

# Understanding the Risks in Geo Tagging



The Geo tagging feature is, an awesome way of letting people know where you had that delightful lunch with your family, or the beautiful view from your room during a holiday trip. It just makes it easier for you to arrange photos and let friends know where they might be able to replicate some enjoyable experience you had.

With its interesting capabilities, there is also risk to consider when using the Geo tag feature.

The primary risk with geo tag is the risk of “**social surveillance.**” If you’ve any social media platform, be it Facebook? Twitter or Instagram. You must have come across social stalkers. These modern creepers make use of the information you publish on social media pages in order to track your movement, your habits, and your associations. Stalkers can make use of public geo tagging information to pinpoint your present location, find out where you live, and even how and where you spend your time with very little effort.

The follow points are best ways to keep you safe while geo tagging.

1. **Take the time to note your default privacy settings:** This

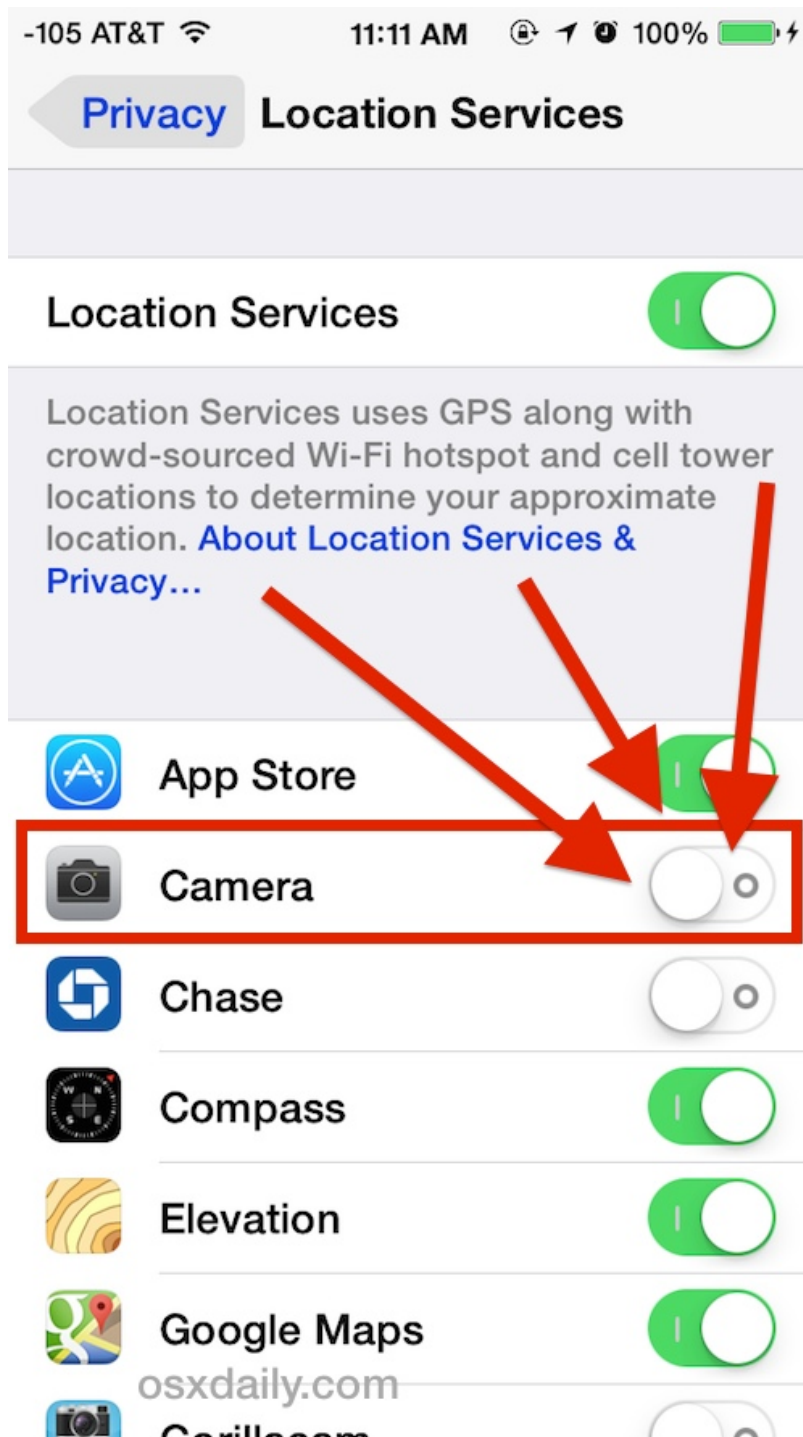
applies both to your smart phone or mobile device and the social media networks you access through your device. Sometimes tagging a location maybe a default setting on your phone or on the social network you're using. It is important to be aware of these settings so you can consciously decide when and where you geo tag, and who the information will be available to.

2. **Understand the Risk:** Realize that geo tagging information gives anyone who views it the opportunity to know your exact whereabouts, particularly in instances where you've posted your location to multiple sites (e.g. Twitter, Facebook, and Instagram). A check-in at the airport with the message "vacation for the next week!" for example lets anyone who might care to look know that you'll be out of town for a week.
3. **Know How to Disable the Geo Tagging Feature:** Every smartphone has a geo tag feature, and many of them will be automatically set up to function without you consciously choosing to have it do so. It's a much better idea to consciously decide to geo tag each time you post rather than having to remember to opt out of geo tagging each time you post

## **How To Disable Geo Tagging Feature**

### **For iPhones:**

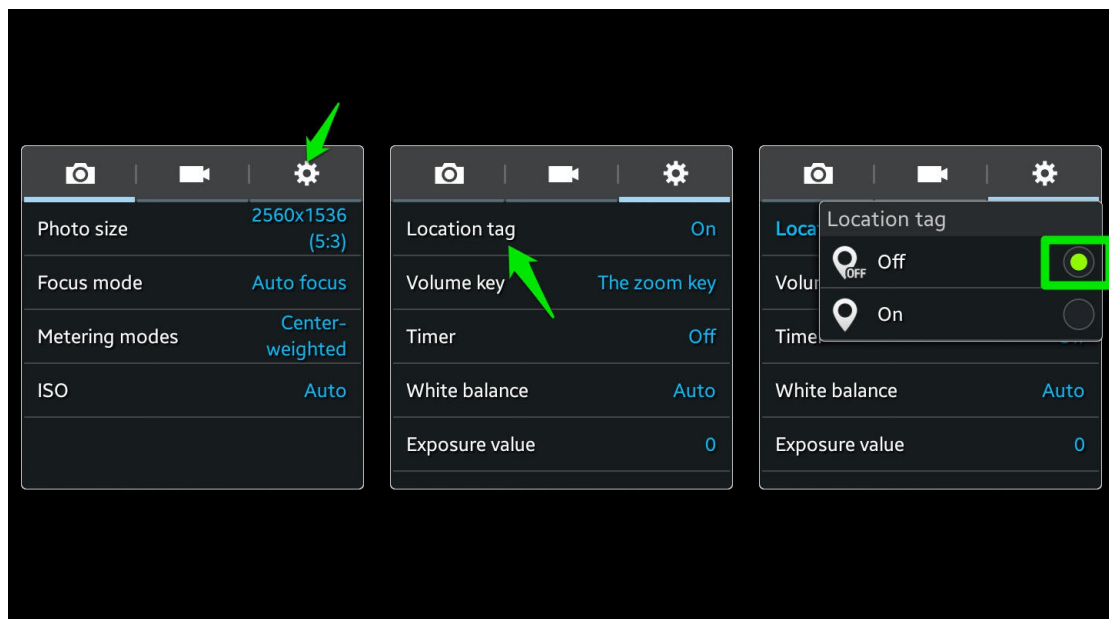
Go to the "settings" page of the geo-tagging program. Go to "settings" then "general" and then "location services." Disable those applications that automatically make use of your GPS tracking data.



### For Android Platforms:

Start the camera application. Open the menu and go to “settings.” Turn off “geo tagging” or “location storage” (depending on the type of Android).

For digital cameras, be sure to consult the user manual. Not all digital cameras come with a geo tagging feature, but it’s important you know how your particular camera operates in relation to location tracking.



---

## How to Protect your Mobile Device



With millions of people getting online through their mobile phones everyday, so has the security threats to target such mobile platforms and operating systems increased.

Due to these results, many users are worried about the security of their mobile devices and the data in it.

But not to worry, there are some measures you can take to protect your devices online.

### **1. Lock Your Device**

The first best way to protect your device and the information in it is to create a phone lock by either using a pin code, patterns or a fingerprint-sensitive lock. This way, if someone else gets hold of your phone, they'll only be able to reset the phone without getting hold of your sensitive data.

### **2. Watch What You Download**

Most of the [antivirus](#) options available for the mobile devices aren't generally as strong as the ones that have been developed for PC. So ensure that the apps you download on your phones are from recognized stores like the App store for Apple devices or the Google Play store for android. Any other site might just contain Viruses or Malware that may steal your information.

### **3. Get Regular Security Updates**

The technology that keeps your mobile information safe is evolving very quickly. In order to take advantage of this, you can set your phone to automatically update its security software. This way, you'll stay protected from new security threats.

### **4. Use Wireless Networks Judiciously**

Getting a free wireless network to connect to can be such a fun thing especially if your data plan is running low. However, you need to be careful about which Wi-Fi networks you sign into.

To prevent this from happening, try to stick with known sources for your Internet connection, If you must use one, don't give any private information like usernames, passwords, Bank details, etc.

**Note:** be sure to turn off your wireless networks unless you absolutely need them at that moment. It's better to be off Internet access for a while, than it is to connect to an unsecured and potentially dangerous WiFi signal.

## 5. Use Remote Wipes

If you have sensitive information that you would like to remain private, it's important to have a [remote wiping system](#) for your phone. In case the information on your phone is compromised or the phone is stolen, you'll be able to erase the data and history from another phone or computer.

Before you set up your remote wipe, it can be helpful to have a copy of your information stored in another place, such as in the cloud or on your desktop computer.

## 6. Security for Businesses

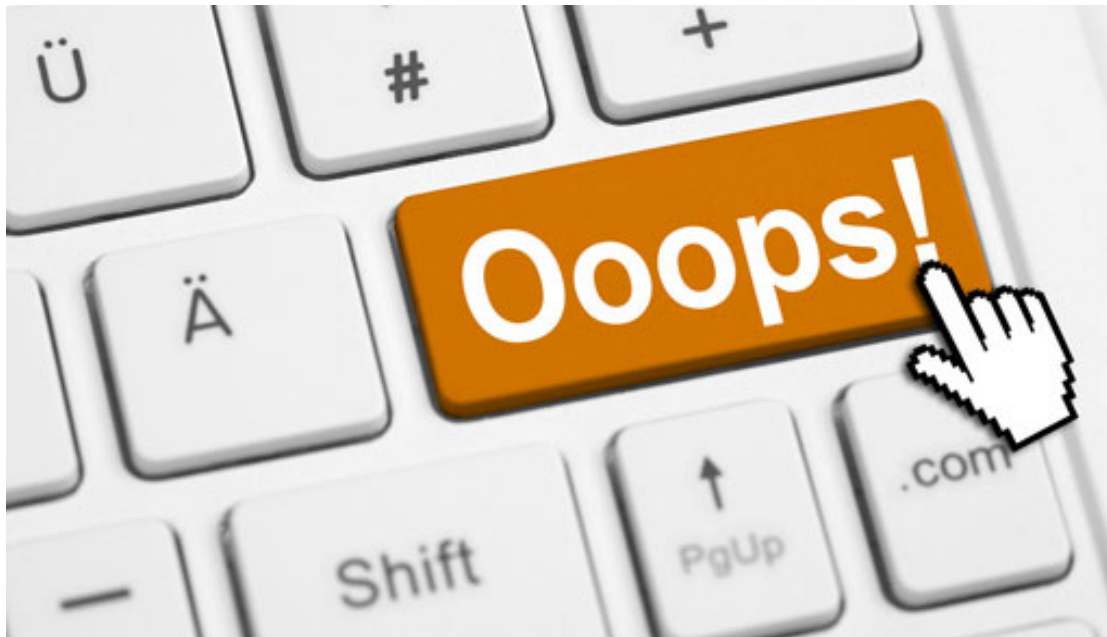
Since more and more workers will access sensitive company information from their phones, businesses may need to consider how they can protect their sensitive and/or valuable information on these mobile platforms. For businesses security, a remote wiping system is crucial when your employees are working on the go.

Your digital devices is important, if you let criminals into your digital system you might as well let them walk all over your company property.

You may also want to place some restrictions about how and what your employees can do on their business-use mobile devices. For instance, if you provide employees with company phones for working remotely, there is a smaller chance that they will download an unsavory app onto the phone and compromise your data.

---

# Common Digital Security Mistakes



*But what exactly are the most common mistakes that users make which expose them to cyber threats?*

1. People tend to leave their passwords hanging on the computer with sticky notes, so it's easier to remember but it's pretty easy for a hacker to get a hold of it. Use a ***password management program*** that makes it easy to create a unique password per site they register with.
2. Don't use weak passwords like 'password' because it takes less time to crack than passwords like this 'Alph4b3t@' and don't use the same ***password twice*** because if a hacker gets through one of your account, he would come for others.
3. **Not opting into extra security offered** – such as the two-factor authentication offered by Dropbox, Facebook, Google and more could give free access to your personal details and private information.
4. **People don't stop to think** about the worst-case scenario of what might happen if their private information is hacked or even company info leaked online to a competitor.
5. **Privacy exposure** is also a huge mistake every user makes. People often say "I have nothing to hide" and as a consequence they expose all their information, sometimes without knowing. It could be through the terms of agreement or terms of condition to an app.
6. The mistake companies make when it comes to securing sensitive data is that **they are clueless** as to where their data resides and how to categorize it or make requirement for



stronger security protocols.

7. Another mistake is the **lack of a correct evaluation** of the surface of attack. In the majority of cases, users totally ignore and overlook cyber threats, threat actors and their tactics, techniques, and procedures (TTPs)
  8. The biggest mistake is to **choose the cheapest option** without considering the supplier's reputation. Take VPNs as an example. If you pay a respectable company to provide you with VPN services, then you stand a greater chance of being secure than if you trust in a provider that you know little about and somehow has the ability to provide free, reliable and secure services.
  9. **Leaving the machine on**, unattended. Its amazing the number of users who leave their machines on, without protection, and walk away. Who needs a password?
  10. **Opening e-mail attachments** from mere acquaintances or even strangers. Users tend to open all their e-mail attachments before thinking about who the sender is.
  11. **Laptops have legs**. Everyone knows how common it is for laptops to be stolen in public places, but it's surprisingly common for a person to leave his laptop in his office, unsecured and unattended, and in full view of passersby. "These things walk," he warns. Users should place their laptop securely out of sight, such as in a locked desk drawer.
  12. **Failing to consider the staff**. "Your greatest [security] threat is from in-house," says Hill. Disgruntled employees and others can cause enormous problems if they're not properly monitored. IT departments should do a good job monitoring incidents and have the forensics capabilities to be able to follow problems to their sources.
- 

## Wipe a stolen android phone

### Wiping your data from your Android phone

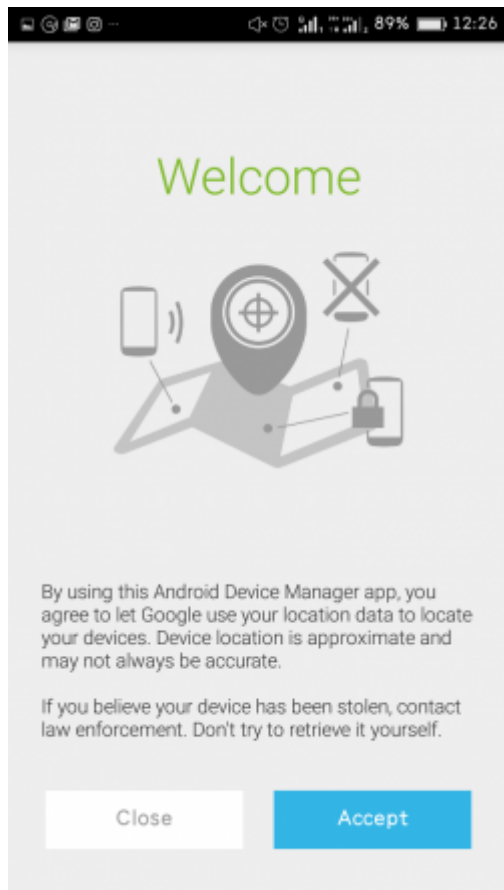
Sometimes things like the above happen and we have to resort to extreme measure like wiping all of the data from our phones. If it's lost and you're afraid that someone might access your data, you may have no other choice. If it comes to this, you have to act quickly before you lose the one chance you 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**

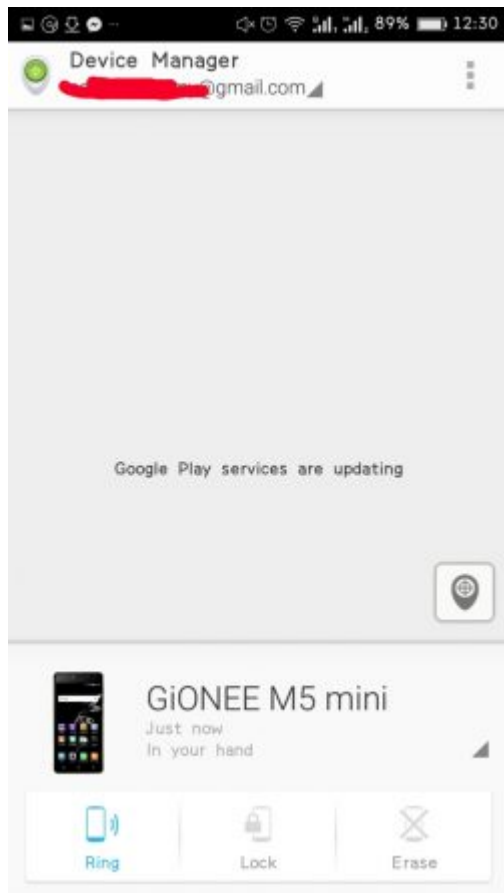


Android Device Manager is the tool that Google uses to track Android device users. Logging in to your device through your Google account will enable you locate or wipe the device. To verify that you're **connected** to your Google account, check if you have Google calendar entries, e-mail messages on 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.

---

## Firewall Protection

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet



A firewall monitors all of the traffic entering your computer network. A two-way firewall does double duty and monitors the traffic exiting your network as well. Information is sent over networks in packets. Those packets are what the firewall investigates to determine if there's something they contain that's potentially hazardous to your network's security. Even you as the sender could transmit something bad, without knowing it, which is why it's important to have a firewall police the contents.

## **Benefits of Firewall**

### **1)Blocks Trojans**

A firewall helps block Trojan horses. These types of intruders latch onto your computer files, and then when you send out a file, they go along for the ride to do more damage at the destination. Trojans are especially dangerous because they silently transmit what they uncover about you to a Web server. You're oblivious to their presence until strange things start happening to your computer. A firewall blocks them from the outset, before they have a chance to infect your computer.

### **2)Stops Hackers**

Having a firewall keeps hackers out of your network. Without firewall security, a hacker could get a hold of your computer and make it a part of what's called a botnet, which is a large group of computers used to conduct illicit activity, such as spreading viruses. While hackers represent an extreme group, individuals who you may not suspect, such as neighbors, can also take advantage of an open Internet connection you may have. A firewall prevents such peeping-tom intrusions.

### 3)Stops Keyloggers

Having firewall security will reduce the risk of keyloggers monitoring you. A keylogger is spyware software that cybercriminals try to put on your computer so they can target your keystrokes. After they can identify what you're typing in and where, they can use that information to do the same thing. This knowledge can help them log in to your private online accounts.

### How to enable Firewall on your windows computer

1. From the Start menu, click **Control Panel**, then click **System and Security**.
2. Under Windows Firewall, select either **Check firewall status** to determine whether the firewall is turned on or off, or **Allow a program through Windows Firewall** to allow a blocked program through the firewall.



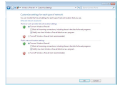
### 2. Select program features.

1. Click **Turn Windows Firewall on or off** from the left side menu.
2. Configure the settings for your home/work (private) or public network.
3. Click **OK** to save your changes.



### 3. Choose firewall settings for different network location types.

1. Turn on Windows Firewall for each network location you use – or **Public**.
  - Click **What are network locations?** for more information on network types.
  - **Note:** Domain network locations are controlled by your network administrator and can't be selected or changed.
2. Select **Turn on Windows Firewall** under the applicable network location type (in image below, both locations are selected).
3. Select **Notify me when Windows Firewall blocks a new program** for each network type, if the box is not already checked.
4. Click **OK** to save your changes.



---

## Prevent Hackers from impersonating you by sending emails that looks like yours



There are chances that you have received an email claiming to be from someone or an organization but you later found out that the email was a scam and not real. Cyber criminals have devised ways to send fake emails and make it seem real by exploiting a flaw in the way the email system works. The email work using an outdated protocol called the SMTP or Simple Mail Transfer Protocol.

Criminals can easily use free malicious software to send fake emails and make them appear real by the process we call email spoofing.

To prevent email spoofing and stop hackers from sending fake emails to your users thereby making it look real you can enable some of these three options from your web hosting control panel.

## Sender Policy Framework (SPF):

The ‘Sender Policy Framework’ (SPF) is an email validation system, designed to prevent unwanted emails sent using a spoofing system.

Basically, SPF helps to weed out abusive emails and also detect email forgery. It allows domain owners to publish trusted IP addresses that are authorized to send emails from the specified domains. For example, if my website “www.xyz.com” is hosted on the IP address 192.168.0.1 I can make sure only the ip address 192.168.0.1 is able to send emails out. Whenever a cyber criminal tries to send an email impersonating my website it would either end up in the spam box or gets rejected.

To configure SPF be sure to ask your web hosting company to help you set these up.

---

# Secure Coding Practices

We would be sharing with you 12 secure coding practices that cuts across different programming languages and have over time, been proven to mitigate security risks that are associated with coding. These practices, if properly implemented, would increase your protection against the numerous attacks that applications face daily.

## Top 12 Secure Coding Practices

**Validate input.** ALWAYS validate input. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software [vulnerabilities](#). Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files.

2. **Heed compiler warnings.** Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code . Use static and dynamic analysis tools to detect and eliminate additional security flaws.
3. **Architect and design for security policies.** Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.
4. **Keep it simple.** Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more



complex.

5. **Default deny.** Base access decisions on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is permitted .
6. **Manage Users, Sessions and Permissions.** Every process should execute with the the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges.
7. **Sanitize data sent to other systems.** Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. This is not necessarily an input validation problem because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.
8. **Practice defense in depth.** Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a [security flaw exploit](#) . For example, combining secure programming techniques with secure runtime environments should reduce the likelihood that vulnerabilities remaining in the code at deployment time can be exploited in the operational environment.
9. **Use effective quality assurance techniques.** Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External reviewers bring an independent perspective; for example, in identifying and correcting invalid assumptions .
10. **Adopt a secure coding standard.** Develop and/or apply a secure coding standard for your target development language and platform.
11. **Define security requirements.** Identify and document security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements. When security requirements are not defined, the security of the resulting system cannot be effectively evaluated.
12. **Model threats.** Use threat modeling to anticipate the threats to which the software will be subjected. Threat modeling involves

identifying key assets, decomposing the application, identifying and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat [mitigation](#) strategies that are implemented in designs, code, and test cases

This guide was written to serve as a secure coding kick-start tool and easy reference, to help development teams and individual developers quickly understand secure coding practices.

---

## Securing your internet browsing using VPN

---

## Protecting your website against attacks using web application firewall



## Introduction

In this tutorial, we will show you how to use CloudFlare's free tier service to protect your web servers against ongoing HTTP-based DDoS attacks by enabling "I'm Under Attack Mode". This security mode can mitigate DDoS attacks by verifying the legitimacy of a connection before passing it to your web server.

## Prerequisites

This tutorial assumes that you have the following:

- A web server
- A registered domain that points to your web server
- Access to the control panel of the domain registrar that issued the domain

You must also sign up for a CloudFlare account before continuing. Note that this tutorial will require the use of CloudFlare's nameservers.


## Configure Your Domain to Use CloudFlare

Before using any of CloudFlare's features, you must configure your domain to use CloudFlare's DNS.

If you haven't already done so, log in to CloudFlare.

### Add a Website and Scan DNS Records


After logging in, you will be taken to the Get Started with CloudFlare page. Here, you must add your website to CloudFlare and Begin Scan:

[Add site](#) [Support](#) [cf.mark.test@gmail.com](#)

[Add Website](#) [Add DNS Records](#) [Select Plan](#) [Update Nameservers](#)


### Get Started With CloudFlare

Follow these four simple steps to get your websites running on CloudFlare.




#### Add Website

Add your first website to CloudFlare. You will be able to add more websites after this initial signup process.




#### Add DNS Records

After adding a website, we will scan your DNS records. You will be able to make changes to your records before moving on.



#### Select Plan

Select the CloudFlare plan that meets your needs.



#### Update Nameservers

Sign into your registrar account to update your current nameserver with the CloudFlare nameservers you will be provided with.

#### Add a domain

For multiple domains separate by comma.

Scan DNS Records








[Send Feedback](#) [Return to Original](#)

The next page shows the results of the DNS record scan. Be sure that all of your existing DNS records are present, as these are the records that CloudFlare will use to resolve requests to your domain. In our example, we used cockroach.nyc as the domain:

Note that, for your A and CNAME records that point to your web server(s), the Status column should have an orange cloud with an arrow going through it. This indicates that the traffic will flow through CloudFlare's reverse proxy before hitting your server(s).

#### Your DNS Zone File

[Export your DNS zone file](#) · [Append a zone file](#)

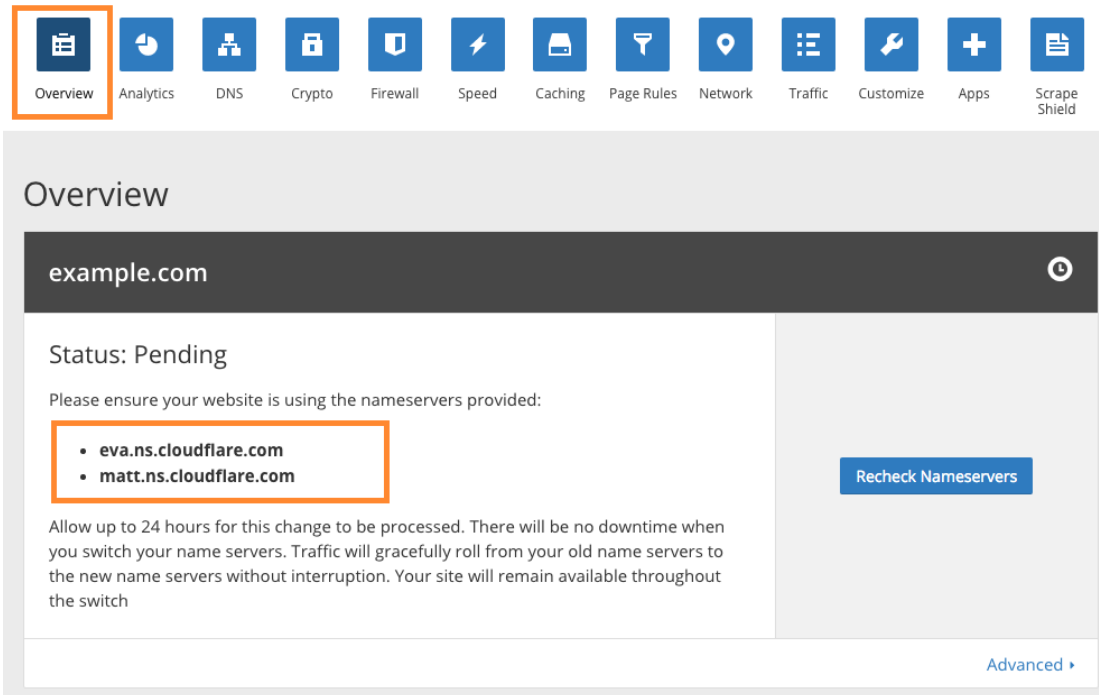
Type	Name	Value	TTL	Active
CNAME	www	is an alias of pankeki-8572.herokuapp.com	Automatic	 
CNAME	 thoughtbot.com	is an alias of pankeki-8572.herokuapp.com	Automatic	 
CNAME	staging	is an alias of gentle-everglades-8739.herokuappapp...	Automatic	 
A	<input type="text" value="e.g. www"/>	points to <input type="text" value="e.g. 127.0.0.1"/>	<input type="text" value="Automatic"/>	<a href="#">Help</a> <a href="#">Add</a>

Next, select your CloudFlare plan.

## Change Your Nameservers

For Godaddy users you can point your cloudflare nameservers from Godaddy by [following this process](#) .

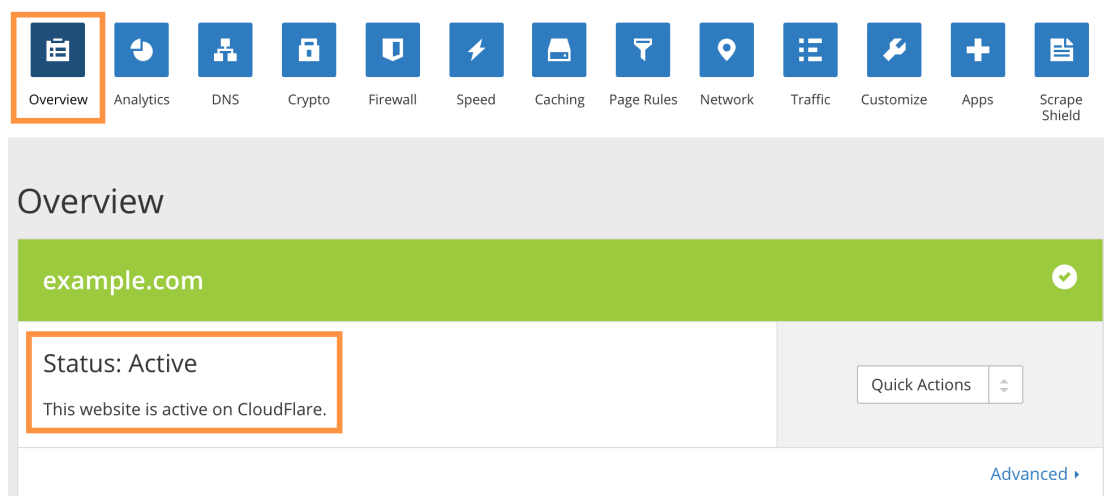
## Wait for Nameservers to Update



The Pending status means that CloudFlare is waiting for the nameservers to update to the ones that it prescribed (e.g. `eva.ns.cloudflare.com` and `matt.ns.cloudflare.com`). If you changed your domain's nameservers, all you have to do is wait and check back later for an Active status. If you click the **Recheck Nameservers** button or navigate to the CloudFlare dashboard, it will check if the nameservers have updated.

## CloudFlare Is Active

Once the nameservers update, your domain will be using CloudFlare's DNS and you will see it has an Active status, like this:



[Recommended First Steps for All CloudFlare Users](#). This is important to ensure that CloudFlare will allow legitimate connections from services

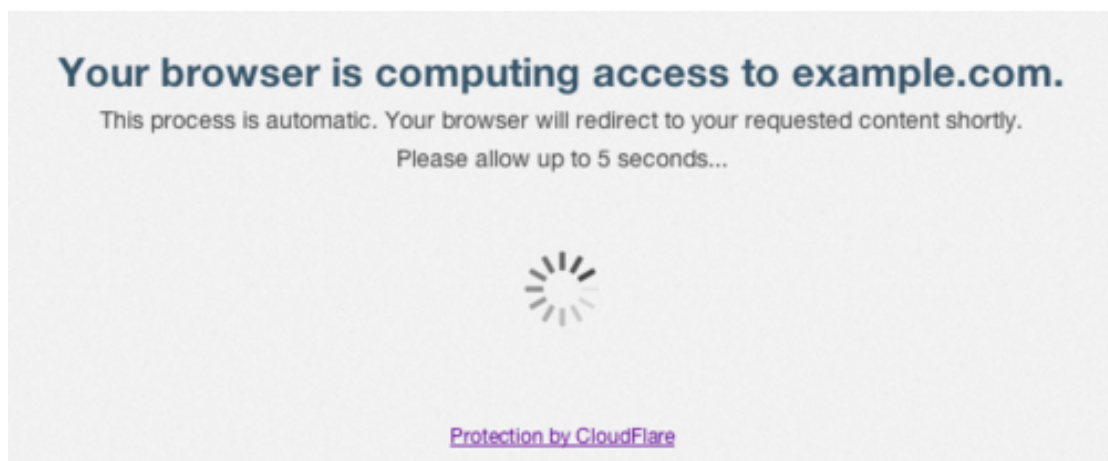
that you want to allow, and so that your web server logs will show the original visitor IP addresses (instead of CloudFlare's reverse proxy IP addresses).

Once you're all set up, let's take a look at the I'm Under Attack Mode setting in the CloudFlare firewall.

## I'm Under Attack Mode

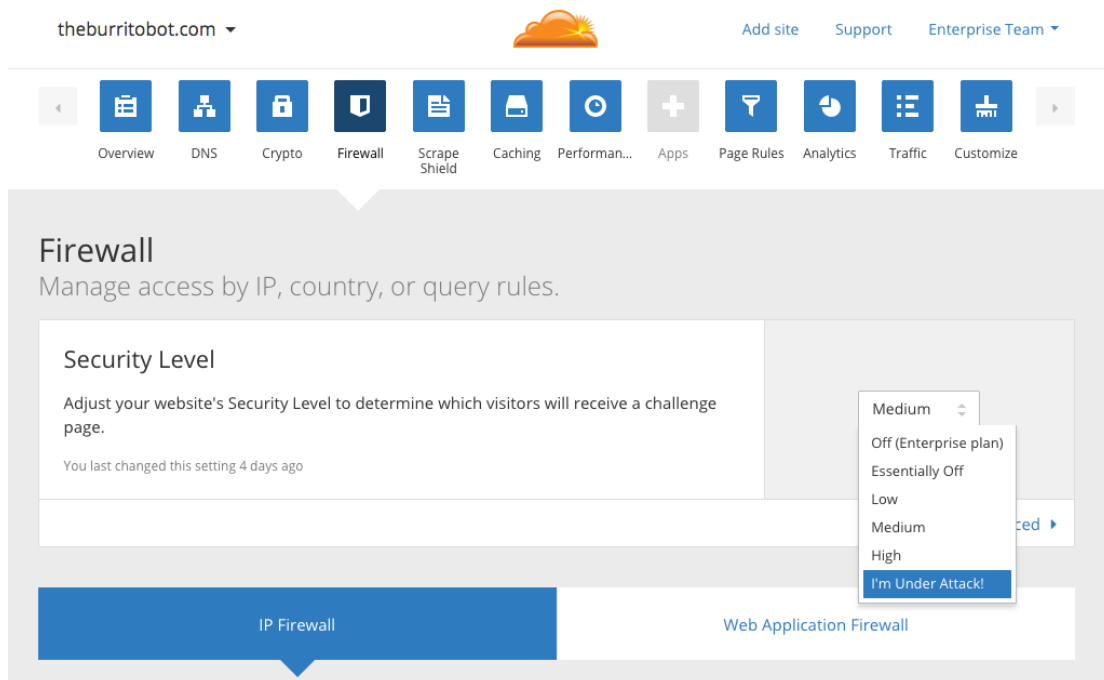
By default, CloudFlare's firewall security is set to Medium. This offers some protection against visitors who are rated as a moderate threat by presenting them with a challenge page before allowing them to continue to your site. However, if your site is the target of a DDoS attack, that may not be enough to keep your site operational. In this case, the I'm Under Attack Mode might be appropriate for you.

If you enable this mode, any visitor to your website will be presented with an interstitial page that performs some browser checks and delays the visitor for about 5 seconds before passing them to your server.



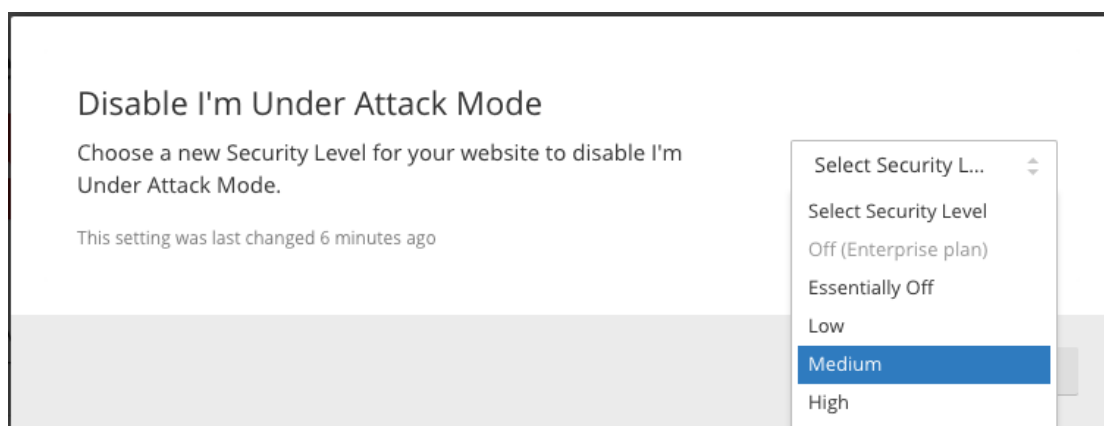
**Note:** Keep in mind that you only want to have I'm Under Attack Mode enabled when your site is the victim of a DDoS attack. Otherwise, it should be turned off so it does not delay normal users from accessing your website for no reason.

## How To Enable I'm Under Attack Mode



## How To Disable I'm Under Attack Mode

As the I'm Under Attack Mode should only be used during DDoS emergencies, you should disable it if you aren't under attack. To do so, go to the Cloudflare Overview page, and click the Disable button:



## Conclusion

Now that your website is using Cloudflare, you have another tool to easily protect it against HTTP-based DDoS attacks. There are also a variety of other tools that Cloudflare provides that you may be interested in setting up, like free SSL certificates. As such, it is recommended that you explore the options and see what is useful to you.

Good luck!



---

# How to protect your system with an antivirus

---

## Check apps that have access to your social media accounts

---

## Securely delete files

---

## Protect your Google account with Two-Step Verification

Two-step verification (2SV) is a login feature available on many online accounts today. It provides an additional step (but not an added factor) in the authentication process by prompting a user to enter a code sent to their computer or pre-verified device.

2SV therefore has the ability to protect a user's account in the event that their corresponding password has been compromised.

One of the most important things a user can protect with 2SV is their Google account, which can be used for personal and business email, social networking on Google+, and other purposes. Provided below is a guide on how you can enable this feature on your Google account.

1. Sign into your Google account.
2. At the top right of your browser screen, you will find a circular icon that either contains the first letter of your username or a picture of yourself. Click on that icon.
3. A profile card containing your username, your full Google email, and a number of buttons will load beneath the icon. Click on the blue button labeled "My Account."
4. A new tab will load that brings you to the home page for "My Account." Scroll down on that page and click on the "Sign-in & security" setting.

5. The Google Sign-in & security page will load up. You can use this page to manage the security settings of your account, including setting up a recovery email and phone, changing your password, and conducting a security checkup of your account. You can also set up 2SV here.

Scroll down the page. Under the “Signing in to Google” sub-heading, you will find a box entitled “Password & sign-in method.” In that box, click on “2-Step Verification.” (NOTE: This feature should be labeled “Off” if you have not already enabled 2SV on your account.)

6. On the right-hand side of the “Signing in with 2-step verification” page that loads up, you will see a box that includes a blue button labeled “Start setup >>”. Click on that button.
7. At this point, Google will likely prompt you to resubmit your login credentials. Enter your password and click the button “Sign in.”
8. Enter your phone number into the available text field and click on one of the radio buttons to indicate whether you want to receive the verification codes via SMS text message or via call. Once Google has verified that you have entered your mobile phone number correctly (i.e. in the format (222) 555-5555), a blue button labeled “Send code” will become clickable at the bottom of your screen. Click that button.
9. A page will load saying that Google has sent you a code. You should receive a code from Google in the next few seconds either via SMS text message or call. Once you have received the six-digit code, enter it into the available text field and press the blue button “Verify.”
10. Next, you will be asked whether Google should trust your computer. This is a setting that allows you to elevate the privilege status of your computer, tablet, or mobile phone so that you don’t have to enter in verification codes when logging into your Google account on that device. A clickable box will appear that will enable you to check off whether you want to trust the device. Check the box ONLY if the device belongs to you and it is not a public device or computer. When you are done, click the blue button labeled “Next.”
11. Click the blue button labeled “Confirm” to finish turning on two-step verification on your Google account.
12. And you’re done! You will be redirected to a page where you can manage the settings of your two-step verification protection feature. On this page, you can edit your pre-verified phone number, create app-specific passwords, manage your registered (i.e. trusted) computers, or even designate a security key if you are using Google’s Chrome browser. (NOTE: Now that you have set up 2SV on your account, a boxed feature to the right of

your screen will list the feature as “On.”)

You can also set up a back-up phone and print out or save backup codes that allow you to access your account in the event that you lose your device.

It is **STRONGLY** recommended that you set up at least one of these two backup settings.

13. Now whenever you sign into your Google account, you will see this screen after you enter in your password.

Simply enter in the code once you receive it via SMS text message or call. If the code is correct, you will automatically be directed to your account.

Source: grahamcluley

---

## How to prevent Unwanted access to your facebook account



### 1. Create a strong password

Chances are, you already have your Facebook password. But you should make sure it is unique, meaning that you don't use it anywhere else.

To change your password, go to Account Settings > General > Password.

### 2. Confirm your mobile number

Doing this ensures that, even if you lose or forget your password, Facebook will be able to send you a new one via text message.

To add your mobile number, go to Account Settings > Mobile and click on Add a Phone.

### **3. Activate secure browsing, now**

Another way of making sure your Facebook browsing activity is safe is to turn on Secure browsing. This automatically prevents any external applications that are integrated with Facebook from doing any harm or taking your personal information without your knowledge or approval.

To secure your account, click the drop down menu from the top right corner of your Facebook account and go to Account Settings.

Select 'Security' from the left menu.

At the Secure Browsing section, click on the Edit link at the right.

When the option panel appears, check the box 'Browse Facebook on a secure connection,' then click the Save Changes button.

### **4. Activate 'Login Approvals'**

Login approvals is an extended security feature offered by Facebook. It requires you to enter a security code each time you try to access your Facebook account from an unrecognised device. To activate Login Approvals, go to Account Settings > Security, look for Login Approvals and click on the Edit button.

When the option to activate Login Approvals will appear, tick the check box to activate.

When a popup window will appear with descriptions of login approvals, click on the 'Set Up Now' button to continue.

If your mobile number is already registered, Facebook will automatically send you a code via SMS. Enter this code in the given box and click Submit Code.

Now you have completed the Login Approvals request, so you can click Next to continue.

Next, Facebook will offer you to setup a Code Generator from your mobile phone. This would help in case you are unable to receive SMS. Click Continue.

[Code generator for Android phones](#) .

### **5. Disconnect previous active sessions**

The good thing about Facebook is that it lets you know about your previous active sessions, where you log in from, and what devices you used to access your Facebook account. Now, to make sure your account is safe, from the Account Settings > Security page, look for 'Active

Sessions' and click on Edit.

Click on the link 'End Activity' to kill the sessions on all other devices.

## **6. Activate Private Browsing**

Another way to prevent another person from accessing your account is by activating 'Private Browsing' from your browsers. All browsers have this feature, which prevents them from logging your browsing history.

Safari

If you are using the Safari Browser on Mac, activate Private Browsing from the menu with Safari > Private Browsing.

Firefox

For Firefox, go to Tools > Start Private Browsing.

Chrome

If you are using Chrome, you can browse privately in the Incognito window. To open this window, go to File > New Incognito Window.

## **7. Don't 'Keep Me Logged In'**

The moment you want to login to your Facebook account, at the Log In page, there's a small checkbox that says Keep me logged in. Make sure this box is unchecked. Then, log in as usual. With this on, you will be asked for your email and password every time you launch Facebook.

## **8. Avoid clicking on links from spam email**

Facebook is serious about protecting its users from spam and often enhances its features to make sure you do not become a victim. The types of attacks include requests for via Facebook messages, chat, phishing links that will redirect you to fake websites, or malicious links that could retrieve your personal information or even harm your computer. There are also chances you may receive emails that at first glance look like they're from Facebook, are actually from a phishing website.

**There are many ways you can avoid being a victim:**

Never click on suspicious links.

Never give out your username or password to anyone, especially not to websites with suspicious-looking links and layouts.

Log in only from [www.facebook.com](http://www.facebook.com) and not from any other link or website.

Update your browser to its latest version to ensure your browser's security is up to date. This will enable it detect attacks and alert you when you are navigating to a suspected phishing site.

## **9. Sign out after use**

Lastly which is the most important of all, and definitely worth repeating,

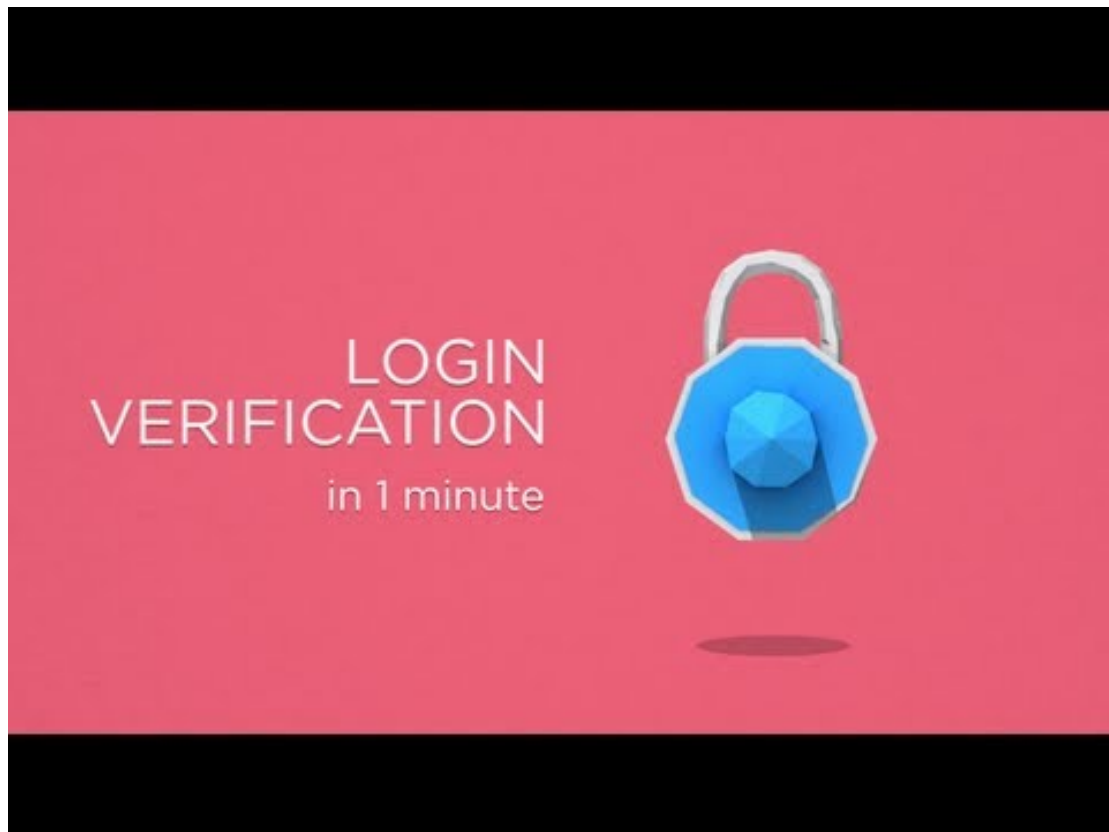
is, never forget to log out from your Facebook account.

---

## Deleting your browser history

---

## Protecting Twitter with Login Verification



**2-Step Verification** is an extra layer of security for your Twitter account. Instead of only entering a password to log in, you'll also enter a code which is sent via text message to your mobile phone. This verification helps make sure that you, and only you, can access your account.

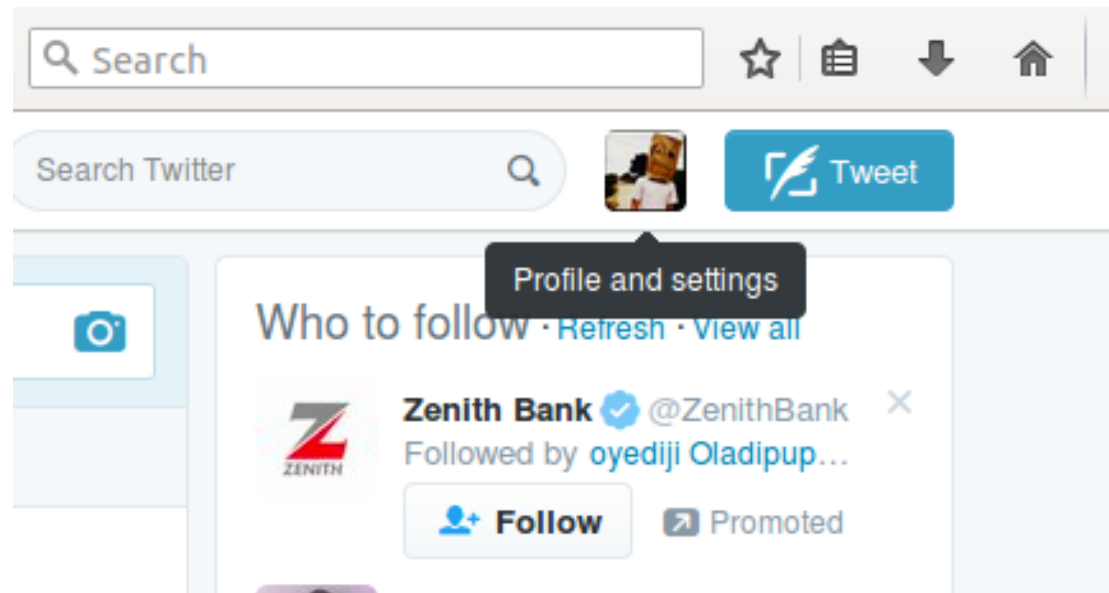
The Twitter implementation of 2SV is called "Login Verification".

To get started, follow these steps:

### **SMS login verification**

1. Log in to your Twitter account via a web browser.

2. At the top-right corner of your Twitter homepage, you will find a box-like icon that displays either your profile image or an egg against a colored background (in the event you have not uploaded an image). If you hover over that icon, the text “Profile and Settings” will drop down just below it. Click on that icon.

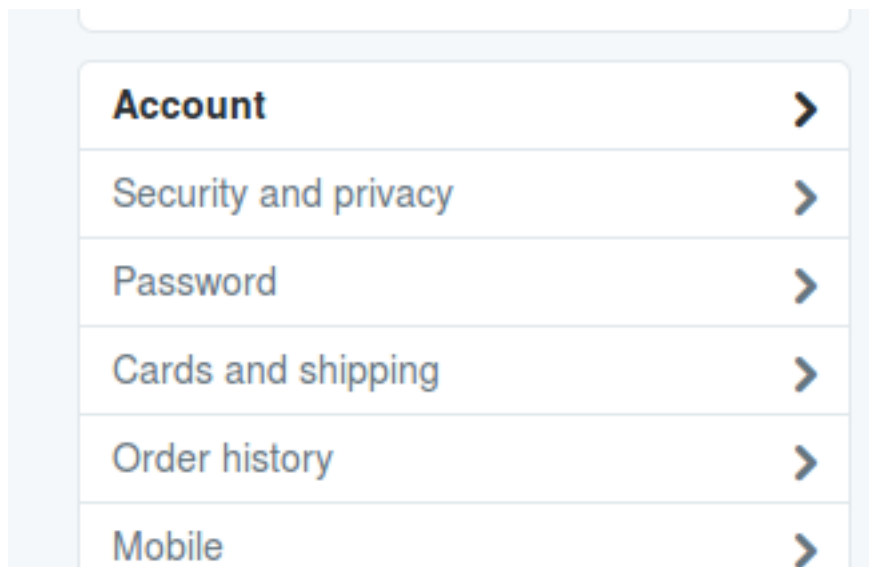


3. A dropdown menu containing your name, your lists, and a number of other features will appear. Just above “Log out,” which should be the last feature in the menu, you will find “Settings.” Click on that option.

4. You will find yourself on your account overview page, which displays your Twitter handle, your registered email, and some other basic pieces of information about your account.

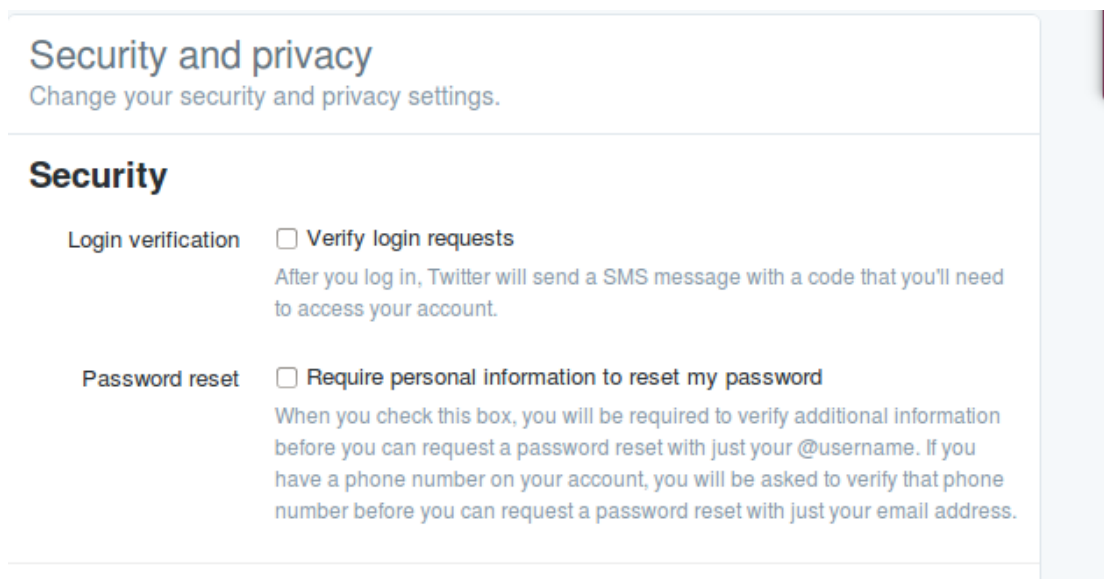
On the left-hand side of the page, you will see a menu with “Account” selected in bold font. Click on “Security and privacy” located just beneath the “Account” option on that list.





5. The first item under the “Security” section of the page is named “Login verification.”

Next to that title, you will see an unchecked box with the text “Verify login requests” displayed next to it. Click on that box.



6. A dialog window will appear. It will state that you must receive a test message on your phone before you can activate login verification via SMS. Click on the blue button “Okay, send me a message.”

**NOTE:** This message will display only if you have previously verified both your account and a valid mobile phone number with Twitter. If you have not already done so, go back to “Account” on the left-hand sidebar list and complete those steps.

7. If your mobile settings are correct, you should have received a text message to your phone that reads, “Twitter can send verification codes to

this device!” Click the “Yes” button in your web browser to confirm that you received that code.

8. A new dialog box asks you to reenter your password in order to save your new account preferences. Enter in your password and click the button “Save changes.”

9. Your account is now protected with SMS login verification! A message at the top of your “Security and Privacy” page will confirm that your settings have been saved. You will also see that the “Verify login requests” box is now checked.

### **Twitter app login verification**

1. If you have not already done so, download the Twitter app on your mobile device. Once the download is complete, set up your account in the app.

2. On your Android device, tap the overflow icon, which should look like three dots displayed vertically, at the top of Twitter app’s homepage. (On an iOS device, click on the gear icon.)

3. In the dropdown menu that appears, click on the “Settings” option.

4. A list of settings will appear below your Twitter handle. Click on “Account.”

5. Your Account page will display your registered phone number and email. It will also give you the option to change your password and review your security settings. Click on “Security.”

6. On your Android device, click on the unfilled box that sits adjacent to the “Login verification” option. (For iOS devices, you will need to flip a Login verification switch to “On.”)

7. A dialog box will open up alerting you to the fact that you will need your device in order to log into your Twitter account from now on. Click “OK.”

8. At that point, you’ll be redirected to a screen where the Twitter app will ask you to take a screenshot of a backup code for your Twitter account. It is very important that you remember this code in case you lose your device. Take a screenshot of the code or write it down and store it somewhere safe.

9. And you’re done! The next time you log into your Twitter account from a web browser, your computer will display a screen indicating that it has sent you a verification request to your Twitter app.

Click on the checkmark to verify your login access, and you will automatically be redirected to your home feed.

If you do not receive the verification request, you can also have Twitter send your mobile device an SMS code. If that doesn't work, you can use your backup code to log in.

There you have it! Your Twitter account is now protected with 2SV, and you can receive verification codes either via SMS text messaging or via Twitter's mobile app.

### **To disable login verification:**

1. Go to your [Security and privacy settings](#) and deselect the **Verify login requests** option.
2. Save changes (**Note:** you'll have to enter your password).

Source: grahamcluley

---

## **using twitter safely**

As with any social network, Twitter is vulnerable to over sharing, data leakage and unintended consequences.

Like Facebook and Google, Twitter is also driven by ad revenue so it's very interested in what its users are up to when they're using Twitter and when they aren't (you did realise that [Twitter tracks the websites you visit](#) didn't you?).

First things first. You'll find the privacy settings at twitter.com under the gear icon, then Settings.

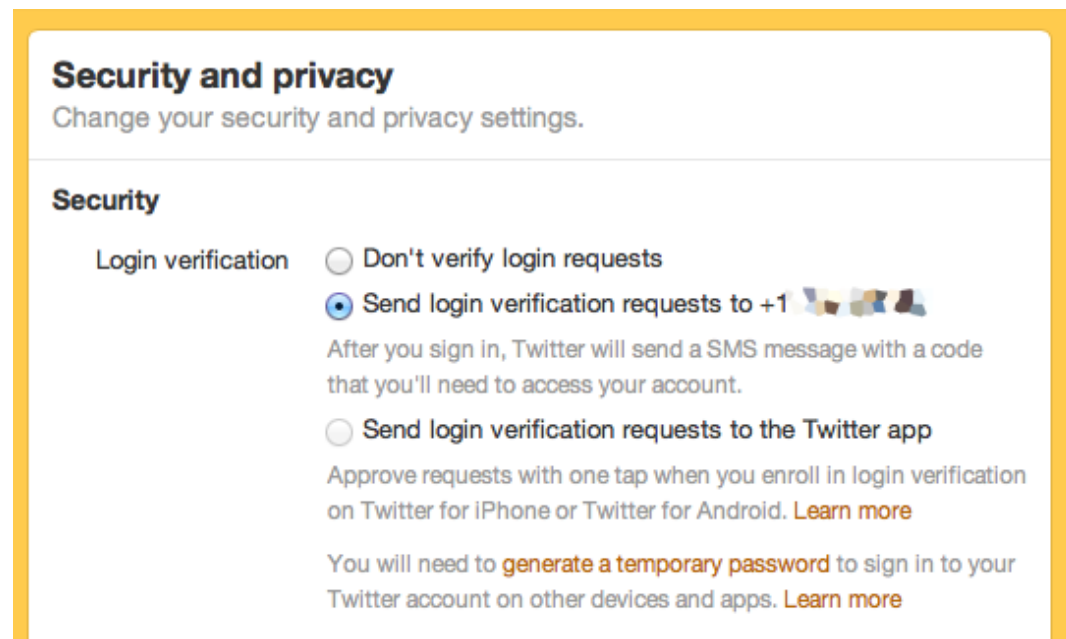
Then click Security and privacy over on the menu to the left of your screen.

### **Twitter's security settings**

The first section is about Security and how you access your Twitter account.

#### **LOGIN VERIFICATION.**

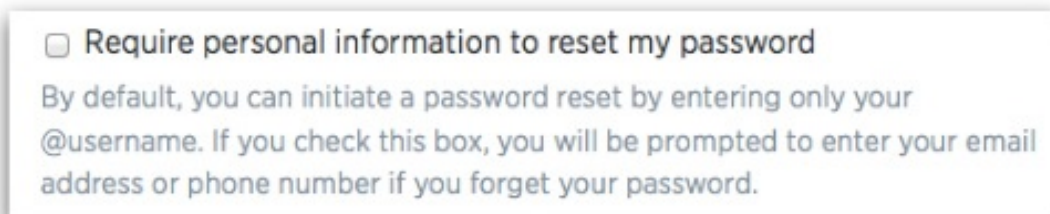
This is set by default to off. Make it harder for an unauthorised person to login to your account, by choosing to receive login verification requests via a text message on your phone or the Twitter mobile app.



## PASSWORD RESET.

Set by default to off, you only need to enter your Twitter username.

Check the Require personal information to reset my password so that two factors are required and, most importantly, so you can avoid reset emails and get a code sent by SMS to your phone instead.



## Twitter's privacy settings

The second section is about how private you choose to make your Twitter account.

## PHOTO TAGGING.

Like Facebook, others can tag you in a photo, which is just like a 'mention' on Twitter – you get 'mentioned' in the uploaded photo.

This is set by default to on, meaning anyone can tag you in a photo. Use the radio buttons to restrict tagging to people you follow back, or disable photo tagging altogether.

## Privacy

Photo tagging

☒ Allow anyone to tag me in photos  
☐ Only allow people I follow to tag me in photos  
☐ Do not allow anyone to tag me in photos

Tweet privacy

☐ Protect my Tweets  
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more](#).

Tweet location

☐ Add a location to my Tweets  
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)

Delete all location information

This will delete all location information from past Tweets. This may take up to

Photo tagging

☐ Allow anyone to tag me in photos  
☐ Only allow people I follow to tag me in photos  
☒ Do not allow anyone to tag me in photos

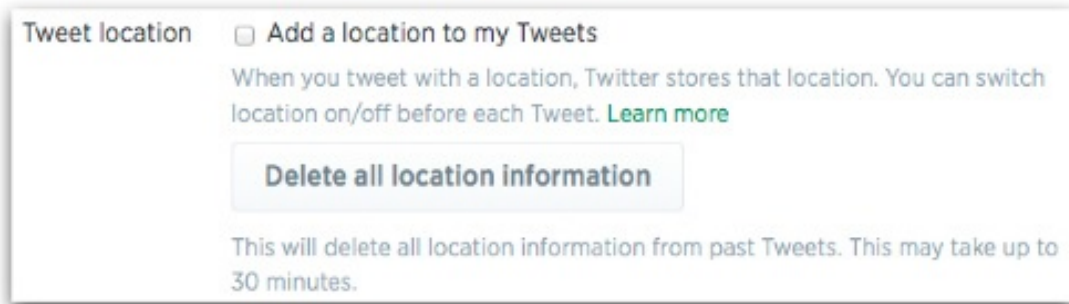
## TWEET PRIVACY.

By default, Protect my Tweets is off, and anyone on Twitter, all your followers, and anyone searching Google can see your tweets. If you check the box to protect your Tweets, it locks down your visibility. A lot.

## TWEET LOCATION.

This is set as 'off' by default and you have to opt-in to use it. You can also specify before you tweet whether you want the location information on or off.

Keep locations off, there are too many [unintended consequences](#), and delete all past location information to be on the safe side.



Tweet location ☐ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)

[Delete all location information](#)

This will delete all location information from past Tweets. This may take up to 30 minutes.

## DISCOVERABILITY.

Let others find me by my email address is on by default and enables people who may not know your Twitter handle, but do know your email address, to find you.

Apply the ‘principle of least privilege’ here. If you can think of a really good reason why you want to be discoverable by your email address (we can’t) then switch it on, otherwise turn it off.



Discoverability ☐ Let others find me by my email address

## PERSONALIZATION.

Personalization is about tailoring suggestions of which accounts to follow, based on information that Twitter gathers about you around the internet.

You can turn it off by unchecking the box next to Tailor Twitter based on my recent website visits.

## PROMOTED CONTENT.

Twitter has ads. These are in the form of paid-for sponsored tweets, Twitter Cards, and promoted accounts. If you want Twitter to “bring you more useful and interesting advertising content”, you won’t uncheck this box. Twitter has partnered with third party ‘behavioural advertising’ companies (behavioural ads are the ones that follow you around from website to website). If you visit a website that’s in of those advertisers’ networks then their ads can now follow you on to Twitter too.

The setting Tailor ads based on information shared by ad partners is on by default. Switch it off by unchecking the box.

You can also disable personalization and promoted content by switching on Do Not Track in your browser. As we mentioned, Twitter has been



honouring Do Not Track for a long time, and it [says in a support article](#), “When you have DNT enabled in your browser, Twitter would not receive browser-related information from our ads partners for tailoring ads.”

Promoted content ☐ Tailor ads based on information shared by ad partners.

This lets Twitter display ads about things you've already shown interest in. [Learn more](#) about how this works and your additional privacy controls.

Source: NakedSecurity

# How to Manage Your Social Media Privacy Settings



We post a lot of information about ourselves across many social media websites, like Facebook, Twitter, or Instagram, among others.

In doing so, a lot of people who use social media share far too many personal details. But they have to be careful because cybercriminals use this sensitive information to create fraudulent identities, and compromise



careers. But, overall, remember, the fewer details you share online, the safer your information will be.

Below are steps to help protect your sensitive information on Facebook and Twitter, two of the most popular social media sites.

## Facebook

Facebook has different privacy settings for many aspects of a user's social profile, which must be adjusted individually.

*The categories of audience are:*

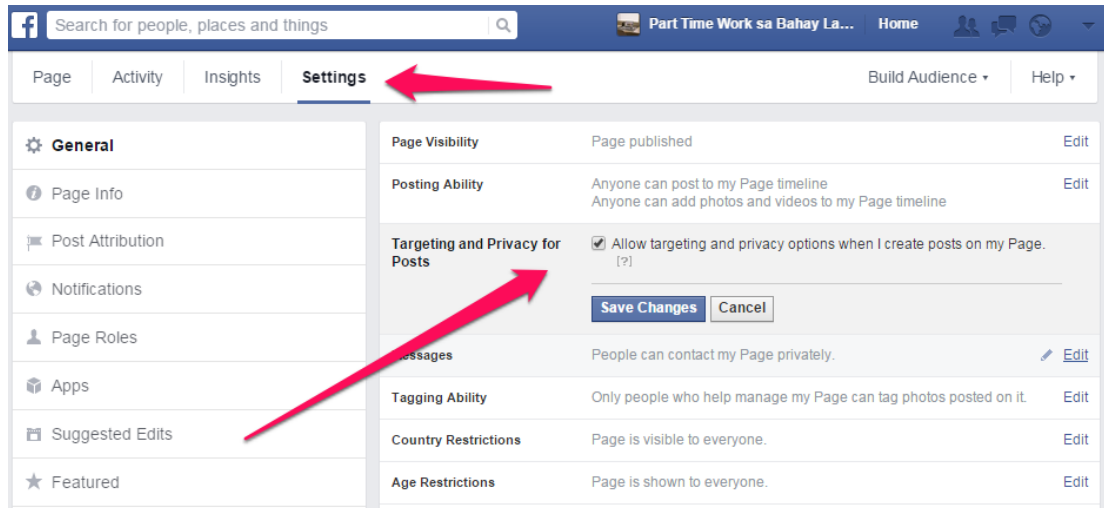
- **Public**
- **Only me**



If you want to keep your information private, don't use any of the "Public" settings.

Also, before posting a status, see who your potential audience will be. You can adjust this setting in two places.

- The first is under "Privacy Settings and Tools." Click the downward-pointing arrow in the top right corner. Choose "Settings," then find "Privacy" on the left. Choose a privacy level for your posts.
- Click in the "Update Status" field ("What's on your mind?"). Then use the drop-down menu to the left of the "post" button. Choose a privacy level for your posts.
- Remember, these settings apply to all posts unless you change them again.



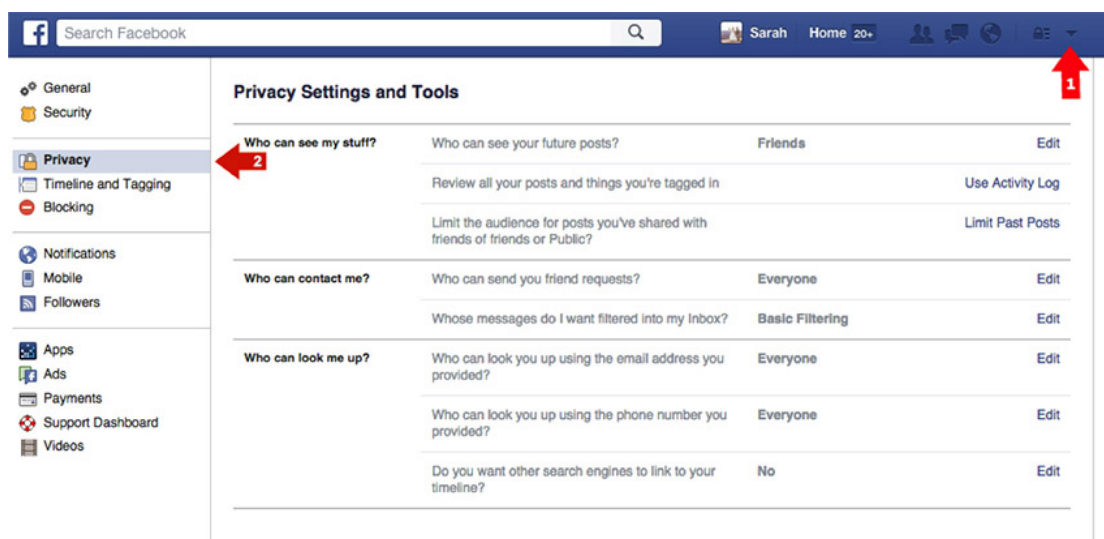
For the most privacy, select “Friends” so only your friends see your posts.

## Manage your privacy settings

With the “Privacy Settings and Tools,” you can control more settings for maximum security:

- “Who can see my stuff?” Select “Friends.” Also review your Activity Log and audience for past posts, to make sure they’re secure.
- “Who can contact me?” Choose “Friends” or “Friends of Friends” for people who can contact you.
- “Who can look me up?” Choose “Friends.”

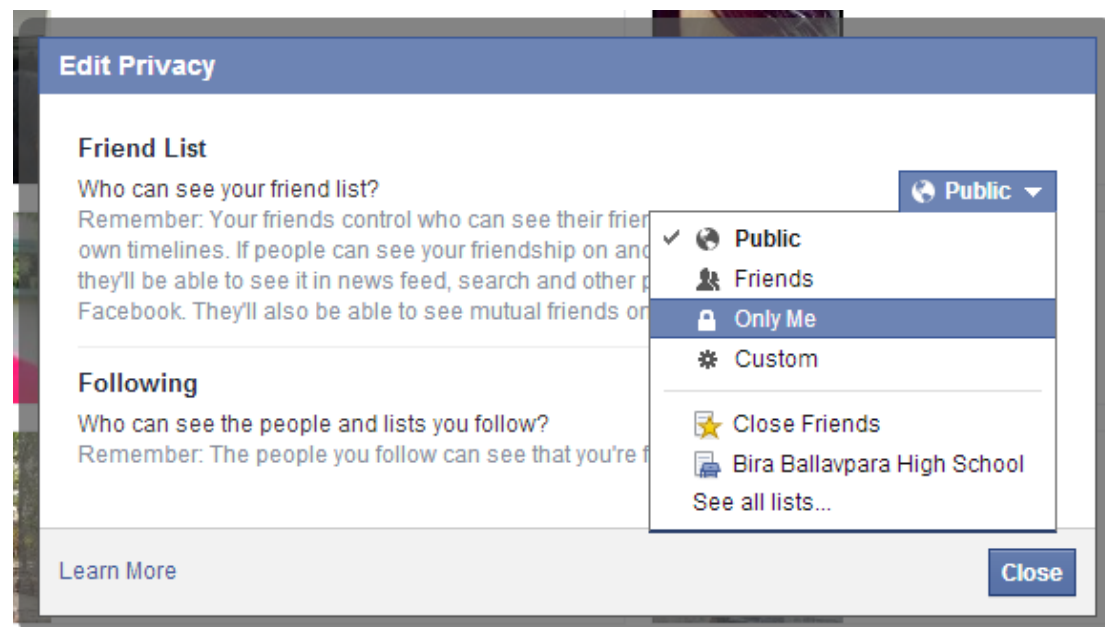
The last option in this panel is “Do you want other search engines to link to your timeline?” Select “No.” It might take some time for search engine results to stop showing the link to your timeline.



## Guard your personal information.

Edit the personal information in your profile and consider sharing only the bare minimum in order to limit what cybercriminals can use to compromise your bank accounts or identity.

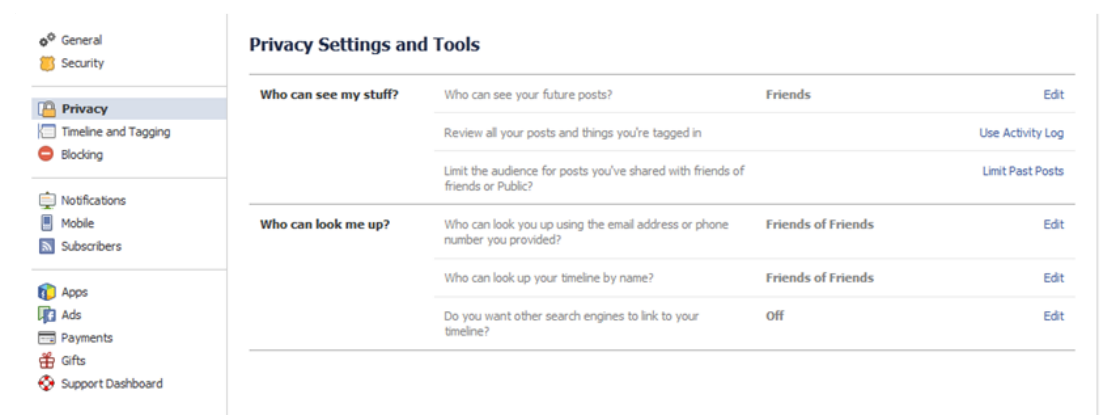
Also edit your “Friend List” privacy settings.



## Manage your apps

Consider examining which third-party applications have access to your Facebook profile. To view which apps you have previously approved, access the “Privacy Settings and Tools” panel you found above, and select “Apps” from the left-side bar navigation.

## Control your own timeline



Despite your best efforts to remain private, sometimes a friend’s post will give away your location and personal information. Posts that friends tag you in appear in the News Feed, the search, and on your timeline. You

can counter this by altering your “Timeline and Tagging” options under “Privacy Settings and Tools.”

- Enable the feature that allows you to review posts before they are published to your Timeline.
- It is important to note that these updates from friends still appear in News Feed and search.

## **Twitter**

Twitter is the second largest social networking site in the U.S. and allows users to share 140-character updates, called “tweets,” with their friends and followers. Tweets can also include links and photos. Twitter’s default settings set your account to public, meaning your tweets and information can be viewed by anyone, even by non-Twitter users. There are some simple settings that can allow you to make your Twitter account private.

*With a private account:*

- Only Twitter users you approve can subscribe and see your tweets.
- Any tweets previously made public will be hidden, and can only approved followers can see or search them.
- Your tweets will also no longer appear in Google searches or be “re-tweetable,” (which means they can be sent on to another user).
- Only approved followers will see any @replies you send.

To make your Twitter account private, click the wheel icon in the top right of your Twitter homepage and select “Settings” from the drop-down menu, then select “Security and Privacy” from the side-bar menu.

Under “Privacy,” check the box “Protect my tweets.”

Account >

Security and privacy >

Password >

Cards and shipping >

Order history >

Mobile >

Email notifications >

Notifications >

Web notifications >

Find friends >

Muted accounts >

Blocked accounts >

Apps >

Widgets >

Your Twitter data >

Accessibility >

© 2016 Twitter

[About](#)

[Help](#)

[Terms](#)

[Privacy](#)

[Cookies](#)

[Ads info](#)

[Brand](#)

[Blog](#)

[Status](#)

[Apps](#)

[Jobs](#)

[Advertise](#)

[Businesses](#)

[Media](#)

[Developers](#)

Password reset

☐ Require personal information to reset my password

When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

Privacy

Photo tagging

☒ Allow anyone to tag me in photos

☐ Only allow people I follow to tag me in photos

☐ Do not allow anyone to tag me in photos

Tweet privacy

☐ Protect my Tweets

If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. [Learn more](#).

Tweet location

☒ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. [Learn more](#)

Delete location information

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Discoverability

☒ Let others find me by my email address

☐ Let others find me by my phone number

This setting will take affect once you add a phone number. [Add now](#)

[Learn more](#) about how this data is used to connect you with people.

Address book

Manage your contacts

Contacts you've uploaded to Twitter from your address book.

Personalization

☒ Tailor Twitter based on my recent website visits

[Learn more](#) about how this works and your additional privacy controls

Contacts you've uploaded to Twitter from your address book.

Personalization ☒ Tailor Twitter based on my recent website visits

[Learn more](#) about how this works and your additional privacy controls.

Promoted content ☒ Tailor ads based on information shared by ad partners.

This lets Twitter display ads about things you've already shown interest in.

[Learn more](#) about how this works and your additional privacy controls.

Twitter for teams ☒ Allow anyone to add me to their team

☐ Only allow people I follow to add me to their team

☐ Do not allow anyone to add me to their team

Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck. [Learn more](#).

Direct Messages ☐ Receive Direct Messages from anyone

If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

☒ Send/Receive Read Receipts

When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see receipts from other people. [Learn more](#)

Save changes

---

## How to Spot a Social Media Fake



# Spotting **Fake** Profiles

More and more people, regardless of age and gender, are signing up for profiles on online social networks. Some have hundreds or thousands of followers spread across multiple profiles. But pollution of social media networks through creation of fake profiles is becoming increasingly common. Fake profiles often spam legitimate users, posting inappropriate or illegal content. Several signs can help you spot a social media fake who might be trying to scam you.

## **Step 1**

Read through the updates posted on the profile of the suspected faker. Accounts that only broadcast or push out updates and content instead of having conversations and engaging with other community members are often fake. If users do engage with you, be wary of requests to wire money or reveal sensitive information — a tactic often used by scammers. Such requests might come from users posing as a friend or family member. For example, if a friend contacts you via a social network asking for money, call him to confirm that the request came from him.

## **Step 2**

Keep an eye out for accounts that repeatedly push out spam. Signs include sharing the same link repeatedly in a short period of time and providing misleading information about the destination of a link.

## **Step 3**



Look for a verification indicator on the social media accounts of **high-profile users**. Accounts without verification might belong to an imposter. Consult the social media network's FAQs or user guidelines to familiarize yourself with the look and location of a legitimate verification indicator. For example, Twitter displays a light blue verification badge (check-mark icon) at the top left corner of a verified account, above the profile name, Twitter handle and bio. Badges that appear on a different part of the profile, such as a user's avatar, are not legitimate.

## Step 4

Watch for profiles created to provide phony reviews on social ratings and reviews sites. Fake reviews often do not comment on the specifics of a company's product or service. Instead, they tend to give overwhelmingly positive or negative feedback about only the brand.

---

# Creating Secure Passwords



Passwords — especially those not supported by [two-step verification](#) — 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?

There are a few ways your account passwords can be compromised.

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, user-names, pronouns, IDs, and any other predefined number or letter sequences.

Ideal passwords, however, are a huge inconvenience. How can we be expected to remember 12-character passwords for each of our various Web accounts? That's where many people turn to password managers like LastPass, Dashlane and 1Password.

## 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. Using numbers, symbols and mix of upper and lower case letters in your password makes it harder for someone to guess 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 because it has 30,000 times as many possible combinations than an eight-character password with only lower case letters.

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



**verification**

**Enable**

**two-step-**

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.

You only have to do this once for "recognized" computers and devices.

### **Securing your passwords 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. If you want super secure passwords for your online accounts (which is recommended), but you don't want to memorise them all (also recommended), this is the way to go. There are many options available, but a few crowd favourite are [LastPass](#), [Dashlane](#) and [1Password](#).

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.

---