Content Unit

[Personal data protection in social media]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: EDIT VALUE®
Last processing date: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Personal data protection in social media

First introduction

In 2010, the famous comedy show *Saturday Night Live* made a sketch about social media. In it, an actor impersonating Julian Assange (founder of the platform WikiLeaks) stated, in a joyous and sarcastic manner, *"I give you private information on corporations for free, and I'm a villain. [Facebook creator Mark] Zuckerberg gives your information to corporations, for money, and he's [Time Magazine's] Man of the Year*." Do you see a connection of this comedy sketch and reality? How do you feel about providing your data to an enterprise for free while this making money with it. Is our data safe while using social media?

Obviously, in these days, personal data protection in social media is a very important topic. Social media usage is exponentially growing and is now an essential part of day-to-day life for the majority of people worldwide. From our white collar-co-worker to our sweet grandmother, almost everyone uses social media to share photographs, videos and conversations with friends or relatives, publishing personal information overall, and creating a sense of closeness.

However, as social media usage is so embedded in our habits as individuals and society, most people let their guard down when it comes to cybersecurity, which can have serious consequences in a long run.

Who else will see this data?

Therefore, there is plenty to learn about the protection of data and personal information while using social media, as you will see in this content unit.

Practical relevance – This is what you will need the knowledge and skills for

After working through this content unit, you will be able to identify the most relevant privacy risks associated with the use of social networks as well as you'll know how to protect yourself accordingly.

Overview of learning objectives and competences

In LO_Personal data protection in social media_O1 you will learn the most important aspects related to people most important social media rights in some social media networks and the meaning of social media

In LO_Personal data protection in social media_O2 you will be taught what are the most common risks in social media

In LO_Personal data protection in social media_03 you will familiarize yourself with some security tips using social media accounts

Learning objectives	Fine objectives
LO_Personal data protection in social media_O1: You know the meaning of social media and what includes	FO_Personal data protection in social media_O1_O1: You know what is meant by the term social media and what it includes FO_Personal data protection in social media_O1_O2: You know about people most important social media rights in some social media networks
In LO_Personal data protection in social media_O2: You will be taught what are the most common risks in social media	FO_Personal data protection in social media_O2_O1: You can name the most relevant statistics about social media use FO_Personal data protection in social media_O2_O2: You are familiar with the most common risks in social media
In LO_Personal data protection in social	FO_Personal data protection in social

media_03: You will familiarize yourself with some security tips using social media accounts	media_O3_O1: You will see some recommendations about how to stay safe online FO_Personal data protection in social media_O3_O2: You will know some security tips regarding the use of social media accounts

1.Build knowledge - Personal data protection in social media

Definition
Social media are interactive computer-mediated technologies that facilitate the **creation or sharing** of information, ideas, career interest and others forms of expression by creating virtual communities and networks. The purpose of social media is **to connect and share information with anyone on Earth or with many people simultaneously**. It can be used as a way to interact with friends and family or as a marketing tool by businesses. Social media is any digital tool that allows users to quickly create and share content with the other people.

In the box above is presented a broad definition of social media. The reality is, as there are 3.5 billion active social media users worldwide, social media evolved in a way that, currently, it's divided in different categories, in terms of interests and intentions of the user. Next, it is presented a list of 10 types of Social Media, according to their aim:

	Purpose	Example
Social Networks	To connect with people (and brands) online	Facebook; Twitter; LinkedIN
Media sharing networks	To find and share photos, video, live video, and other media online	Instragram; Youtube; Tik Tok
Discussion forums	To find, discuss, and share news, information, and opinions	Reddit; Quora
Content curation network	To discover, save, share, and discuss new and trending content and media	Pinterest; Flipboard
Consumer review network	To find, review and share information about brands, products, and services, as well as restaurants, travel destinations, *etc*	Yelp; Zomato, Tripadvisor
Blogging and publishing network	To publish, discover, and comment on content online	Wordpress; Tumblr
Social shopping network	To spot trends, follow brands, share great finds, and make purchases	Etsy

		Etsy
Interest-based network	To connect with others around a shared interest or hobby.	Goodreads; Last.Fm
"Sharing economy" network	To advertise, find, share, buy, sell and trade products and services between peers	Airbnb; Uber; Glovo
Anonymous social network	To gossip, vent and snoop	Whisper; Ask.fm

There's no doubt that we are living in the age of social media. Because of that, there are **multiple social media legal issues** that arise when people share content online across different platforms such as Instagram, Pinterest, Facebook and so on. The most important social media rights are related to **who owns the content being shared, when and where sharing is appropriate and what limits may be imposed on sharing** often raise issues relating to **trademark infringement, copyright infringement, social media marketing, labor relations** and more. Please find a brief list about the most important social media rights for Instagram, Whastapp, Youtube and Facebook.

1. Officially you own any picture and/or video you post but other people might pay to use them and Instagram will not pay you for that
2. You are responsible for anything you do using Instagram and anything you post
3. Although you are responsible for the information you put on this social media, Instagram may keep, use and share personal information with companies connected to Instagram
4. You can close your Instagram account. If you do, your photos, posts and profile will disappear from your account but if anyone has shared your photos or personal details, or if someone use this type of information for any reason, they might still appear on this social media

1. You can change your profile name, picture and status message whenever you want
2. Anyone who uses WhatsApp may be able to see your mobile phone number, profile name, photo, status, status message, last seen status and receipts. You can change this if you want and you can also use your settings to block people and control who you chat with
3. After your messages are delivered, we delete them from our system and they are only stored on your own phone or device. Your messages are "encrypted" which means that the company that owns WhatsApp can't read them
4. Other companies are not allowed to place advertisements across your WhatsApp screen unless you are connected with them

1. When you create a YouTube account, your data will be collected by Google. You can decide whether Youtube should collect some of this information by going to your Google account “activity controls”. In addition, your personal information stay inside of Google companies without your consent

2. You can ask Youtube for the information that they hold about you and you can ask the company to correct or delete it

3. If you want to make a complain about your appearance in a Youtube video, you can give Youtube the URL of the video, tell the exact time in the video that you or your information appears and explain why you stand out from other people in the video

4. If someone complains about a video that you have in your channel and Youtube agree with them, you will be notified have to take the video down or edit their personal details

1. Even if your profile is private, please remember that people can see and share information that others post about you. Other people can also save information you have posted about yourself on their own phones and devices

2. Some companies will share information about you with Facebook and Facebook will share information about you with them

3. If you agree to use an app on Facebook, that app might be able to use, share and keep the information you post on Facebook

4. If you delete your account, things you have posted will be deleted but not things other people have shared about you

1.1.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Personal data protection in social media_01_01

Situation: What is “Social Media”?

Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Website and applications that enable people to send messages and photos.
- Social media are a form of electronic communication (such as websites for social networking).
- Website and computer programs that allow people to communicate and share information on the internet using a computer or mobile phone.
- Social media refers to website and applications that are design to share content quickly.

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_Personal data protection in social media_01_02

Situation: Which personal data protection rights are applied in WhatsApp?

Task: Pick the right options following the multiple-choice principle: Only one answer is false.

- You have the right to have encrypted messages which means that WhatsApp can’t read the messages that you send to other people.
- You have the right to delete your WhatsApp account and with that the messages that have been delivered to other people won’t be.

- If you just delete the application WhatsApp on your device but don't delete the account the information will be kept.
- WhatsApp saves and keeps information about you but can't use your information anywhere in the world.

2.Build knowledge - Most common risks in social media

Nowadays, it is common knowledge that social media integrates our daily interests and activities. However, do we share the habits and behaviours regarding social media usage? To understand the relevance of social media in our society, it is important that we stay on top of the latest social media statistics. Next, we present the 10 most relevant statistics for social media:

10 MOST RELEVANT STATISTICS FOR SOCIAL MEDIA

1. 73% marketers believe that social media marketing has been very effective for their business (Buffer, 2019)
2. 3.5 billion active social media users world wide, equivalent to 45% of the population (Emarsysm, 2019)
3. Daily active Instagram stories users increased from 150 million in January 2017 to 500 million daily active stories worldwide in January 2019 (Buffer, 2019)
4. Facebook remains the most common social media platform (Pewinternet, 2018)
5. 91% of all social media users access social channels via mobile devices (Buffer, 2019)
6. 71% of consumers want brands to push social platforms to better secure their personal data (Edelman, 2008)
7. 91% of all social media users access social channels via mobile devices (Buffer, 2019)
8. Digital consumers spend nearly 3 hours per day on social networks and messaging (Globalwebindex, 2018)
9. 81% of Small and Medium Businesses currently use social media to drive business growth and 9% are planning to use it in the future (LinkedIN, 2014)
10. On average, people have 7.6 social media accounts (Clement, 2019)

With this kind of statistics, it’s no wonder that social media networks are becoming one of the famous platforms to gather users’ data, either perpetuated by network itself in a legal manner, or by hackers with malicious intent.

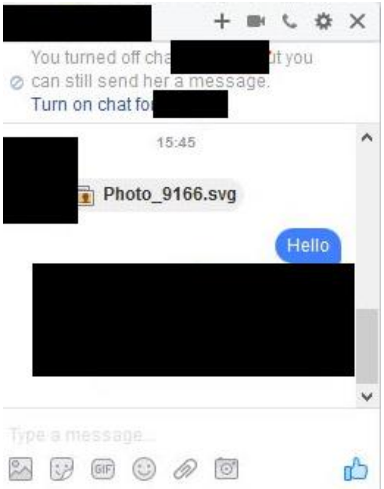
The most preeminent risk of social media is malware that can compromise all of your data. There are different kinds of malware with different purposes, as you can see below:

1. Ransomware - software that uses encryption to disable a target’s access to its data, like photographs or documents, until a ransom is paid. This malware is activated when the user clicks in a hyperlink posted in a social media platform or in an image that redirects the user to an external website that spreads the malicious code.

Example of a Ramsomware

Chat apps like WhatsApp or Facebook Messenger are common means to ransomware attacks.

In this example, cybercriminals sent deceptive messages that contain SVG image attachments via Facebook Messenger. Users who clicked on the image fond themselves on a website that pushed a popup to install a browser extension or add-on to view a video. Later, after the malicious code infected the users system, another pop-up appeared, demanding payment in order to unlock user’s files.


[redacted]

You turned off cha[redacted]t you can still send her a message.

Turn on chat fo[redacted]

15:45

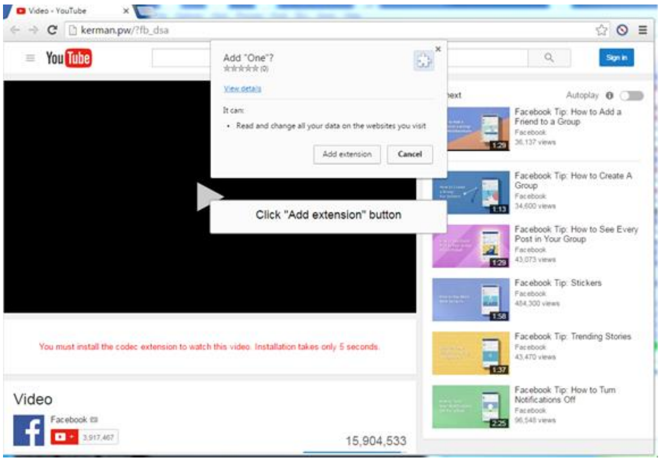
[redacted]

Photo_9166.svg

Hello

[redacted]

Type a message...


Video - YouTube

kerman.pw/?fb_dsa

Add "One"?

View details

It can:

- Read and change all your data on the websites you visit

Add extension | Cancel

Click "Add extension" button

You must install the codec extension to watch this video. Installation takes only 5 seconds.

Video

Facebook

3,917,467

15,904,533

YouTube
Sign in
Up next
Autoplay
Facebook Tip: How to Add a Friend to a Group
Facebook
36,137 views
1:29
Facebook Tip: How to Create A Group
Facebook
34,600 views
1:13
Facebook Tip: How to See Every Post in Your Group
Facebook
43,073 views
1:29
Facebook Tip: Stickers
Facebook
484,300 views
1:58
Facebook Tip: Trending Stories
Facebook
43,470 views
1:37
Facebook Tip: How to Turn Notifications Off
Facebook
96,548 views
2:25

2. Trojan horse - Type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed steal data (logins, financial data, even electronic money), install more malware, modify files, monitor user activity (screen watching, keylogging, *etc.*), use the computer in botnets, and anonymize internet activity by the attacker. A Trojan acts like a legitimate application or file to trick you into downloading and installing malware. Once installed, a Trojan can perform the action it was designed for.
   Usually, a Trojan horse is hidden in fake advertising or is send to users by instant messaging.

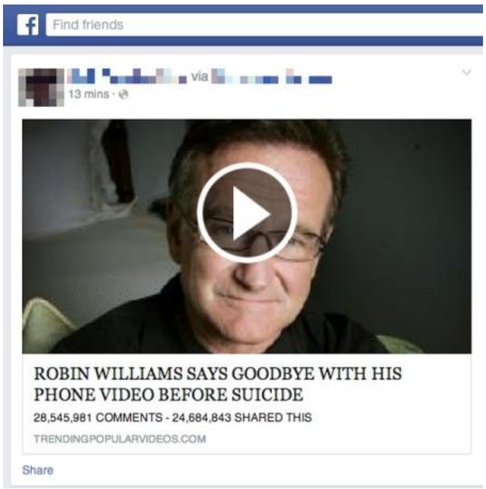
3. Virus - Form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.

4. **Greyware** –form of malware that doesn't really do any physical damage to your data as other malware can, and it presents itself in a more bothersome matter, such as adware and spyware. It has a high prevalence in social media, usually in the form of "click bait", where an enticing article will lead you to a website that asks that you to do an action, like install a fake social media plugin or fill out a quick survey before accessing the media. That information is then collected and sold to other cybercriminals and can be used in attempts to hack into your personal accounts.

Example of Greyware

Over the years, scammers have used both real and fake celebrity deaths as a way to convince users to click on links and perform actions.

One infamous example followed the death of the actor Robin Williams, in 2014. Only 48 hours after his death, a video started circulating in Facebook claiming to link to a supposed goodbye video by Williams. Users that clicked on the link to the supposed video were taken to a fake BBC News website. Then, they were instructed to share the video on Facebook before watching. After they shared the page as requested, a second fake page appeared and requested the filling of an online survey. Personal information were collected and then sold to unscrupulous Internet marketers.



[redacted] via [redacted]

13 mins ·

ROBIN WILLIAMS SAYS GOODBYE WITH HIS PHONE VIDEO BEFORE SUICIDE

28,545,981 COMMENTS - 24,684,843 SHARED THIS

TRENDINGPOPULARVIDEOS.COM

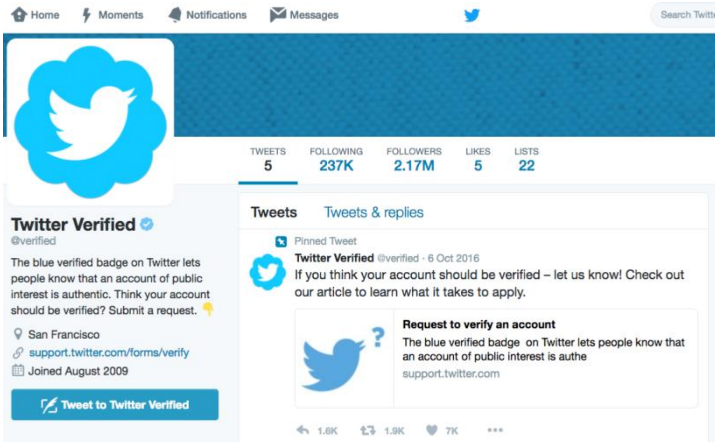
5. **Worms** – Worms are among the most common types of malware. Worms can modify and delete files, steal data, install a backdoor and allow a hacker to gain control over a computer and its system settings. They can even inject additional malicious software into a computer. Worms can be transmitted via software vulnerabilities or could arrive as attachments in spam emails or instant messages. Once opened, these files could provide a link to a malicious website or automatically download the computer worm. Once it's installed, the worm silently goes to work and infects the machine without the user's knowledge. Worms often spread by sending mass instant messages with infected attachments to users' contacts.

As you can notice, all of this malware uses the same strategic to lure the user, namely, phishing scams or attacks. **Phishing attacks** use malicious sources to collect personal and financial information or infect user's machine with malware.

The first step of a phishing attach is always the same: In your social media feed or in your instant message application appears a link, photo, video, an article, or an advertisement. This could appear to be from anybody - a news source, a celebrity, a business, the social network itself or even a trusted contact. Most of the time those sources are impersonators of real accounts or users whose social media account has been compromised or their identity has been stolen.

Example of an impersonator account

Twitter has a tool that verifies accounts in order to reduce fraudulent activity, named “Twitter Verified”. This is the real account for it:

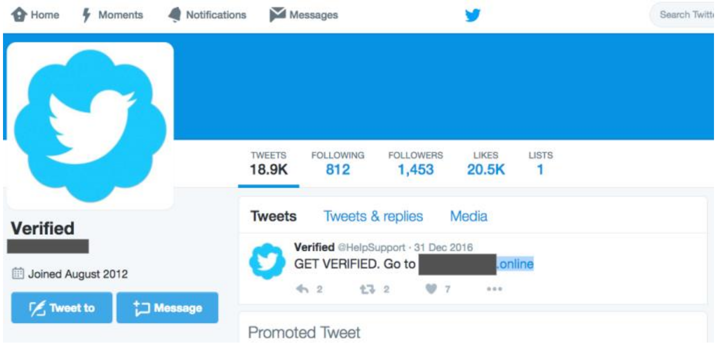


Twitter Verified
@verified
The blue verified badge on Twitter lets people know that an account of public interest is authentic. Think your account should be verified? Submit a request.
San Francisco
support.twitter.com/forms/verify
Joined August 2009

Pinned Tweet
Twitter Verified @verified · 6 Oct 2016
If you think your account should be verified – let us know! Check out our article to learn what it takes to apply.

Request to verify an account
The blue verified badge on Twitter lets people know that an account of public interest is authe
support.twitter.com

It didn’t take long to the appearance of a cloning account, claiming to be the authentic verification help account, and directing users to all sorts of malicious payloads.



Verified
[redacted]
Joined August 2012

Verified @HelpSupport · 31 Dec 2016
GET VERIFIED. Go to [redacted].online

Social media phishing plays on your basic human emotions and needs, such as trust, safety, grieving, fear of losing money, getting something for nothing, eagerness to find a bargain or desire to find love or popularity/status. They also generally state or imply the need for your urgent action to either avoid an issue or take advantage of an offer.

Examples of Phishing Scams

OMG! Did you see this picture of you?
Secret details about Michael Jackson's death!
Only 1% of people can solve this problem! Take the quiz now!
Adidas is giving away 3,000 Free Pair of Shoes to celebrate to celebrate its 93rd anniversary. Get your free shoes now!

These are very common phishing scams that involve a question, a celebrity, a brand or a fact that piques the user's interest and then directs them to a fake login screen to obtain login information or automatically installs malware onto a computer.

The second step of a phishing attack is to redirect the user to a website that requests confidential details or causes your computer or mobile device to be infected with malware. This malware can be installed automatically or after requesting the download of a program, browser extension or application.

Alternatively, the post, tweet or message may instruct you to make a phone call to a specified number. This can either result in confidential details being requested, or an exorbitant charges being added to your phone bill.

2. Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Personal data protection in social media_02_01

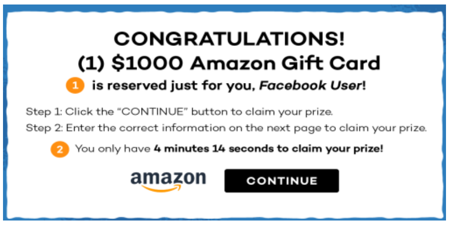
Situation: Which fact is false?
Task: Pick the right option following the multiple-choice principle: Only one option is correct.

- Social media is an effective marketing tool for businesses
- Facebook is the most used social media platform
- Most of all social media users access social channels via mobile devices
- Small and medium businesses currently use social media to drive business growth
- Users tend to chose one social network, using it every day

Exercise SINGLE CHOICE (nur Text)

Associated fine objective: FO_Personal data protection_02_02

Situation: You are scrolling through Facebook and you see the following publication:



CONGRATULATIONS!
(1) $1000 Amazon Gift Card
1 **is reserved just for you, *Facebook User*!**

Step 1: Click the "CONTINUE" button to claim your prize.
Step 2: Enter the correct information on the next page to claim your prize.

2 You only have **4 minutes 14 seconds to claim your prize!**

What would you do?
Task: Pick the right option following the multiple-choice principle: Only one option is true.

- OMG, today is my lucky day! I click "CONTINUE" and give them all the data necessary to win the gift card. After that, I share the opportunity with all my cyber-friends!
- I only have 4 minutes to claim my price! I click "CONTINUE" and give them all the data necessary to win the prize. But after seeing that I must give banking details, I give up. Too much work.
- I get curious and click on "CONTINUE". After seeing that it is necessary to give them personal data I close the tab. I think it's a scam.
- I don't click in the publication. I can't win a lottery that I never entered! I signal the post to Facebook as "scam".
-

3.Build knowledge - some security tips using social media accounts

Now that you know the broad variety of risks of using social networks, please don’t feel that the only solution to secure your safety and privacy is to delete your social accounts! The secret is to use social media while understanding the risks and knowing how to act accordingly.

There are some common behaviours by fraudsters and hackers that can alert us to the possibility of a phishing scam. While you are browsing your favourite social media network, always be aware to these red flags that indicate that that post is a phishing scam:

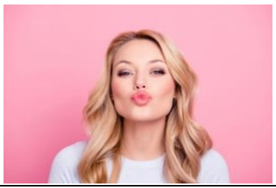
Red Flag #1: Friend requests from strangers

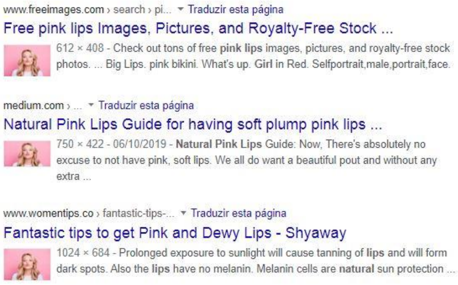
You received a friend request from a stranger? Someone that you don’t recognise sent you a private message? A business or a public figure asked you to start following them?

Platforms like Facebook, Instagram and Twitter are full of fake profiles with the intent of phishing users. Don’t accept any friend request without verification. If someone is disturbing you, it's good to report and block such profiles.

Quick Tip

Do a reverse image search of the profile photograph. Most of the times, hackers use stock photos. If you have results for different websites that uses that photo for different purposes, it’s a fake account.





www.freeimages.com › search › pi... ▾ Traduzir esta página
Free pink lips Images, Pictures, and Royalty-Free Stock ...
612 × 408 - Check out tons of free **pink lips** images, pictures, and royalty-free stock photos. ... Big Lips. pink bikini. What's up. **Girl** in Red. Selfportrait,male,portrait,face.

medium.com › ... ▾ Traduzir esta página
Natural Pink Lips Guide for having soft plump pink lips ...
750 × 422 - 06/10/2019 - **Natural Pink Lips** Guide: Now, There's absolutely no excuse to not have pink, soft lips. We all do want a beautiful pout and without any extra ...

www.womentips.co › fantastic-tips-... ▾ Traduzir esta página
Fantastic tips to get Pink and Dewy Lips - Shyaway
1024 × 684 - Prolonged exposure to sunlight will cause tanning of **lips** and will form dark spots. Also the **lips** have no melanin. Melanin cells are **natural** sun protection ...

Quick Tip

Ever notice the blue checkmark beside the names of high profile or businesses on social platforms? It looks like this:

Twitter: **Stephen King** ✓
Facebook: adidas ✓
Instagram: cristiano ✓

This checkmark is available in almost every social media platform and it means that the **account is verified** as authentic and belongs to a celebrity or an industry leader.

For example, if you get a DM from “Twitter Verified” account without the check mark, watch out – it’s likely to be a fake!

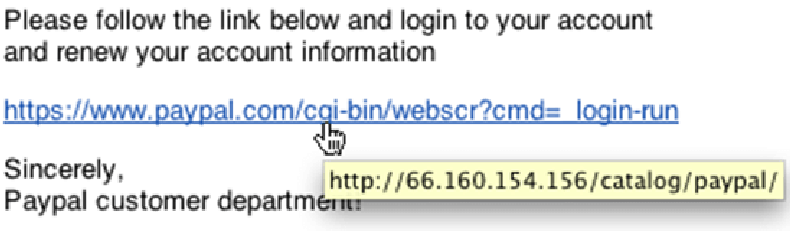
Redflag #2: Click in this link!

The aim of a phishing attack is usually to get you to download an attachment (for example, a photo sent in a direct message) or to click on a link. Sometimes criminals impersonate trustworthy sources to get you to click on a link (or download an app) that contains malware. What looks like a legitimate hyperlink can be a disguised link to a criminal website.

Therefore, don't click in any link that redirects you to other website. Instead, go to directly to the source - brand website, bank page, *etc.* - and confirm if you see in the social media it's true advertisement or announcement.

Quick Tip

A quick way to attest if the hyperlink will re-direct you to a trustworthy source it's to hover your mouse over the text of the hyperlink. You should see the full URL, which will help to show whether it leads to a legitimate website.



Please follow the link below and login to your account
and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

What is the main clue that we should be looking is the URL?

Please pay attention to the beginning of the URL: safe URLs begin with "https" instead of just "http" to indicate that they are encrypted. The "s" in "https" stands for "secure".

So, this hyperlink is a phishing scam!

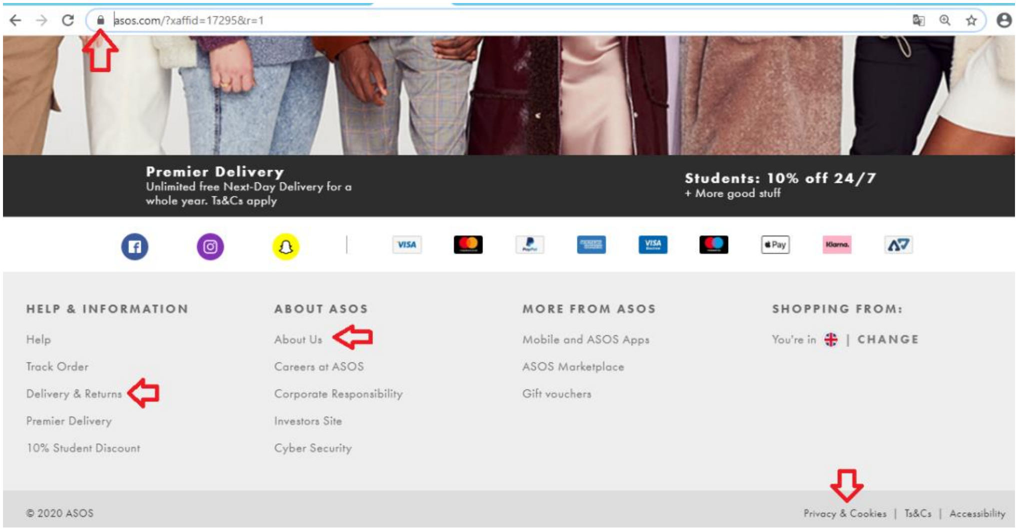
Quick Tip

What if you click in a link? What should you do?

If that link re-directs you to a website there are a few signs that you can look for to help you know if a company is real or not.

So, before you do anything, like enter your login credentials or click in the download button, look for these hints:

- In the search bar appears "https" or a "lock" symbol – that means that **the website is secured.**
- **Look at the Domain** – cyber attackers are very sneaky. Most of the times, domains are very similar to the real one, for example "as0s.com" or "asos.net".
- **There are a physical address and phone number** - reputable companies will list their information so you can contact them if there is a problem.
- **Return policy** - reputable sites should list their return policy as well as their shipping policy
- **Privacy statement** - reputable sites should tell you how they protect your information and whether they give your information to third parties.



Redflag #3: Promotions and contests too good to be true!

This is a very common phishing scam. By presenting very low prices, offering irresistible prizes or giving away discounts, fraudsters can trick users into giving private information.

Quick Tip
What are the common signs of a contest scam? • The social page has a low follower count; • Poor grammar and spelling; • They ask very personal information, like your mother's name, first pet, if you have kids, *etc.* All they want are clues to crack your password! • They are very persistent in their dialog! They just want you to feel the sense of "urgency".

As you can conclude, there are ways to detect phishing scams in social media, preventing you to become a victim of a cyberattack that compromises your personal data. But having an attentive eye is not enough. In regard of cyberattacks the best remedy is prevention. So, what can you do to always be one step ahead from cybercriminals in social media?

Check your privacy settings

Reliable social media networks allows you set the privacy settings to a level of your comfort. What kind of information do you want to make public? Your photos? Your hobbies? And with whom do you want to share that information? Your social media friends or everybody?

Altering the privacy settings can allow you to block strangers and people who are not your friends from viewing your profile and the information that you share.

To do this, you should check the "definitions"of your social media account.

Keep security software updated

Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

You can also install in your browser an extention that blocks unwanted advertisements.

Keep passwords strong

Creating a strong password will prevent hackers from gaining access to your account and using it to post spam or malicious attacks. A strong password has no less than 8 characters and consists of both letters and numbers. It also should be changed every 3 months and unique to every account.

Tip: *use a passphrase instead of a password, for example "IAte27P0tat0s"*

Keep your secrets to yourself

Avoid sharing personal information online because your information, including your email address, phone number, and social security number, is worth a lot of money to hackers and data mining companies. That data could be use for ransom, identity theaft or a hint for guessing your passwords.

Take a look at your social media profiles and try to keep them barren—the people who need to know your birth date, email address and phone number already have them.

Use a VPN

If you want to keep your conversations, messages and calls secure you can use an Virtual Private Network (VPN). A VPN is an encrypted tunnel between two devices that lets you access every website and online service privately and securely.

Because the data is encrypted, hackers, governments and even internet service providers cannot see or gain control of your information while you are connected to a VPN server.

There are a lot of VPN providers online and they vary in terms of prices and customization.

Don't forget to log out

Keep in mind this golden rule: always log out of all of your social media platforms when you are done using them. If you don't log-out you're allowing anyone with access to your computer, legally or not, to open the browser or application and have instant access to your accounts on such sites, without entering any passwords or usernames.

3. Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Personal data protection in social media_03_01
FO_Personal data protection in social media_03_02

Situation: What are the signs of a possible phishing scam that you must always be alert while browsing social media?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Grammar and spelling of the publication.
- The presence of hyperlinks: only a credible source posts can publish a link to their website.
- The hyperlink doesn't match with the URL.
- If a friend sends me a photo to download, there is no danger to do so.
- The account of a famous brand must me verified to be trustworthy.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_Personal data protection in social media_03_01 and FO_Personal data protection in social media_03_02

Situation: What should you do to guarantee that you use your social networks platform in a safe way?

Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- It's safer to use the same password for all my accounts. That way I'll never forget it.
- **Before I accept a new friend request I should verify the authenticity of their profile and account.**
- **I should never reveal the details of where I am vacationing, shopping or traveling, as well as when I am expected to leave or return home.**
- It's ok to operate an internet-enabled computer without installing anti-malware and antivirus software.
- In order to keep track of all my cyber-friends' social activity I must be logged in to my account at all times.

Sources

Akilawala, T. (August 16, 2014) *Fake Robin Williams goodbye video on Facebook is a scam*. Retrieved from https://www.bgr.in/news/fake-robin-williams-goodbye-video-on-facebook-is-a-scam-321750/

Crowdstrike (October 15, 2019) *The 11 most common types of malware*. Retrieved from https://www.crowdstrike.com/epp-101/types-of-malware/

Constanza, T. (August 19, 2019) *Scam on Facebook exploits Robin Williams' suicide.* Retrieved from https://www.siliconrepublic.com/enterprise/scam-on-facebook-exploits-robin-williams-suicide

DuPaul, N. (October 12, 2012) *Common Malware Types: Cybersecurity 101.* Retrieved from https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Foreman, C. (June 20, 2017) *10 Types of Social Media and How Each Can Benefit Your Business*. Retrieved from https://blog.hootsuite.com/types-of-social-media/

Get Safe Online (n. d.) *Social Media Phishing*. *https://www.getsafeonline.org/social-networking/social-media-phishing/*

GMA News Online (August 15, 2014) *Beware of Robin Williams goodbye video scam.* Retrieved from https://www.gmanetwork.com/news/hashtag/content/375009/beware-of-robin-williams-goodbye-video-scam/story/

Kietzmann, J. H. and Hermkens, K. (2011) *Social media? Get serious! Understanding the functional building blocks of social media*. Business Horizons (Submitted manuscript). 54 (3): 241–251. doi:10.1016/j.bushor.2011.01.005.

Mohsin, M. (Frebruary 7, 2020) *10 Social Media Statistics You Need to Know in 2020 [Infographic].* Retrieved from https://www.oberlo.com/blog/social-media-marketing-statistics

NortonLifeLock (n. d.) *What is a Trojan? Is it a virus or is it malware?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

NortonLifeLock (n. d.) *What is a computer worm, and how does it work?* Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Obar, J. A. and Wildman, S. (2015) *Social media definition and the governance challenge: An introduction to the special issue.* Telecommunications Policy. 39 (9): 745–750. doi:10.1016/j.telpol.2015.07.014. SSRN 2647377

SNL. 2010. Saturday Night Live. Season 36, Episode 10. First aired December 18. NBC. Retrieved from https://www.youtube.com/watch?v=md3of7O02e4&list=PLS_gQd8UBhLghdS1aaLqVJ74rWi4ffT8&index=14

Woodfield, M. (November 26, 2014) *Should I Buy from This Site? How to Know if a Website is Secure*. Retrived from https://www.digicert.com/blog/how-to-know-if-a-website-is-secure/

ZeroFOX Alpha Team (February 15, 2017) *Social Media Impersonators Go Phishing: 3 Emerging Tactics*. https://www.zerofox.com/blog/social-media-impersonators-phishing/

Save Knowledge

We live in a world of globalization where the internet allows us to communicate to everyone anywhere in the world. Social media platforms have become an **integral part of our lives** and are a great way to stay connected with others.

Social networks like Facebook, Instagram or YouTube are popular among all ages and are constantly working to captivate currents and new users.

Nevertheless, despite of all the advantages that this kind of platforms offers to users, there are a lot of **security and privacy risks** related to their constant and careless use. In fact, fraudsters take advantage of users' social media habits to lure them to **phishing scams and attacks** that compromise their devices and data. Therefore, everyone should acknowledge their responsibility in maintaining a **safe online environment,** while understanding the risks of an online presence. Being **cautious, choosing a strong password or installing antivirus software** are some of many measures that a user must adopt to gain control of their safety while using social networks.

As the world evolves to a single digital market it is fundamental that everyone is aware of the laws applied to the protection of personal data, like the **GDPR** and how that applies to different digital scenarios.

In conclusion, **government, society and end users must work together to protect the privacy and safety of personal data in social networks.**