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

# Wipe a stolen android phone

Published Date : October 14, 2016  
Author : tayo

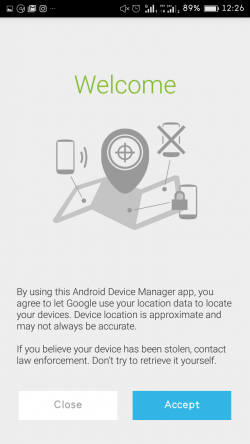
### Wiping your data from your Android phone

Sometimes things like the above happen and we have to resort to extreme measure like wiping all of the data from our phones. If it’s lost and you’re afraid that someone might access your data, you may have no other choice. If it comes to this, you have to act quickly before you lose the one chance you have to connect to your phone remotely and delete your data. But as long as your Android phone is connected to your Google account and to the Internet, you have a good chance.

Wipe the data from your Android device using the **Android Device Manager**



Android Device Manager is the tool that Google uses to track Android device users. Logging in to your device through your Google account will enable you locate or wipe the device. To verify that you’re **connected** to your Google account, check if you have Google calendar entries, e-mail messages on your Gmail account, or if you’ve used Google Drive through your device. If the answer is yes to any of these, then your’e connected.



Now, Google created restrictions to prevent people from mistakenly losing their data. One of these is disabling the ‘***Remote lock and erase***‘ function on your device, which you’ll have to enable yourself.

To enable the feature, go to your Android Device Manager and log in with your Google account. The system will then attempt to connect to and find your device so that you can send commands to it. Now, send the ‘Erase’ command; if for some reason your device isn’t connected at that moment, the command will go through the next time it’s connected to the Internet. But remember that once the data is wiped, the connection to the device will be gone, and you won’t be able to find it again.  


**Note:** Losing your phone isn’t ideal but it’s very important that no one sees your personal data.

### Comments

# Safe Backup and Data Storage

Published Date : September 8, 2016  
Author : tayo

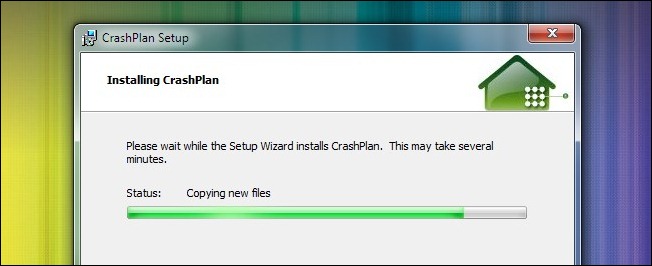


Backup is a process of producing additional copies of data, file or other item made in case the original is lost or damaged.

There are so many software that you can use to backup your files in the cloud and they include Google Drive, BOX, DropBox, SkyDrive, iCloud, Crashplan and Mega just to name a few.

In this demo we would be showing you how to use [CrashPlan](https://www.crashplan.com/) ([www.crashplan.com](http://www.crashplan.com))to backup your pc

### Getting Started: What You’ll Need and Installing CrashPlan



For this guide you’ll need the following things:

* A [copy of CrashPlan](http://www.crashplan.com/consumer/download.html) for Windows, Linux, or Mac.
* A free CrashPlan account.
* A friend/relative with a broadband connection and a copy of CrashPlan

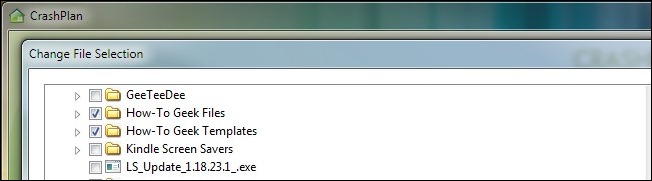
Again, we’re focusing on using your friend’s computer as a remote backup location. If you lack a friend willing to share some hard drive space and/or their broadband connection you can easily follow this tutorial to do the backing up over the local network.

Installing CrashPlan is straight forward. [Download the application](http://www.crashplan.com/consumer/download.html), run the installation file, select a location, and install.



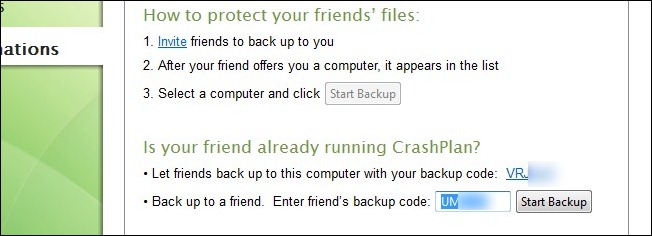
It might seem a bit sluggish for the first minute or so as it scans for files. For this guide we’re going to cut down on the size of the backup considerably so we don’t have to wait for all 16.2 GB in our user folder to seed. The size of your remote backup is limited only by your broadband speed and the space your friend is willing to share.

### Configuring Your Backup



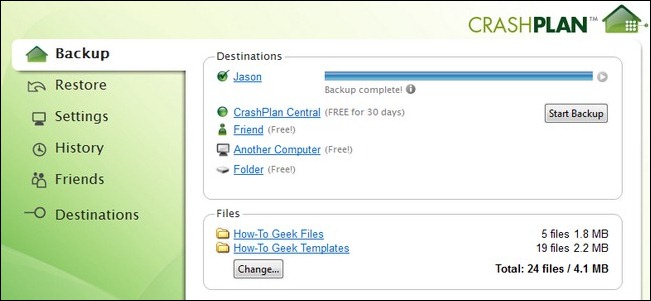
Depending on how large the original sweep was you may want to reconfigure the size of your backup before dumping it to your friend’s computer. Look at the bottom of the interface in the **Files** section and click **Change**. There you’ll find a directory list with your entire User directory checked. If your backup size is reasonable you can leave it as is. If it captured a lot of bulky directories (like your entire MP3 collection for instance) you might want to opt to locally backup your music instead of chewing up the time and bandwidth transferring it all to your friend’s computer. As we mentioned above, we opted to reduce the number of files for our tutorial in order to avoid a lengthy seed time.

Once you’ve selected the folders you want included in your backup, click on the **Friend** link in the**Destinations** section. You’ll see this in the lower section of the screen:



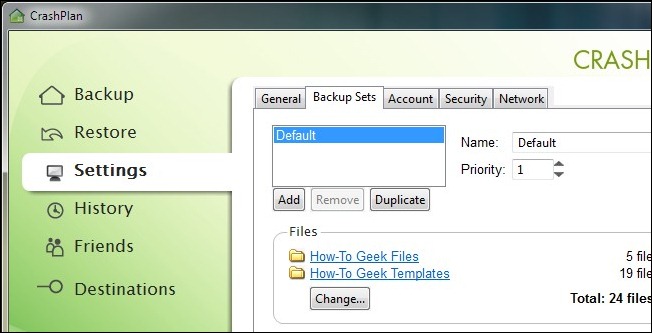
Here you can get your backup code (to share with a friend who wants to backup to your computer) or plug in the code they’ve sent you. We’ll presume that you’ve already cleared this backup-sharing plan with your friend or relative and have their code on hand (and thus can skip the invitation step).

With the code in hand, plug it into the **Enter friend’s backup code** slot and click start backup. It will immediately start backing up the files if your friend is online. When it’s done you’ll see a screen like this one:



Your files are now stored on the remote machine, a veritable Poor Man’s Cloud Storage. It’s worth noting here that if your total backup size is small (say, a few GBs of documents and photos) it’s worth it  to set up this arrangement with multiple friends. You’ll backup their documents and in turn you’ll be able to spread your documents and such across even *more* remote locations.

### Advanced Configuration and Backup Sets



### Comments

# Password Manager and How to Get Started

Published Date : September 8, 2016  
Author : tayo



Most times we need to create strong unique and memorable passwords for all the website we visit but it is quite difficult to remember all passwords to every website you signed up to. To solve this problem of remembering you can use a password manager to save all your passwords in a secured encrypted manner.

Password managers store your login information for all the websites you use and help you log into them automatically. They encrypt your password database with a master password – the master password is the only one you have to remember.

### Don’t Reuse Passwords!

Password reuse is a serious problem because of the many password leaks that occur each year, even on large websites. When your password leaks, malicious individuals have an email address, username, and password combination they can try on other websites. If someone gains access to your email account in this way, they could use password-reset links to access other websites, like your online banking or PayPal account.

### What Using a Password Manager is Like

A password manager will take a load off your mind, freeing up brain power for doing productive things rather than remembering a long list of passwords.

When you use a password manager and need to log into a website, you will first visit that website normally. Instead of typing your password into the website, you type your master password into the password manager, which automatically fills the appropriate login information into the website. (If you’re already logged into your password manager, it will automatically fill the data for you).

### Password Managers to Use

A variety of password managers are available, but three stand out as the best options. Each is a solid option, and which you prefer will depend on what’s more important to you:

**[Dashlane](https://www.dashlane.com/)**

[](https://www.dashlane.com/)

**[LastPass](https://lastpass.com/)**



**[KeePass](http://keepass.info/)**

[](http://keepass.info/)

### Getting Started with Your Password Manager

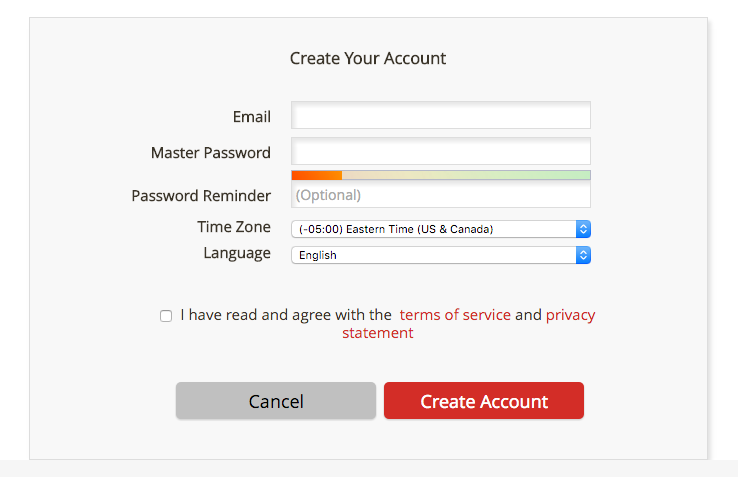
The first big decision you will need to make with a password manager is choosing your master password.

After installing a password manager, you will likely want to start changing your website passwords to more secure ones.

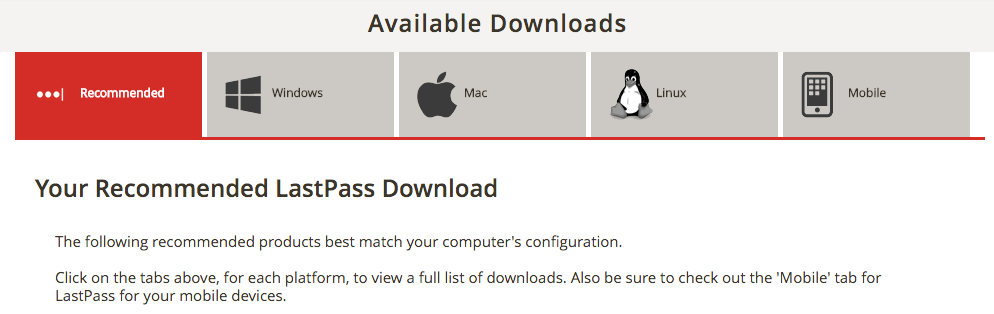
Password managers can even help against [phishing](https://en.wikipedia.org/wiki/Phishing), as they fill account information into websites based on their web address (URL).

**DEMO: How to Install and use Lastpass**

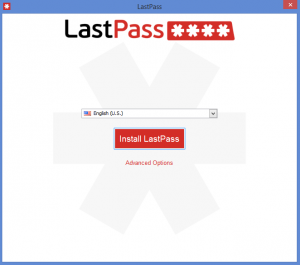
If you haven’t already, create your [LastPass account here](https://lastpass.com/create_account.php). This account will give you access to your data anywhere you can log into LastPass since your stored data is securely synced to our servers. So downloading the plugin/app to a new browser/OS/device allows you to easily access everything in your one LastPass account.



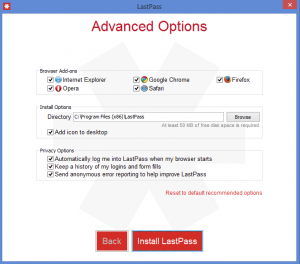
Begin by visiting the [downloads page](https://lastpass.com/download.php) where LastPass will recommend the appropriate installer for you. Click ‘Download’ to download LastPass full installer, or you cal click on any of the tabs to specify the product you wish to download and install. All of LastPass’ products can be found here.



After downloading the recommended installer, a menu will present you with the following dialog screen:

[](https://helpdesk.lastpass.com/wp-content/uploads/Installer_win.png)

Click ‘Install LastPass’ to begin installation. If needed, you can alter your installation by clicking ‘Advanced Options’. This provides you with the options below:

[](https://helpdesk.lastpass.com/wp-content/uploads/installer_adv_win.png)

At the end of the installation process, you will be asked if you would like to import any passwords located on your computer. Select ‘Import’ to import the items listed. If you would rather do this later, click ‘No Thanks’. To import later, please see our [Import page](https://helpdesk.lastpass.com/getting-started/importing-from-other-password-managers/).

[](https://helpdesk.lastpass.com/wp-content/uploads/installer_import_win.png)

Once successfully installed, you will see a LastPass icon in your browser toolbar.

### Comments

# How to Turn on Private Browsing in Firefox

Published Date : September 8, 2016  
Author : tayo

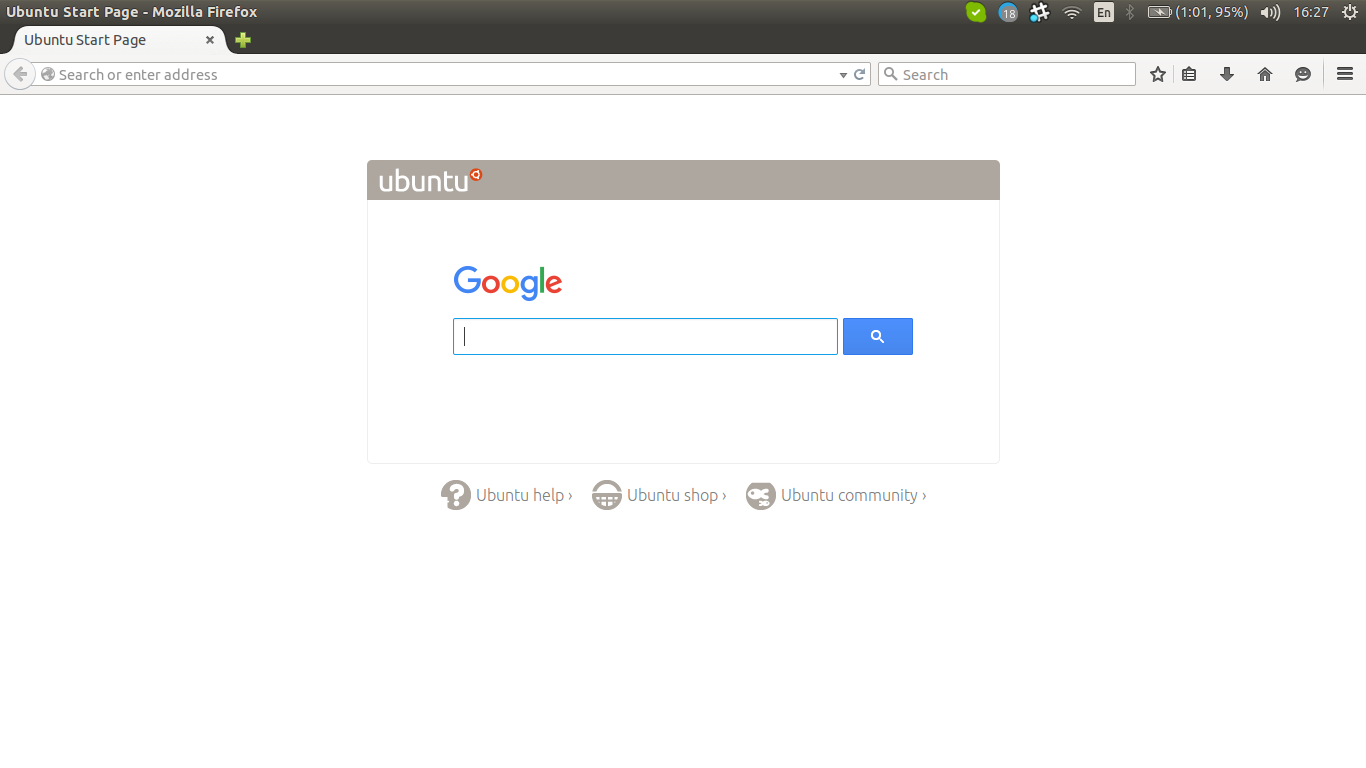
### As you browse the web, browsers remembers lots of information for you – like the sites you’ve visited. There may be times, however, when you don’t want people with access to your computer to see this information, such as when shopping for a present. Private Browsing allows you to browse the Internet without saving any information about which sites and pages you’ve visited.

Private Browsing also includes [Tracking Protection in Private Browsing](https://support.mozilla.org/en-US/kb/tracking-protection-pbm), which prevents companies from tracking your browsing history across multiple sites. To learn more about Private Browsing with Tracking Protection in Firefox, see [Tracking Protection in Private Browsing](https://support.mozilla.org/en-US/kb/tracking-protection-pbm).

We’ll show you how it works.

#### Important: Private Browsing doesn’t make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn’t protect you from [keyloggers](http://en.wikipedia.org/wiki/Keylogger) or [spyware](http://en.wikipedia.org/wiki/Spyware) that may be installed on your computer.

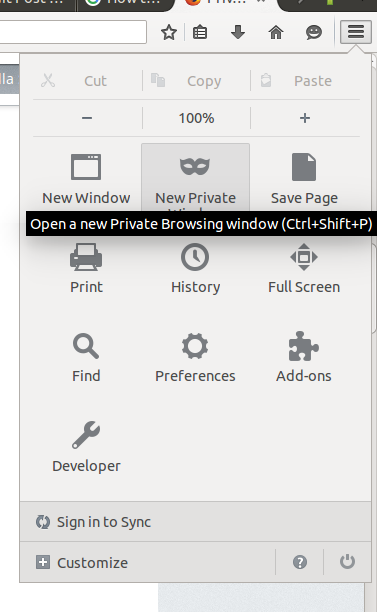
## How do I open a new Private Window?

1. **Open the browser.**
2. 

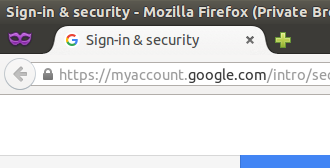
**On the top right hand corner, you should see the and Mozilla Firefox menu icon.**Click on the menu icon  New Fx Menu  and the Mozilla Firefox menu should appear right below the icon.

1. **In the menu, click on the ‘New Private Window’ tab.** Iits just right above the ‘History’ icon(the icon which has a clock). A new window should appear.

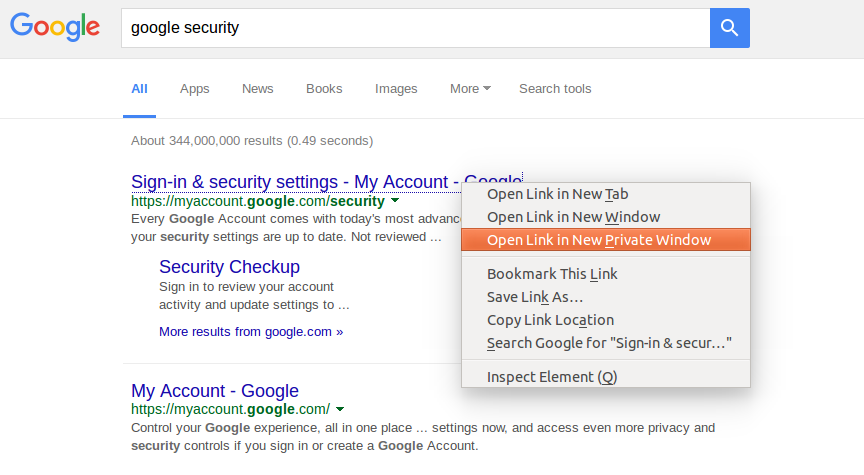
Use Ctrl+⇧ Shift+P for a keyboard shortcut would directly open a Private Browsing window.



1. **Start browsing in Private Mode**

****

1. You could also open the Private Browsing mode by right-clicking a link and then clicking on Open Link in New Private Window.



Now, you’ll be wondering, what does Private Browsing protect me from or what does it not save.

They are:

**Visited pages**: No pages will be added to the list of sites in the History menu, the Library window’s history list, or the [Awesome Bar](https://support.mozilla.org/en-US/kb/awesome-bar-search-firefox-bookmarks-history-tabs) address list.

* **Form and Search Bar entries**: Nothing you enter into text boxes on web pages or the [Search bar](https://support.mozilla.org/en-US/kb/use-search-bar-firefox) will be saved for [Form auto-complete](https://support.mozilla.org/en-US/kb/control-whether-firefox-automatically-fills-forms).
* **Passwords**: No new passwords will be saved.
* **Download List entries**: No files you download will be listed in the [Downloads Window](https://support.mozilla.org/en-US/kb/where-find-and-manage-downloaded-files-firefox) after you exit Private Browsing mode.
* **Cookies**: [Cookies](https://support.mozilla.org/en-US/kb/cookies-information-websites-store-on-your-computer) store information about websites you visit such as site preferences, login status, and data used by plugins like Adobe Flash. Cookies can also be used by third parties to track you across websites.
* **Cached Web Content** and **Offline Web Content and User Data**: No temporary Internet files ([cached](http://en.wikipedia.org/wiki/Web_cache) files) or files that websites save for offline use will be saved.

### Comments

# How to secure your android device

Published Date : September 8, 2016  
Author : tayo



We have to assume that our information is at risk, and take steps to protect our data. To help you with this, we’ve outlined a few steps below.

**Do not save your passwords on your device**

Many people save their passwords to online services and sites on their device, but don’t seem to consider what could happen if someone accessed their phone. For your security, do not store important passwords on your device.

**Use Android’s built-in security features**

If you are running on Kit Kat or Lolipop, there are both screen lock and encryption functions for increased security. There are several types of screen locks such as password, pin, pattern and face unlock, and you can find them in your Android settings. Try to use patterns of PINs that are difficult for other people to guess, but that you’ll easily remember.

**Lock your apps**

Please lock your apps, especially the ones containing private information that you don’t want anyone to see. Try a free app like [App Lock](https://play.google.com/store/apps/details?id=com.domobile.applock&hl=en).

And to add more security, don’t use a combination of a pin or pattern lock that can be traceable from the smudges of your screen – yes, people can trace this.

**Why app permissions are important**

Before installing an app from Google Play, a list of requested permissions will pop up to show you what permission the app requires. Apps require permissions to do things but not all of them are necessary.

Always read through the permissions to make sure they make sense and correspond to what the app actually does. For example, an **alarm app** does not require access your text messages. Not all apps in the Play Store are safe, so beware.

**Secure your network**

Don’t use public WiFi when you want to do something that transmits sensitive data, such as online banking. They can easily sniff out your packets and translate it into actual data of your private information, i.e., your passwords.

You can protect your information by using apps like [Hideninja VPN](https://play.google.com/store/apps/details?id=com.cryptninja.vpn" \l "?t=W251bGwsMSwxLDIxMiwiY29tLmNyeXB0bmluamEudnBuIl0.) so that your outgoing connection is always encrypted, making it harder for anyone to sabotage your data. If you suspect that your device is being attacked, [WiFi Protector](http://forum.xda-developers.com/showthread.php?t=1350941) can help fend off these attackers.

**Use a mobile security app**

It will make your life easier to have an app that handles most of your security. Find a mobile security app that you are comfortable using like [Lookout Security & Antivirus](https://play.google.com/store/apps/details?id=com.lookout) or [avast! Mobile Security](https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&feature=related_apps).

**Back up  your data**

It is imperative in this day and age that you back up your important data. If your device is lost, stolen, damaged or hacked, and you haven’t backed up the data, you may still be forced to do a remote wipe to prevent the person from accessing your information. But this will mean that you will lose all your information in your device.

**Track Your Lost Device**

So you have a backup already but you really want to get your lost device back. There are plenty [device-tracking apps](http://www.hongkiat.com/blog/track-lost-stolen-android-devices/) for Android can help you locate your lost or stolen device, and some can even remotely activate your phone’s GPS.

**Enable remote wipe**

So you are at the point where you have everything installed and ready to go. But, you still need one last feature – the ability for you to wipe your device remotely. This is necessary, especially when you are sure that you cannot retrieve your Android device.

### Comments

# Delete Your Data Securely on Windows

Published Date : September 8, 2016  
Author : tayo



In case you thought deleting a file removes it from your computer, you’re in for a surprise – it doesn’t. A copy of the file remains in a part of your computer called the Master Boot Disk. Someone intent on seeing them can use special software to do so.

If you want to make sure that data you erase is actually gone from your computer, you need secure deletion software. There’s a good one called Eraser. It’s popular, open-source (free), and uses the same principles as other tools. We’ll show you how to use it.

**What is Eraser?**

Eraser is easy to use and lets you delete data securely by overwriting the files with carefully selected random data, rendering them useless. You can delete files on demand or schedule a time for future deletion.

**Step 1**. Download the latest stable version of [Eraser](http://eraser.heidi.ie/" \o "Eraser 6" \t "_blank)  (avoid using beta versions) and install it, accepting all the default settings.

[Download Eraser 6](http://cdn2.pcadvisor.co.uk/cmsdata/features/3365492/Eraser6-1.jpg)

Step 2. Run Eraser  and you’ll see an empty Erase Schedule. We’re going to securely delete a file manually, though, so select New Task from the Erase Schedule menu to display the Task Properties window and ensure Run Manually is selected as the Task Type. Click on Add Data to display the Select Data to Erase window.

[Create a new task](http://cdn2.pcadvisor.co.uk/cmsdata/features/3365492/Eraser6-2.jpg)

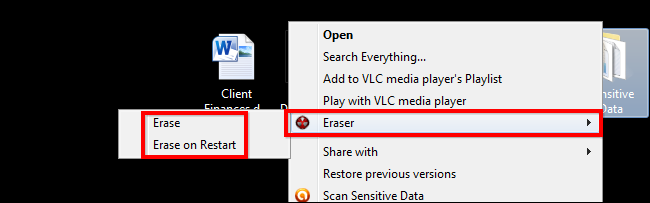
Step 3. Make sure File is selected and click Browse to select the file or files you want to delete before clicking on Ok. Note that we’re choosing to delete the photo of a sign carrying the words “Keep Out”. Click on Open (a misnomer) and then OK and OK again. Finally, in the ‘Erase Schedule’ right-click on the file and select Run now from the menu.

[Choose which files to delete](http://cdn2.pcadvisor.co.uk/cmsdata/features/3365492/Eraser6-3.jpg)

Step 4. The file is now deleted without trace so you can close Eraser .

**Securely Delete Files in Explorer or From Your Recycle Bin**

But if you don’t want to schedule deletion, and just want to delete individual files from Explorer, you can do that with the right-click context menu. Find a file you want to delete, then right-click on it. Then select the Eraser context menu and select whether you want to erase the file now or on the next computer restart.



You can follow the same process for files in the recycle bin.

**Optional: Using the Portable App**

[Download it from PortableApps](http://portableapps.com/apps/security/Eraser-portable)

Using the scheduler on the portable app works the same way, but you should plug in your flash drive when the tasks are to be carried out. Remember, the portable version of Eraser has no right-click context menu entry, making it somewhat harder to erase files in Explorer. You first need to run the app by double-clicking “EraserPortable.exe” from its installation folder.

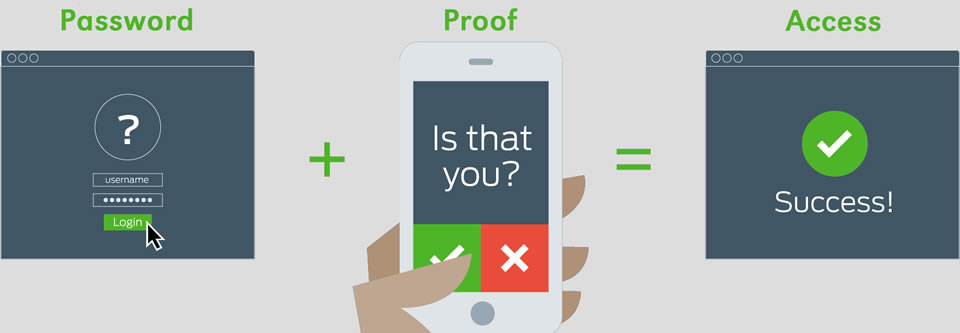
Open the app and find the files you want to securely delete using Windows Explorer and drag them into the Eraser window. After they show on the list, simply click Play to securely delete the files.

Now you have an overview of how to securely delete your files using Eraser.

### Comments

# Setting up extra level of security using Two factor authentication

Published Date : September 8, 2016  
Author : tayo



In today’s world of increasing digital crime and internet fraud many people will be highly familiar with the importance of online security, logins, usernames and passwords but if you ask them the question “What is Two Factor Authentication?” the likelihood is they will not know what it is or how it works, even though they may use it every single day.

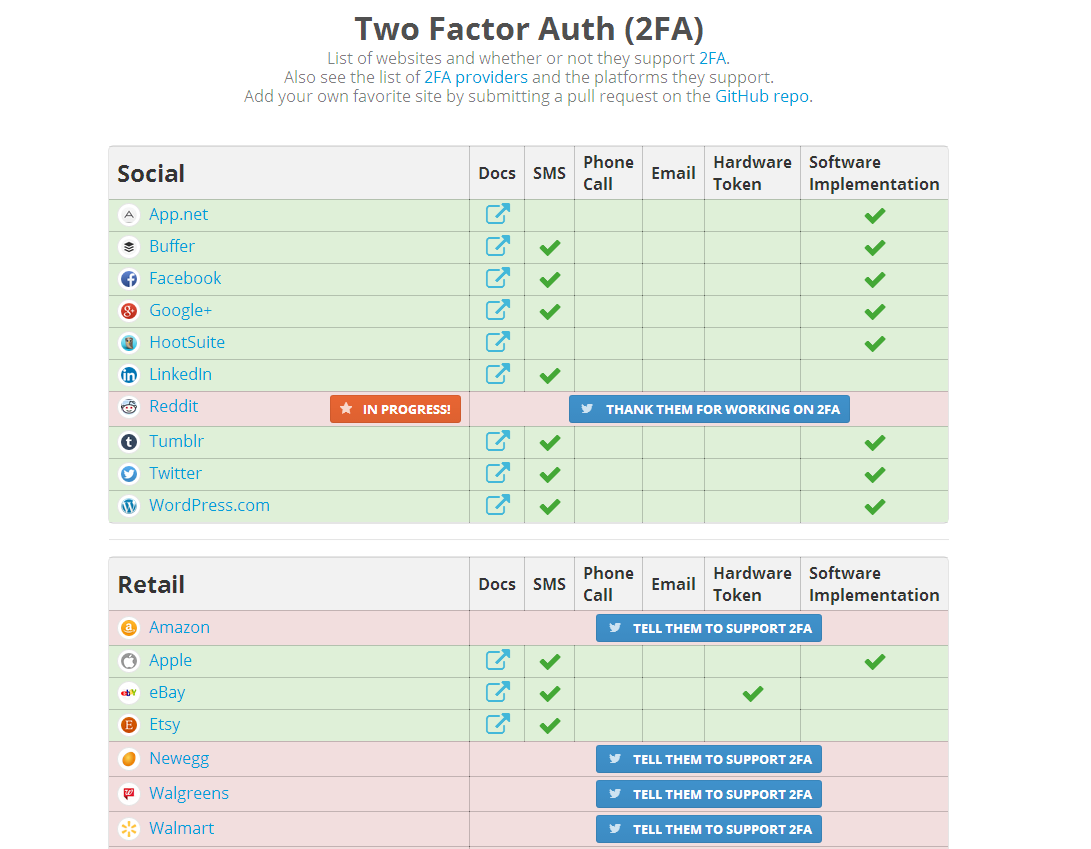
**How does it work?**

Two Factor Authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as “multi factor authentication” that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand – such as a physical token.

Using a username and password together with a piece of information that only the user knows makes it harder for potential intruders to gain access and steal that person’s personal data or identity.

Using a Two Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email, because the criminal would need more than just the users name and password details.

To check out the list of site that supports two factor you can check this website <https://twofactorauth.org/>



### Comments

# iCloud: Erase your device

Published Date : September 8, 2016  
Author : tayo

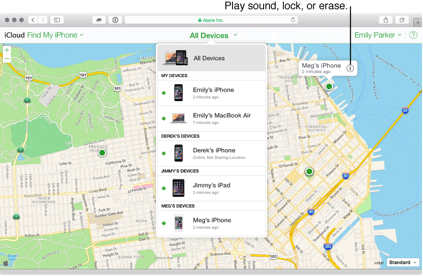


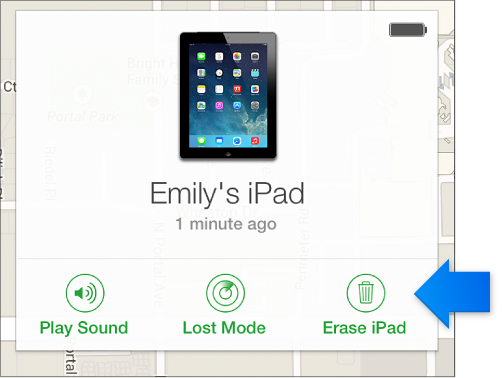
If your iOS device or Mac is lost or stolen, you can erase it if you set up ‘Find My iPhone’ on the device before it was lost. If you have Family Sharing set up, you can erase your family members’ devices, too.

**Important:**   Before you erase your device, try to locate it or play a sound on it. After you erase it, you can’t use Find My iPhone to do either. You may still be able to locate your Mac if it’s near a previously used Wi-Fi network.

### Erase your device or a family member’s device

1. [Go to Find My iPhone on iCloud.com](http://www.icloud.com/find).
2. If you only see Pages, Numbers, Keynote, and Settings on iCloud.com, your account just has access to iCloud web-only features. To gain access to other iCloud features, set up iCloud on your iOS device or Mac.
3. Click All Devices, then select the device you want to erase.
4. In the device’s Info window, click Erase [device].
5. To erase:
   * *An iOS device:* Enter your Apple ID password or your family member’s Apple ID password. If the device you’re erasing has iOS 7 or later, enter a phone number and message. The number and message are displayed on the screen after the device is erased.
   * *A Mac:* Enter your Apple ID password or your family member’s Apple ID password. Enter a passcode to lock the Mac (you need to use the passcode to unlock it), then enter a message. The message is displayed on the screen after the Mac is erased.

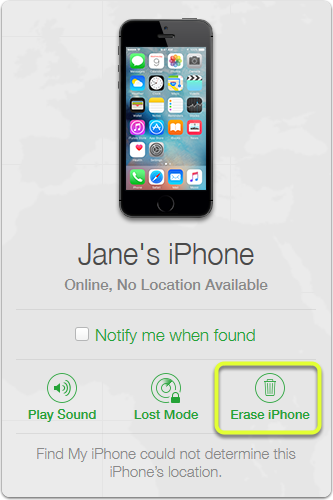




### After you set a device to erase

* If your device is online, the remote erase begins. A confirmation email is sent to your Apple ID email address.
* If your device is offline, the remote erase begins the next time it’s online.
* If you erase then find your iOS device, you can restore the information on the device using iCloud Backup (if backup was turned on before you erased it) or iTunes. For more information, see iCloud storage and backup overview, or the “Safety, handling, and support” section of the iOS user guide for iPhone, iPad, or iPod touch. For a device that doesn’t use the latest iOS version, get the user guide for iPhone, iPad, or iPod touch from the Apple Support manuals website.

**Note:** If you erase then find your Mac, you can restore the information on the Mac using a Time Machine backup, if you have one.





### Comments

# Physical/ Hardware security

Published Date : September 8, 2016  
Author : tayo

****

Securing information is not limited to the encryption and authentication of data processed and received by an individual’s device. There are physical threats that can easily compromise the integrity and confidentiality of information, this can be a simple glance over the shoulder on your plain text email before it is encrypted with that strongest encryption algorithm known. Employing electronic security mechanisms is as important as physical security techniques to protect information.

**AT YOUR WORK**You should position your computer screen carefully, both on your desk and when you are away from the office, in order to prevent others from reading what is displayed there. In the office, this means considering the location of windows, open doors and the guest waiting area, if you have one.



Most desktop computer cases have a slot where you can attach a padlock that will prevent anyone without a key from getting inside. If you have cases like this in the office, you should lock them so that intruders cannot tamper with their internal hardware. You might also consider this feature when purchasing new computers.

Use a locking security cable, where possible, to prevent intruders from stealing the computers themselves. This is especially important for laptops and small desktops that could be hidden inside a bag or under a coat.

**SOFTWARE AND SETTINGS RELATED TO PHYSICAL SECURITY**

Make sure that, when you restart your computer, it asks you for a password before allowing you to run software and access files.

Again, be sure to choose a secure password.



**PORTABLE DEVICES**

Keep your laptop, your mobile phone and other portable devices that contain sensitive information with you at all times, especially if you are travelling or staying at a hotel; even if you are stepping out for a meal.



If you have a laptop, tablet or other mobile device, try to avoid putting them on display. There is no need to show thieves that you are carrying such valuable hardware with much information. Avoid using your portable devices in public areas, and consider carrying your laptop in something that does not look like a laptop bag.

The goal is to reduce the exposure of information to unauthorized access, you may not be able to completely prevent physical attacks but how do you make sure that your information are not compromised when the attack occurs, how do you prevent compromising your correspondence and collaborators.. These are the ultimate goals of enforcing physical security controls.

### Comments

# How to delete your browsing history

Published Date : September 8, 2016  
Author : tayo

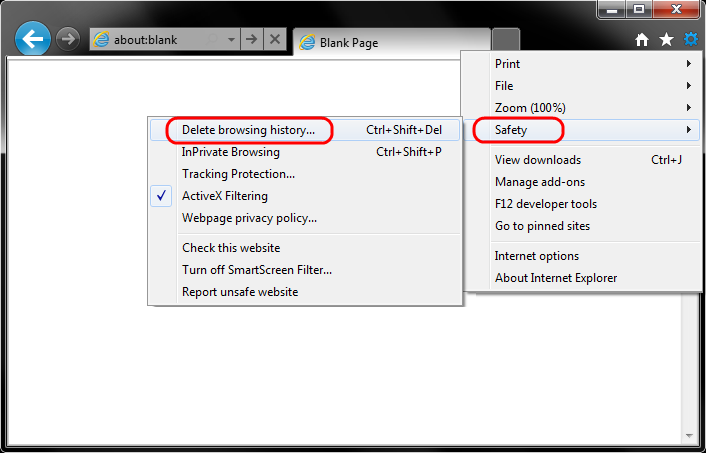
Keep your web searches from prying eyes by wiping your internet footprint, whatever browser you use.

Web browsers record everything you do on the Internet. This can be useful because when you want to return to a previously visited website you’ll find it in the web browser’s history. But it could also hurt because it exposes your private activity to prying eyes, who may sometimes want to do you harm, and you are particularly vulnerable when you share the computer with other people.

But you can protect yourself. All web browsers have a feature that purges your web browsing history so that your habits can remain private. They work on the same principle, but each browser has a different method. We’ll explain how to delete your online tracks in all major browsers and on all major computers and devices and demonstrate how in the video above.

**Step 1: Internet Explorer (PC)**

Internet Explorer 11 (IE 11) is the last version of Microsoft’s traditional web browser. If you’re using an older version of IE you should consider upgrading because Microsoft stopped technical support for them in January 2016.



The main version of Internet Explorer 11 is available on all types of Windows, except Windows 8 and 8.1 which use a full-screen app version.

Click or tap the cog icon in the top right corner. But in older versions of the browser, open the **Tools** menu.

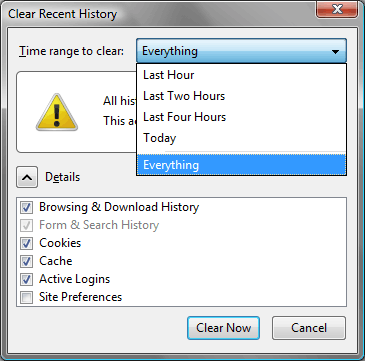
Now choose **Internet options** and, in the **Browsing history** section, click or tap **Delete**. Select the boxes that correspond to what you want to delete, then click **Delete.**

In Windows 8.1, click **Settings**. Click **Options** and scroll down the list to find **History.** Next, click **Select** and select the **Browsing history** checkbox. Then click **Delete.**

**Step 2: Firefox (PC)**

Open the Firefox menu by clicking the box made of three horizontal lines. Then, select **History** and then click **Clear Recent History.**

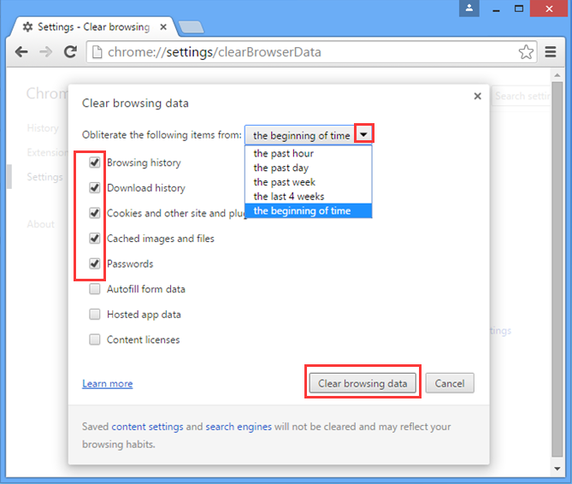
In the **Clear Recent History** dialogue box that appears choose a time frame, and use the tick boxes to choose what you want to delete. When you’re done with that, Click **Clear Now**.



**Step 3: Chrome (PC)**

Click the menu button at the top right – it’s a small box with three stacked horizontal lines – choose **History** and **History** again**.**

To remove individual items from your History, click the down-pointing arrow to the right of the relevant entry and choose **Remove from history**.



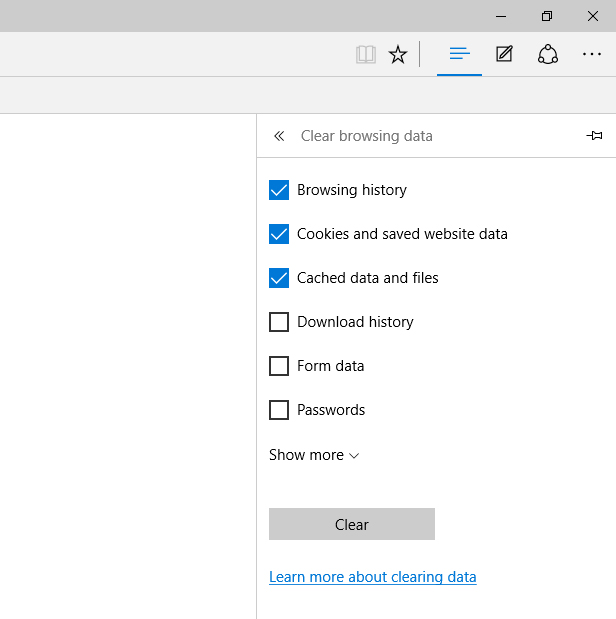
To delete your online past en masse, first click the ‘**Clear browsing data…**‘ button. Now choose an option from the **Obliterate the following items from** dropdown menu (choosing **the beginning of time** if you wish to wipe out everything) then click the **Clear browsing data** button.

**Step 4: Edge (PC – Windows 10)**

Edge is Microsoft’s brand new web browser which will eventually replace Internet Explorer.

To clear all of your browsing data, click the options menu (the three dots situated at the top right) and select **Settings**.

Under **Clear browsing data**, click the **Choose what to clear button**. Select all the types of history data you’d like to clear and click **Clear**.



### Comments

# Disaster Management and Recovery

Published Date : September 8, 2016  
Author : tayo



The quest for survival of businesses and organizations has resulted in the usage of modern technology by these organizations to become connected to the rest of the world. The interconnectedness of businesses is such that information sought on the go can be gotten quite easily.

Disasters are bound to happen one time or the other. The computers being used could get crashed and resources would therefore become inaccessible thereby making work more stressful. Also, it should be noted that the entire organization is prone to disaster, hence the need to prepare to tackle it as it occurs.

**Disaster Management**

It is therefore worthy of note, with the notion that a disaster could occur at any time, to implement a pre-disaster plan. This is because it is much better to spend N100 in order to save N100,000. Since you cannot prevent every catastrophic event and no matter how carefully constructed a network is, unforeseen events can still occur that will damage resources. It is therefore important to manage the disaster that comes up.

The aim of Disaster Management is to reduce or avoid the potential losses from hazards with the aim of achieving rapid and effective recovery.

***There are 4 phases of Disaster Management:***

a. Mitigation – This phase must be in place before the disaster occurs. This phase involves minimizing the effects of the disaster and this can be done through public education, analyzing the IT infrastructure and surroundings for vulnerabilities.

b. Preparedness – This phase involves planning how to respond, through emergency trainings, warning systems etc. At any disaster occurrence, do not panic.

c. Response – This involves the efforts put in place to minimize the hazards created by the disaster. In a networked environment, it is noticed that a system is under attack, and you cannot see anybody carrying out the attack, it simply means that an intruder has gotten connected to the network. The best response to this is to pull the network cable from that system under attack.

d. Recovery – this phase involves returning to the statusquo. Managing disaster caused by natural factors include avoiding disaster prone situations, good planning, excellent documentation and physical security. Among other ways of Disaster Management for man-made disaster include physical security and installation of Anti-virus.

**Disaster Recovery**The major aim of every recovery process is to bring a failed system back online as quickly as possible.

*In every recovery plan, the following are very necessary:*

1. Documented hardware and software inventory: This include the machines, systems and the software installed on the.

2. Back-up media: There must always be back-ups that can be referred to in the case a disaster occurs. These can be external hard disk drives, USB sticks, CDs etc.

3. Cloud: Nowadays, with the sophistication in technology, resources can be stored in the cloud to have access to them much later. Therefore in the case of a disaster, the uploaded resources in the Cloud can always be recovered.

The inevitability of a disaster is a reason why preparation must always be made to cushion the effect a disaster will have on a business or organization. The need to create recovery channels is of utmost importance. No matter what, disasters can be managed and lost data recovered if adequate preparation is made.

### Comments

# Browse in private with incognito mode chrome

Published Date : September 7, 2016  
Author : tayo

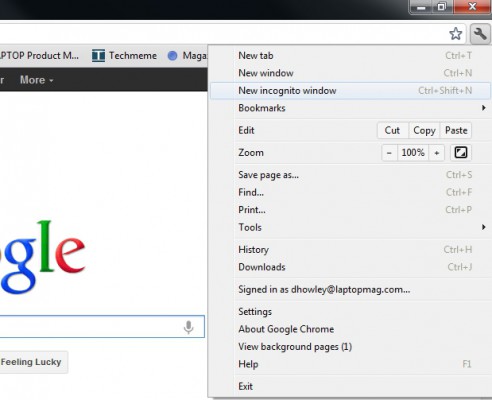
If you don’t want Google Chrome to save a record of what you visit and download, you can browse the web in incognito mode.

### How to go incognito:

You can open an incognito window on your computer and mobile devices to prevent Chrome from saving your browsing history. You can switch between an incognito window and any regular windows you have open. You’ll only be in incognito mode when you’re using the incognito window.

Computer

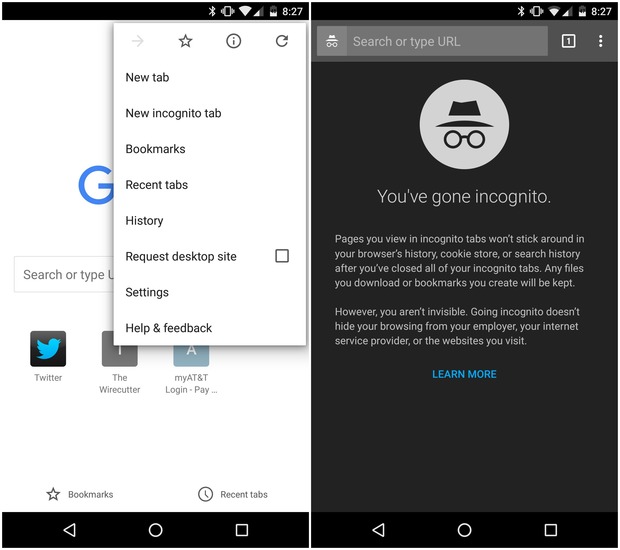
1. Open a Chrome window
2. In the top right, click the icon you see: Menu or More .
3. Select **New Incognito Window**.
4. A new window will open with a gray incognito icon .
5. To close incognito mode, go to the corner of each of your incognito windows and click the **X**.



Incognito mode isn’t available if the account is a part of Windows 10’s “Family Mode.”

Android device

1. Open the Chrome app.
2. Tap More .
3. Tap **New incognito tab**.
4. A new window will open with a gray incognito icon .
5. To close incognito mode:
   * If you have Android 5.0 (Lollipop) or later, swipe from the top and tap **Chrome: Close all incognito windows**.
   * If you have an earlier version of Android, go to the corner of each of your incognito windows and tap the **X**.



iPhone or iPad

1. Open the Chrome app.
2. Tap More .
3. Select **New Incognito Tab**.
4. A new window will open with a gray incognito icon .
5. To close incognito mode, tap the square button in the top right to open tab switcher. In the corner of each of your incognito windows, tap the **X**.



### How incognito mode works

#### What you view

Incognito is a mode that opens a new window where you can browse the Internet in private without Chrome saving the sites you visit. You can switch between an incognito window and any regular Chrome browsing windows you have open. You’ll only be in incognito mode when you’re using the incognito window.

Be careful. Incognito mode only prevents Chrome from saving your site visit activity. It won’t stop other sources from seeing your browsing activity, including:

* Your internet service provider
* Your employer (if you’re using a work computer)
* The websites you visit themselves

#### What you’ve downloaded

Chrome won’t save a record of the files you download in incognito mode. However, the downloaded files will be saved to your computer’s Downloads folder, where you and any other users of your computer can see and open them, even after you close your incognito tabs.

For more information about what’s stored in incognito mode, visit the [Chrome Privacy Policy](https://www.google.com/chrome/browser/privacy/).

### 

Source Google

### Comments

# How to prevent mobile malware

Published Date : July 27, 2016  
Author : tayo

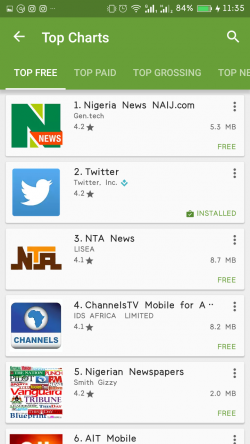


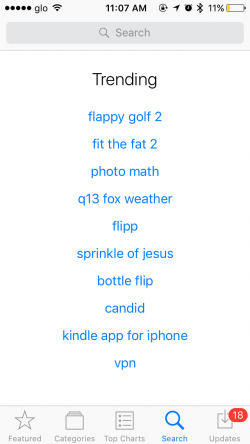
With every passing day, new mobile malware are being discovered and many more are being developed.

Google run checks on mobile apps that developers submit to the Google Play store, on which there are about 1.5 million pieces of software. Any applications that violate the company’s policies are removed.

***Third-party app stores carry the most risk***Most malicious software is found in third-party app stores – i.e., app stores that are not native to either Google or Apple – that are popular in a selected group of countries. This software is often loaded with pirated versions of software or applications with Trojan horses.

**To protect yourself from mobile malware. we recommend these simple steps:**

1. **Use an official app store**The official app stores — namely, Google’s Play store and Apple’s App Store—regularly check uploaded software for malicious activity. While the checks are automatic and can be fooled, they do act as an initial bar that attackers have to circumvent. The companies will remove programs later found to be malicious as well.

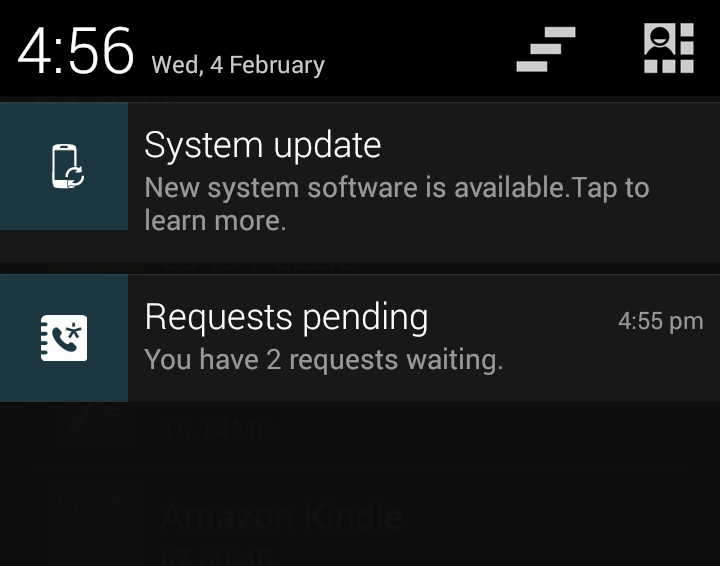


Loading in applications from other app stores or web sites is called **sideloading** and gives attackers opening to install their own code. Many of those app stores do not perform the same security checks as Apple and Google. “Potentially harmful applications are 7 to 10 times more likely to be installed outside of Google Play.”

2. **Don’t jailbreak your phone**Mobile devices come with a lot of built-in security. Using programs to hack the devices to remove the carriers’ and manufacturers’ restrictions—an activity known as “jailbreaking”—can lead to freer markets, but also undermines much of the security protecting the devices. For instance With a **jailbroken apple device**, you can install apps and tweaks that aren’t authorized by Apple, but you also remove the tough security protections that Apple has built into iOS.

  
Finally, users who jailbreak their devices need to rely on their own technical know-how to protect the devices and their data. This poses a risk if the user jailbreaks the phone but doesn’t have the required technical knowledge to keep the phone secure.

3. **Update often**Patches to discovered vulnerabilities are released as updates by app developers and OS developers. So constant update provides you cover and immunity from these vulnerabilities.



### Comments

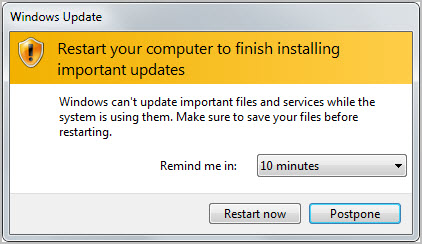
# How to protect your Windows computer from viruses

Published Date : July 27, 2016  
Author : tayo



Viruses are malicious software that try to get into your email, operating system, or your files. While the effect of unchecked viruses can be devastating, on the other hand, it’s actually quite easy to protect your Windows PC or laptop computer from viruses and other threats. Here’s what you need to do:

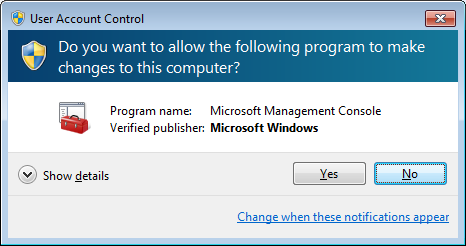
* **Install antivirus software.** Doing so and ensuring it’s up to date will go a long way to protecting your machine against viruses because new viruses appear almost every day. Antivirus software will scan your computer for viruses and update itself automatically.
* **Don’t click on email attachments that you’re not expecting.** Many viruses find their way into your PC through files attached to email messages and will spread as soon as you open the email attachment. So, unless you’re expecting an attachment, don’t  open it. If you’d like to read more, please see [When to trust an email message](http://windows.microsoft.com/en-us/windows7/when-to-trust-an-e-mail-message-ie9)
* **Keep your computer updated.** Microsoft releases security updates to pr  
  otect your computer. So you don’t forget, set your PC to update automatically – that way you’re always protected, no matter what.. To know how to do it, read [Turn automatic updating on or off](http://windows.microsoft.com/en-us/windows7/turn-automatic-updating-on-or-off).http://cdn.ghacks.net/wp-content/uploads/2012/01/restart-your-computer-to-finish-installing-important-updates.jpg



* **Use a firewall.**‌ You can use any firewall – it doesn’t have to be Windows Firewall. These will give you alerts about suspicious activity, such as  a virus or worm trying to connect to your computer. But firewalls do more than just warn you – they also block viruses, worms, and hackers from downloading dangerous programs to your computer.



* **Use your browser’s privacy settings.** You should familiarise yourself with the ways in which web sites use your private information, in order to combat identity theft and fraud. You can change privacy settings in browsers such as Internet Explorer, or just use the default ones. For more information, take a loot at [Change Internet Explorer 9 privacy settings](http://windows.microsoft.com/en-us/windows7/change-internet-explorer-9-privacy-settings).
* **Use a pop-up blocker with your browser.** Pop-up windows are small browser windows that appear on top of the website you’re looking at.  Advertisers make most of them, but sometimes they contain unsafe code. Using a pop-up blocker will help prevent some or all of these windows from appearing. The Pop-up Blocker feature in Internet Explorer is turned on by default. To learn more about changing its settings or turning it on and off, see [Change Internet Explorer 9 privacy settings](http://windows.microsoft.com/en-us/windows7/change-internet-explorer-9-privacy-settings).
* **Turn on User Account Control (UAC).** To make administrator-level changes to your computer’s settings, UAC will alert you so you can approve that change. It also helps prevent viruses from changing settings without your knowledge. To learn more about turning on UAC and adjusting the settings, see [Turn User Account Control on or off](http://windows.microsoft.com/en-us/windows7/turn-user-account-control-on-or-off).



### Comments

# Encrypting your files

Published Date : July 27, 2016  
Author : tayo

****

***What is encryption?***

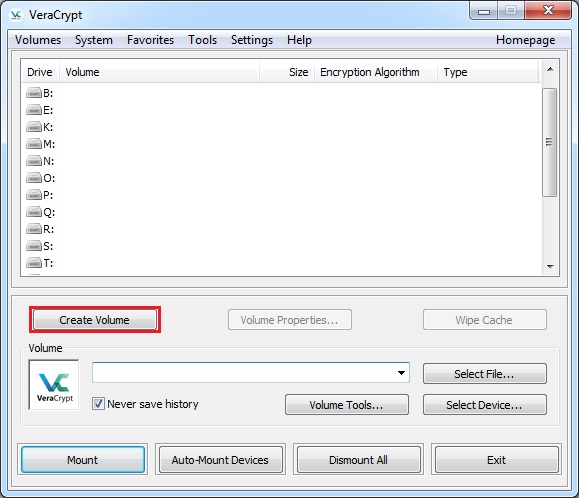
Encryption is the process of scrambling information so that no one can read or understand it. The only way to decipher the information – convert it into a readable format – would be with an encryption key. Many good open-source (free) and paid encryption tools are on the Internet.

For this lesson, we would show you how to use VeraCrypt software. It’s easy, free, and works on many platforms.

**Creating a VeraCrypt container**

Now, we’ll tell you how to create, mount, and use a VeraCrypt volume. There’s also a lot of information in the other parts of this manual.

**Step 1:** Download and install VeraCrypt. Then launch it by double-clicking the file VeraCrypt.exe or by clicking the VeraCrypt shortcut in your Windows Start menu. When the window appears, click Create Volume.



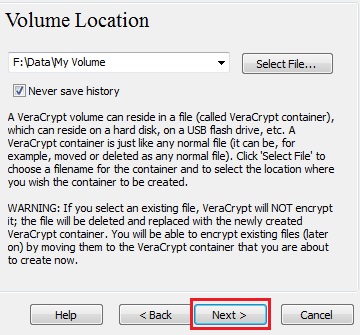
**Step 2:** After this, the VeraCrypt Volume Creation Wizard window will appear. Here, you have to choose where you want to create the VeraCrypt     volume. You can put it in a file – also called a container – in a disk partition, or a drive. Here, we will use the first choice.



**Step 3:**  Here, you must select either a standard or hidden VeraCrypt volume. These instructions will use the first choice.



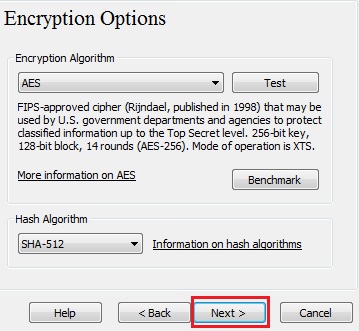
**Step 4:** Next, you must choose the location of the VeraCrypt volume (file container). A VeraCrypt container is just like any other file and can be moved or deleted. Please choose a filename in the following step.



**Step 5:** Click Select File choose where you want the file saved, and pick a name for the file. Do not select an already existing file as VeraCrypt will delete it and replace it with a new VeraCrypt container.

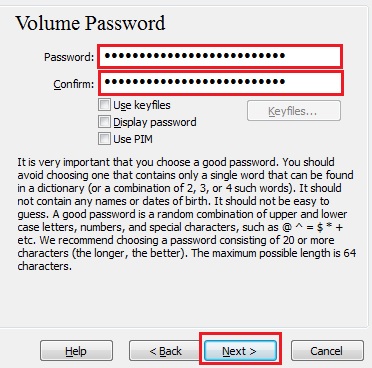
Click Save. The file selector window should disappear.

**Step 6:** Here you can choose an encryption algorithm and a hash algorithm for the volume. If you don’t know what these mean, use the default settings and click Next. (To learn more, read the chapters [Encryption Algorithms](http://algorithms) and [Hash Algorithms](http://algorithms))



Here we selected the size of our VeraCrypt container as 250 megabytes but you can choose another size. Click next.

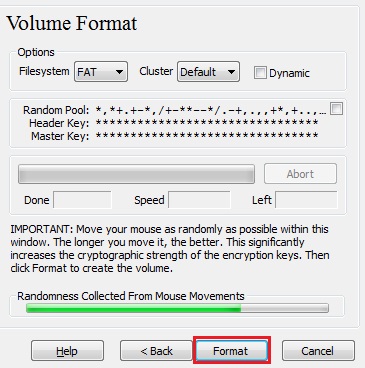
**Step 7:** This is one of the most important steps. Here you have to choose a good volume password. Carefully read the information in the Wizard window about how to choose a good password.



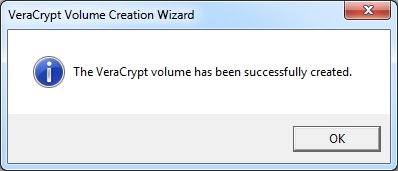
Type the password in the first input field. Then re-type it in the input field below the first one and click Next.

**Step 8:** Move your mouse as randomly as possible within the Volume Creation Wizard window at least until the randomness indicator becomes green. The longer you move the mouse, the better, so do it for at least 30 seconds. This increases the cryptographic strength of the encryption keys, which increases security.

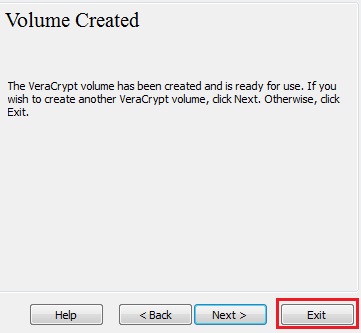
Click Format.



**Step 9:** Volume creation will begin. VeraCrypt will create a file called My Volume in the folder F:\Data\ from Step 6. This will be a VeraCrypt container containing the encrypted VeraCrypt volume. The duration of the volume creation depends on the size of the volume. When it finishes, the following dialog box will appear:

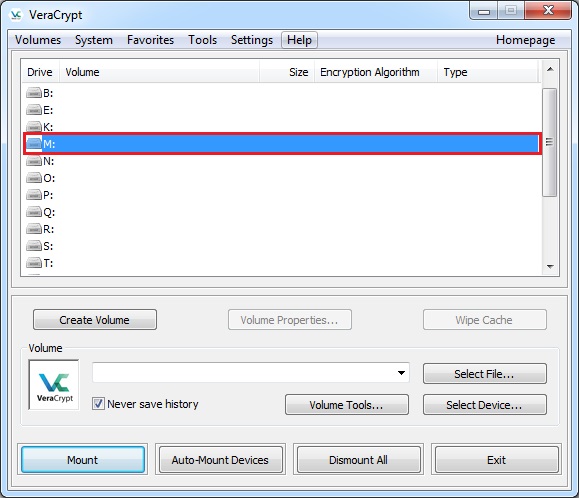


We have just successfully created a VeraCrypt volume (file container). In the VeraCrypt Volume Creation Wizard window, click Exit.



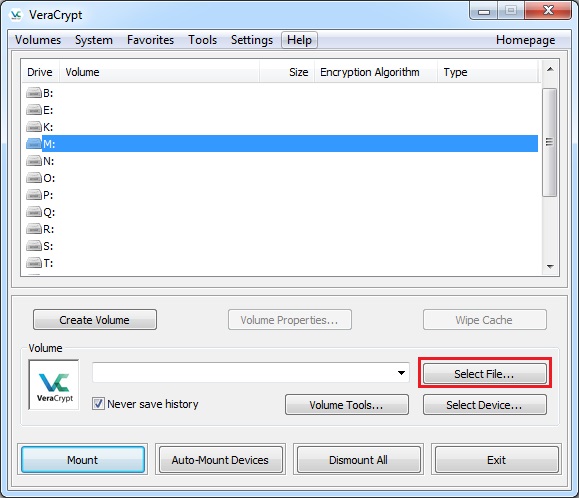
Next, we will **mount** the volume we just created. Return to the main VeraCrypt window, which should still be open. If it isn’t, repeat Step 1 to launch VeraCrypt and then continue from the next step

**Step 10:**   Select a drive from the list. The container will be mounted to this drive.

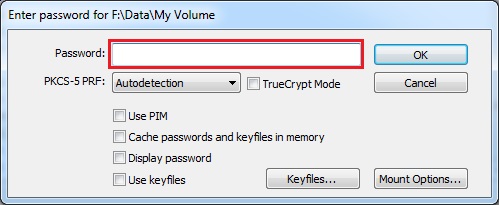


Note: Here, we chose the drive letter M, but you can choose another.

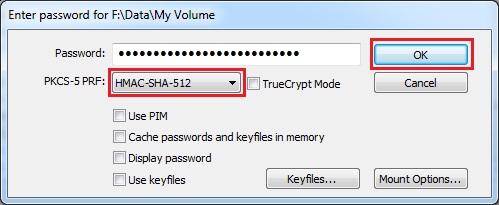
**Step 11:** Click Select File.



**Step 12:** In the main window, click Mount. A password prompt dialog window will appear



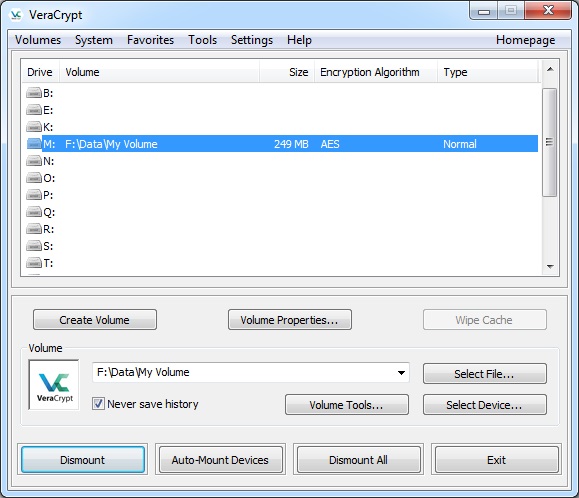
Type the password you selected in the password input field.



**Step 13:** Select the PRF algorithm that was used when the volume was created (SHA-512 is the default PRF). If you don’t remember,  leave it on “autodetection,” but the mounting process will take longer. After entering the password, click OK.

VeraCrypt will now attempt to mount the volume. If the password is incorrect, VeraCrypt will notify you and you will need to type it again and click OK. If the password is correct, the volume will be mounted.

FINAL STEP:



We have just successfully mounted the container as a virtual disk M:

### Comments