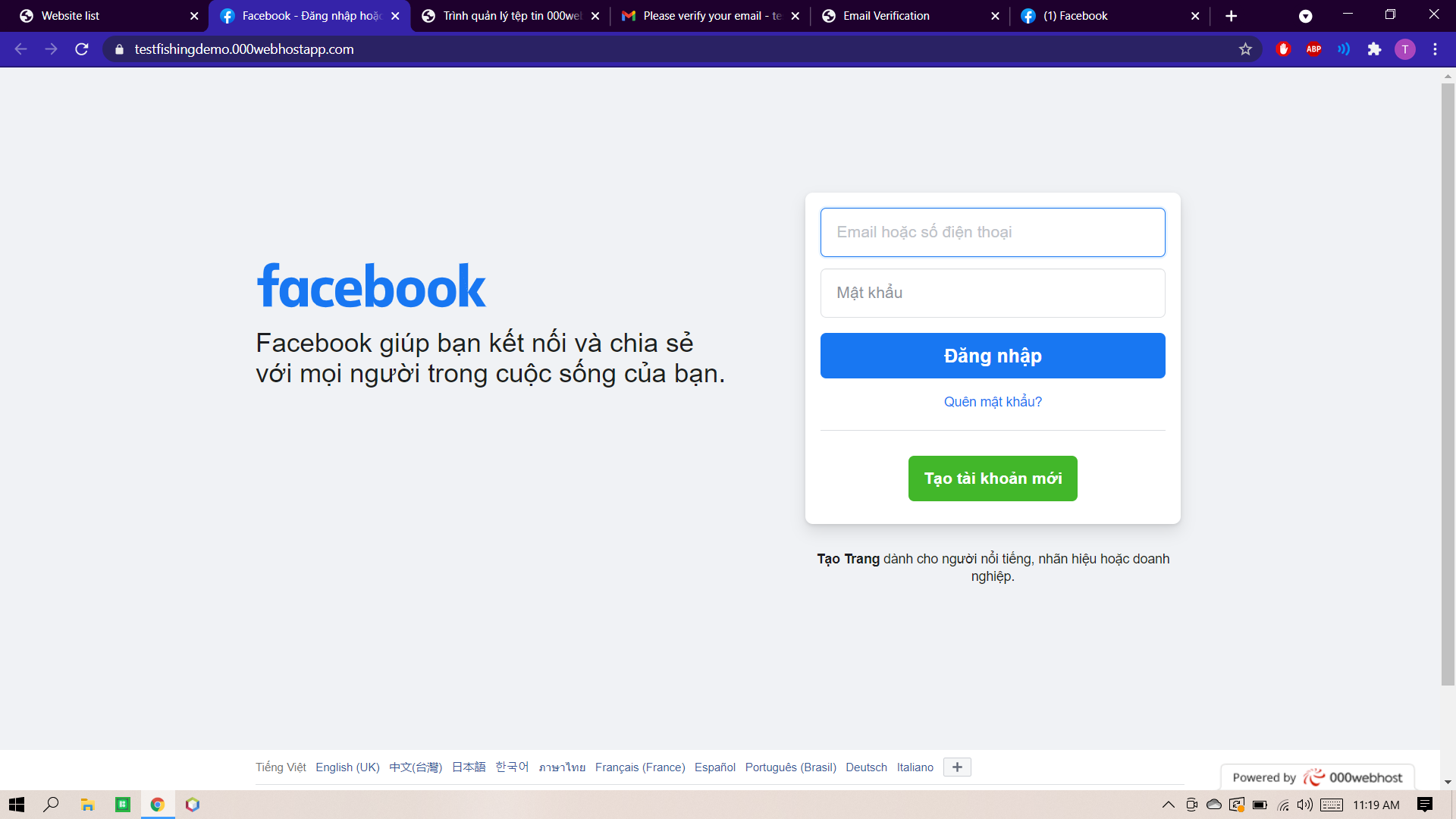
**6. Để ý đường dẫn https hoặc biểu tượng ổ khóa**

Đảm bảo các trang web yêu cầu thông tin cá nhân mà bạn truy cập là đáng tin cậy và được bảo mật. Xác nhận đường dẫn chứa https trong địa chỉ web hoặc biểu tượng ổ khóa trong cửa sổ trình duyệt. Nếu một trang web không an toàn, không được cung cấp bất kỳ dữ liệu cá nhân nào.

# CHƯƠNG 3. KẾT QUẢ THỰC NGHIỆM

## 3.1. Giao diện sản phẩm

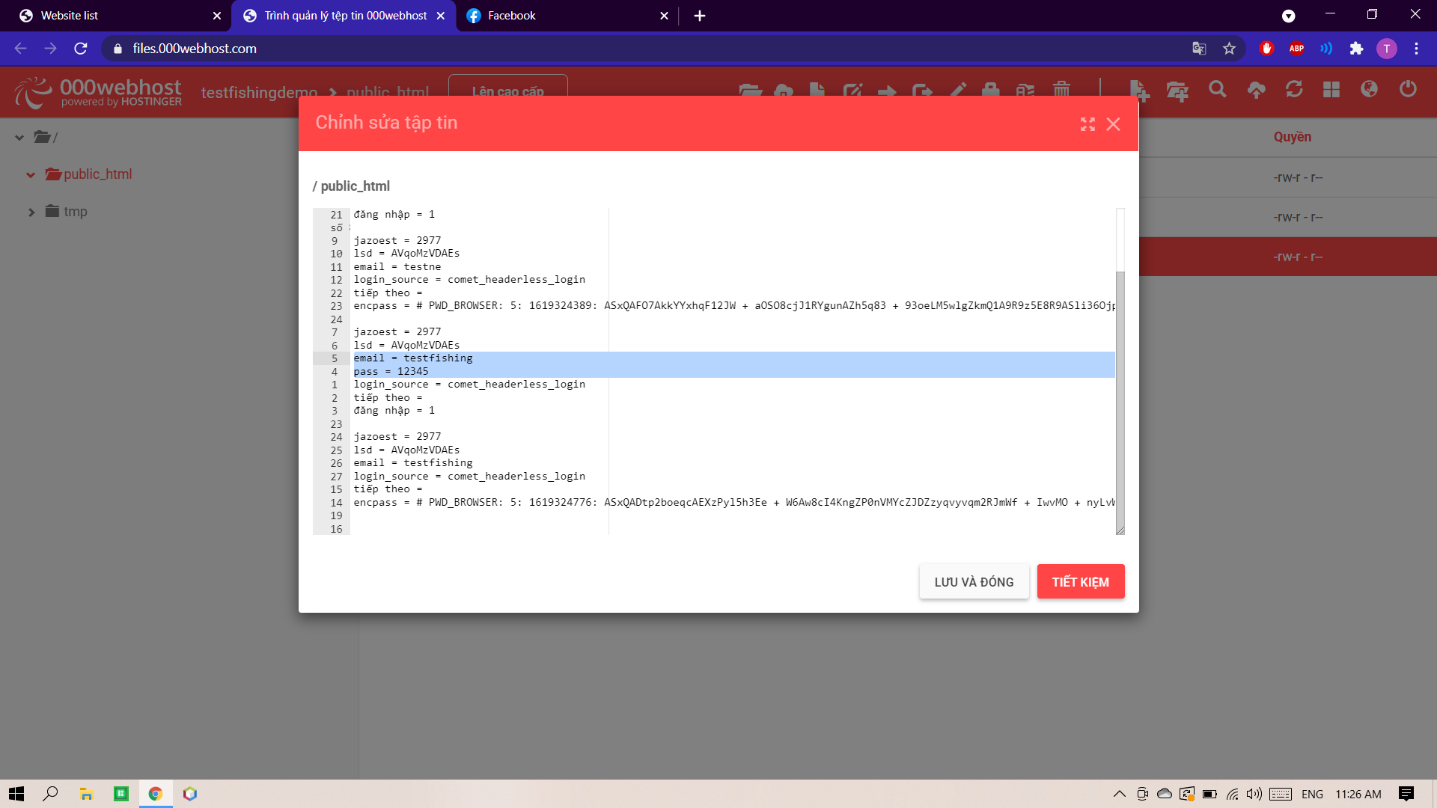
### 3.1.1. Giao diện trang chủ đăng nhập



*Giao diện trang chủ đăng nhập giả mạo trang mạng lớn Facebook*

Trong giao diện đăng nhập, để có được thông tin của người sử dụng, thì bắt buộc họ phải nhập tài khoản, mật khẩu và click vào chức năng Đăng nhập.

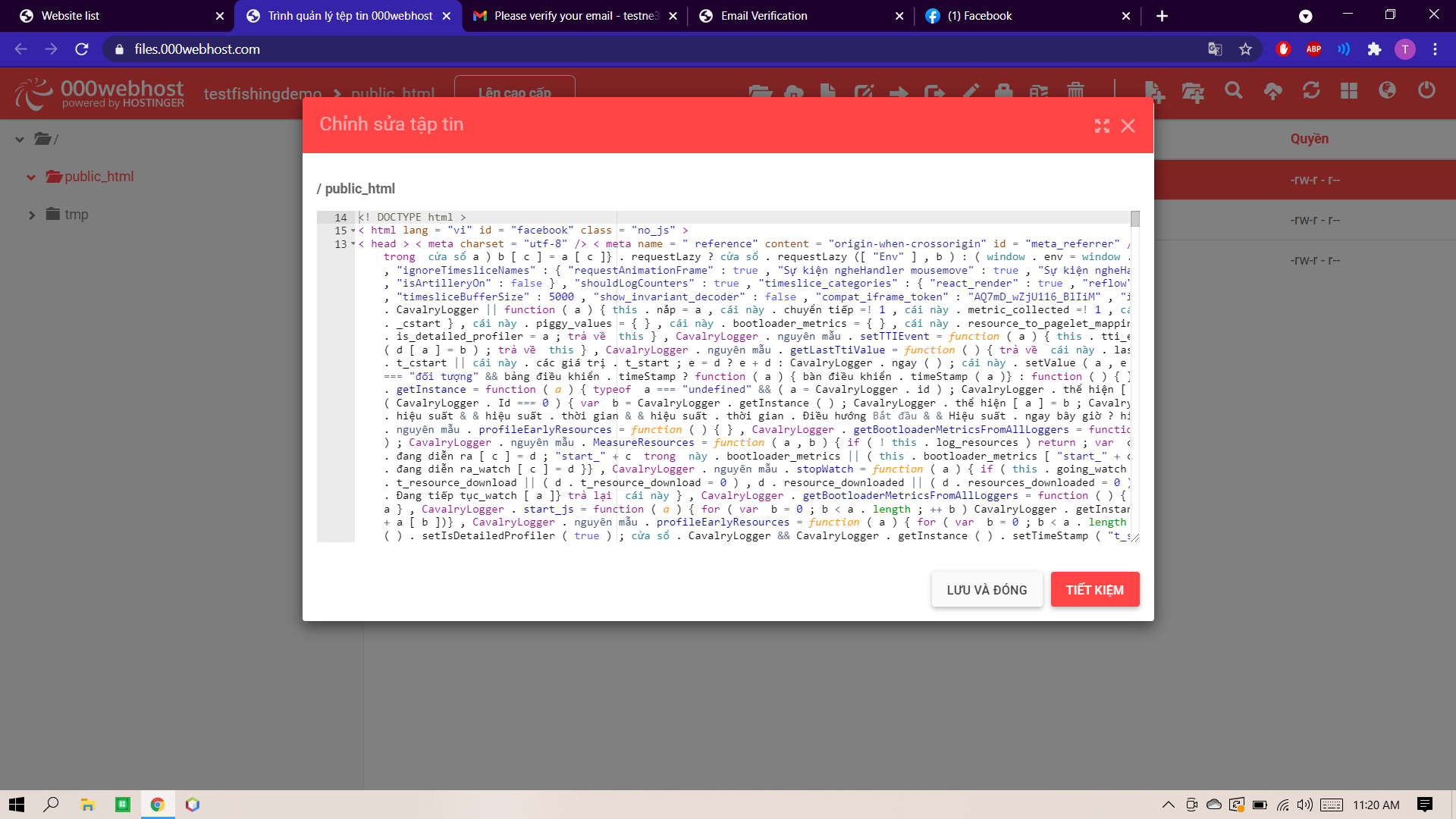
### 3.1.2. Form lưu trữ dữ liệu



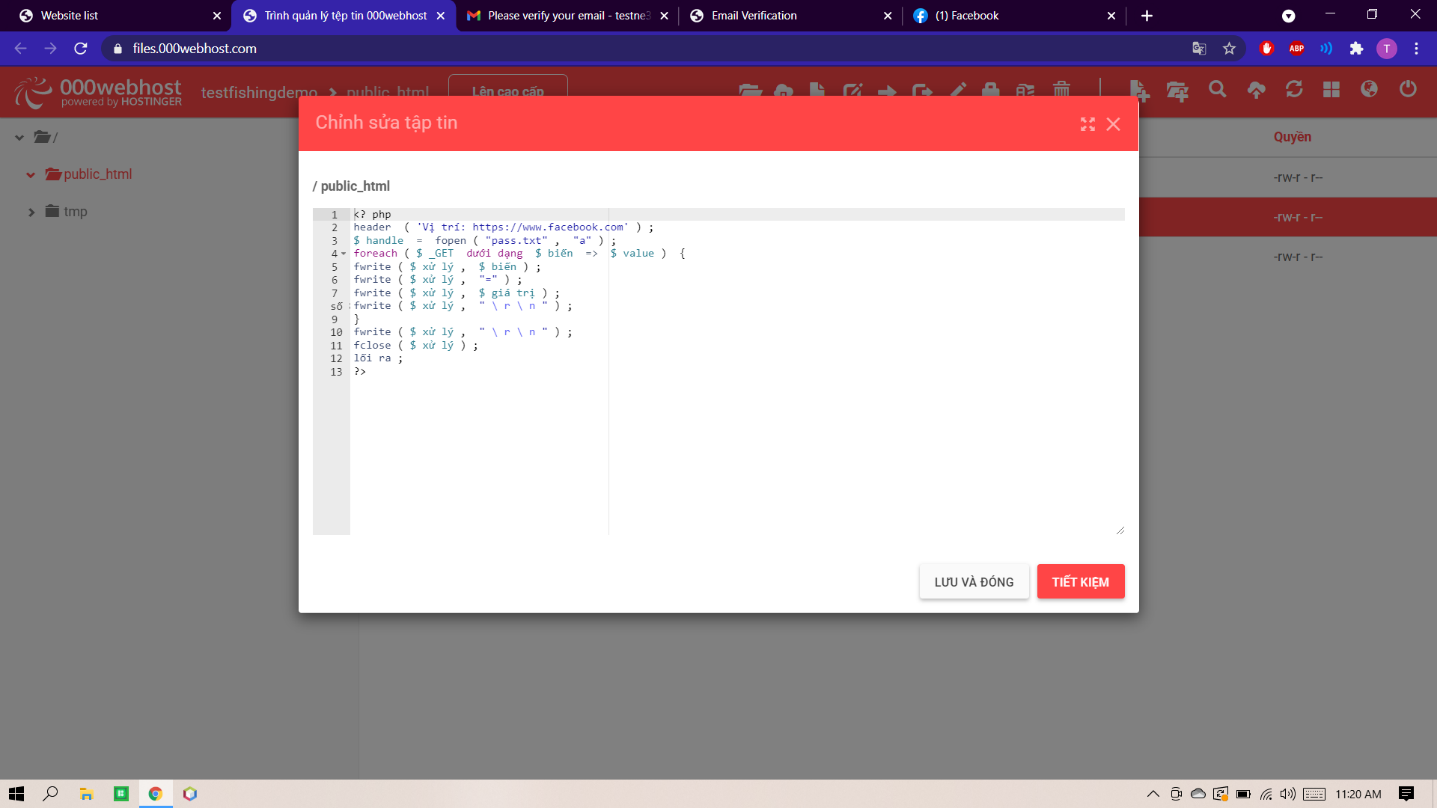
*Form lưu trữ dữ liệu sau khi người dùng đã nhập vào*

Sau khi người dùng nhập tài khoản, mật khẩu và nhấn chức năng Đăng nhập thì dữ liệu sẽ được lưu vào đây và người đánh cắp có thể lấy được dữ liệu của người nhập.

### 3.1.3. Source code giao diện sản phẩm

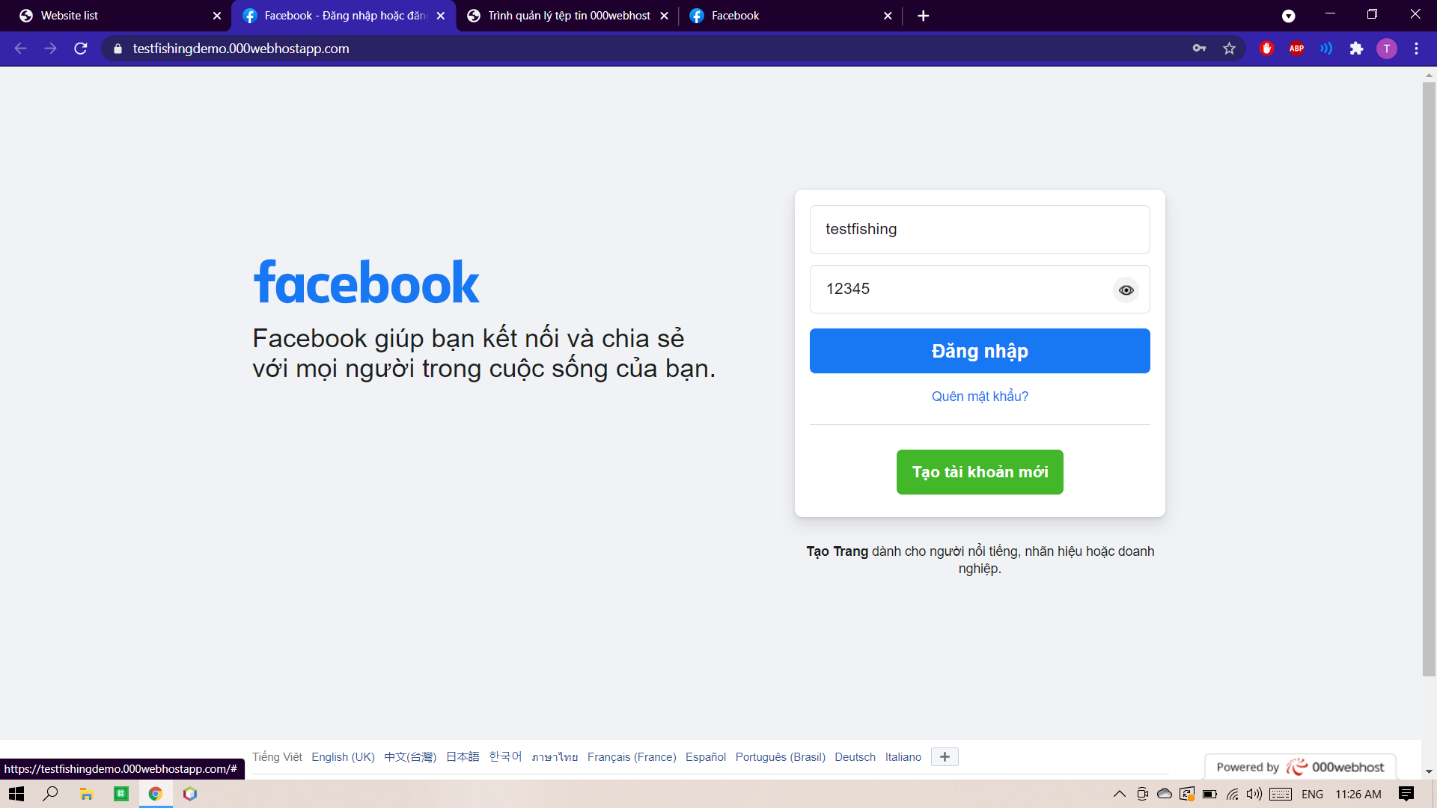


### 3.1.4. Source code giao diện để lấy cắp dữ liệu



Trong source code còn có đường link dẫn đến facebook thật, khiến người dùng khó nhận ra là mình đã bị đánh cắp thông tin.

## 3.2. Cách sản phẩm đánh cắp dữ liệu

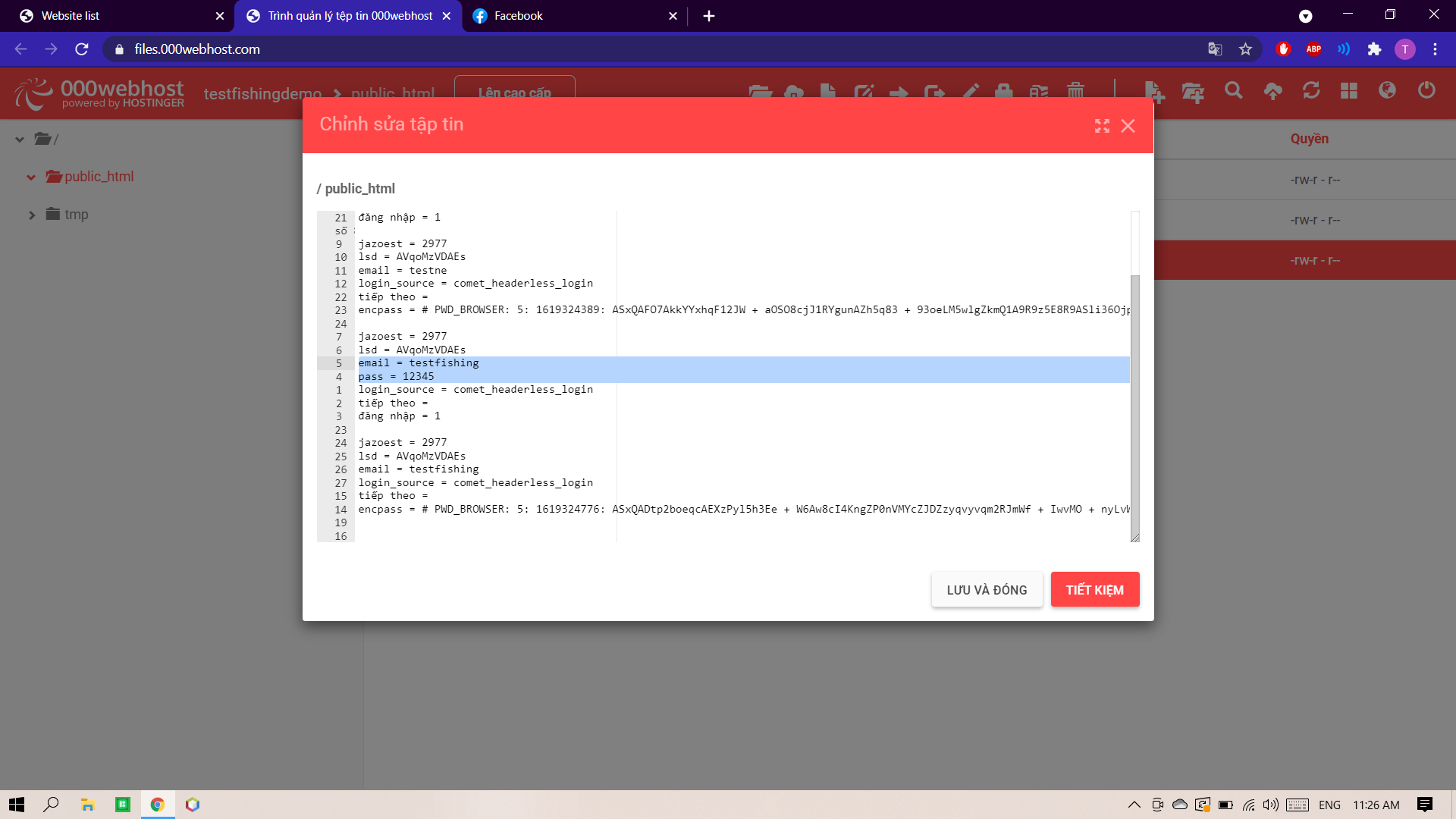


Người dùng không cẩn thận, truy cập đường link facebook giả, chỉ cần nhập vào thanh URL của trình duyệt “face..” là sẽ hiện ra đường link facebook giả

Đường link facebook thật: <https://www.facebook.com/>

Đường link facebook giả: <http://fakeceboook.000webhostapp.com/>

Sau khi truy cập đường link giả, người dùng sơ hở nhập tài khoản mật khẩu, và bấm vào chức năng Đăng nhập thì dữ liệu sẽ được lưu lại ngay lập tức.



Ngay lập tức tài khoản “testfishing” và mật khẩu “12345” lập tức được lưu lại, và người đánh cắp có thể dùng tài khoản này truy cập vào đường link facebook thật nhằm mục đích xấu.

## 3.3. Kết luận

Phishing là một trong những kỹ thuật tấn công trực tuyến phổ biến nhất. Mặc dù các công cụ lọc email của các dịch vụ email phổ biến khá hiệu quả trong việc lọc các thư giả mạo, người dùng vẫn cần cẩn thận và thực hiện các biện pháp để bảo vệ các thông tin của bản thân. Hãy cẩn thận với những email yêu cầu các thông tin nhạy cảm hoặc riêng tư của bạn. Nếu có thể, hãy luôn tìm một phương thức liên lạc khác để có thể xác nhận người gửi và yêu cầu đó là hợp pháp. Đừng bấm vào các liên kết trong email về các trường hợp bảo mật và hãy tự điều hướng đến trang web bằng trình duyệt của mình, đồng thời kiểm tra các đường dẫn URL có bắt đầu bằng giao thức HTTPS hay không. Cuối cùng, hãy đặc biệt cẩn trọng về các giao dịch tiền điện tử vì không có cách thức nào có thể đảo ngược chúng, nếu người bán không thực hiện phần việc của mình trong giao dịch. Hãy luôn bảo mật các mã khóa cá nhân và mật khẩu của bạn và đừng bao giờ quá tin tưởng vào điều gì đó.

**3.4. Tài liệu tham khảo**

1. Phishing là gì? Cách phòng chống tấn công Phishing hiệu quả - cystack.net

2. Phishing là gì, 3 hình thwusc tấn công Phishing phổ biến – Vnetwork JSC

3. Cách nhận biết và phòng tránh cuộc tấn công Phising – quantrimang.com

4. Mổ xẻ và tìm hiểu chi tiết về nhà cung cấp hosting miễn phí 000webhost – viettelidc.com.vn

5. 000webhost Đánh giá 2021 – khuyết điểm ở đâu? – websiteplanet.com

6. Đánh giá 000webhost: Hosting miễn phí… nhưng đáng để thử ? – webhosttingsecretrevealed.net.