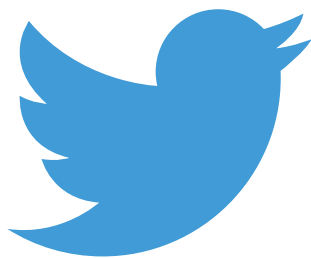# Media Literacy and Digital Security

Twitter Best Practices

OAS

More rights for more people

Media Literacy
and Digital Security

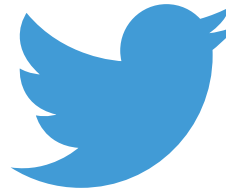*Twitter Best Practices*

Media Literacy
and Digital
Security

*Twitter Best
Practices*

CREDITS

OAS | More rights for more people

Luis Almagro
Secretary General
Organization of American States (OAS)

Francisco Guerrero
Secretary for Strengthening Democracy
Organization of American States (OAS)

Farah Diva Urrutia
Secretary of Multidimensional Security
Organization of American States (OAS)

OAS Technical Team

Alison August Treppel
Gerardo de Icaza
Gonzalo Espariz
Belisario Contreras
Miguel Angel Cañada
Yeruti Méndez
Rolando Ramírez
Kerry-Ann Barrett
David Moreno
Mariana Cardona
Diego Subero
Jaime Fuentes
Geraldine Vivanco
Diego Paez

Jack Dorsey
CEO
Twitter

Colin Crowell
Global VP for Public Policy and Philanthropy
Twitter

Twitter Technical Team

Andrea Pereira Palacios
Hugo Rodriguez Nicolat

@TwitterSafety

INDEX

Media Literacy
and Digital Security

Twitter Best Practices

INTRODUCTION

In the digital and social media era, availability of information is both immediate and abundant. These two features help us keep up to date, at once, with what is happening in the world, but in order to receive and process all the information currently within our reach, we need to develop certain skills, and understand the media on which it circulates.

To help you comprehend certain tools, accessible to you, to be able to develop these skills and attain digital literacy, Twitter and the Organization of American States (OAS) have prepared this guide on Digital Literacy and Security. We present the best practices on account security, and on monitoring, consumption and distribution of information, as well as tips to keep you safe on Twitter.

We would like you to be part of the conversation and to be able to do it safely and responsibly. We hope this guide offers you a starting point but you must bear in mind that the technology and tools available for use are constantly developing. Therefore, always be aware of product and policy updates that may affect your performance and engagements in digital media and social networks.

PART 1:
Digital Literacy

What is Digital Literacy?

According to Common Sense Media, digital literacy is the ability to effectively find, identify, evaluate and use information in digital media.[1] Basically, it is the same traditional definition of literacy, but adapted to the digital age and non-traditional information sources.

The 2016 UNESCO yearbook on "Media and Information Literacy for the Sustainable Development Goals," refers to the "Five Laws of Media and Information Literacy":

1. Information, communication, libraries, media, technology, the Internet and other sources of information providers fall into the same category. Neither is more relevant than the other nor should be treated as such.

2. Every citizen is a creator of information or knowledge and has a message. They must be empowered to access new information and express themselves.

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

3. Information, knowledge and messages are not always value neutral, or independent of biases. Any conceptualization, use and application of digital literacy must make this truth transparent and understandable to all citizens.

4. Every citizen wishes to know and understand new information, knowledge and messages, as well as to communicate, and his/her rights should never be compromised.

5. Digital literacy is a lived and dynamic experience and process. It is complete when it includes knowledge, skills and attitudes, when it covers access, evaluation, use, production and communication of information, media and technology content.
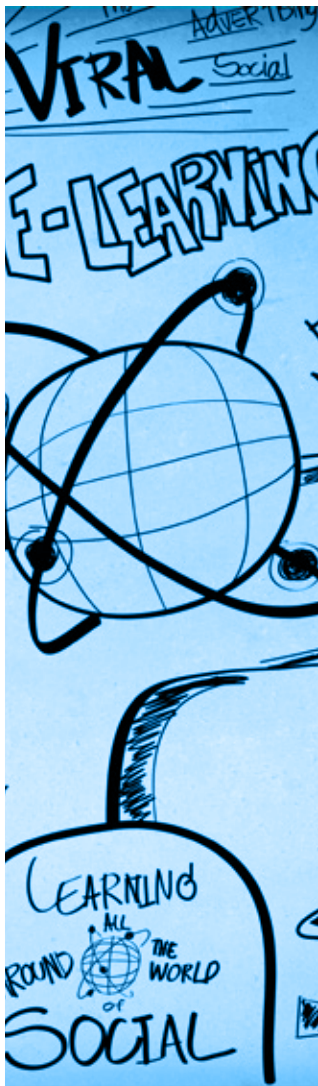
How do we achieve digital literacy?

In the UNESCO yearbook, 10 skills must be developed to achieve digital literacy, or as the document defines it: media and information literacy (MIL).[2] These skills are:

• Engaging with information regarding media and technology.

• Being able to apply technical information communication skills to process information and produce media content.

• Using the information, ethically and responsibly, and communicating the acquired understanding or knowledge to an audience or readers in appropriate form and media.

• Extracting and organizing information and content.

• Critically evaluating the information and content presented in the media and other sources of information, including online media, in terms of authority, credibility, purpose and possible risks.

• Locating and accessing relevant information and content.

• Synthesizing ideas extracted from content.

• Understanding the conditions under which those ideas or functions can be fulfilled.

• Understanding the role and functions of the media including online media in society, and its development.

• Recognizing and articulating the need for information and media.

PART 2:

Securing Your Device While on Social Networks

The Internet is a tool that has transformed and defined communication in the 21st century. Through its multiple interfaces, the Internet has been successful for both individuals and organizations to connect, communicate and exchange information. Technology platforms and social media networks have accelerated the speed through which users can access and retrieve information, simplifying the process in which news is disseminated, updated, and even communicated. Nowadays, it is practically instantaneous to become aware of a news event without being necessarily communicated to traditional means such as newspapers or radio. The ease through which people are now able to communicate has brought a sense of democratization to freedom of speech. Transforming freedom of expression by creating new capabilities to create and edit content has generated new possibilities for alternative journalism; new capacities for organization and mobilization (which largely support other rights, such as freedom of association); and new possibilities to innovate and generate economic development (supporting social and economic rights).[3]

Yet, this facility in the exchange and creation of information also presents challenges to both organizations and individuals that are users of such networks, both as source and as end-user. These challenges vary in scale, but all of them are equally significant. Some of the more prominent ones include the challenge of superficial quality of information, susceptibility to misinformation, and

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

exposure to cyberattacks. Therefore, the need to mitigate and maintain the integrity of this information has become a growing area of work for many public and private organizations.

This section provides an array of techniques and best practices to mitigate and counter the above-mentioned challenges. However, it is important to keep in mind, when reading these recommendations, the position you represent or are associated with. Some of the recommendations may not be applicable to a public figure such as politicians, activists or other actors whose social media best practices are subject to greater scrutiny. In this sense, the exercise of the rights of expression, assembly and protest should, and must be, respected in the digital realm while ensuring safer practices of the internet.

Check Your Privacy Settings

Managing the privacy settings of social networks is one of the simplest forms a user can employ to control the security and privacy of the devices and data. Prior to engaging in any social network, it is crucial to thoroughly read the privacy agreements and check the settings when signing up.

Not only by reading the privacy agreements will the user become aware of what data is or is not shared, but it also provides the option to select or deselect privacy, security or administrative options to secure the account and device.[4] These are some general recommendations to keep in mind to better manage the privacy settings of a social media account:

• Select who has viewing access to the past, present and future social media activity (e.g. Tweets, likes, etc.).

• Review what content can be added (i.e. tagged) into an account when this is uploaded or posted by other people.

• Review, understand and define the audience with whom content can be shared.

• Review, understand and determine the forms through which other users can find and connect with your account.

• Review, understand and determine the amount of personal information when blogging or posting information online.

• Periodically monitor the security and login information of the accounts and revise the likelihood of any suspicious activity.

• Select a trustworthy backup, which could detect or be alerted of any suspicious activity.

• Monitor if and what apps are able to access any of your social media data and/or information, especially in the background.

• Be mindful of the implications of including location when posting content on line.

• Set up a two-factor authentication to log-in.

• Review the platform privacy policy to know what data the services collect, with whom it is shared, and select your preferences on both these issues.

Manage Your Profile Online; Personal Information Included

When creating into a social media account, by default, all information included under a profile becomes public, meaning that any content which has been included into an account could be accessed by anyone. However, the needs and preferences for privacy vary from person to person. While some users prefer having greater exposure and being able to promote their social media content, others prefer including very little or no information. For better protection of the user and the user's information, it is important to assess the extent to which the person is willing to include personal information in their profile. Nevertheless, consider the following when:

• Selecting a username: The username is the "digital name" which a person assigns to him/herself or the person's organization in order to be identified online. If there is a preference for not being easily identified in any platform but being able to continue using these networks, a person is able to assign and use a pseudonym which can be related or unrelated to such person. Additionally, a person is able to change his/her username at any point just by going into the configuration of that person's account(s). A username does not have to be consistent in all social media networks; these can vary depending on the person's preference in each.

• Including a picture into the account: A user has the option to personalize an account by including a profile picture. When a user prefers not to be identified, it is suggested to choose a picture in which he/she is not able to be recognized, and change whenever necessary. Take into account that when using the same picture across all social media networks, a simple image search can detect other accounts.

• Including a location: When the location services are activated in a social media platform, it allows users to trace the origin of any online media activity. It is important to keep in mind that once this function is activated, it will remain on until user chooses to disable it in the privacy settings. Despite allowing this feature to be active in the past, platforms have the functionality of disabling the location of any content that has been published in the accounts. Nevertheless, even if the user activates or deactivates the sharing of location function, potentially, a user's location can be revealed by the content shared or the images chosen to be shared. [2]

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices
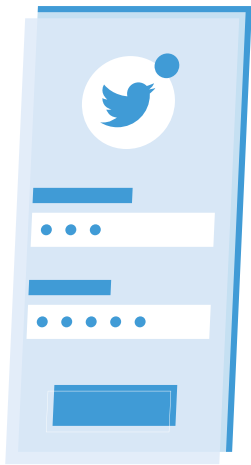
Password Do's and Don'ts

The password is the most essential piece of information required to access all electronic information, whether personal or non-personal. Having a strong password often contributes to securing access to social media accounts. Consider the following when creating or maintaining your password secure.[5]

| Do's	Don'ts
• Passwords are best when they incorporate a combination of words, numbers, symbols and both upper- and lower-case letters. • Use words or phrases that are not associated with the owner of the account. • Use a private browser when accessing sites on a public device that require you to enter your login credentials (name and password).	• Refrain from using a single or similar password for all accounts. • Avoid using the same name of your network as a password. • Do not reuse or recycle passwords. • Abstain from adding personal information when creating a password (e.g. date of birth, unique country registry code or relatives' names). • Do not store a list of passwords in your computer or personal electronic device. • Do not send passwords online or via text. • Avoid sharing passwords. If you suspect someone has come across your password, change it immediately.

Use of Password Managers

A password manager has two main roles: (1) storing passwords, and (2) generating strong and unique passwords. This application is essentially like a digital book which stores all of your passwords using a "master key." By entering this key, access is granted to the rest of the passwords. Therefore, such key or password has to remain highly protected. But its second use is much more practical. The password manager automatically generates passwords which contain a complex combination of uppercase and lowercase characters, numbers, symbols and special characters, which can complicate the unscrambling or detection of the password by hackers. The use of a password manager prevents the common error of using a single password across the various online platforms, thus averting credential stuffing attacks.

Blocking and Filtering

Utilizing blocking, reporting and filtering for emails, posts, as well as users, allows the social networking services to monitor and ensure that the services remain safe, secure and resilient. Every time a user or a post is blocked, it allows the social media platform to impede similar content from reappearing in your account's (or any other account) feed. Refrain from simply ignoring suspicious content: it is best to report it on an ongoing basis, and when necessary, report serious threats to law enforcement.[6]
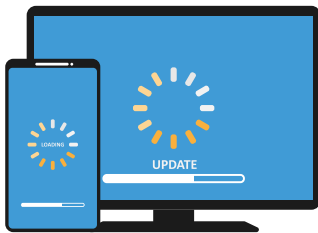
Update Your Device Software

It is highly recommended for the software of any device to be updated as often as possible. Not only will it be faster and afford a better experience; it will provide better security. Updating the software can lead to protection from scams, viruses, Trojans, phishing attacks, among many other threats. Additionally, it can quickly resolve all vulnerabilities which previous versions of the software may not be able to counter.[7]

Use of Antivirus

Because the internet is an open network, any computer or device can connect from anywhere. The use of antivirus software serves as an initial scanner of any suspicious or malicious activity to which users are exposed, through social media. Antivirus software can aid in overseeing the newsfeed and can provide an added level of protection for the user from wrongfully clicking on suspicious links which may contain spam and different types of viruses such as worms.[8] However, having anti-virus software installed is not a blanket protection as it cannot catch all malware; a device can still

become infected. But it still adds a layer of protection that can be beneficial to the user. That is why it is critical to use common sense and be wary of any messages that seem odd or suspicious.[9]

VPN Use

A Virtual Private Network, or VPN, is another tool through which internet activity can remain undisclosed or hidden to cyber threats, such as hacking. A VPN encrypts data and information while it travels from one place to another on the internet. By using a VPN, internet users connect to a unique IP address, allowing the initial IP connection or address to remain hidden.[10]

Encryption of information is the process of converting internet data into a code. The level of encryption or coding may vary according to the difficulty assigned by the VPN. Despite most government information being encrypted at the most secure combination, there are lower-tier combinations used for personal devices. Ciphering grants any activity privacy and security. The information remains encrypted between the device and the server to which it is connected to VPNs.

If you are not able to connect through a VPN, remember to use caution when connecting. Delete all emails, Tweets and posts which look suspicious; connect only to trustworthy WiFi hotspots; and if connected to a WiFi hotspot, limit the type of business you conduct while connected. And when connected, look for web addresses with https://, which means the site takes extra measures to keep information secure. Http:// is not secure.

The above are just some of the means by which an individual or an organization can be proactive in ensuring high levels of cybersecurity in social media and electronic devices. Yet it is the responsibility of every user to remain informed and continually revise privacy settings, update passwords, antiviruses and VPNs to mitigate any risks associated with the use of social media.

PART 3:

Distribution and Consumption of Information on Twitter

Twitter is what is happening and what people are talking about right now. With so much information available, we know that sometimes it can be complicated to keep up with the conversation. We have prepared different tools to help you keep up with what is happening in a simpler way: TweetDeck, Lists, Advanced Search, Notifications, Bookmarks.

In the next section, we provide recommendations to implement when you are consuming information on Twitter, as well as tips on the use of different tools and best practices.

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Verification of information on Twitter

On Twitter, you can check information and verify accuracy in no time at all. As an open and public platform, you can converse with other people or search a hashtag[11] or keyword quickly, to allow you to assess the authenticity of the information you receive.

When reading information, it is important to consider our own prejudices and be aware of our reactions. Often, when we read information with which we disagree, we naturally ask ourselves certain questions that support us refuting that information. The problem is that we generally do not conduct this scrutiny when we read something that confirms our ideas and prejudices. That is why we must get into the habit of always asking ourselves the who, what, where, when, how and why of a piece of news or information.

Who ------------------------------
Who is the source?
Who writes the article?
Is the person a journalist, academician, or what is the writer's profession?

What ------------------------------
What did they say?
What are their motives?
What kind of article is it: news or opinion?
Is the article intentionally false or a joke?

Where ------------------------------
Where did they say it?
Is it a reliable source?
What is the website URL? Https:// or http://?
What other media or people covered this news?

When ------------------------------
When did they say it?
When was it published? Maybe it's old news, is it dated?

Why ------------------------------
Why was the news published?
Is it to generate traffic?
Is it to provoke an action? If yes, whose?

How ------------------------------
How is it written?
Does it have excessive punctuation marks and capital letters?
Is the headline deceptive?
Does it have a conspiratorial tone?

---

11. Hashtags (written with the "#" sign before the word) are used to index keywords or topics on Twitter. This feature was created by Twitter and it allows users to easily find content around the topics that interest them.

Twitter Tools for Information Consumption

TweetDeck

TweetDeck is the most powerful Twitter tool to monitor conversations in real time, organize them, and engage. Its flexibility and customizable design to have several timelines in a single interface allows you to keep up to date on what is happening on Twitter, on multiple topics and accounts, in real time.

How to start using TweetDeck
1. Go to http://tweetdeck.twitter.com or open the desktop app for Mac.
2. Log in with your Twitter account. We recommend that you use a Twitter account that is not shared with other people.
3. When you are logged in, you can connect multiple Twitter accounts to your TweetDeck account.

Using TweetDeck columns
Instead of a single timeline, TweetDeck allows you to add columns to show specific content that interests you and view them side by side. Add columns that show, for example, all your Mentions, Search Results, a list of Likes, the latest Tweets from a hashtag or a trend, etc. You can also create columns with information based on actions from other accounts, such as their Mentions, Lists, or Tweets marked Like. The column options are:

- Home - Home timeline for any specific account
- User - Tweets from a specific account
- Notifications
- Search
- Lists
- Collections
- Trending
- Likes
- Messages
- Mentions
- Scheduled

Add and remove columns
To add a column, click ➕ in the navigation bar and select "Add column." Then, select the type of column you would like to add.

To remove a column, click ⚙ in the column header next to the column title and then click the "Remove" button to remove the column.

Column filters
You can easily control the type of Tweets you would like displayed in each of your columns. You can select from Content, Location, Users, Engagements or Alerts; or a combination of all.

- The **content** filter allows you to filter the column according to a certain type of Tweet, such as Retweets, Tweets containing a specific word or phrase, or Tweets with photos.

- The **location** filter allows you to filter for Tweets geotagged in specific locations.

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

• The **user** filter allows you to filter Tweets within a specific column written by a certain author and those they mention.

• The **engagement** filter allows you to filter Tweets with a minimum number of Retweets, likes or replies.

• The **alert** filter allows you to enable pop-ups or sounds for a particular column.

> *Note:* *If you create a search column, you can also filter results by location, date and engagement. When applying location filters, keep in mind that only unprotected Tweets geotagged with a location will appear in search results.*
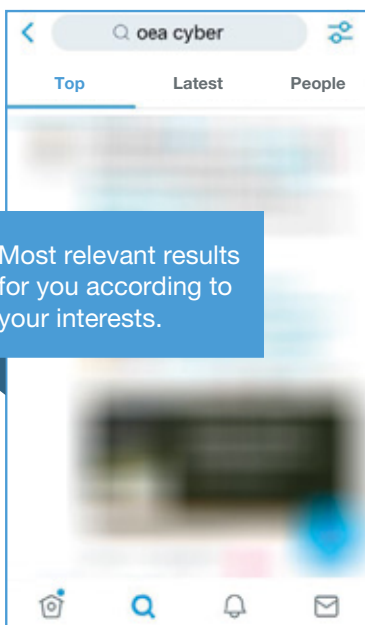
Search Results

Every time you do a search on Twitter, either from twitter.com or from the application, you will receive results that can be filtered according to when they were shared, or to the type of content.
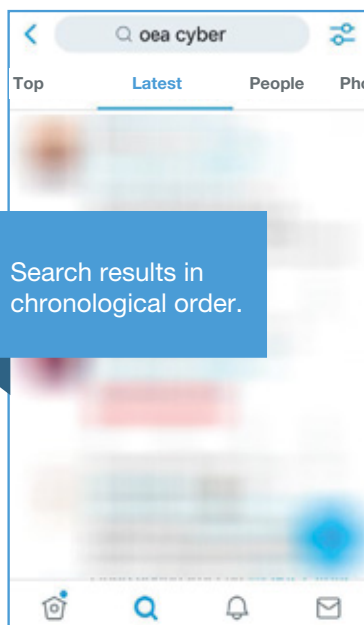
Each search will give you the following options to filter using different tabs that are displayed at the top of the search. These filters are applied using an algorithm; a manual selection of search results is not made.
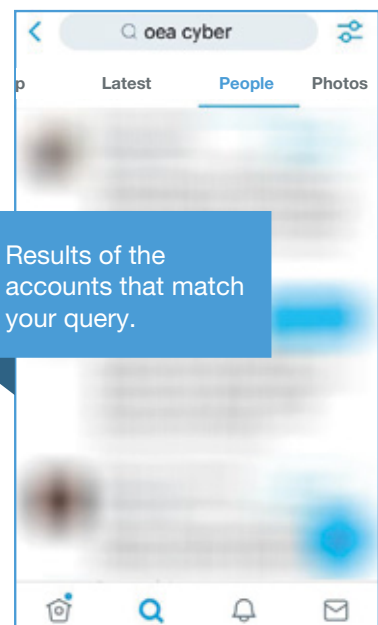
The tabs give you the option to see the Tweets:

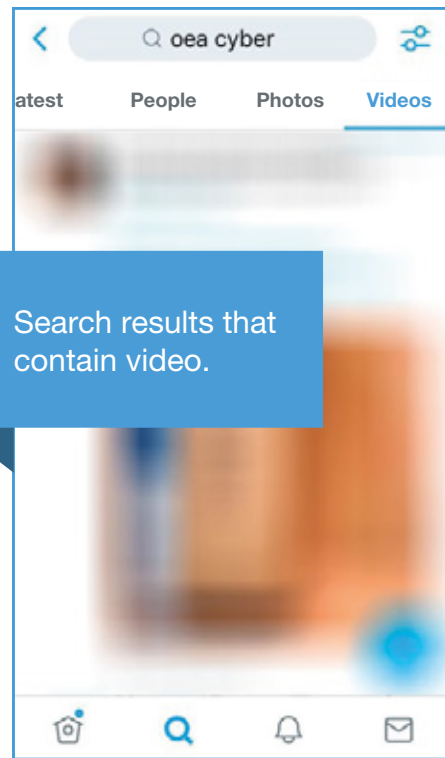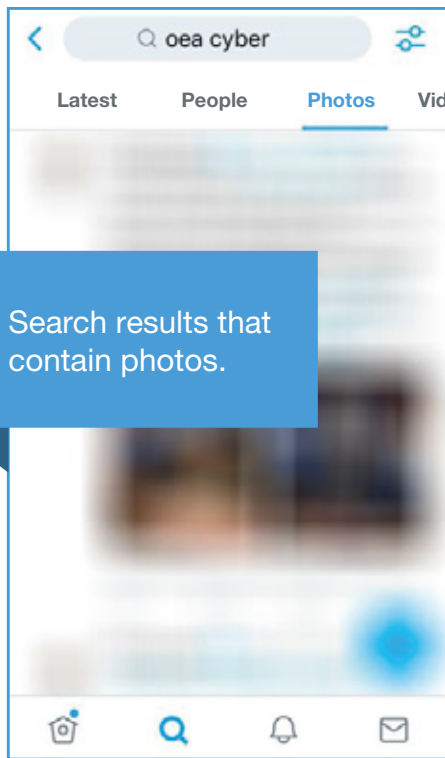• Top • Latest • People • Photos • Videos

Most relevant results for you according to your interests.

Search results in chronological order.

Results of the accounts that match your query.

Search results that contain photos.

Search results that contain video.

Advanced Search

Both on TweetDeck and on twitter.com or in the app, you can use advanced search. This allows you to customize the search results according to certain ranges of dates, people, etc., to find the content you are seeking, more straightforwardly and faster.

On twitter.com, after entering your search item in the search bar, you can click on the top of the results page in the drop-down menu for more options and then on Advanced search. A series of fields are displayed for you to refine your search.

You can also do specific searches from TweetDeck or from the app using the following formulas in the search bar:

According to the Tweet content:

Occurring now	*contains both terms occurring and now*
"Occurring now"	*contains the exact phrase "Occurring now"*
Tuesday OR Wednesday	*contains the term Tuesday or Wednesday (or both)*
Advanced -search	*contains advanced but not search*
#Live	*contains the hashtag #Live*

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

	contains traffic and asks a question
Traffic ?	*traffic filter:media contains traffic and an image, video or GIF. For a more specific search of multimedia content you can place after filter: native_video, periscope, images, or links*

According to the Tweet information and engagements:

near:Bogotá	*posted near Bogotá and not protected with geotagging. For a more specific search you can also add: within:15km, to see the Tweet published within a 15km radius near Bogotá*
autos since:2015-12-21	*contains autos and was published starting on 2015-12-21 (year-month-day)*
#Live until:2016-06-23	*contains #Live and was published before 2016-06-23 (year-month-day)*
From:jack	*posted from the @jack Twitter account*
list:CruzRojaVe/medios	*posted from a Twitter account included in the @ CruzRojaVe List titled media*
to:jack	*responding to the @jack Twitter account*
@jack	*mentioning the @jack Twitter account*
traffic filter:verified	*only Tweets of verified users with the term traffic*
traffic source:tweetdeck	*contains traffic and was published from tweetdeck. Other options are: twitter_for_iphone, twitter_for_ android, and twitter_web_client*
traffic min_retweets:5	*contains traffic with a minimum number of 5 Retweets*
traffic min_faves:10	*contains traffic with a minimum number of 10 likes*
traffic min_replies:100	*contains traffic with a minimum number of 100 responses*
traffic filter:nativeretweets	*Retweets containing the term traffic*

Bear in mind that all of these formulas can be excluded from your search results using the "-" symbol before it. For example, if you would like @NASA Tweets with multimedia content excluding photos, you can use the search:

*from:NASA filter:media -filter:images.*

You can also combine the formulas above. For complex combinations, use parentheses to add different filters. For example, if you would like to see:

Tweets that use the terms dog or cat, together with the terms love and hate, excluding Retweets, and with at least 10 likes, you can use the search:

(dog OR cat) AND (love OR hate) -filter:nativeretweets min_faves:10

Tweets that use the term traffic and also the terms from or to, published by members of the @ CruzRojaVe Media list, sent from an iPhone or from twitter.com, with images, excluding the term avoid, you can use the search:

traffic (from OR to) list:CruzRojaVe/medios (source:twitter_for_iphone OR source:twitter_web_client) filter:images -avoid
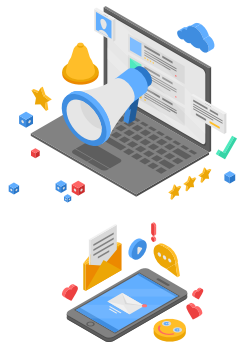
Push Notifications

On Twitter, you can receive a lot of information, but we know that there are certain accounts the Tweets of which you would not like to miss. This is why we have set up Push Notifications, which will inform you when the selected accounts you follow publish Tweets. You have the option of selecting to activate Push Notifications for all Tweets of a specific account, or only for Tweets containing live broadcasts, from Periscope. These notifications can be activated and deactivated at any time as follows:

To receive notifications when an account you follow posts a Tweet or streams a live video:

1. From the account profile, tap 🔔 .

2. From twitter.com, you can only activate all types of notifications. From the app, you will have the option of choosing between two notification types: All Tweets or Only Tweets with live video.

To cancel Tweet Notifications for accounts you follow, return to the account profile, tap the highlighted 🔔 and select None.

You can view Tweet notifications from accounts you follow, at any time, from twitter.com or from the app:

1. In the top menu, tap your profile icon.
2. Select Settings and privacy.

3. Tap Notifications and then tap Push Notifications.
4. Tap Tweets.

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Bookmarks

From articles and threads, to videos and GIFs, timelines are full of Tweets that you don't always have time to fully explore. That is why we have the Bookmarks.

To Bookmark a Tweet, click ⬆ below the Tweet and select Add Tweet to Bookmarks. When you would like to go back it, select Bookmarks from your profile settings. You can remove Tweets from your Bookmarks at any time. In addition, only you can see what you have bookmarked. This feature helps you keep up with the best of Twitter, with the content you need more time to explore, or merely one you would like to save for later reference.

Timeline of Top Tweets vs. Latest Tweets

When you see your timeline on Twitter, you see the most relevant Tweets, according to your interests, at the top. However, sometimes you may want to see the Tweets in chronological order, that is, see the latest Tweets first. This not only depends on your preferences, but also on the information you are looking for. For example, during a sports event or in crisis and emergency situations, it is more useful to receive the most current information.

Therefore, on Twitter you have the possibility to change your timeline settings between Top Tweets and Latest Tweets. To do this, press the ✦ in the upper right corner and choose the option of your preference.

Note that the default option is Top Tweets, so if you have changed your preference to Latest Tweets and stop using Twitter for a while, the settings will automatically revert to Top Tweets.

Lists

A List is a filter that shows you a customized timeline displaying only the Tweets of the accounts on that List. You can create your own lists or subscribe to lists created by other users. Likewise, lists can be private, for your own monitoring, or public, to share information with other people about specific groups of accounts.

Create a list:

1. Click on your profile ⊛ to open the drop-down menu.
2. Click Lists.
3. Click Create new List.
4. Choose a name for your List and write a brief description. The name of the List cannot exceed 25 characters or begin with a number. Specify if you would like the List to be private (only you will be able to see it and access it) or public (anyone can see and subscribe to the List).
5. Click Save List.

Add people to a List – You don't need to follow an account to add them to your List.

1. Click the ⊙ in their profile page.
2. Select Add/remove from Lists. A pop-up window will display the lists you have created.
3. Click the checkbox next to the lists you would like to add the account to, or uncheck the box or boxes next to the lists you would like to remove the account from.

Edit or delete a List:

1. Go to your profile page.
2. Click Lists.
3. Under Subscribed to, you will see the lists you have created and other people's lists that you follow.
4. Click or tap on the list you would like to edit or delete from the lists you have created.
5. Click or tap on Edit to update your list details or Delete to remove the list entirely.

Subscribe to other people's Lists:

1. Click the ⊙ in the other person's profile.
2. Click Lists.
3. Select the Lists you would like to subscribe to.
4. On the Lists page, click or tap the Subscribe option to follow the List. You can follow a List without having to follow each of the accounts that are part of that List.

Twitter Best Practices for Information Consumption

As mentioned earlier, we must acquire the habit of always asking ourselves certain questions about any information we receive to assess veracity, and this is no different with Twitter. Here are some specific questions relating to Twitter that you can ask yourself before sharing a content.

Pause, read carefully and analyze the information before sharing it, Retweeting it, Tweeting with comment, or giving it a Like. And ask yourself:

Who

Do you know the person or organization that is sharing the information and do you know whether or not it is a reliable source?

Go to their profile and check bio, location, account age, previous Tweets and the engagements they have received. Is it a verified account? Who does it follow and who is following it? What is the website appearing in the profile? If the profile is suspicious, go to their website.

- *Pay attention to the website URL. Organizations, institutions, and media generally have standardized domains which you are probably familiar with. Sites with endings like ".com.co" should make you doubt their legitimacy and prompt you to find out more about them and their sources. This is true even when the site looks professional and has semi-recognizable logos. For example, abcnews.com is a legitimate news source, but abcnews.com.co is not, despite its similar appearance.*

- *Read the About us section. Most sites will have a lot of information about the organization, its administration, mission and objectives. You should also be able to find more information about the organization and its leaders on other websites.*

What

Does the Tweet reflect an opinion or information?

Information: Is it sharing an article or stating where you can get more information?

- *Read beyond the headline, and review the comments. Headlines are intended to get readers' attention, but they are also expected to accurately reflect what the story is about. This is not always the case. Headlines are often written in an exaggerated language that can be quite misleading, so it is very important to scan the story and not get carried away by the headline.*

- *Look at the quotes–or lack thereof–in the story. The majority will have multiple sources, coming from professionals with experience in the field they are writing about. The quotes will mention other sources you can check to verify the information.*

• Are the people being quoted a reliable source, with a title that can be verified through a quick search? Search those quotes to find the context. Learn what the entire speech or article was about, to whom it was addressed and when it happened.

How much interaction did the Tweet have? - Watch for Retweets and likes.

What responses did the Tweet receive? While responses should not be considered a reliable source of information without first studying it more in depth, seeing other people's responses will give you a good idea of the reactions to the news and you may find comments that dismiss it if it is false or misleading.

When
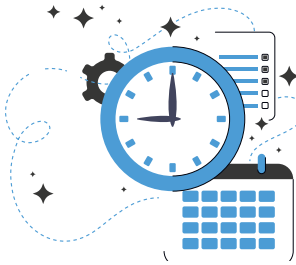
Be sure to look at the date of the Tweet(s) to know if the content is current or if the date is relevant to the information being shared.

How

How is the content presented? Is it an RT, a QT, a thread, a Moment, a video, a live broadcast, or is it sharing a link to a web page?

Is it using hashtags relating to the topic? Be careful if the Tweet is using a hashtag that is trending without it relating to the information being shared, since this is a deceptive strategy to get people's attention.

Why

What seems to be the motivation to share the information?

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Best Practices for Authorities and Organizations When Sharing Information

For individuals, tweeting their status is a quick way to reach the maximum number of people and corresponding authorities, with minimal effort. For organizations and authorities, Twitter is the fastest way to spread the most important information, to the largest number of people.

To use Twitter effectively it is necessary to have a good content plan and be consistent. Your daily communications help you grow your audience and credibility for when you need to share key and perhaps urgent information.

- **Update your name and profile information:** bio, location and website

- **Add a header and profile picture.**

- **Define your tone.** Share who you are and/or what the purpose of the institution is, show your voice to the world. Start a conversation, not a speech. People go to Twitter to chat with you; if they simply wanted to know what you or your organization have to say, they would visit your website.

- **Set your best Tweet.** You can set one of your Tweets at the top of your profile so that your followers know what topics interest you most. Change it as many times as you wish.

- **Engage with other users.** Basic interactions (Likes, Retweets, mentions and replies) will help to develop conversations around the topics that interest you.

- **Tweet multimedia content.** Post Tweets with photos and videos, and share a small part of your day to day. Remember to share native videos and not from other platforms.

- **Broadcast news.** People come to Twitter to find out "what's going on." Take advantage of this and use Twitter to give first-hand news and share official announcements (use the Twitter Threads).

- **Discuss live events.** Participate in the moment when it comes to breaking news, unexpected situations, specific moments, etc.

- **Make question sessions.** Encourage your followers to send questions and use Twitter as a direct channel to answer them and to educate about the topics you are working on.

- **Stream live with Periscope.** Stream live from Twitter and allow your followers to be part of what is happening.

PART 4:
Safety on Twitter

Twitter is a space of free expression, where we want people to communicate openly and freely. To ensure that people feel safe in expressing various opinions and beliefs, we have rules in the use of our service to improve the health of public conversation and prevent voices from being silenced. In this section we explain our rules, as well as tools that help you control your Twitter experience.

Twitter Rules

Twitter reflects the real conversations that are happening in the world, and this sometimes includes perspectives that others may find offensive, controversial or intolerant. While we accept that all express themselves on our platform, we do not tolerate behaviors that use harassment, intimidation or fear to silence other people's voice. Our rules are intended to ensure that all people can participate in the public conversation freely and safely. Our rules are divided into three main categories: safety, privacy and authenticity:

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Safety

- ***Violence:*** You may not threaten the use of violence against an individual or a group of people. We also prohibit the glorification of violence.

- ***Terrorism/violent extremism:*** You may not threaten or promote terrorism or violent extremism.

- ***Child sexual exploitation:*** We have zero tolerance for child sexual exploitation on Twitter.

- ***Abuse/harassment:*** You may not engage in the targeted harassment of someone, or incite other people to do so. This includes wishing or hoping that someone experiences physical harm.

- ***Hateful conduct:*** You may not promote violence against, threaten or harass other people on the basis of race, ethnicity, nationality, sexual orientation, gender, gender identity, religious affiliation, age, disability or serious illness.

- ***Suicide or self-harm:*** You may not encourage or promote suicide or self-harm.

- ***Sensitive media, including graphic violence and adult content:*** You may not post media content that is excessively gory or share violent or adult content within live videos or in profile or header images. Media depicting sexual violence and/or assault is also not allowed.

- ***Illegal or regulated goods or services:*** You may not use our service for any unlawful purpose or to promote illegal activities. This includes the sale, purchase or facilitation of transactions of illegal goods or services, as well as certain types of regulated goods or services.

Privacy

- ***Private information:*** You cannot publish other people's private information (such as home phone number and address) without their authorization and permission. We also prohibit threatening to disclose private information or encourage others to do so.

- ***Non-consensual nudity:*** You cannot post or share intimate photos or videos of another person that were produced or distributed without that person's consent.

Authenticity

- ***Spam and platform manipulation:*** You may not use Twitter's services for the purpose of artificially amplifying or suppressing information, or carrying out actions that manipulate or disrupt the user experience on Twitter.

- ***Election Integrity:*** You may not use Twitter services for the purpose of manipulating or interfering in elections. This includes posting or sharing content that can deter voter participation or mislead people about when, where or how to vote.

• *Impersonation:* You may not impersonate individuals, groups or organizations in a way that is intended to, or in fact, does confuse, deceive or mislead other people.

• *Copyright and trademark:* You may not violate the intellectual property rights of others, including copyright and trademark.

More detailed information about our rules is available in our Help Center https://twitter.com/rules. Always keep in mind that we may have to change our rules occasionally to support our goal of fostering a constructive public conversation. The most updated version is always available at https://twitter.com/rules.

Enforcement of our Rules

We can take action at the level of the Tweet, the Direct Message and the account; we may even use a combination of them. In enforcing our rules, we assume that people do not intentionally violate our Rules. Unless a breach is so flagrant that it forces us to suspend an account immediately, we first try to educate people about our Rules and give them the opportunity to correct their behavior. We show them the Tweet(s) that violate our policies, we explain which Rule was broken and we request removal of the content in order to be able to Tweet again. If a person violates our Rules repeatedly, our enforcement measures become more serious. Some of the measures we can take are the following:

Tweet-level enforcement:

We take action at the Tweet level to ensure that we are not overly harsh with an account that made a mistake and violated our Rules but, which otherwise, has not presented problems. Among the actions we may take at the Tweet level, are the following:

• **Limiting Tweet visibility.** This measure reduces the visibility of content on Twitter, in search results, in replies and in timelines. The decision to limit the visibility of the Tweet depends on a series of signals about the nature of the interaction and the quality of the content.

• **Requiring Tweet removal.** If we determine that the Tweet violated the Twitter Rules, we require the violator to remove it in order to Tweet again. We send an email notification to the violator, which identifies the Tweet(s) that violate our rules. The violator must eliminate the offending Tweet or appeal our decision if the person believe that we made a mistake.

• **Hiding a violating Tweet while awaiting removal.** In the period between when Twitter takes enforcement action and the person deletes the Tweet in question, we hide that Tweet from public view and replace the original content with a notice stating that the Tweet is no longer available because it violated our Rules. This notice will be available for 14 days after Tweet removed.

Direct Message-level enforcement:

• Stopping conversations between a reported violator and the reporter's account. When one of the participants of a private Direct Message conversation reports the other participant, we will stop the violator from sending messages to the person who reported the violator. In addition, the conversation will be removed from the reporter's inbox. However, the conversation will resume if the reporter decides to continue sending Direct Messages to the violator.

• Placing a Direct Message behind an interstitial. In a group Direct Message conversation, the violating message may be placed behind an interstitial so that no one else in the group can see it again.

Account-level enforcement:

We take account-level action if we determine that a person violated the Twitter Rules flagrantly, or that the person repeatedly violated them even after receiving our notifications.

• Requiring media or profile edits. If an account's profile or media content does not comply with our policies, we may make it temporarily unavailable and require that the violator edit the media or information of the profile to come into compliance. We also explain what policy violated the profile or media content.

• Placing an account in read-only mode. If an account that otherwise has no problems has an abusive behavior episode, we can temporarily modify its settings to be read-only, which limits its ability to Tweet, Retweet or use the Like function, until it calms down. The person can read timelines and can only send Direct Messages to followers.

When an account is in read-only mode, others can continue to view and engage with it. The duration of this enforcement action may vary from 12 hours to 7 days, depending on the type of violation.

• Verifying account ownership. To ensure that violators do not abuse the anonymity we offer and harass other people on the platform, we may require the account owner to verify ownership with a phone number or an email address. This also helps us identify and take action regarding violators who are operating multiple accounts for abusive purposes.

• Permanent suspension. This is the most severe enforcement action. Permanent suspension of an account will cause it to be removed from global view, and the violator will not be allowed to create new accounts. When we permanently suspend an account, we inform the user about suspension for abuse violations, and explain what policy or policies they violated and which content was in violation.

Appeals:

In the case of any of the aforementioned actions, the respondents or violators can appeal our actions if they believe we made a mistake. They can do so through the platform interface or by filing a report

on help.twitter.com/forms. Upon appeal if we find that the suspension is valid, we respond to the appeal with information about the policy that the account has violated.

Reporting Violations to the Rules

If on Twitter you find content that you believe violates any of our rules, please report it. When reporting, remember that the context you can provide is very important. Similarly, keep in mind that not all content that some may consider offensive or intolerant is necessarily in violation of our rules.

When determining whether actions will be taken regarding a report, we may consider a number of factors, including:

- If the behavior is directed at an individual, a group or a protected category of people.
- If the reporter is the subject of the abuse or a witness.
- If the user has a history of violating our policies.
- The severity of the violation.
- If the content is a matter of legitimate public interest.

At help.twitter.com/forms you can find the direct forms for any type of report you would like to make about violations of the Twitter Rules. And you also have direct options from twitter.com and from the application to report Tweets, accounts, or direct messages.

Reporting an account:
1. Open the profile you would like to report.
2. Select the ⊙ .
3. Select Report and then select the type of problem you would like to report.
4. Depending on your selection, we will ask you for additional information selected on the problem you are reporting. In addition, we may ask you to select other Tweets from the same account so that we can have more context to evaluate your report.

Report a Tweet:
1. Navigate to the Tweet you would like to report.
2. Tap the ⚑ located at the top of the Tweet.
3. Select Report Tweet.
4. Depending on your selection, we will ask you to provide additional information on the problem you are reporting. In addition, we may ask you to select other Tweets from the same account so that we can have more context to evaluate your report.

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Report a Direct Message:

    1. Click into the Direct Message conversation you would like to report.

    2. Click the report icon.

    3. Select Report @username.

    4. Depending on your selection, we will ask you to provide additional information on the problem you are reporting. In addition, we may ask you to select other messages from the same account so that we can have more context to evaluate your report.

    5. Once you submit the report, we will recommend other actions you can take to control and improve your Twitter experience.

Control Your Experience on Twitter

Twitter is a place designed for sharing ideas and information, connecting with our communities and seeing the world around us. In order to protect the best aspects of this experience, we provide tools to help you control what you see and what other people can see about you, so you can express yourself with confidence on Twitter.

Muting

Muting another Twitter account means that Tweets from that account will not appear in your timeline. It is a great way to stay connected with friends, even if you are not interested in seeing all their Tweets. Muted accounts do not receive any notice that you have muted them. In addition, you will continue to receive notifications when they mention you in Tweets and send you Direct Messages. You can also mute accounts you do not follow so that you do not see their Tweets in your notification timeline.

Muted accounts have no way of knowing that you muted them, and you can unmute them at any time. To access this option, click the icon on a Tweet and click Mute. To unmute an account, visit the Twitter profile of the muted account, click the Mute icon to unmute. On the Twitter app for iOS or Android, tap Unmute next to "You have muted Tweets from this account."

You can Mute Tweets that contain certain words, phrases, usernames, emojis or hashtags. Muting will cause these Tweets to be removed from your Notifications tab, push notifications, email notifications, Home timeline and replies to Tweets. You will still see these Tweets in searches. To add or remove items from your mute list:

1. Click Settings and privacy in the drop-down menu of your profile image.
2. Click Muted Words.
3. Click Add.
4. Enter the word or hashtag you would like to mute, one at a time.
5. Select Home timeline if you would like to mute the word or phrase from your Home timeline. Select Notifications if you would like to mute the word or phrase from your Notifications.
6. Choose the option From anyone or From only people I do not follow.
7. Under For how long? choose between Forever, 24 hours from now, 7 days from now or 30 days from now.
8. Click Add.

Blocking

By blocking a Twitter account, you prevent that account from interacting with yours. Blocking can be useful to control unwanted interactions from accounts that you are not interested in. The accounts you have blocked will not be able to view your Tweets, your follower or following lists, your likes or lists of selected accounts, when logged in on Twitter. You will also not receive notifications of mentions directly from those accounts. You will also stop viewing the Tweets of those accounts in your timeline.

Users of blocked accounts may notice that you blocked them if they try to visit your profile or follow you, but they will not receive notifications that you blocked them. To access this option, press the icon on a Tweet of that person and click Block.

To unblock an account, visit the blocked account's profile on Twitter, click the Blocked button and confirm that you wish to unblock the account by selecting Unblock on Twitter for iOS or Yes on Twitter for Android.

Notifications Filter

The Notifications timeline shows engagements with other Twitter accounts, such as mentions, Likes, Retweets and who has started following you. If you receive unwanted replies or mentions of accounts that you don't follow, you can filter the types of notifications you receive. In the notification settings, you have three options to filter the notifications you receive: quality filter, muted words and advanced filters.

• When the Quality Filter is turned on, it filters lower-quality content so that it does not appear in your notifications (for example, duplicate Tweets or content that seems to be automated) but it does not filter notifications from the people you follow or accounts you have interacted with recently. You have the option to this on or off in your notifications settings.

 • You can use the muted words option to mute notifications that include specific words and phrases that you do not wish to see in your notifications.

• The Advanced Filters option allows you to disable notifications of certain types of accounts that you would like to avoid. Also, if your account receives a lot of sudden attention, we may insert a notification in your Notifications tab inviting you to adjust these filters in order to give you more control over what you see.

REFERENCES

1. News and Media Literacy: What is Media Literacy, Common Sense Media:
https://www.commonsensemedia.org/news-and-media-literacy/what-is-digital-literacy
(consulted August 18, 2019).

2. Media and Information Literacy for the Sustainable Development Goals.
Grizzle, A and Singh, J. (2016). In the MILID Yearbook 2016

3. Standars for a Free, Open, and Inclusive Internet. IACH, OAS:
http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf
(consulted March 15, 2017).

4. Social Media Guide. Homeland Security, US Government:
https://www.dhs.gov/sites/default/files/publications/Social%20Media%20Guide_5.pdf

5. Password. Get Safe Online Free expert advice:
https://www.getsafeonline.org/protecting-yourself/passwords/

6. Social Media Guide. Homeland Security, US Government:
https://www.dhs.gov/sites/default/files/publications/Social%20Media%20Guide_5.pdf

7. Update Your Browser. Get Safe Online Free expert advice:
https://www.getsafeonline.org/protecting-your-computer/update-your-browser/

8. Privacy. Norton:
https://us.norton.com/internetsecurity-privacy-5-tips-for-social-media-security-and-privacy.html
(consulted in 2019).

9. Security Awareness Tip of The Day. SANS:
https://www.sans.org/tip-of-the-day?
(consulted September 2019).

10. Secure VPN. AVG:
https://www.avg.com/en-us/secure-vpn

MEDIA LITERACY AND DIGITAL SECURITY
Twitter Best Practices

Media Literacy
and Digital
Security
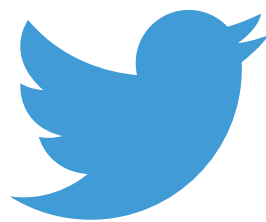
*Twitter Best
Practices*

Media Literacy
and Digital
Security

*Twitter Best
Practices*

Media Literacy and Digital Security

Twitter Best Practices

OAS

More rights for more people