Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email CCIU

CCIU Webpage

CPF 00004-16-CID361-9H 19 September 2016

Configuring Twitter for a More Secure Social Networking Experience

Basic Notes About Twitter Configuration

Twitter is an integral thread in the fabric of the internet. Assume that if it is posted on Twitter, it is also posted on the internet and the world will be able to see it. Therefore, do not post anything to Twitter, or any social media site for that matter, that you do not want the world to know.

Always assume that once it is posted to Twitter, and by extension the internet, no amount of effort will eliminate it from Twitter or the internet. The internet does not forget. Also, there are several sites that scrape Twitter content and keep copies of Tweets and images posted with those Tweets even after you delete content from Twitter.

Twitter is an open platform. Participation is open to everyone with access to an internet connection and an email address. Anyone, whether they have a Twitter account or not, can read posted Tweets unless the person posting the Tweets has configured their account to make their Tweets private.

Images on Twitter

Posting images on Twitter is generally a bad idea and should be avoided. Digital images frequently contain metadata. Although some social networking sites strip off image metadata during the upload process, Twitter does not. Image metadata can contain considerable information such as the location where the image was captured (accurate to within a few feet), the date and time the image was captured, and the make, model and serial number of the camera that captured the image, and more.

Twitter User Identities

Twitter does not vet their users. Although users are, by Twitter rules, required to use real information when they register for an account. The extent of Twitter's verification is that someone at the email address associated with the account clicked a verification link in a received email.

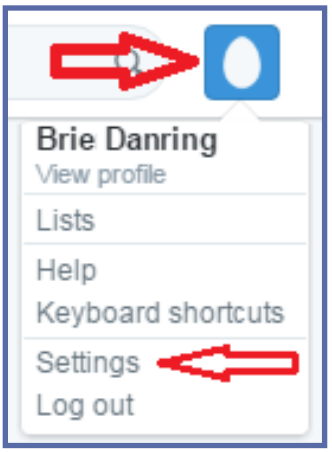
Later, in the Protect My Tweets section, you will see how to change settings so that you can decide who follows you. Once that setting is complete, do not accept as followers anyone you do not know or cannot verify.

Social engineering is common on the internet. Given that Twitter does not vet users, the person you think you are accepting as a follower may not be who they purport to be and could be someone trying to

* This Twitter configuration guide supersedes CID Crime Prevention Flyer CPF-00009-15-CID361-9H.

Cybercrime Prevention Flyer

General Account Settings



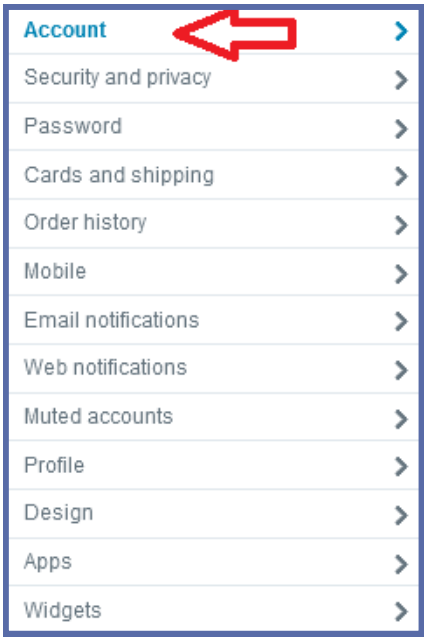
The Settings menu is available by clicking the Twitter Egg in the upper right side of the Twitter command bar and then clicking **Settings** in the drop down menu.

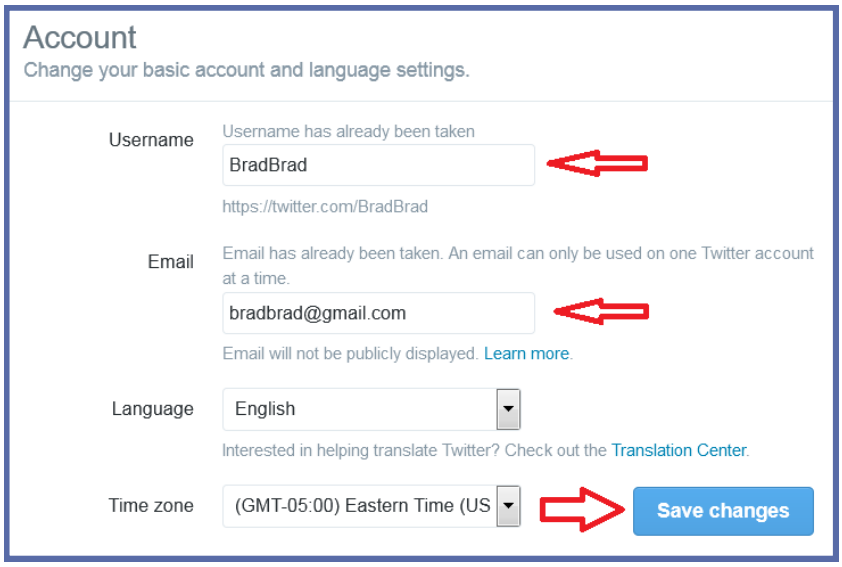
Email

This is where you change your email address if the address you registered with Twitter is disabled or retired for any reason. Twitter's policy is that the email address is not displayed. Testing indicates this is true; however, depending upon email settings covered under Discoverability, it may be possible for people to locate your Twitter profile using just your email address.

To change your email address, from the Settings menu,

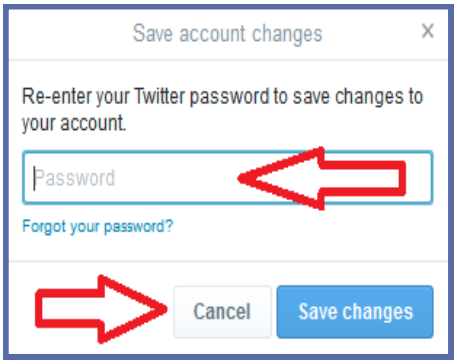
1. Click **Account**.





2. Make changes as you feel appropriate.
3. Click **Save Changes**.

An email address can be associated with only one Twitter account at a time.



4. Enter your password and click **Save Changes.**

Twitter will send an email message to the new email address confirming the change. Check your email and follow included instructions.

Cybercrime Prevention Flyer

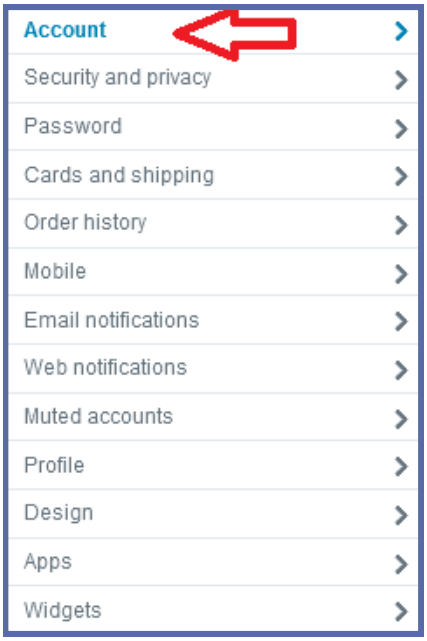
Your Twitter Archive

Perhaps, over the years, you have forgotten some of the things you've posted on Twitter. Perhaps you've tried to review your activity but found scrolling through page after page too tedious to finish. Fortunately, there is a means by which you can download to your local computer an archive of your information and activity.

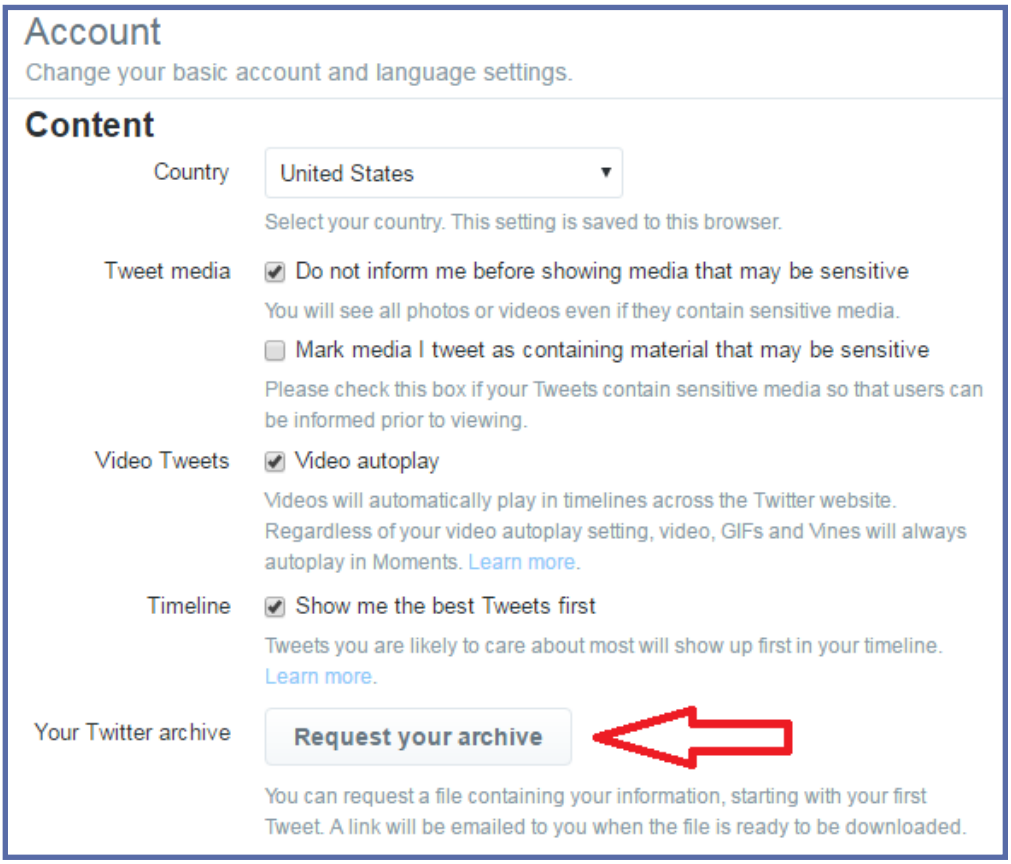
A few points to bear in mind before you start the process:

- Depending upon your level of activity, the download could be quite large.
- Downloading the archive could require substantial bandwidth—best to use a high speed, high capacity internet connection.
- DO NOT download your archive to any computer that you do not have total ownership of—that would be a borrowed computer, a public computer like those you might use at a library, community center or school, or your work computer.

To download your archive of Twitter activity, from the Settings menu,



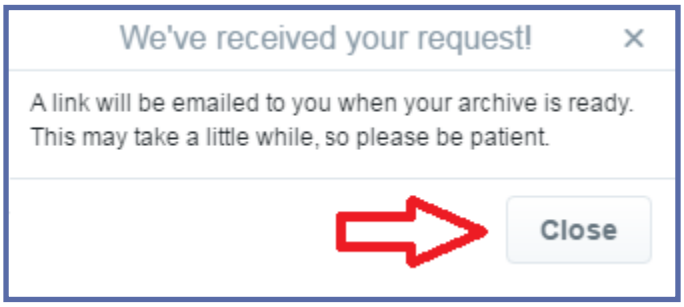
1. Click **Account**.
2. Scroll to the bottom of the **Account** settings.



3. Click **Request your archive**.

These Twitter configuration recommendations are based upon best information available at the time of publication but are not a guarantee of social networking safety. Twitter may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

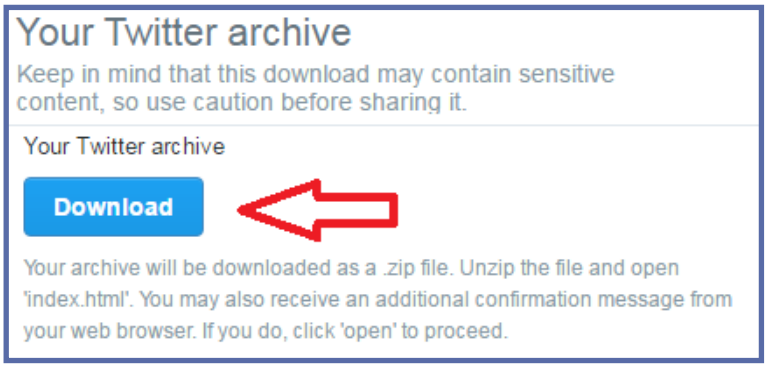
Cybercrime Prevention Flyer



4. From the Twitter pop-up, click **Close**.

   Periodically check the inbox of the primary email associated with your Twitter account for a message telling you your archive is ready to download.

5. Click **Download now**. (Clicking this link returns you to Twitter.)



6. Click **Download**.

   When the download is complete, open the .zip file and follow the instructions in README.txt.

Passwords

Passwords, secret elements of authentication, are the front line of defense preventing people and automated tools (e.g., password crackers) from illegally accessing your online accounts. Therefore, your choice of password and the frequency with which you change it are important security considerations.

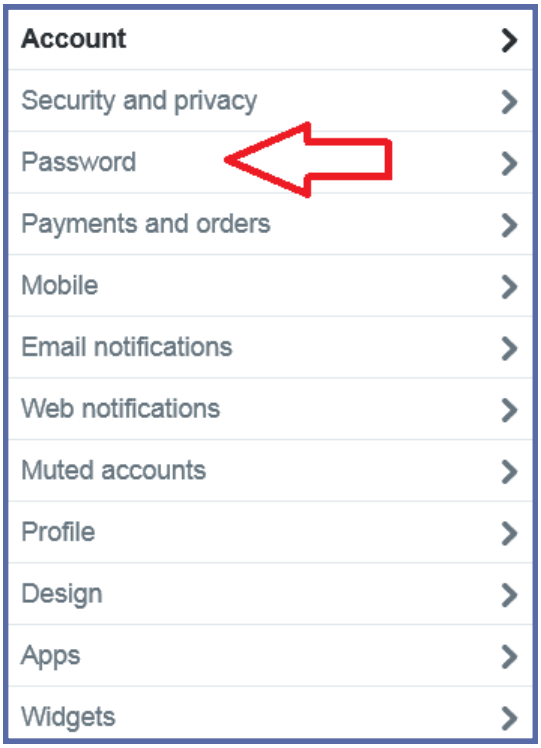
A password, however, need not be limited to a word. It can be a passphrase. A passphrase is a string of characters that forms a phrase. An example passphrase might be, “The song remains the same” or “I’ll see you on the dark side of the moon”. Passphrases are generally easier to remember than are complex passwords and are more likely to survive a dictionary attack than is a single password.

Cybercrime Prevention Flyer

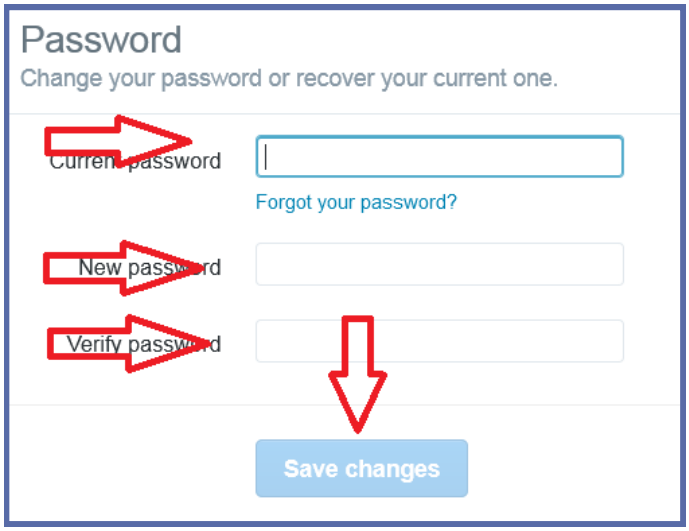
Guidelines for passwords to avoid, especially if you are a public figure or in a situation where much of your personal information might be in the public domain, include:

- your name or any permutation of your name
- your user ID or any part of your user ID
- common names
- the name of any relative, child, or pet
- your telephone number, social security number, date of birth, or any combinations or permutations of those
- vehicle license plate numbers, makes, or models
- the university you attended
- work affiliation
- the word “password” or permutations including “password” prefixed or suffixed by numbers or symbols
- common words from dictionaries, including foreign languages or permutations of those words
- names or types of favorite objects
- repeating patterns of digits or numbers or sequences of characters found on keyboards

To change your Twitter password, from the Settings menu,



1. Click **Password**.



2. Enter your current password.
3. Enter your new password or passphrase.
4. Reenter your new password or passphrase.
5. Click **Save changes**.

Cybercrime Prevention Flyer

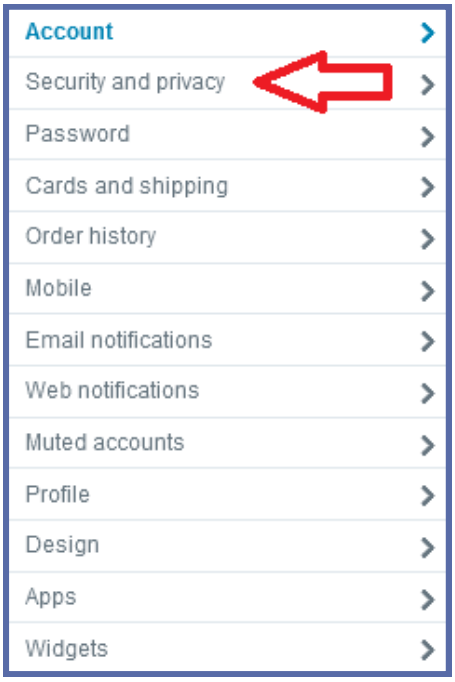
Security and Privacy

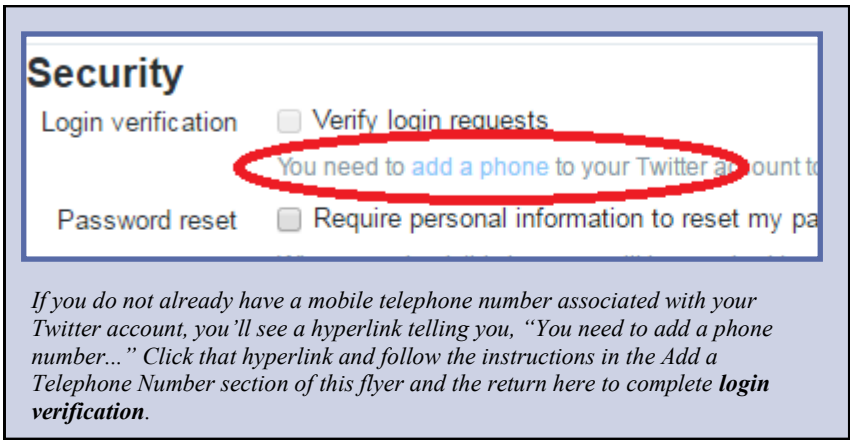
Login Verification
Twitter provides a second means to verify your identity when logging in. **Login verification** helps prevent and identify attempted compromises to your Twitter profile. Whenever you access your Twitter account and pass the initial username/password test, Twitter will hold continued access until an unlock code is correctly entered.

Twitter sends the unlock code as a text message to the mobile telephone number you entered when you established your account or, if one is not on file, Twitter will ask you to enter one. Providing Twitter with a telephone number creates another vulnerability which presents a separate issue. See the included section entitled **Discoverability.**

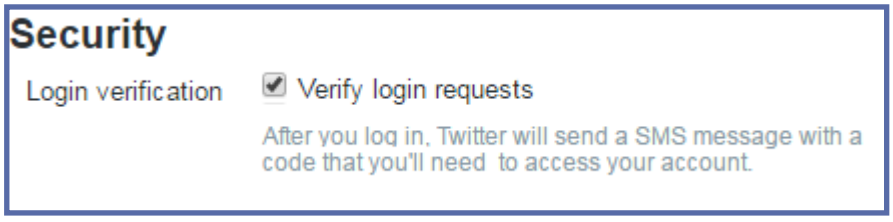
To implement **Login verification,** from the Settings menu,

1. Click **Security and privacy**.

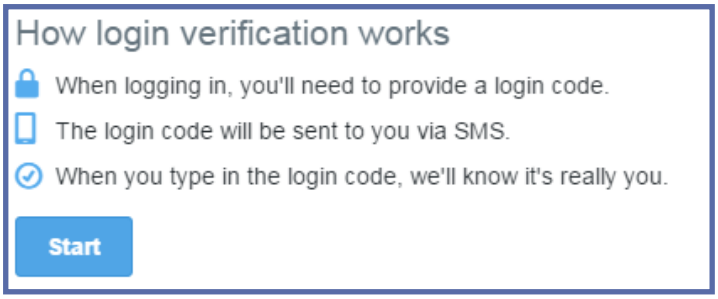




If you do not already have a mobile telephone number associated with your Twitter account, you'll see a hyperlink telling you, "You need to add a phone number..." Click that hyperlink and follow the instructions in the Add a Telephone Number section of this flyer and the return here to complete ***login verification****.*



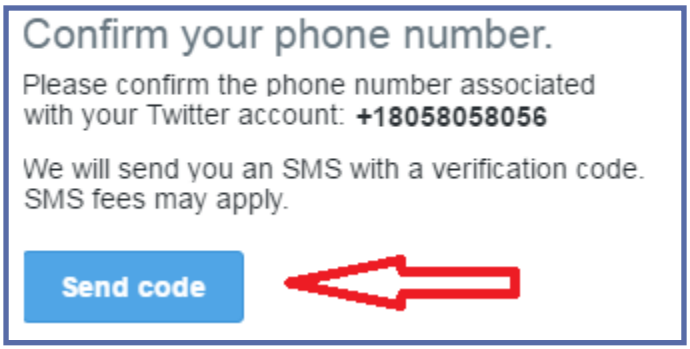
2. Click **Verify login requests**.



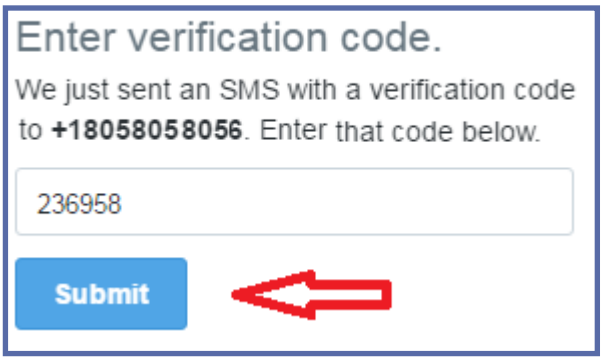
3. Click **Start**.

Warning—If you use login verification and retire the telephone number without first updating the default number in Twitter, you will likely lock yourself out of your Twitter account.

Cybercrime Prevention Flyer



4. Click **Send code**.
5. Check your mobile phone for an SMS message with the six digit code.



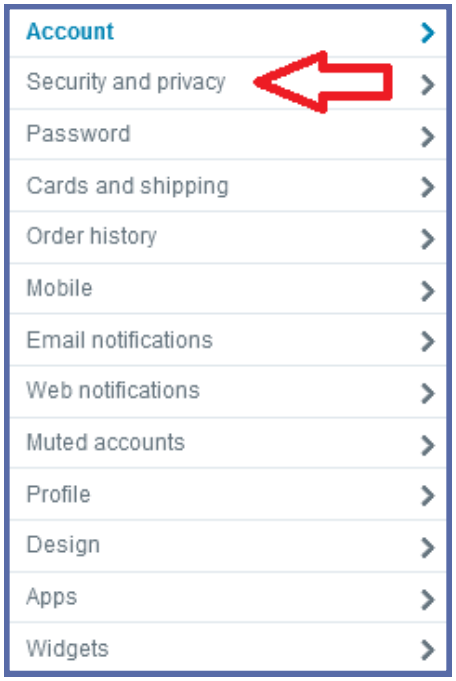
6. Enter the SMS code and click

Photo Tagging

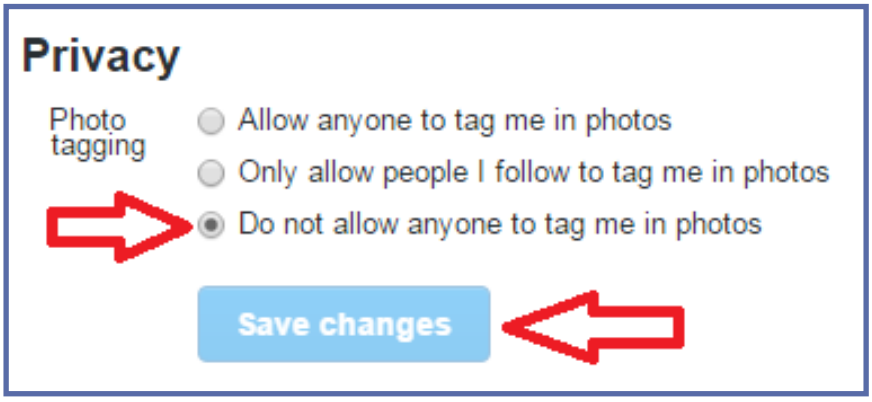
Photo tagging is a feature common to many social networking sites that facilitates the fast and easy sharing of photos in which you are pictured. This makes it easier for other Twitter users and your Twitter followers to locate you and participate in social exchanges. However, because the actual presence of a tagged individual in a photo is not independently verified, you could be associated with photos you are not even in and unpleasant images you do not ever want to be associated with.

Photo tagging by anyone other than you should be prevented.

To change **Photo tagging,** from the Settings menu,



1. Click **Security and privacy**.



2. Click the radio button opposite **Do not allow anyone to tag me in photos**.
3. Click Save changes.

These Twitter configuration recommendations are based upon best information available at the time of publication but are not a guarantee of social networking safety. Twitter may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

Cybercrime Prevention Flyer

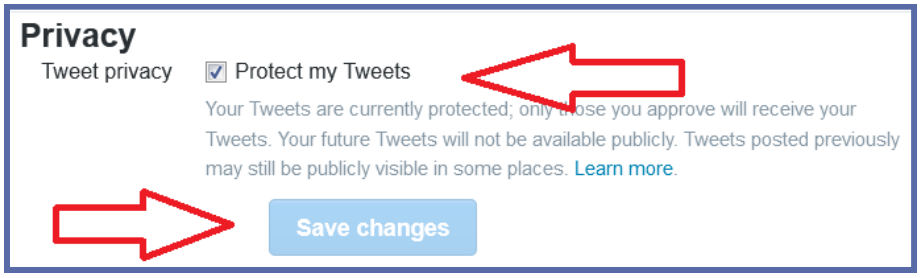
Protect My Tweets

By default, all of your Tweets are available to every Twitter user and, because Twitter content is available in most search engines, to most internet users whether they are Twitter users or not. You can limit who sees your Tweets by changing the default setting to **Protect my Tweets**.

Protecting your Tweets has far reaching security benefits, such as:

- All prior Tweets are protected.
- People will have to request to follow you before they can view your Tweets.
- You will be required to approve every follower request before they can view your Tweets.
- Other users will not be able to retweet your Tweets.
- Protected Tweets do not appear in search engines.*

To protect your Tweets, from the Security and privacy menu,



1. Click **Protect my Tweets**.
2. Click **Save Changes**.

Tweet Location Privacy

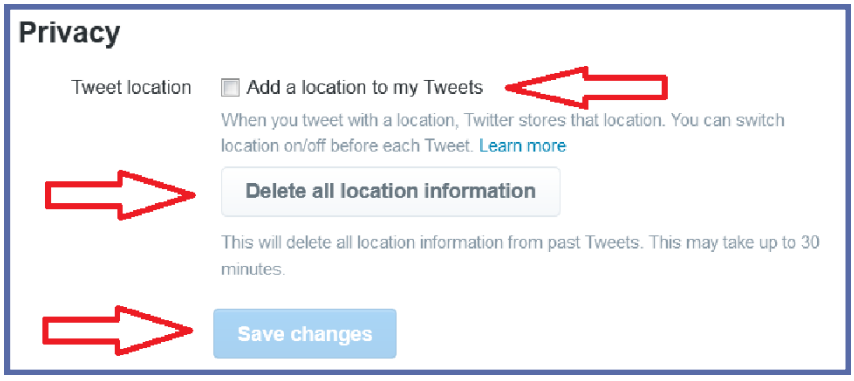
Twitter uses several means to capture your physical location. The location information Twitter captures oftentimes is accurate to within a few feet. Tweet location is **OFF** (unchecked) by default and should be left **OFF**.

If Tweet location is turned on it should be turned off (unchecked) and **Delete all location Information** executed.

To change **Add a location to my Tweets**, from the Privacy and settings menu,

1. Uncheck **Add a location to my Tweets**.
2. Click **Delete all location information**.
3. Click **Save Changes**.

Deleting location information could take several minutes to complete depending upon how extensively you have used Twitter.



* *Tweets already indexed by search engines, or location information already captured by third party websites, will persist for an indefinite period of time.*

These Twitter configuration recommendations are based upon best information available at the time of publication but are not a guarantee of social networking safety. Twitter may have instituted configuration changes since publication. Users must exercise caution whenever interacting with social media.

Cybercrime Prevention Flyer

Discoverability

Let Others Find Me by My Email Address and My Phone Number

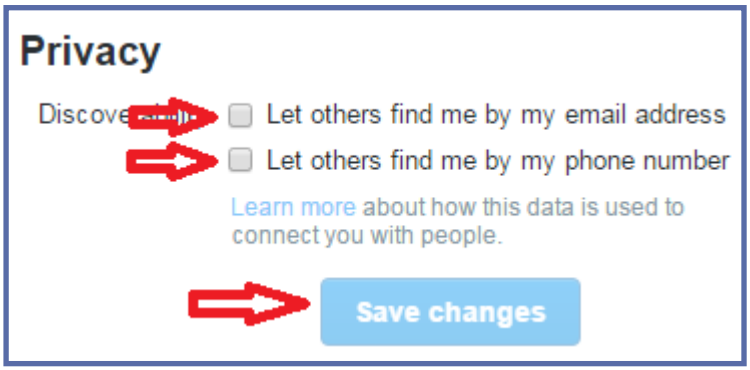
In order to create a Twitter account, users must provide a valid email address. The email address is verified when Twitter sends an email with a link the user must click in order to demonstrate the validity of the email address.

If you have enabled **Login Verification** then you have provided Twitter with your telephone number or perhaps you provided Twitter with your phone number when you created your account.

Regardless of how Twitter obtained your email or telephone number, it could be possible for any Twitter user to locate your profile using only your email address or telephone number. This option should be turned off for both contact methods.

This small step of validation should not be interpreted to mean that Twitter user's identities are properly vetted. Anyone can use any of many free email providers to create a "single use" email thereby creating circular verification - a fake email address is used to verify a fake social media account.

To update your **Discoverability** settings, from the *Privacy and settings* menu,



1. Uncheck **Let others find me by my email address**.
2. Uncheck **Let others find me by my phone number**.
3. Click **Save changes**.

Return to Social Networking Safety Tips

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.