



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

Phone: 571.305.4482 (DSN 2401)

Email

MCU Web Page

CID LOOK OUT
ON POINT FOR THE ARMY

DISTRIBUTION:
This document is authorized for the
widest release without restriction.



"DO WHAT HAS TO BE DONE"

CPF 0002-20-CID361-9H

04 February 2020

Configuring Twitter for a More Secure Social Networking Experience

Basic Notes About Social Media

The internet's social media ecosystem is vast. To some people, social media is the internet. Searches are secondary. Staying in touch with relatives, friends, keeping current on events are primary.

But there are risks to consider when using social media.

Anyone with a Twitter account can read your tweets unless you've configured your account so your tweets are private—visible only to your followers. But even though your tweets are visible only to your followers, could one of your followers have reposted it to another site? Would you even know?

A good practice is to assume that once posted to social media your information is a permanent part of the internet and no amount of effort will eliminate it entirely. Did you know there are several websites that scrape Twitter content and keep copies of tweets and images even after the Twitter content has been deleted?

Twitter User Identities

Twitter is an open platform!
Participation is open to anyone with access to an internet connection and an email address.

***The internet does not
forgive! The internet
does not forget***

Twitter does not effectively vet their users. Although users are, by Twitter rules, required to use real information when they register, that information is not verified in a meaningful way. Twitter sends an email to the address used for registration that includes a verification link. This is only meaningful if the email subscriber used valid information to open the email address. And there are plenty of free online email providers that do nothing to verify their users.

Social engineering is common on the internet. Given that Twitter does not vet users, the person who follows you may not be who they purport to be and could be someone trying to access personal information about you.

Posting to Twitter

Posting to any social media site should be done with an abundance of caution. Intentionally or otherwise, your posts can reveal a lot about you. That picture of your fourth grader's first day at school tells where your child attends school and where he or she can be found Monday through Friday in the morning and afternoon.

That funny video of your 40th birthday party you posted last night might be more embarrassing than funny in the harsh clarity of the following morning. Might it be something a nefarious actor could use against you?

Settings and Privacy

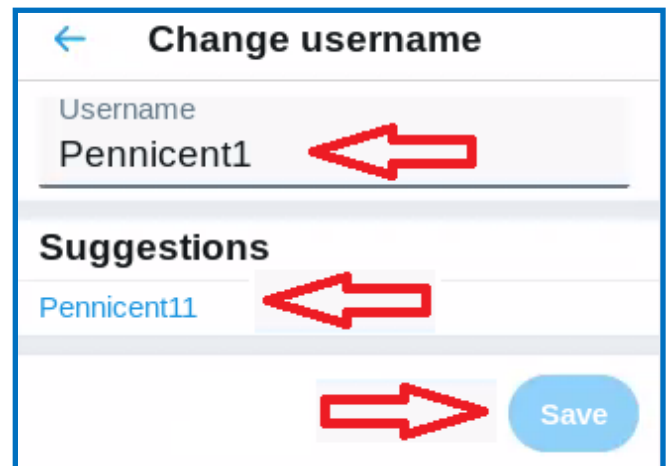
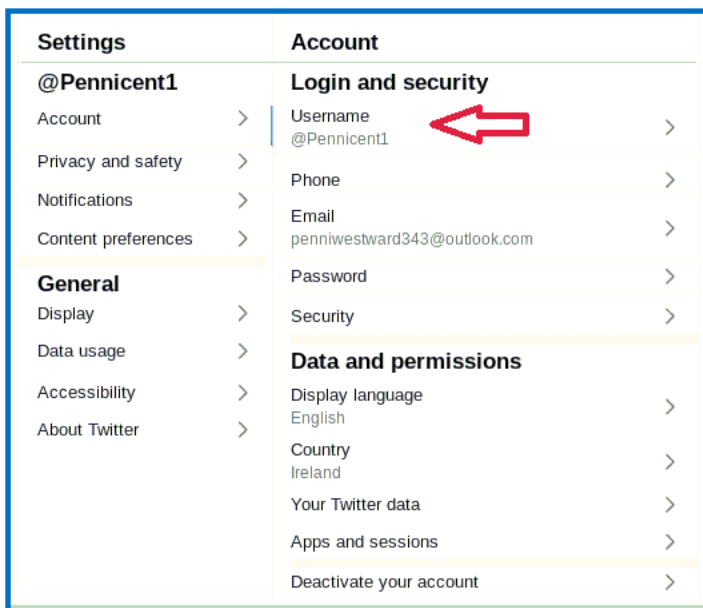
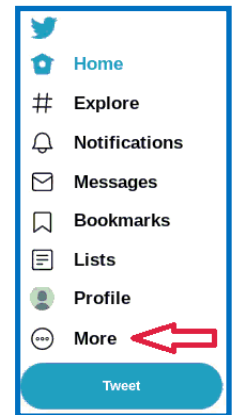
Most of Twitter's settings are available from the **More** menu option. From most locations within Twitter, that button is in the menu along the left side of the screen.

When you click that profile icon a menu will appear beneath the Twitter profile icon. Clicking **Settings and Privacy** takes you to another menu with many of the settings you should be concerned with.

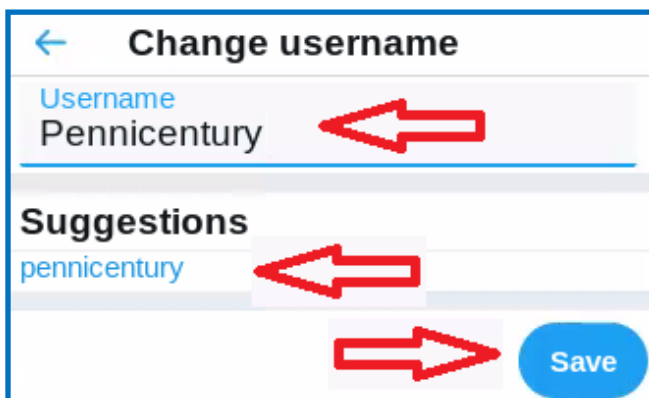
Username

To change your username, from the Settings and Account menu:

1. Click **Username**.



2. Twitter will suggest alternate usernames similar to your current username. If one is acceptable, click on it.
3. Click **Save**.



4. If you want an entirely new username, type it in the username field. It will echo in the suggestions box and show you how it will appear in Twitter.
5. Click **Save**.

← **Change username**

Username
Pennicent

That username has been taken. Please choose another.

Suggestions
Pennicent2

Save

6. If you happen to select a name already in use, Twitter will highlight the fact and suggest available and similar usernames.
7. Accept one of Twitter's recommendations or try another username that is not already in use.
8. Click **Save**.

Email

This is where you change your email address if the address you registered with is disabled or retired for any reason.

To change your email address, from the Settings and Account menu:

1. Click **Email**.

Settings | **Account**

@Pennicent1

Account > Login and security

Privacy and safety > Username @Pennicent1

Notifications > Phone

Content preferences > Email penniwestward343@outlook.com

General

Display > Password

Data usage > Security

Accessibility > **Data and permissions**

About Twitter > Display language English

Country Ireland

Your Twitter data

Apps and sessions

Deactivate your account

← **Change email**

Current
penniwestward343@outlook.com

Update email address

2. Click **Update email address**.

Twitter logo

Verify your password

Re-enter your Twitter password to continue

Password
.....

Reveal password

Next

3. Enter your password and click **Next**.

Change email

Your current email is penniwestward343@outlook.com. What would you like to update it to? Your email is not displayed in your public profile on Twitter.

Email address
penniwestward344@outlook.com

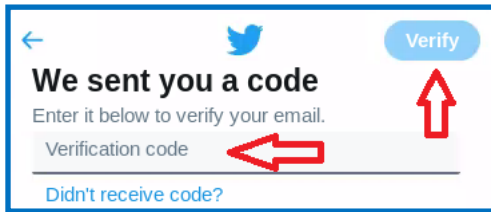
Let people who have your email address find and connect with you on Twitter. ☐

Learn more

4. Enter your new email and click the **Next**.

5. Check the inbox of the new email address for an email with a verification code from Twitter.

If the email isn't in your inbox, check your junk or spam folder as well.



6. Enter the verification code.
7. Click **Verify**.

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.

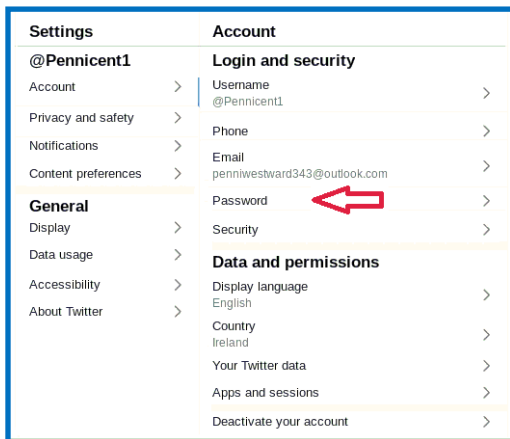
A password, however, need not be limited to a word. It can be a passphrase. A [passphrase](#) is a string of characters that forms a phrase. An example passphrase might be, "The song remains the same" or "I'll see you on the dark side of the moon". Passphrases are generally easier to remember than are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

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 and Account menu:

1. Click **Password**.



Change password

Current password
.....

Forgot password?

New password
.....

Confirm password
.....

You have 14 applications with access to your account. Updating your password will not revoke access.

Save

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

Your password has been successfully updated.

6. If successful, a confirmation note appears for a few seconds.

Two-factor Authentication

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 when you setup login verification.

Providing Twitter with a telephone number creates another vulnerability which presents a separate issue. See the included section entitled Discoverability.

To implement two-factor authorization, from the Settings and Account menu:

1. Click **Security**.

Settings	Account
@Pennicent1	Login and security
Account >	Username > @Pennicent1
Privacy and safety >	Phone >
Notifications >	Email > penniwestward343@outlook.com
Content preferences >	Password >
General	Security ←
Display >	Data and permissions
Data usage >	Display language > English
Accessibility >	Country > Ireland
About Twitter >	Your Twitter data >
	Apps and sessions >
	Deactivate your account >

Security

Two-factor authentication

Two-factor authentication >

Protect your account from unauthorized access by requiring a second authentication method in addition to your Twitter password. You can choose text message, authentication app, or security key. [Learn more](#)

2. Click **Two-factor authentication**.

Two-factor authentication

Text message ☒ **Text message**

Use your mobile phone to receive a text message with an authentication code to enter every time you log in to Twitter.

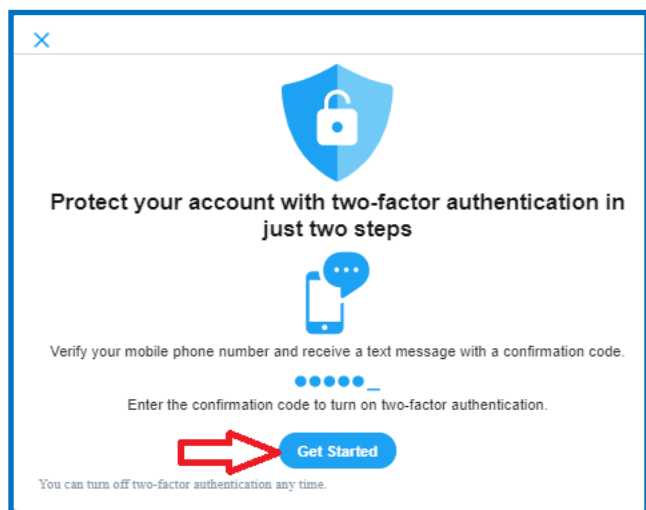
Authentication app ☐

Use a mobile authentication app to get a verification code to enter every time you log in to Twitter.

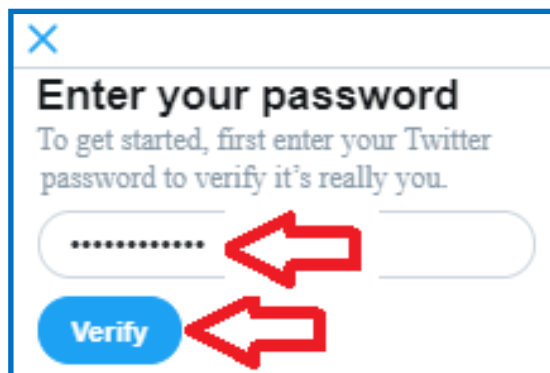
Security key ☐

Use a physical security key that inserts into your computer or syncs to your mobile device when you log in to twitter.com using a supported web browser. Currently, you can't use a security key to log in to the Twitter app. [Learn more](#)

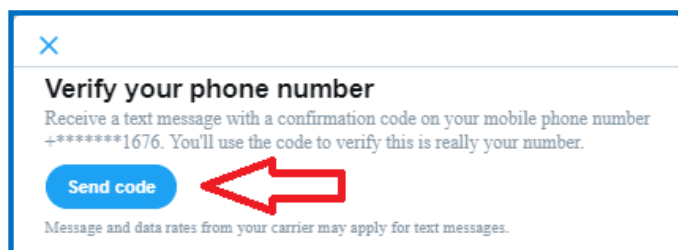
3. Click **Text message**.



4. Click **Get started**.

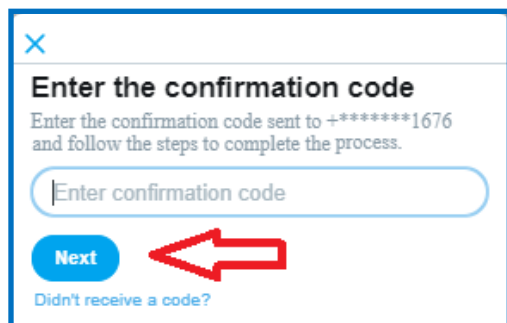


5. Enter your password and click **Verify**.



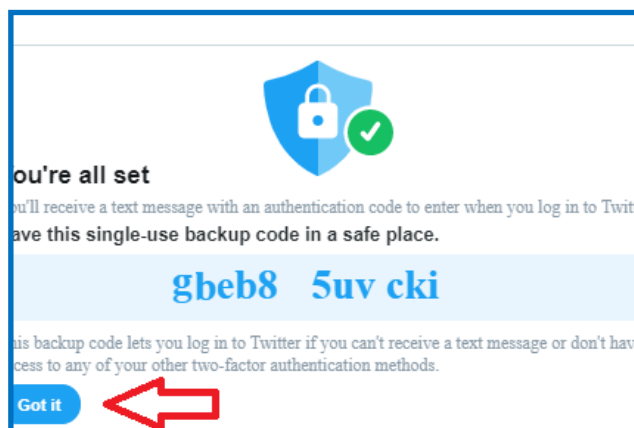
6. With your mobile telephone nearby, click **Send code**.

Twitter will send a confirmation code to your mobile phone.



7. Enter the confirmation code you received on your mobile phone in the box and click **Next**.

It's a good idea to keep this code in a safe place. That way, if the mobile phone you used to establish two-factor authentication is lost or replaced, you'll still be able to access Twitter.



8. If the adding two-factor authentication has been successful you'll see this announcement.
9. Click **Got it**.

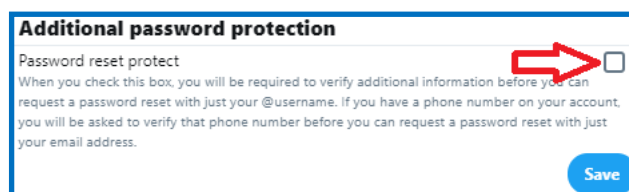
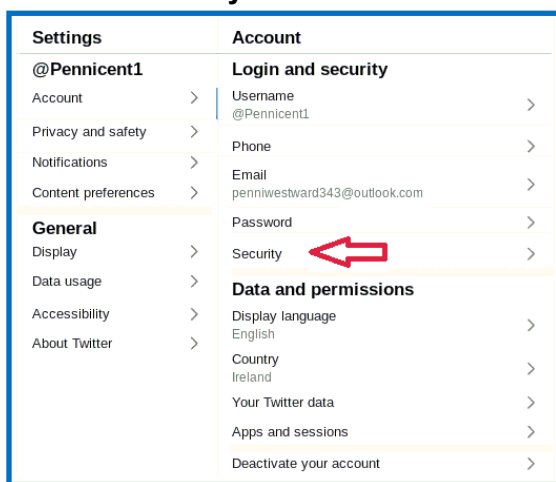
Additional Password Protection

With seemingly hundreds of unique passwords to remember, it's not uncommon to forget one or more of them. Most often, forgotten passwords can be recovered by following instructions for just that purpose. Security of the process is maintained when an email with a link is sent to the email address associated with your Twitter account. Of course, this assumes only you have access to your email account or that your email account has not been compromised.

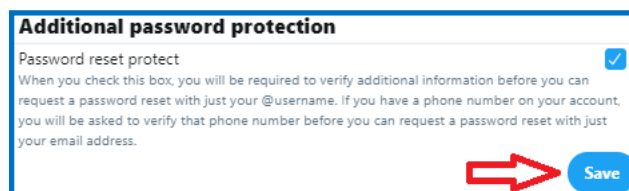
Enabling Additional Password Protection adds another layer of security to password recovery. In addition to sending a message to the email on file, Twitter will ask to verify your telephone number.

To enable Additional Password Protection, from the Setting and Account menu:

1. Click **Security**.



2. Click the box to enable additional password protection.



3. Verify that the additional password protection box is checked.

Applications

There are hundreds of available Twitter applications on the internet. The applications do a range of different things. With few exceptions, in order to interact with Twitter, you must authorize the application to access your Twitter profile.

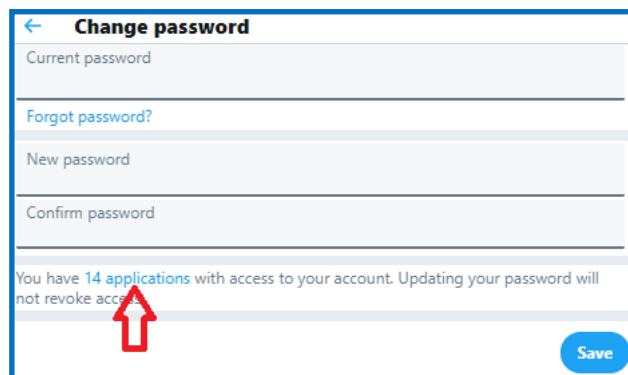
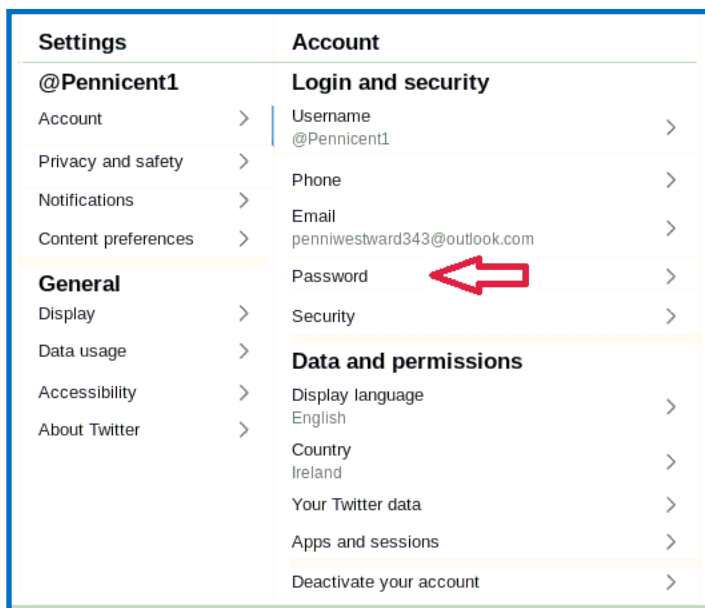
There are valid reasons why you might want to provide that kind of access but there are also reasons why you might not. Many applications have useful functionality and features and are from trustworthy, reputable software providers. Some, however, could place your Twitter profile and data at risk of compromise—not everything on the internet is as it purports to be—not everything on the internet is safe.

Over time it's possible you'll authorize various applications access to your Twitter profile. Some you might want to allow access for an extended period of time. Others you might not. But, after a period of time you might not remember which applications you have allowed to access your Twitter profile. There is a means by which you can determine the applications that you've allowed to access your Twitter profile.

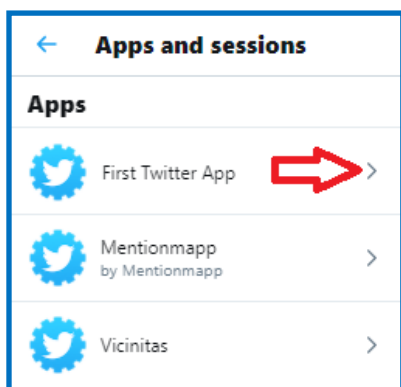
Hidden in the password configuration area is a feature where you can audit the applications that you have allowed to access your Twitter profile, when you provided that access and, allow you to remove that access.

To see which applications you've allowed access, from the Setting and Account menu:

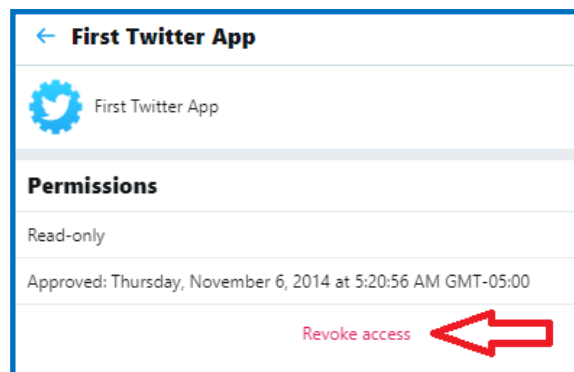
1. Click **Password**.



2. Click **applications**.



3. Click on the application in question.



4. Click **Revoke access**.

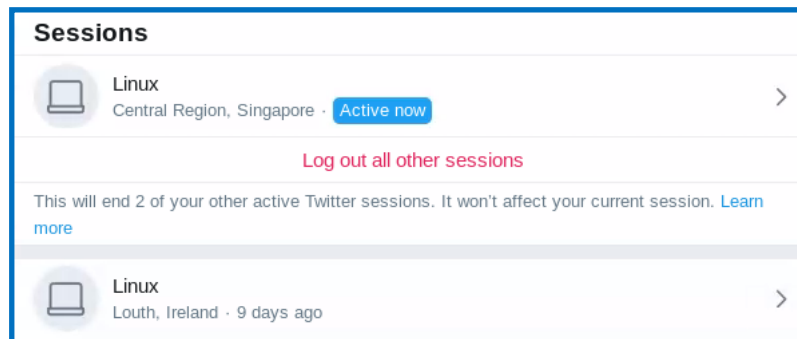
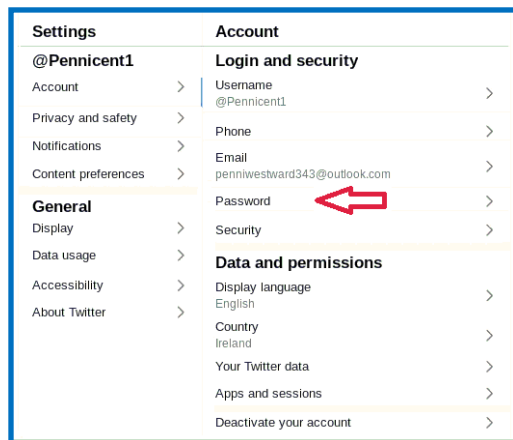
Sessions

This feature can be used to end any active Twitter session, including the one from which you are accessing your Twitter account. This is more of a security audit tool than a security measure. Sessions will identify those computers from which you might not have properly logged out of Twitter and can tell you if unauthorized access to your account has occurred.

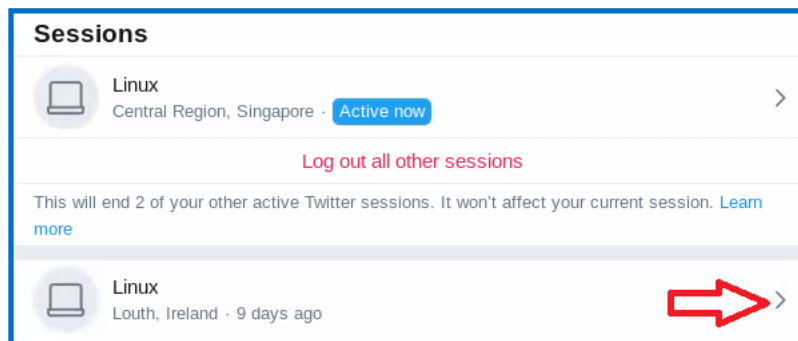
A generally good security practice is to log out of any internet activity that requires a login; logging out is a specific menu choice. Closing the browser or restarting the computer may be insufficient to fully log out. In some circumstances, like accessing your Twitter account from a public computer or any computer that multiple people use, not fully logging out of Twitter could be disastrous. Quite possibly, the next person who opens Twitter from that computer could open to your account without being challenged for a password, inadvertently giving them unintended full access.

To check where you might have open Twitter sessions, from the Settings and Account menu:

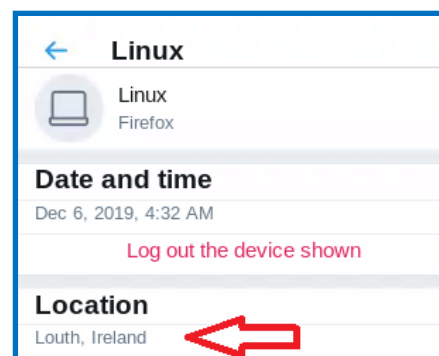
1. Click **Password**.



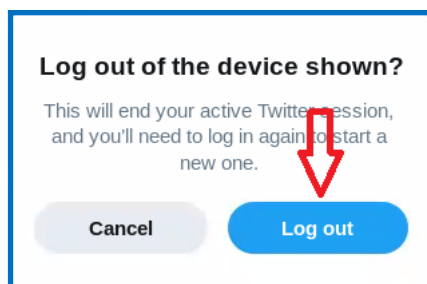
2. Scroll down past the list of applications that you have authorized to have access to your Twitter data to the Sessions section.



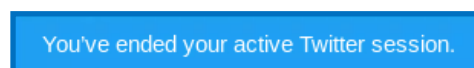
3. Review the sessions that are open.
4. Click on the open session you want to close.



5. Click **Log out of device shown**.



6. Click **Log out**.



7. Look for a message that the selected session has ended. It will appear just briefly along the bottom of your browser.

Sessions also reveals if your Twitter account is currently being accessed maliciously.

If, when you view the list of active sessions, you see a login that is completely out of place, you should consider the possibility that your Twitter account (and perhaps your other social media accounts) has been compromised. Someone not you has accessed your Twitter.

If you access sessions and see a logged in browser you believe to be an unauthorized connection you should:

- End the session associated with that browser,
- Change your Twitter password,
- Recheck Sessions to verify that the suspect sessions have been terminated and that a new session was not started.

If you have used your Twitter password on any other accounts, you should consider changing the passwords on those accounts as well to minimize the risk of further unauthorized access.

Privacy and Safety

There are three important settings under privacy and safety: protect your tweets, location information, and photo tagging. Properly configured, these three settings go a long way to protecting your Twitter activity.

Protect Your Tweets

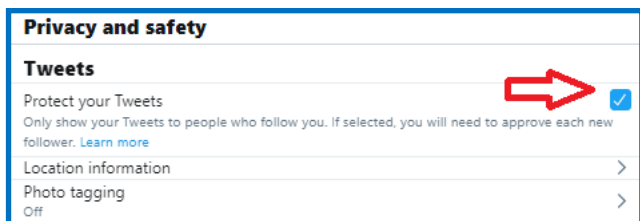
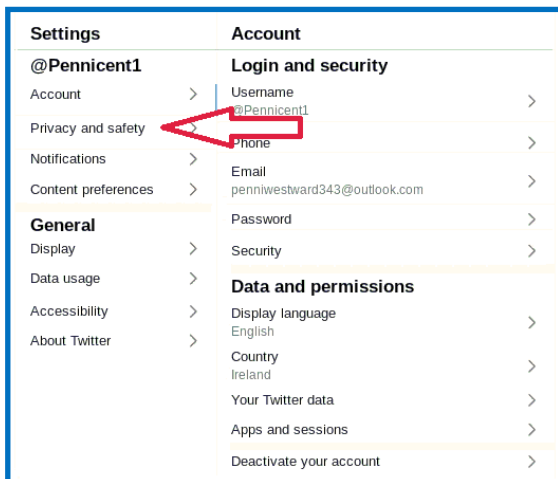
By default, all of your tweets are available to every Twitter user and, because Twitter content is available in most search engines, it is also available to most internet users whether they are Twitter users or not. You can limit who sees your tweets by changing the default setting to Protect your Tweets.

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

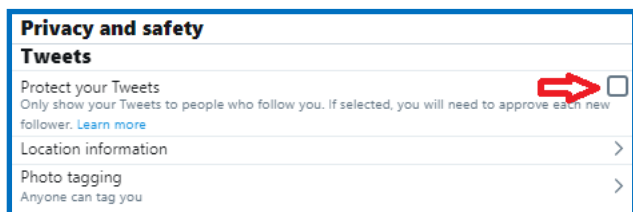
- All prior tweets are protected.
- People will have to request to follow you before they can view your tweets.
- You will be required to approve every follower request before they can view your tweets.
- Other users will not be able to retweet your tweets.
- Protected tweets do not appear in search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

To enable protect your tweets, from the Settings and Account menu:

1. Click **Privacy and safety**.



2. If protect your tweets is enabled, you'll see a blue box with a white check mark. You need do nothing more. Protect your tweets is already enabled.



3. If the box is open, protect your tweets is NOT enabled. Click the empty box to enable protect your tweets.

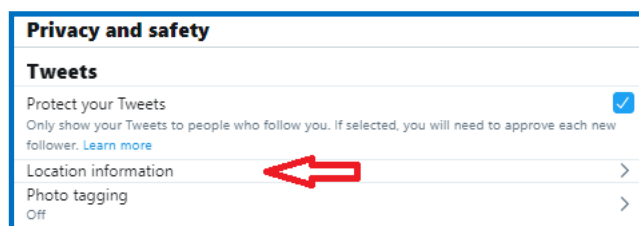
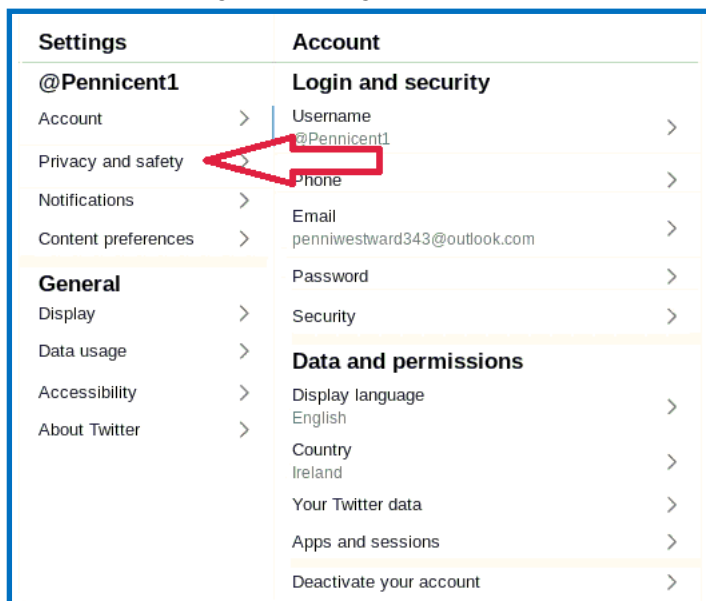
** Tweets already indexed by search engines, or location information already captured by third party websites, will persist for an indefinite period of time.*

Location Information

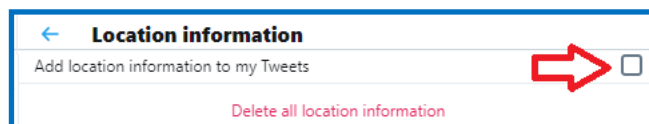
Twitter uses several means to capture your physical location. The location information Twitter captures oftentimes is accurate to within a few feet. Tweet location is OFF (unchecked) by default and should be left **OFF**. If tweet location is turned on, it should be turned off (unchecked) and Delete all location information executed.

To change the location information setting, from the Settings and Account menu:

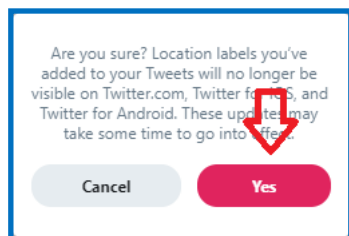
1. Click **Privacy and safety**.



2. Click **Location information**.



3. Make sure the location information box is not check marked.



4. Click **Yes**.

Photo Tagging

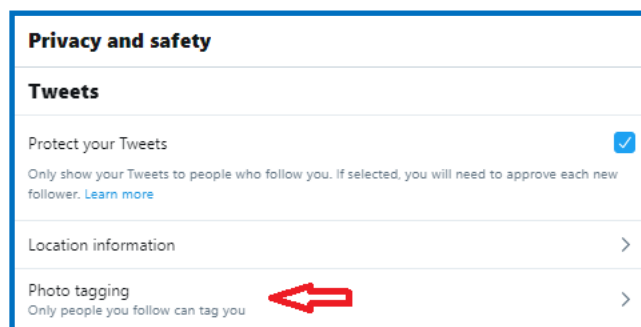
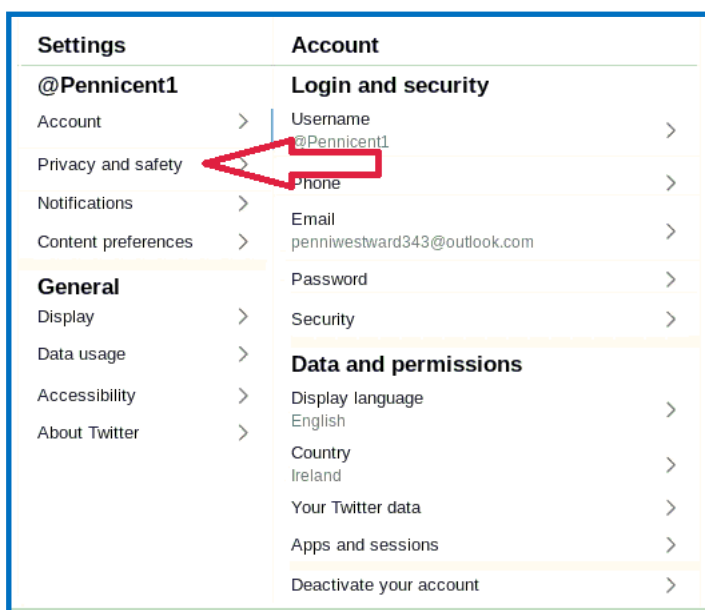
Photo tagging is a feature common to many social networking sites that facilitates the fast and easy sharing of photos in which you are pictured. This makes it easier for other Twitter users and your Twitter followers to locate you and participate in social exchanges.

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 or unpleasant images you do not ever want to be associated with.

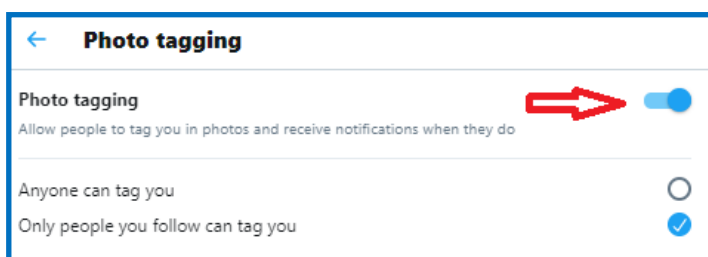
Photo tagging by anyone other than you should be prevented.

To change Photo tagging, from the Settings and Account menu:

1. Click **Privacy and safety**.



2. Click **Photo tagging**.



3. If photo tagging is enabled (the slider is blue), click the slider to disable photo tagging.

If you decide to allow others to tag you in photos, you should keep the option as limited as possible. You should select Only people you follow can tag you.

Discoverability

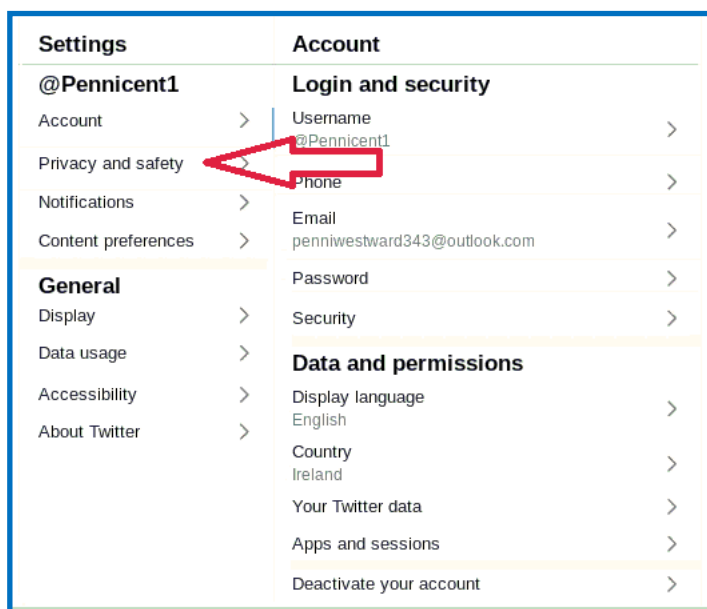
Let Others Find Me by My Email Address and My Phone Number

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

If the option to be found by either your email address or telephone number is enabled, it could be possible for any Twitter user to locate your profile using these data points. This option should be turned off for both contact methods.

To change discoverability, from the Settings and Account menu:

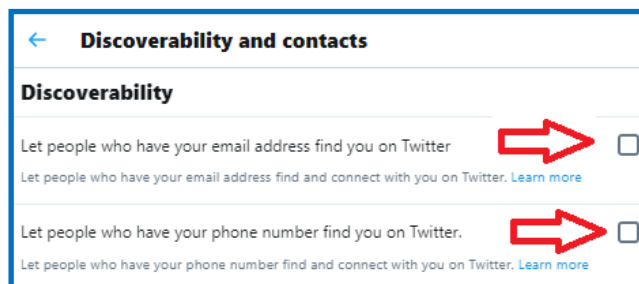
1. Click **Privacy and safety**.



When disabled, the option boxes will be empty.



2. Scroll down until you find the Discoverability and contacts menu.
3. Click **Discoverability and contacts**.



4. Disable **Let people who have your email address find and contact you on Twitter**.
5. Disable **Let people who have your phone number find and connect with you on**

Your Twitter Archive

Perhaps, over the years, you've 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.
- You can download your Twitter archive once every 30 days.


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


1. Click **Your Twitter data**.

Settings	Account
@Pennicent1	Login and security
Account >	Username @Pennicent1 >
Privacy and safety >	Phone >
Notifications >	Email penniwestward343@outlook.com >
Content preferences >	Password >
General	Security >
Display >	Data and permissions
Data usage >	Display language English >
Accessibility >	Country Ireland >
About Twitter >	Your Twitter data <
	Apps and sessions >
	Deactivate your account >

Download your Twitter data

Please enter your password in order to get this.


Password 

[Forgot password?](#)  **Confirm**

2. Enter your password.
3. Click **Confirm**.

Download an archive of your data

You can request a ZIP file with the information that we believe is most relevant and useful to you. You'll get a notification and an email sent to [pennwestward343@outlook.com](#) with a link when it's ready to be downloaded. The file will include a README.txt describing in detail the data contained in your archive and how to navigate it. [Learn more](#)

Twitter  **Request archive**

Periscope **Request archive**

4. On the Twitter line, click **Request archive**. (Periscope is an entirely different application and not included in this Cybercrime Prevention Flyer.)

Twitter

We're getting your data ready. You won't be able to make another request for 30 days.  **Retrieving archive**

5. The **Request archive** button changes to **Retrieving archive** when the archive collection process begins.
6. Check your email for notice that the archive is complete and follow the directions there to download it.

[Everything you need to know so you can use Twitter like a pro](#) — Twitter Help Center

To receive future MCU Cybercrime Prevention Flyers, send an email to: usarmy.belvoir.usacidc.mbx.mcu-cyber-crime-intelligence@mail.mil with "SUBSCRIBE: CPF" in the subject line.

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.