Created in the cloud with Aspose.Words for Cloud. http://www.aspose.com/cloud/word-api.aspx

# How to Avoid Phishing Scams

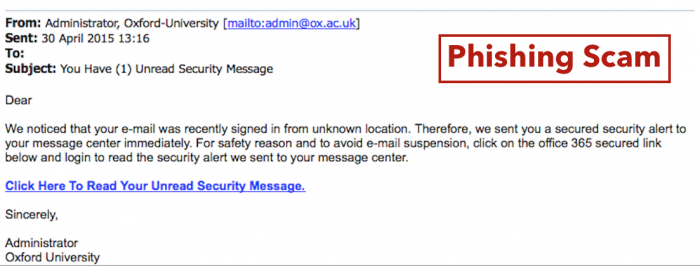
Published Date : September 7, 2016  
Author : tayo

You got an email saying that your email account has just been blocked and you need to login to verify some information before you can gain access back. You noticed that website looks just exactly like the real website but your instincts tells you that this is a fake website.



**Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Just below is an example of a Phishing email:



As a general rule, you should be careful about giving out your personal financial information over the Internet.

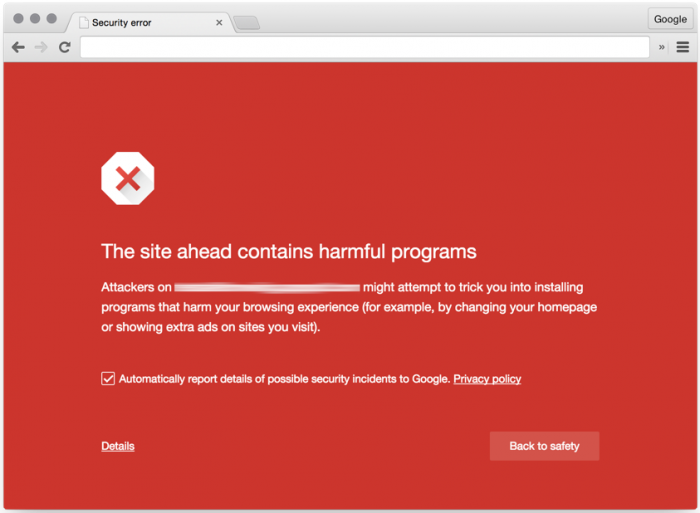
Here are some steps you can take to avoid becoming a victim:

1. Be suspicious of any email or communication (including text messages, social media post, ads) with **urgent requests** for personal **financial information**.
2. **AVOID** clicking on links. Instead, go to the website by typing the Web address directly into your browser or by searching for it in a search engine. Calling the company to verify its legitimacy is also an option, too
3. Don’t send personal financial information via email, and avoid filling out forms in email that ask for your information.
4. Use a secure website **(https:// and a security “lock” icon)** when submitting credit card or other sensitive information online. A secure website always start with **‘https://’**.
5. Never use public, unsecured WiFi for banking, shopping or entering personal information online, even if the website is secure.
6. Double-clicking the “lock” icon on a website will display the security certificate for the website. If the certificate isn’t displayed, or you get a warning message that the address of the website does not match the certificate, do not continue.
7. Typically, phisher emails are not personalized, but they can be. Valid messages from your bank and e-commerce companies are personalized, and addressed specifically to you. When in doubt, call the company directly to see if the email is in fact from them.
8. Phishers have the ability to spoof and/or forge the https:// that you normally see on a secure Web server and a legitimate-looking Web address, which – again – is why you should **always type the web address yourself instead of clicking** on displayed links.

### Comments

# Protect Yourself from an Unsafe Website

Published Date : September 7, 2016  
Author : tayo



With more people storing personal information on their computers, it has never been more important to protect yourself from internet predators looking to gain access to your files. One of the many ways they can do this is by attacking your computer or trying to gather your information from an infected or malicious website you may visit, even if only once. The best thing you can do is to avoid malicious websites altogether

Here are the most prevalent tell-tale signs of a threatening website and some ways that you can protect yourself:

* Never click on a link embedded in an email. Even if sent from someone you trust, always type the link into your browser
* Use your common sense. Does a website look strange to you? Is it asking for sensitive personal information? If it looks unsafe, don’t take the risk.
* Look for signs of legitimacy. Does the website list contact information or some signs of a real-world presence. If doubtful, contact them by phone or email to establish their legitimacy.
* Read the URL carefully. If this is a website you frequent, is the URL spelled correctly? Often times, phishers will set up websites almost identical to the spelling of the site you are trying to visit. An accidental mistype may lead you to a fraudulent version of the site.
* If it looks too good to be true, it probably is. Is the website offering you a product or service at an unheard of price? Or maybe they are promising you a huge return on investment? If the offer looks too good to be true, trust your instincts. Do some research to find reviews or warnings from other users.
* Check the properties of any links. Right-clicking a hyperlink and selecting “Properties” will reveal the true destination of the link. Does it look different from what it claimed to lead you to?

You should also always be on the lookout for the clues and telltale hints that you are on a malicious website.  After all, it is by smart people noticing something wrong and reporting it that the above tools can do their job.

### Things to look for in a secure website

When visiting a website that asks for sensitive information such as credit card numbers or your social security number, the first step you can take to securing your privacy is creating a strong password (link to infosec site). Equally important is verifying that any information you enter on this site is transmitted and stored properly. Once your information is entered online, it is transmitted as plain text for anyone to intercept. To avoid this, make sure that the website is encrypted over a secure connection.

* HTTPS

One such sign to look for is in the URL of the website. A secure website’s URL should begin with “https” rather than “http”. The “s” at the end of “http” stands for secure and is using an SSL (Secure Sockets Layer) connection. Your information will be encrypted before being sent to a server.

* THE LOCK ICON

Another sign to look for is the “Lock” icon that is displayed somewhere in the window of your web

browser. Different browsers may position the lock in different places, but a few examples of what it may look like can be found here:



**Google Chrome**

Clicking on the Lock icon will give you detailed information on the security status of this website

**Mozilla Firefox**

With Firefox, the Lock icon may not be displayed directly. Clicking on the site’s icon next to the URL should reveal the Lock icon and the secure verification

**Internet Explorer**

Clicking on the Lock icon will give you detailed information on the security status of this website

Be sure to click on the “lock” icon to verify that a website is trustworthy. Do not simply look for the icon and assume a website is secure! Your web browser will have detailed information on the website’s authenticity if you click on the icon, so be sure to read this carefully before entering any of your information on the site.

### Protect Yourself

Utilize your internet browser’s security tools

Be sure to install the most current version of your web browser. Most browsers have sophisticated filters that can identify and warn you of potential security threats. For information on browser-specific security tools, explore their security features here:

[Internet Explorer](http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/features/smartscreen-filter)

[Mozilla Firefox](http://support.mozilla.org/en-US/kb/Site%20Identity%20Button)

[Google Chrome](http://support.google.com/chrome/bin/answer.py?hl=en&answer=95617)

Make sure that the proper online protection tools are enabled for your [Anti-Virus Software](http://www.bu.edu/infosec/howtos/906-2/)

[McAfee’s SiteAdvisor](http://www.siteadvisor.com/)

[Norton’s Safe Search](http://us.norton.com/theme.jsp?themeid=safe_search)

You may also want to consider downloading an add-on for you browser that is specially designed to identify any unsafe elements of a website

[Web of Trust](http://www.mywot.com/)

[AVG Link Scanner](http://linkscanner.avg.com/)

Source : Bu.edu

### Comments

# How to Protect Your Computer

Published Date : September 7, 2016  
Author : tayo

***Below are some key steps to protecting your computer from intrusion***

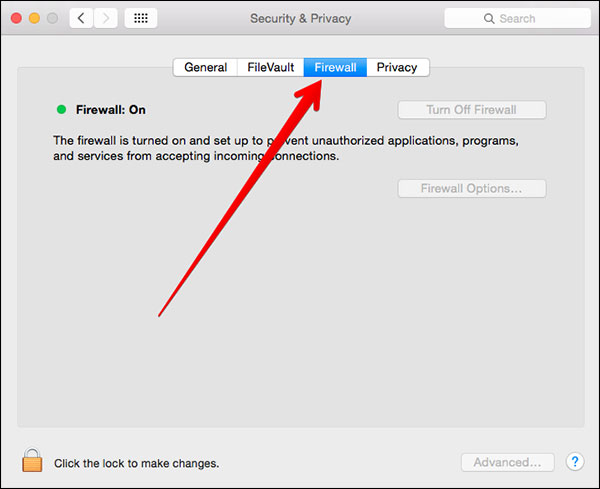
#### Keep Your Firewall Turned On

A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers.

#### Turn On Firewall on Windows

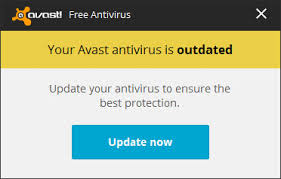


#### Turn On Firewall on Mac OS



#### Install or Update Your Antivirus Software

Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users’ knowledge. Most types of antivirus software can be set up to update automatically.



**Install or Update Your Antispyware Technology:** Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It’s like buying groceries—shop where you trust.

**Keep Your Operating System Up to Date**

Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

**Be Careful What You Download**

Carelessly downloading e-mail attachments or software from pop-ups online can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don’t know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.



**Turn Off Your Computer**

With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being “always on” renders computers more susceptible.

### Comments

# Guide to Secure your Online Browsing: Chrome, Firefox and Internet Explorer

Published Date : September 7, 2016  
Author : tayo

# Secure your web browser: Internet Explorer, Mozilla Firefox, Google Chrome

Since we use our browser for most of our online activities, it is important to know how to configure it correctly.  Not securing our browser, may result in attacks on our computers.

Though we can not guarantee complete safety from malware attempts and online attacks, we know that following the steps below will increase your web browser security. At the same time, we can not name one single browser as the best possible selection for a user, since so many studies and articles name one over the other. For this reason, we will simply choose to present the 3 most popular web browsers for Windows: Google Chrome, Internet Explorer and Mozilla Firefox.

### Tips for Secure Browsing with Microsoft Internet Explorer 10



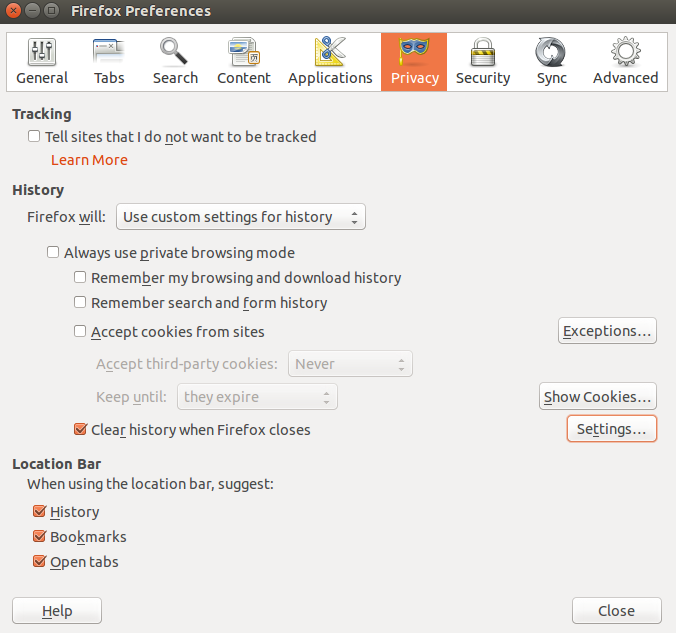
These settings can be accessed through the “Internet Options” menu.

* **Configure security settings:** Under the “Security” tab, do the following:
  + *Set security zones:* IE offers the option to configure different security settings for different “zones,” including the Internet, local intranet, trusted sites, and restricted sites. Set up the zones for Intranet, Trusted Sites, and Restricted sites to your desired security level.
  + Set Internet zone security to “Medium High” or higher. This blocks certain cookie types, enables ActiveX filtering, and implements several other default settings for increased security.
* **Automatically clear history:** Select “Delete browsing history on exit” under the “General” tab. Clearing your history at the end of each session helps to limit the amount of information IE saves when you browse.
* **Configure privacy settings:** Under the “Privacy” tab, complete the following steps:
  + *Privacy setting:* Set the Internet zone privacy to “Medium High” or higher. This blocks certain cookie types to prevent sites from tracking or contacting you without your consent.
  + *Location:* Select “Never allow websites to request your physical location.”
  + *Pop-up Blocker:* Double check that Pop-up Blocker is enabled.
* **Configure Advanced Security settings:** Scroll down to the “Security” section under the “Advanced” tab and do the following:
  + Ensure that all default settings are in place. If you aren’t sure, click “Restore advanced settings” before making any other changes.
  + Select “Do not save encrypted pages to disk.” This will delete files cached from HTTPS pages when the browser is closed.
  + Select “Empty Temporary Internet Files folder when browser is closed.” This prevents IE from storing your personal info (logins, passwords, activity, etc) beyond your browsing session.
  + *Turn off autoComplete:* The AutoComplete feature should be turned off for forms and usernames/passwords. Keeping AutoComplete turned off ensures that your sensitive information isn’t being stored unnecessarily.
* **Tracking protection:** IE’s Tracking Protection feature keeps your browsing private from specified third-party websites. This feature can be accessed through IE’s “Safety” menu. In order to use Tracking Protection you will need to provide a Tracking Protection List that names all of the sites you don’t want your information being sent to. You can create a list yourself or download lists online.

### Tips for Secure Browsing with Mozilla Firefox

These settings can be accessed through the “Options” menu.

* **Configure privacy settings:** Under the “Privacy” tab, complete the following steps. These measures ensure that Firefox is storing only as much of your information as it needs to function normally.
  + Select “Use custom settings for history.”
  + Deselect “Remember my browsing and download history.”
  + Deselect “Remember search and form history.”
  + Deselect “Accept third-party cookies.”
  + Set cookie storage to “Keep until I close Firefox.”
  + Select “Clear history when Firefox closes.”



* **Configure security settings:** Under the “Security” tab, choose the following settings. These steps prevent Firefox from saving your passwords and keep you from visiting potentially harmful sites.
  + Verify that “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries” are all selected.
  + Deselect “Remember passwords for sites.”
* **Enable pop-up blocking:** Verify that “Block pop-up windows” is selected under the “Content” tab. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.
* **Don’t sync:** Avoid using Firefox Sync. By doing so you prevent Firefox from storing your logins, passwords, and other sensitive information.
* **Turn on automatic updates:** Verify that “Automatically install updates” is selected in the “Update” tab under “Advanced.” Doing so will ensure that your browser receives critical security updates. Verify that “Automatically update Search Engines” is selected as well.
* **Use secure protocols:** Verify that “Use SSL 3.0” and “Use TLS 1.0” are selected in the “Encryption” tab under “Advanced.”

### Tips for Secure Browsing with Google Chrome

### chrome-privacy-settings

These settings can be accessed through Chrome’s “Advanced Settings” menu or by navigating to “chrome://settings/.”

chrome

* **Enable phishing and malware protection:** Make sure that Chrome’s phishing and malware protection feature is enabled under the “Privacy” section. This feature will warn you if a site you’re trying to visit may be phishing or contain malware.
* **Turn off instant search:** The Instant search feature should be turned off for optimal security. While it offers some convenience in searching, having this feature enabled means that anything you type in the address bar is instantly sent to Google.
* **Don’t sync:** Disconnect your email account from your browser under the “Personal Stuff” tab. Syncing your email account with your Chrome browser means that personal information such as passwords, autofill data, preferences, and more is stored on Google’s servers. If you must use sync, select the “Encrypt all synced data” option and create a unique passphrase for encryption.
* **Configure content settings:** Click “Content settings” under the “Privacy” section and do the following:
  + *Cookies:* Select “Keep local data only until I quit my browser” and “Block third-party cookies and site data.” These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.
  + *Pop-ups:* Select “Do not allow any site to show pop-ups.
  + *Location:* Select “Do not allow any site to track my physical location.”
* **Configure passwords and forms settings:** Disable Autofill and deselect “Offer to save passwords I enter on the web” under the “Passwords and forms” section. Doing so will prevent Chrome from saving your logins, passwords, and other sensitive information that you enter into forms.

In this fight for online protection, keeping your main tool – the BROWSER – secure is a vital step. That is why our operating system defense should contain multiple layers of protection, from security products to manually customizing our browsers, since our web browser is actually the central tool we use to access our social media accounts, our e-mail addresses and our online banking websites.

But,  there is an ongoing fight and challenge for online security and we have to be open and accept alternative means to protect our private data. Therefore, we want to know your opinion.

### Comments

# Safe Browsing on the internet

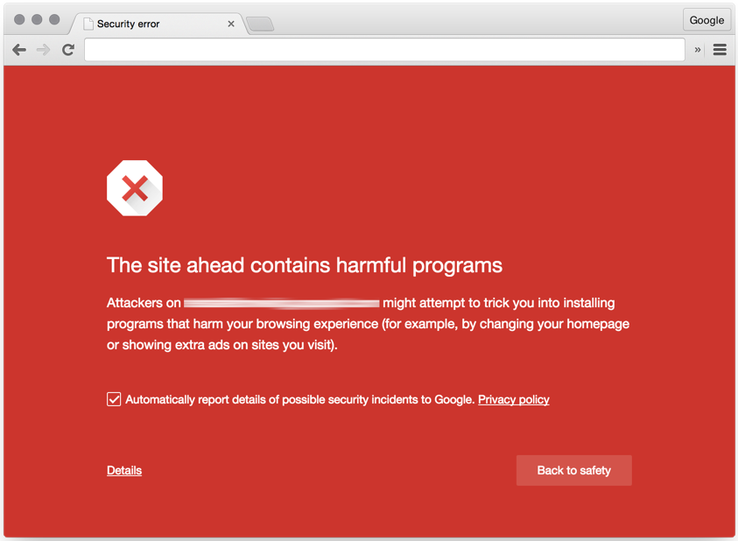
Published Date : September 7, 2016  
Author : tayo

#### 

#### While you are innocently surfing the Web, you may not realize that you could be picking up spyware, downloading malware, or even visiting fraudulent sites. Of course, you do not have to be afraid of every click you make, but there are some simple precautions you should take to stay safe while you’re browsing.

#### *Protecting your computer against malicious sites*

Every browser has security features that protect you against visiting malicious sites that contain **malware** or **phishing scams**. When you visit a malicious site, your browser will display a **red warning message**.

****

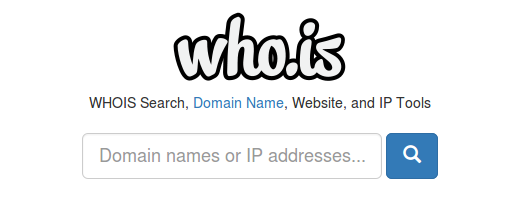
#### *Keeping your browser updated*

New malware and phishing threats are constantly being introduced, so it is important to keep your browser updated. **How do you do this?**

1. **Make sure you have the latest version of your browser.**
2. **Make sure you have installed all recent updates.**

#### *Domain checking*

Malicious sites often use **deceptive domains** to trick users into believing they are on a legitimate site. For example CBN site should be www.cbn.com.ng **and not** www.cbnn.com.ng with an extra **n.**



**Internet Explorer** has a feature called **Domain Highlighting** for checking domains.

#### *Verifying secure sites*

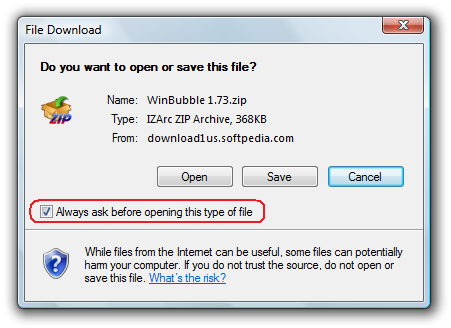
### Downloading precautions

One of the easiest ways **malware, spyware**, and **adware** can access your computer is through **downloads**; The following tips will help you download content safely.

#### *Download only from trusted sites*

You should only download from well-established sites you trust. **[CNET](http://download.cnet.com/)** is one reputable site where you can download files that have been checked for malware, spyware, or adware.

#### *Save downloads vs. running them*



#### *Be cautious of freeware*



Common types of **freeware** (free software) include desktop backgrounds, free images, emoticons, computer games, etc.

#### *Avoid illegal downloads*



When you illegally download **copyrighted material** like music, books, software, games, and videos, you are violating federal laws, which can lead to fines and even jail time.

#### *Be cautious of P2P file sharing*

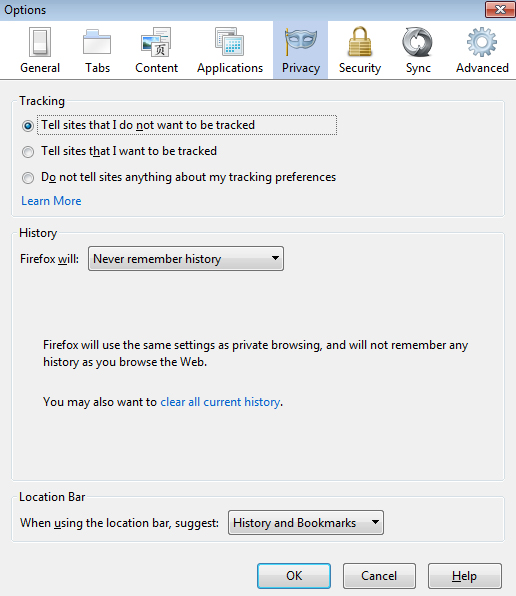
**Peer-to-peer (P2P)** file-sharing programs like BitTorrent and LimeWire have been known to contain malware, adware, and illegal downloads; therefore, it is best to practice caution when downloading and sharing from P2P sites.

### Understanding how your browsing activity is tracked

Did you know that your actions and what you click on may be tracked when you browse the Internet? Here are a few examples of how that can be done:

* Websites like Amazon, eBay, and Netflix **collect data about your preferences** so they can make suggestions to you for products or movies they think you might like.
* Google tracks and analyzes activity **to provide statistical data to companies**. These companies may use this data for marketing or advertising purposes, or to analyze the effectiveness of a website.
* Some governments may collect data about your online activity in case it is needed for **criminal investigations** or **national security purposes**.

It is important to have an awareness of this tracking to practice safe browsing habits based on your desired level of privacy.



### Pop-up blockers

**Pop-ups** are small browser windows that automatically pop up when you visit certain sites. They may sometimes be part of the legitimate functioning of a site, or they may contain **advertisements** that can be annoying or objectionable. However, some pop-ups may contain **malware**; therefore, it’s a good idea to make sure your browser’s **pop-up blocker** is turned on.

#### Turn on Pop-up blocker in Chrome

#### 

#### Turn on Pop-up blocker in Internet Explorer

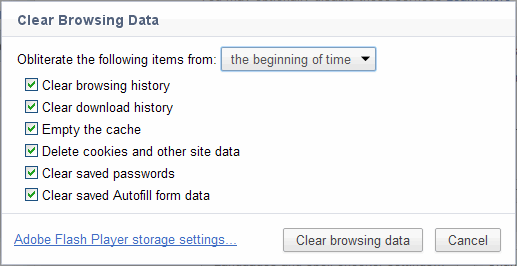
#### 

**Important:** If you encounter a pop-up that seems suspicious, do not click **OK**, **Cancel**, or **Agree** to try and close the window because this may access malware. Close the window by clicking the **X** in the upper-right corner or by pressing **ALT+F4**on your keyboard (if you use Windows).

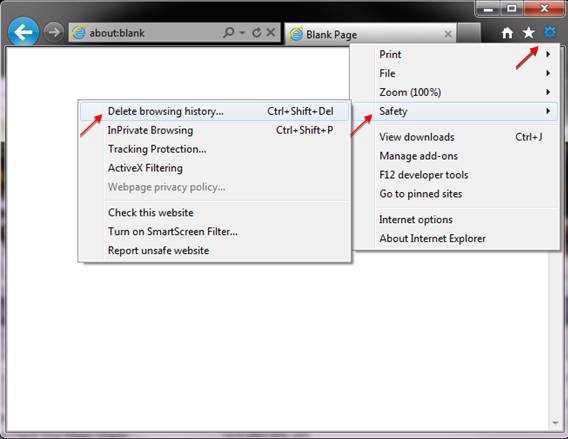
### How to clear your cache

Web browsers store pages, images, and downloaded content to the **cache** when you visit websites. The browser can speed up access to sites by loading pages from the cache rather than re-downloading content when you return to a site. However, with a high-speed Internet connection you may not notice the difference. In addition, the cache can take up space over time, causing your browser to slow down. Therefore, it’s a good idea to **clear the cache on a regular basis** to help free up space on your computer.

#### Clearing the Cache in Google Chrome



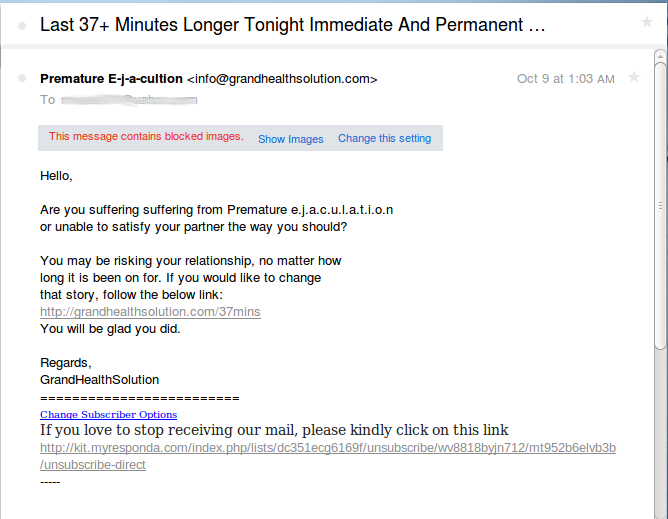
#### Clearing the Cache Internet Explorer



### Comments

# 10 Tips to Avoid Spam

Published Date : September 7, 2016  
Author : tayo



Below are 10 tips on how one can protect his email address to minimise the risk of getting spammed. Conveying these tips to all the users in your organization could help reduce the volume of spam received.

1. Spammers in most cases need to know your email address before they can spam you so **keep your email address to yourself** as much as possible and use it only for work purposes.
2. When posting on a forum **do not include your email address as part of your signature**. If need arises to post your e-mail address, format it so that it cannot be easily harvested such as “name –at- gmail – dot- com,” Or if you need to include your e-mail address in your signature, include a small graphic image containing your e-mail address.
3. Guest books are a prime source for the harvesting of email addresses that spammers use. Some guest books automatically hyperlink your email to your username; avoid posting in such forums and **never include your email address in the post** itself. Do not use your work email for this kind of personal use. If you do not have an alternative email address consider using free services such as Google mail, Yahoo! mail or Hotmail.
4. When signing up for forums, offers and other public services **never use your work email address**; if it doesn’t break the terms of use, consider using disposable email addresses. If terms prohibit the use of disposable email, use free email services that include spam filtering.
5. **Never click on links in a spam email**; in some cases clicking will result in you confirming to the spammer that the email address is valid and the user is likely to click on links thus making you a prime target for more spam and phishing attacks.
6. Always **review the privacy terms on sites before registering**. You need to know that whoever you’re signing up with will not give away your email address to third parties who might actually end up selling your email address for money.
7. If you use IRC and chatrooms **ensure that you’re not displaying your email address publicly**(some IRC clients do this by default).
8. If you have a personal website, **do not publish your work or personal email** on it. Spammers use scanners that harvest such emails as well. Use free email services for this purpose.
9. **Do not use the unsubscribe links in spam emails**, in some case that will actually confirm the email address is valid to the spammer.
10. **Do not open attachments in spam**, you could get infected with Trojans that will send your email contacts to a spammer as well as entrap you in a spammer distribution chain i.e. your computer might be the one that the spammer uses to send spam emails.

Source : GFI

### Comments

# Most common attack vectors for breaking into websites and computer systems

Published Date : September 7, 2016  
Author : tayo



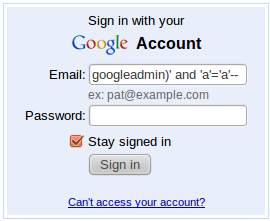
It seems that there are more and more news reports every day about how hackers have broken into the networks or website of a company or government department, and it happens everywhere around the world. How do attackers do it? They do it by following one or more of the following steps, and the ones they use depend on the nature of the attack.

**Reconnaissance**The hacker tries to find out basic but important information about the system she’s targeting. For instance, they need to know the operating system, if there’s a firewall, what connection ports are open, what content management system (CMS) is used, and the identity of the main users. A good hacker will know how to harvest this information from open sources such as social media networks and search engines.

**Known Vulnerabilities**A number of online sources publish information about different systems’ security weaknesses and as a way of establishing bona fides, will also frequently publish the code that was used to attack the system. Hackers will use this information in planning and executing their attack.

These attacks normally work when there are security lapses like improper configurations of servers and applications, the lack of firewalls on a network, or missing security patches.

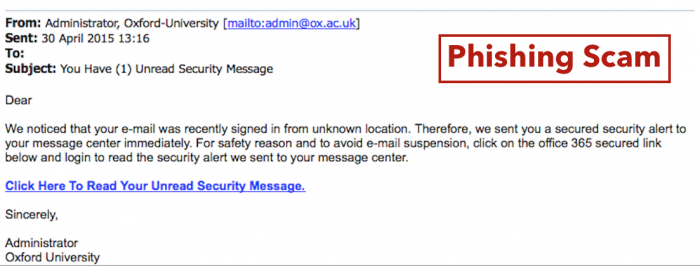
**SQL Injection**This type of attack works by manipulating the database queries that the web application sends. An application can be vulnerable if it does not sanitize user input properly or uses untrusted parameter values in database queries without validation.



**Some of the ways of protecting against SQL injection are:**

* Using parameterized SQL
* Sanitizing/validating all untrusted parameters before using them in database operations
* Using tested and code reviewed libraries for database operations
* Using least privilege for database access (never let application use administrator user for database access)

**Phishing**This type of attack is very old and still effective. The attacker normally sends out a lot of spam email to many people, and the messages contain links to fraudulent websites that have been made to look like, a bank’s website, for example. The message will ask the reader to enter some type of sensitive credential, which the fake website will capture and enable the attacker to impersonate the recipient or steal other valuable information – or in the case of payment card details, money.



To best protect yourself, don’t ever click on a link in an email message from an unknown person, or in a suspicious-looking message. If you want to verify any requests for credentials such as your password, always type in the link directly into your browser and verify the information on the website that loads.

**Spear Phishing**This is a type of phishing attack, but directed at a particular person or organisation. The email message will contain information that will convince the recipient that they know the person in question, as a way of trying to establish trust.

****

**Malware Attacks**Malware is a malicious software installed on your computer, mostly without your knowledge. This happens when an attacker sends out phishing emails with attachments containing the malicious code, or if you click on a file containing malware from a website.

Note: Avoid clicking on Illegitimate links to win stuff, download free antivirus, Instant prize draw, etc…

Malware can control the user’s computer, capture key strokes, or look for documents on the computer.

**Weak Authentication**Poor security such as weak passwords, insecure password reset methods, or allowing an indefinite number of invalid login attempts. A strong password is one that is difficult to guess or figure out.

**Conclusion**The above mentioned methods are just a few common ways in which hackers can break into websites or computers. Everyone must bear responsibility for their individual and their organisation’s security, and know the latest methods of attack.

### Comments

# Dangers Of Wireless Connection and How To Secure Yourself Using Public Wireless Connection

Published Date : September 7, 2016  
Author : tayo



The reasons why people moved to Wireless connection is to overcome  the physical limitations of internet access. But from an attackers view, wireless connections are easy to target and intercept.

### What Are Dangers Of Using Open/Public Wireless

People are always eager to use free wireless  without considering the dangers that comes with it.



Man in the Middle Attack (MITM) can be described as a way in which an attacker intercepts connection between two systems i.e The Access Point and The Victims.  Here’s how it Works: An Attacker sets up a Fake Access point (free wi-fi) in a Public place and you quickly connect to it.The attacker has his own motive for creating this; to spoof your entire browsing history, including your usernames and passwords.



Another method is when you connect to a public wireless from a restaurant, airport, or an open space. and you’re Browsing through Facebook or Gmail. Since these sites are both encrypted with HTTPS and you’re pretty sure it is secured, And you think no one can intercept your connection since you’re browsing on  a secure site. The hacker intercepts this network through an attack called [SSL Stripping](http://sectools.org/tool/sslstrip/).

DNS Cache Poisoning is another method similar to SSL Stripping, Let’s say you want to browse Facebook?, Your Computer send request to the Wireless router to access Facebook and the Router send back the response back to your computer with Facebook. But with DNS Cache Poisoning, The **Attacker** is the one between the connection i.e the Wireless Connection and Your Computer.

When you Browse Facebook, instead of your Computer to communicate with the free wireless Connection directly it will pass through the **Attackers** Computer, Then to the **Access Point**, get response from the Wireless Connection back to the Attacker Computer, Then Back to you. With this he can do **modifications** right from his computer so that whenever you browse Facebook or Gmail it may appear to you as Facebook but if you look closely, it’s just a [Phishing site.](https://safety.yahoo.com/Security/PHISHING-SITE.html)

### How To Secure Yourself From Public/Open Wireless

If you want to use  a Public Connection always check that your website is accurate. That’s what most people don’t do, Browse On HTTPS site as we have mentioned earlier. Don’t do transactions with your Bank online as that’s the main reason for an attacker to intercept your connection. If you want to do that get yourself a private connection and do that.

Important: Don’t forget to turn off your wireless connection when its not in use

### Secure Yourself with the Use of a VPN

To protect against this type of attack you should use a VPN to make your online activities safe, secured and encrypted. There are many VPNs available on the internet, we have VyprVPN, Hide My Ass, OpenVPN and VPNGate. For this session, we would talk about VPN Gate.

VPN Gate is a free, non-commercial ‘Academic Experiment Project’ developed by the University of Tsukuba. The VPN Gate network consists of VPN relay servers located all over the world.

**How to setup VPN GATE**

1. Visit www.vpngate.net/en/download.aspx
2. Download and install the VPN GATE client.
3. Open the VPNGATE client
4. CHoose the server you want to connect to.
5. Once connected your connection becomes secured and you can browse the internet safely

### Comments

# Creating Secure Passwords

Published Date : September 7, 2016  
Author : tayo



Passwords — especially those not supported by [two-step verification](http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/) — are your last lines of defense against prying eyes. This guide will help you understand how those passwords are exposed, and what you can do to keep them locked down.

### How are passwords exposed?

1. **Someone’s out to get you.**
2. **You become the victim of a brute-force attack.**
3. **There’s a data breach.**

### What makes a good password?

Ideally, each of your passwords would be at least 16 characters, and contain a combination of numbers, symbols, uppercase letters, lowercase letters, and spaces. The password would be free of repetition, dictionary words, usernames, pronouns, IDs, and any other predefined number or letter sequences



### Creating secure passwords

Create a phrase like “I hope Nigeria will win the FIFA World Cup  in 2016!” Then, take the initials of each word and all numbers and symbols to create your password. So, that phrase would result in this: **IhNwwtFWCi2016!**

Also, make sure to use a mix of letters, numbers, and symbols in your password.For example, a password with numbers, symbols and mixed-case letters like **Alph4b3t@** (“Alphabeta” scrambled with numbers and symbols) is harder to guess.

Many password managers like **LastPass** or **Dashlane** also have built in password generator tools.

### Enable two-step-verification

### Any time a service like Facebook or Gmail offers “two-step verification,” use it. When enabled, signing in will require you to also enter in a code that’s sent as a text message to your phone. Meaning, a hacker who isn’t in possession of your phone won’t be able to sign in, even if they know your password.

Here’s a detailed [list how to set up two-step verification](https://twofactorauth.org/) for many popular websites.

### Keeping track of secure passwords

The logic is simple: if you recycle the same password (or a variation of it), and a hacker cracks one account, he or she will be able to access the rest of your accounts.

You can’t be expected to memorize dozens of complicated, 16-character-long passwords but you can use a password manager to help you store them safely and encrypted.

### 

### Using a password manager

Password managers store all of your passwords for you and fill out your log-in forms so that you don’t have to do any memorising. There are many options available, but a few crowd favourite are [LastPass](http://lastpass.com/), [Dashlane](http://dashlane.com/) and [1Password](http://1password.com/).

The tiny caveat is that you’ll still have to memorize one thing: Your master password. This unlocks all your other passwords. Make your master password extra-secure by composing it of at least 12 characters to ensure that it’s not vulnerable to any brute-force attacks.

### Comments

# Using Public Computers Safely

Published Date : September 7, 2016  
Author : tayo



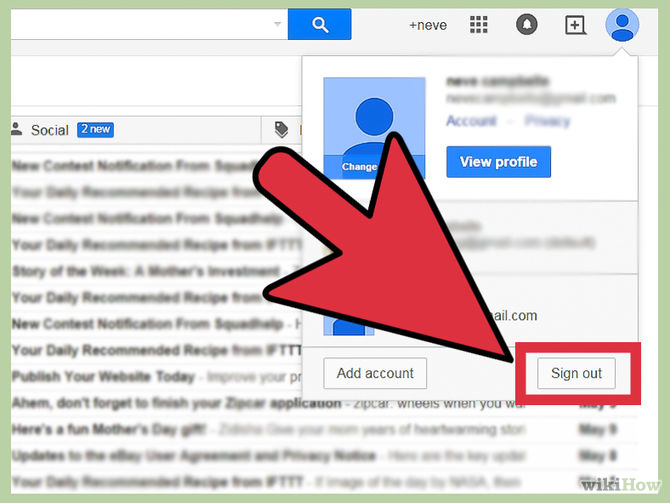
Every browser (Internet Explorer, Firefox, Google Chrome, Opera etc) keeps a copy of the sites you visit, the pages you click and even your password in a place called cache.

The next person to use the computer may be able to check this information if they know what to do.

Using public computers at cybercafes, public libraries and even computers of friends can be safe if you do the following:

## Always sign Out

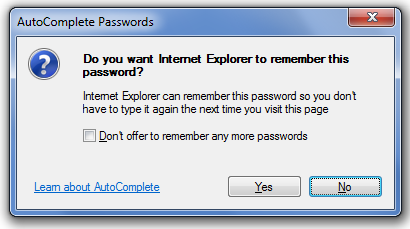
Make sure you sign out of websites by clicking **“log out”** or **“sign out”** on the site. Do not just close the browser and think you are safe. The next person may be able to open the browser and find you are still logged in.



## Do not Save Passwords

Sometimes this feature is turned on, by mistake or on purpose. Make sure it is not enabled.

### Internet Explorer



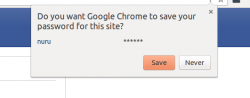
Go to Tools | Internet Options | Content. In the AutoComplete panel, click the Settings button and verify that the Prompt Me To Save Passwords check box is deselected. None of the other AutoComplete features needs to be enabled either, so deselect them as well.

### Firefox

### 

Choose Tools | Options | Security and deselect Remember Passwords For Sites

### Google Chrome



## Do not Leave the Computer Unattended

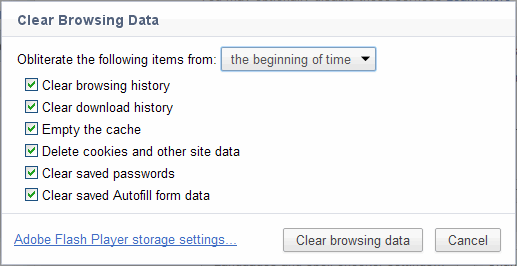
Especially with sensitive information on the screen. If you have to leave the public computer, log out of all programs and close all windows. Then erase your tracks.

## Erase Your Tracks

Web browsers such as Internet Explorer keep a record of your passwords and every page you visit, even after you’ve closed them and logged out.

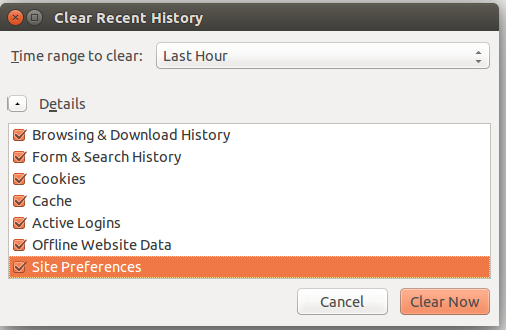
When you finish your use of a public computer, you should delete all the temporary files and your Internet history

### Internet Explorer



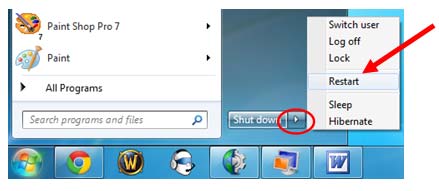
Click **Tools** and then **Delete Browsing History > Delete All**

### Firefox Browser



Go to Tools | Options, click the Privacy tab, and select Always Clear My Private Data When I Close Firefox.

## Reboot When Finished



When you’re finished using the public computer, the final thing you should do is a hard reboot.

## 

## Create a Temporary Email Account

Most email accounts can forward to another one. If you are going away for a few days, create a temporary email account using mailinator.com and forward your emails there.

## Watch Out for Snoops

When you use a public computer, be on the lookout for people who look over your shoulder or watch as you enter sensitive passwords to collect your information.

A cell phone camera or someone with a good memory could capture your information easily. Don’t forget people can watch your hands and see what keys you press.

## Do not Enter Sensitive Information into a Public Computer

These measures provide some protection against casual hackers who use a public computer after you have. If you can, use a USB drive to store your information.

When you get home, change the passwords of any accounts you logged into while on the road. This will mitigate anyone tampering with your account.

But keep in mind that an industrious thief might have installed sophisticated software on the public computer that records every keystroke and then e-mails that information back to the thief.

If you really want to be safe, avoid entering any sensitive information into any public computer.

## Do not Forget to Take your USB drive

It happens. You get in a hurry and leave your USB drive (or floppy) on the public computer. You are forewarned.

****

### Comments

# An Overview of Digital Security; The need and Dangers

Published Date : September 7, 2016  
Author : tayo

Nasir is a journalist who uses social media platforms to meet new people. On Facebook he has about 2k friends, on twitter, he has 5k followers and a generous amount of instagram followers. He puts up his email contact and telephone numbers on all. Nasir receives an email from one of his twitter followers about a new case he might be interested in with a link attached to view more details. Unknown to him, it was a scam in form of Phishing, where they would have access to all his login information and bank details which he had stored on his email draft folder. This was how Nasir was ripped off of about 500,000 naira. This example stresses the need to secure yourself online.

**Definition of Digital Security**Digital security is the protection of one’s digital personality, as it represents the physical identity on the network you are operating on or the internet service in use. Digital Security includes the tools which one uses to secure his/her identity, asset and technology in the online and mobile world. Simply put, let’s think of digital personality as the human body. Now, what are the methods (tools) we use to protect our bodies? Well, we eat and live healthy and put ourselves out of harm’s way.

**Why do we need Digital Security?**Everyday, there are quite a number of cyber-attacks and anybody could be a victim of a cyber-theft, hack or crime. Leading global brands have been hacked with false information put up on them and small businesses and innovative start-ups in all industries are frequently targeted because most of them do not have proper digital security systems in place.  It is very common to see a popular activist tweet “the previous tweets from my account were not from me. I was hacked”. Also, from the above story of Nasir, we can see why it is important to protect ourselves digitally. Nobody is ready to part with things they worked hard to achieve and acquire.

**What digital security tools are available to us?**The most important Digital Security tool available to everyone is actually free and we all have access to that tool. This is none other than being concerns and aware of the fact that the information we share over digital spaces could be used against us. Hence we should be careful as to what we share digitally and he extra cautions when receiving information which we suspect might be fraudulent.  
There are quite a number of digital security tools available to users and these are identified below:

**– Tools for anonymous navigation online**If you intend to navigate the internet without giving off your location, you could install a software called [Tor](https://www.torproject.org/) on your computer, which allows you hide your location and keeps whatever you are doing on the internet private. Very easy to install, Tor is also free. Another software which is also free is [AnonymoX](https://www.anonymox.net/en) and is available to Firefox and Google Chrome web browsers as addons.

**– Tools for telephone encryption**SilentPhone for phone calls. Free, and works on the [Android OS](https://play.google.com/store/apps/details?id=com.silentcircle.silentphone&hl=en) and [iOS devices](https://itunes.apple.com/us/app/silent-phone/id554269204?mt=8).  
[Signal](https://whispersystems.org/) created by a firm called the “Guardian Project”. It is available on almost all device and operating system. Signal encrypts your voice and video conversations and is a better alternative to using Skype.

**– Tools to encrypt instant messaging**If you are someone who shares important information via instant messaging, you should use [Cyph](https://www.cyph.com/) which encrypts messages for both mac and windows users.

[ChatSecure](https://chatsecure.org/)  works perfectly on [iOS](https://itunes.apple.com/us/app/chatsecure/id464200063) and [Android](https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im) platforms

### Comments