



Erasmus+



Co-funded by the
Erasmus+ Programme
of the European Union



USE OF SOCIAL MEDIA



CYBERSECURITY IN SCHOOLS

2020-1-TR01-KA229-094378

Keşan Ticaret Ve Sanayi Odası Mesleki Ve Teknik Anadolu Lisesi, Keşan, Turkey

IPSCEOA "N. Gallo" di Agrigento, Agrigento (Ag), Italy

1ο Γενικό Λύκειο Αγίου Δημητρίου, Agios Dimitrios Attikis, Greece

IES Antonio Menárguez Costa, Los Alcázares, Spain

Escola Secundária Campos de Melo, Covilhã, Covilhã, Portugal



CONSCIOUS *use of the web*

T o o o o
o a o a
o a o a o a

I.P.S.E.O.A. "Gallo"

ITALY



Content

- What is the internet
- World Wide Web
- Security threats
- What is a browser
- Search engine
- Defense systems

What is Internet

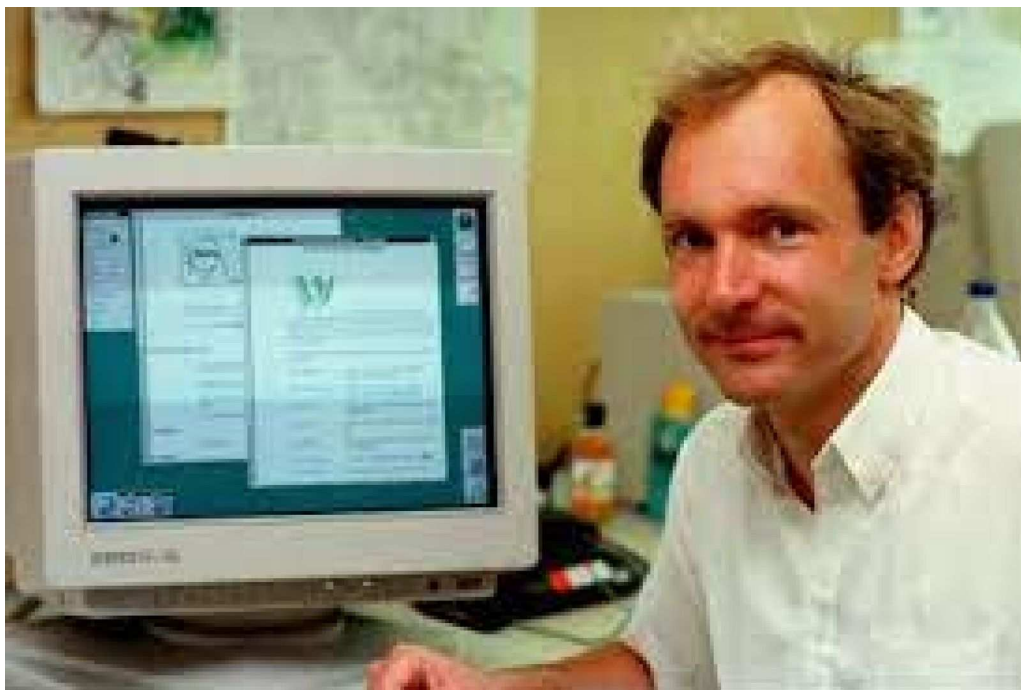
"It is a network of billions of computers connected to each other in order to allow the exchange of data and information all over the world"



What is a browser

It is the main access point to the Internet, it is the program that is used to surf the net

The first browser was developed by Tim Berners-Lee was called Mosaic



What is a search engine

In the context of Internet technologies, a search engine is an automatic system that analyzes a set of data (often collected by itself) and returns an index of the available contents, classifying them automatically based on statistical-mathematical formulas that indicate the degree of relevance given a specific search key.

The most used search engines are: Google, Yahoo, Bing, DuckDuckGo



Security threats

Virus/Worm

It is software belonging to the category of malware which, once executed, infects files in order to make copies of itself, generally without being detected by the user

Spyware/Adware

Is a type of software that collects information regarding a user's online activity without their consent

Spam

Unwanted emails, instant messages and other online communications

Security threats

Trojan Horses

The trojan hides its functioning inside another apparently useful and harmless program. By running or installing the latter program, the user actually activates the code of the hidden Trojan as well

Phishing

Online fraud to deceive credit card numbers, passwords, personal account information



Defense systems

- Updating the operating system and all application software
- Antivirus
- Antispyware
- Firewall



Protect your data and your accounts

A password is, in the IT and cryptographic field, a sequence of alphanumeric characters used to exclusively access a computer resource

- Create strong passwords that have at least 8 characters and are made up of numbers, letters and symbols
- Do not disclose your private passwords to anyone
- Use 2-factor access



Google Authenticator

Do not communicate personal data

When sharing information on the Internet (including through pictures and videos), remember that you are also sharing it with strangers

IMPORTANT

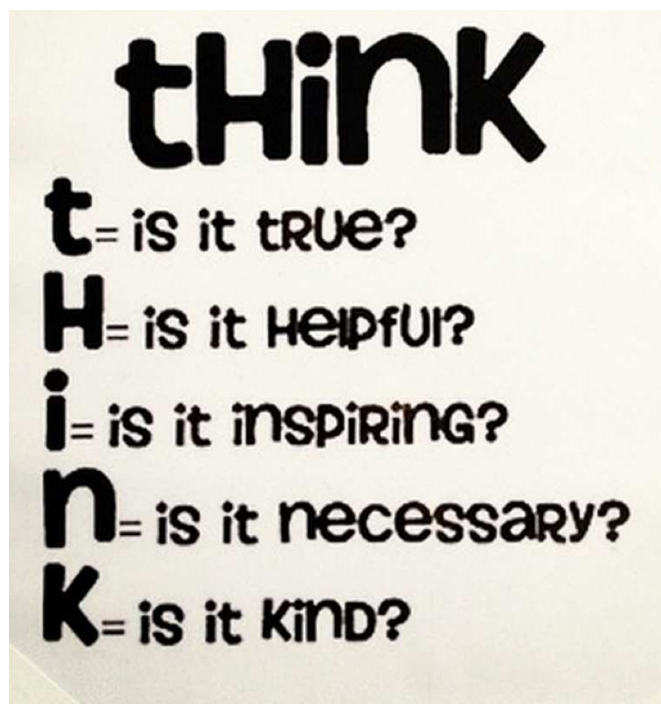
- Delete emails asking for personal information (name and surname, age, home address, telephone number, school name and address)
- Always pay attention to the information you share



"General Data Protection Regulation"

Think before you click

- Be wary of links in emails
- Be wary of eye-catching advertisements and those who want to reward you
- Do not open links if they are not "type" safe! If in doubt, give up!
- Avoid little known sites
- Remember that downloading pirated material is a crime



Be careful when communicating with others

Avoid adding unknown contacts
Knowingly sharing photos or
personal data

Leave environments, such as
chats and forums, in which they
offend or make you
uncomfortable

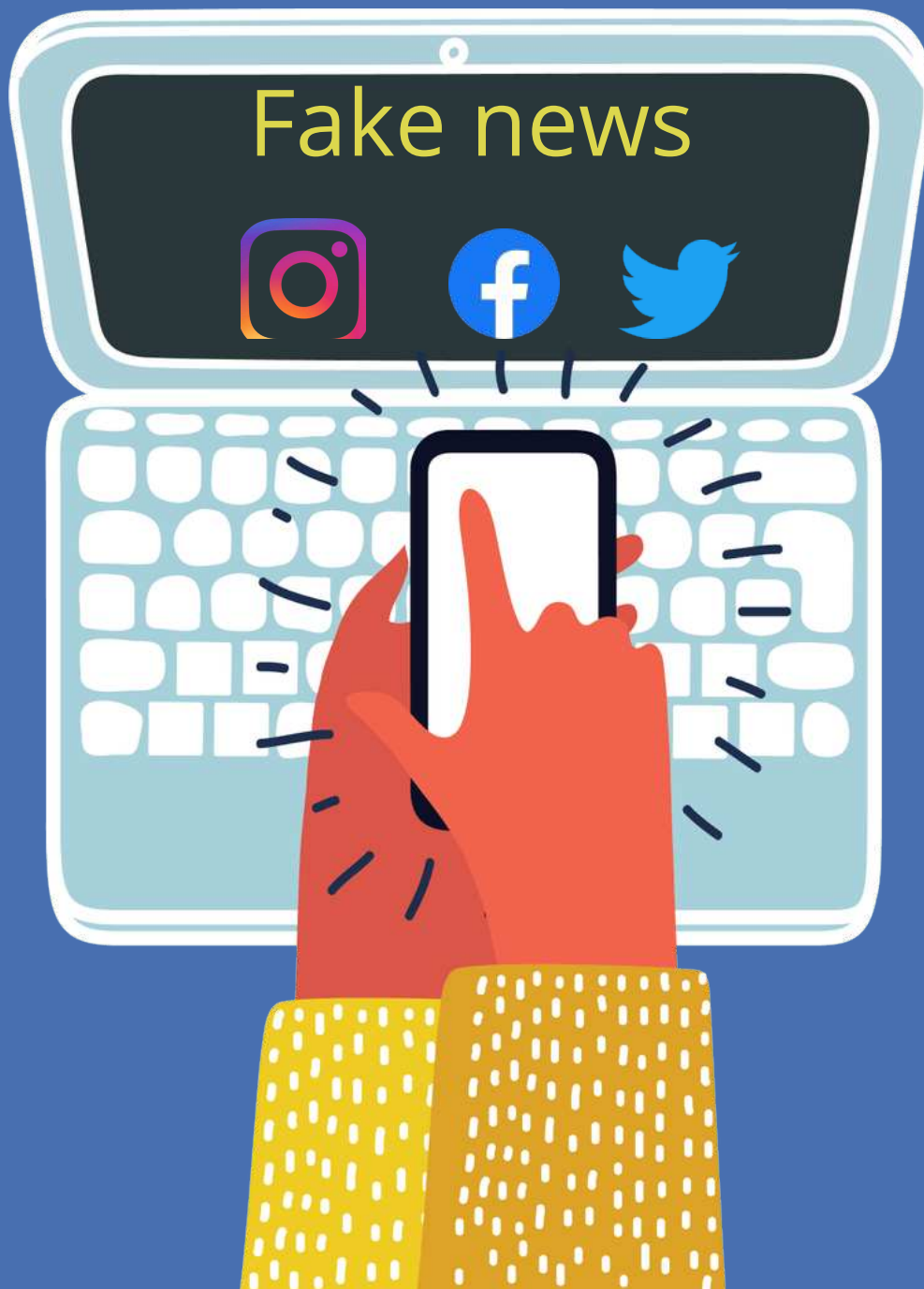
Use webcams wisely

Do not offend and respect the
opinions of others

If necessary, report anomalies,
offenses and abuses on the web
to the Postal Police

Cyber Security in schools

1ο GEL Agiou Dimitriou



contents

Fake news.....3-5

Coronavirus and Fake news.....6-7

Ways to spread fake news..... 8-9

Misinformation and Disinformation...10

How to spot fake news..... 11-12

Conclusion.....13

Sources.....14



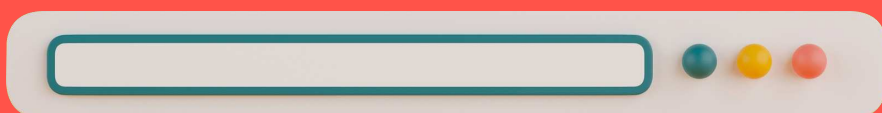
FAKE NEWS

Fake news is false or misleading information presented as news. Fake news often has the aim of damaging the reputation of a person or entity, or making money through advertising revenue. Although false news has always been spread throughout history, the term "fake news" was first used in the 1890s when sensational reports in newspapers were common. However, the term does not have a fixed definition, and has been applied more broadly to include any type of false information, including unintentional and unconscious mechanisms, and also by high-profile individuals to apply to any news unfavourable to their personal perspectives. Furthermore, disinformation is an insidious type that involves spreading false information with harmful intent, and is sometimes generated and propagated by hostile foreign actors, particularly during elections. In some definitions, fake news includes satirical articles misinterpreted as genuine, and articles that employ sensationalist or clickbait headlines that are not supported in the text.



The term "fake news" gained importance with the electoral context in Western Europe and North America. It is determined by fraudulent content in news format and its velocity. According to Bounegru, Gray, Venturini and Mauri, fake news is when a deliberate lie "is picked up by dozens of other blogs, retransmitted by hundreds of websites, cross-posted over thousands of social media accounts and read by hundreds of thousands" that it then effectively becomes "fake news".

The evolving nature of online business models encourages the production of information that is "click-worthy" and independent of its accuracy. The nature of trust depends on the assumptions that non-institutional forms of communication are freer from power and more able to report information that mainstream media are perceived as unable or unwilling to reveal.



The inventor of the World Wide Web, Tim Berners-Lee has stated that fake news is one of the most significant new disturbing trends that must be resolved, otherwise the internet cannot truly serve and benefit humanity.

The prevalence of fake news has increased with the recent rise of social media, especially the Facebook News Feed, and this misinformation is gradually seeping into the mainstream media. Several factors have been implicated in the spread of fake news, such as political polarization, post-truth politics, motivated reasoning, confirmation bias, and social media algorithms.

Fake news can reduce the impact of real news by competing with it. For example, a BuzzFeed analysis found that the top fake news stories about the 2016 U.S. presidential election received more engagement on Facebook than top stories from major media outlets. It also particularly has the potential to undermine trust in serious media coverage. The term has at times been used to cast doubt upon credible news, and former U.S. president Donald Trump has been credited with popularizing the term by using it to describe any negative press coverage of himself. It has been increasingly criticized, due in part to Trump's misuse, with the British government deciding to avoid the term, as it is "poorly-defined" and "conflates a variety of false information, from genuine error through to foreign interference".

Multiple strategies for fighting fake news are currently being actively researched, for various types of fake news. Politicians in certain autocratic and democratic countries have demanded effective self-regulation and legally-enforced regulation in varying forms, of social media and web search engines.



Coronavirus and Fake news



Nowadays as the coronavirus spreads around the world, platforms as Facebook and YouTube have a heavy responsibility on accurate information.

As Rory Cellam-Jones (BBC NEWS) says in his article of February 2020.

These are the platforms that billions now rely on for news and they are already providing fertile territory for those wanting to spread misinformation. On Facebook, it is in groups opposing vaccines and those campaigning against 5G mobile phone networks that scare stories appear most likely to take hold.

I've scanned a number of the 5G groups, and found plenty of comments suggesting there is a link between the virus and the new networks.

The Stop 5G UK group has more than 27,000 members, one of whom has posted this: "I've heard it's not a serious "Virus", it's about as bad as a flu or cold. So really this is a perfect plan to cover up EMF/5G related illnesses."

A YouTube video with the title "WUHAN CORONA VIRUS IS A 5G L.E.D SMART STREET LIGHT TEST BED" is also popular in this group and others.

Other YouTube videos share complex conspiracy theories including a suggestion that the Diamond Princess cruise ship whose passengers had to be quarantined was affected by the virus because it used 5G technology for its connectivity.

Another popular theory is that the virus was engineered in a lab and deliberately released by, take your pick, the Chinese or American government. Over on the Facebook 5G and microwave radiation group, an article from Technocracy News claims: "It is becoming pretty clear that the Hunan coronavirus is an engineered bio-weapon that was either purposely or accidentally released."

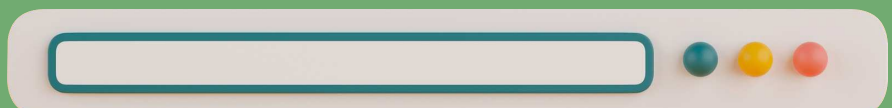
To be fair to Facebook, it appears to have upped its game when it comes to combating misinformation. Search for "coronavirus" on its platform and the top results will be reliable information from sites such as the World Health Organization (WHO). If you find an anti-vaccination group you want to join, a pop-up message appears saying: "Learn why the World Health Organization recommends vaccinations to prevent many diseases."

YouTube too appears to be trying to calm fears, with a WHO banner ad appearing above any videos about the virus. But on at least one conspiracy theory video, adverts are still appearing, meaning that the site's owner Google is still profiting from misinformation.

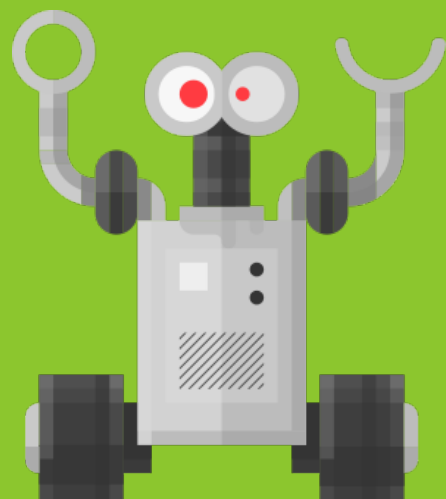
Facebook says that as well as promoting accurate information, it has taken steps to combat the spread of misinformation about the virus. Its third-party fact-checkers investigate dubious claims and when they rate information as false, the company limits its spread across Facebook and Instagram.

Ways to spread fake news

Declines in confidence in much traditional media and expert knowledge have created fertile grounds for alternative, and often obscure sources of information to appear as authoritative and credible. This ultimately leaves users confused about basic facts. The universe of “fake news” is much larger than simply false news stories. Some stories may have a nugget of truth, but lack any contextualizing details. They may not include any verifiable facts or sources. Some stories may include basic verifiable facts, but are written using language that is deliberately inflammatory, leaves out pertinent details or only presents one viewpoint. “Fake news” exists within a larger ecosystem of mis- and disinformation.



The technological ease of copying, pasting, clicking and sharing content online has helped these types of articles to proliferate. In some cases, the articles are designed to provoke an emotional response and placed on certain sites ("seeded") in order to entice readers into sharing them widely. In other cases, "fake news" articles may be generated and disseminated by "bots" - computer algorithms that are designed to act like people sharing information, but can do so quickly and automatically.



Misinformation and Disinformation



Misinformation is false or inaccurate information that is mistakenly or inadvertently created or spread. The intent is not to deceive. Disinformation is false information that is deliberately created and spread "in order to influence public opinion or obscure the truth".

How misinformation and disinformation is produced is directly related to who the author(s) is and the different reasons why it is created.

Who are the authors? They may be:

Someone wanting to make money, regardless of the content of the article,

Satirists who want to either make a point or entertain you, or both

Poor or untrained journalists - the pressure of the 24 hour news cycle as well as the explosion of news sites may contribute to shoddy writing that doesn't follow professional journalistic standards or ethics.

Partisans who want to influence political beliefs and policy makers.



How to spot fake news

We find it's easy to figure out what's real and what's imaginary if you're armed with some critical thinking and fact-checking tools of the trade.

Here's our advice on how to spot a fake:

1. Consider the source. In recent months, we've fact-checked fake news from abcnews.com.co (not the actual URL for ABC News), WTOE 5 News (whose "about" page says it's "a fantasy news website"), and the Boston Tribune (whose "contact us" page lists only a gmail address).

2. Read beyond the headline. If a provocative headline drew your attention, read a little further before you decide to pass along the shocking information. Even in legitimate news stories, the headline doesn't always tell the whole story. But fake news, particularly efforts to be satirical, can include several revealing signs in the text.

3. Check the author. Another tell-tale sign of a fake story is often the byline. The pledge of allegiance story on abcnews.com.co was supposedly written by “Jimmy Rustling.” Who is he? Well, his author page claims he is a “doctor” who won “fourteen Peabody awards and a handful of Pulitzer Prizes.” Pretty impressive, What’s the support? Many times these bogus stories will cite official — or official-sounding — sources, but once you look into it, the source doesn’t back up the claim. if true. But it’s not.

4. Check the date. Some false stories aren’t completely fake, but rather distortions of real events. These mendacious claims can take a legitimate news story and twist what it says — or even claim that something that happened long ago is related to current events.

5. Check your biases. We know this is difficult. Confirmation bias leads people to put more stock in information that confirms their beliefs and discount information that doesn’t.

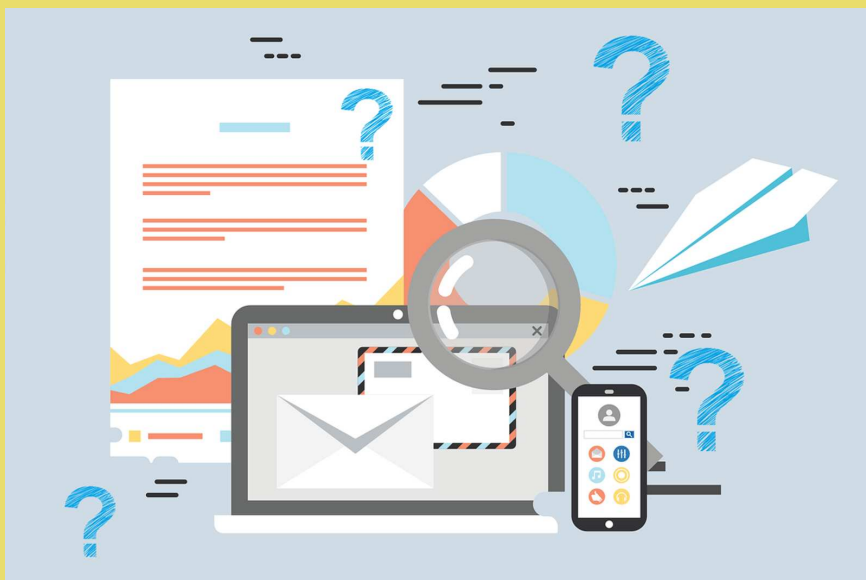
Conclusion

When shared, false information can take on a life of its own and have some serious consequences.

It can lead to health scares, false accusations and potentially damaging hoax stories.

It's not always easy to spot, so use the SHARE checklist to make sure that you are not contributing to the spread of harmful content.

So we all should be really careful!!



SOURCES

https://en.wikipedia.org/wiki/Fake_news

<https://guides.lib.umich.edu>

<https://www.webwise.ie>

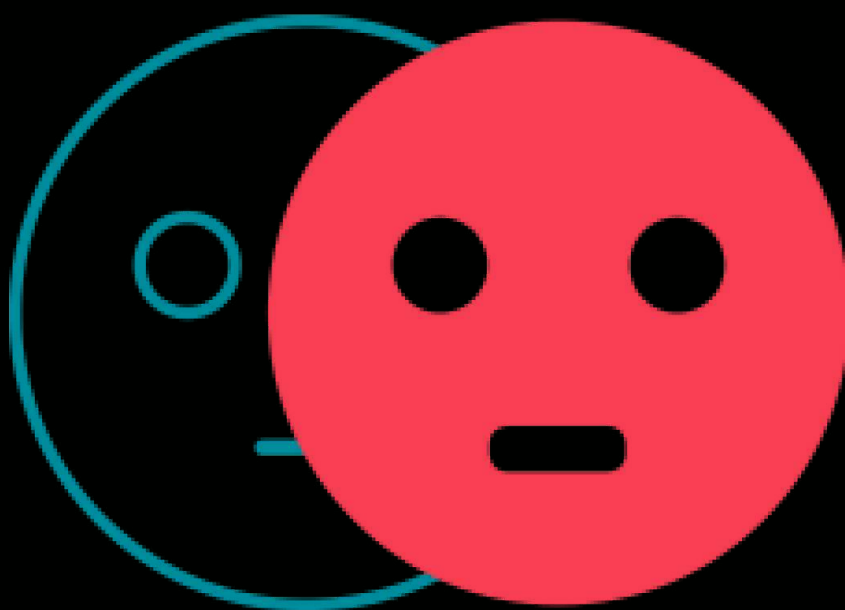
<https://kariera.future-processing.pl/>

<https://www.bbc.com/news/technology-51646309>



DEEP FAKE ON SOCIAL MEDIA

By Spain



Erasmus+

INTRODUCTION

The term deep fake is typically used to refer to a video that has been edited using an algorithm to replace the person in the original video with someone else (especially a public figure) in a way that makes the video look authentic.



HOW TO MAKE THE DEEPPFAKES?

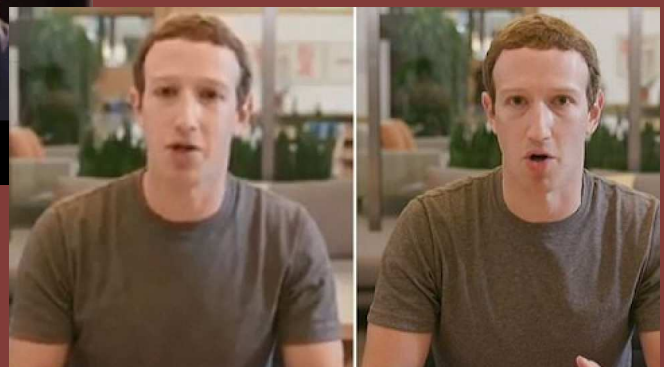
**Here we have
the video of
how a
deepfake is
made**



**~~How to make a~~
deepfake**

FAMOUS DEEPFAKES

There are many deep fakes every day, but there are some that were quite famous and famous. These were made to celebrities on social networks, but luckily they were discovered. An example is the deep fake that was made to Obama who declared that he was returning to public services, or the deep fake to Mark Zuckerberg (the owner of Facebook, WhatsApp, Instagram,...).

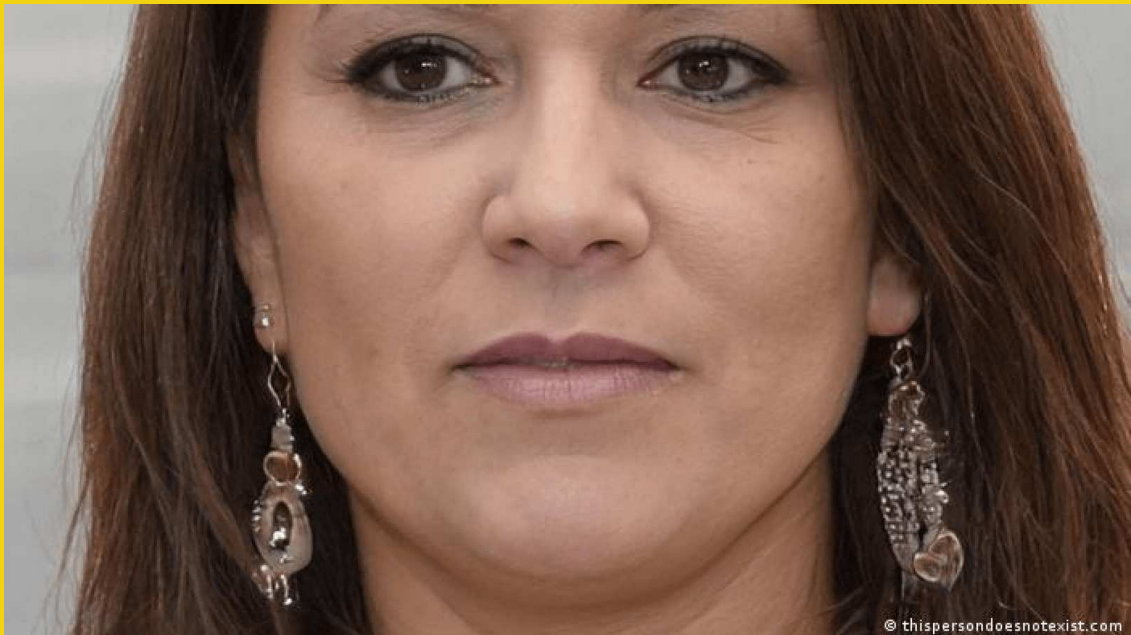


HOW TO DETECT A DEEPPFAKE?

Faults can be seen at the edges
of the image as discontinuities

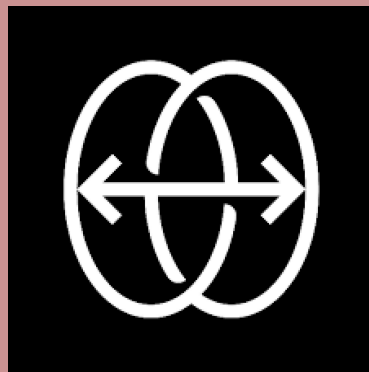


Also on many
occasions you can see
that jewelry such as
earrings do not
match.



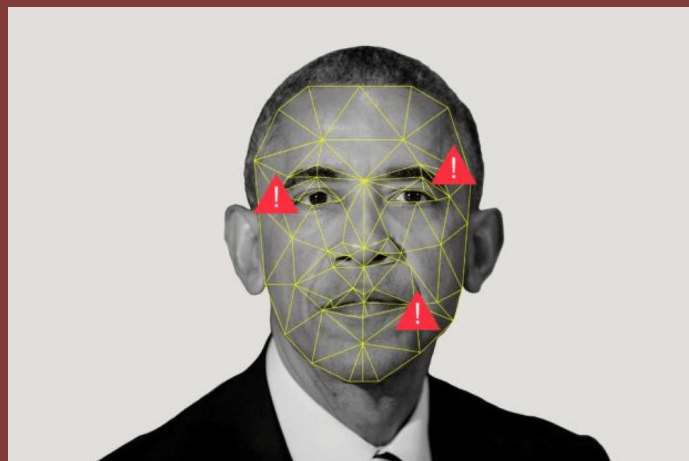
MOST POPULAR DEEPPFAKE APPS

**It is possible to make
a deepfake through
applications like ZAO,
Reface or FaceApp**



Why are they a problem?

While deepfakes do have a number of beneficial uses, including political satire, comedy, entertainment, and education, a number of its associated dangers are severe, even existential threats.



Anti-Deepfake Legislation

For Social Media Safety has
sponsored AB 1280 in the
California State Assembly
which will deter the
production of deepfakes



Alex Cohen said...

Alex Cohen stated one time that make it a deep fake is really easy and There are studios and downloadable tools available that are easy to use and allow people to get started immediately.



~~Video about this.~~

**THANKS
FOR YOUR
ATTENTION!**



SOCIAL MEDIA PRIVACY



THINK FIRST

While social media sites offer privacy tools to help you limit who can see the things you share, it's important to realize that they are fundamentally more open and social than traditional communication tools. Whether or not you realize it, the things you share online also can affect how you're perceived by others. That's why you'll always want to think carefully about what you share over social media.



REVIEW YOUR PRIVACY SETTINGS

All social networking sites have privacy settings that allow you to control who you share with. For example, whenever you share something on Facebook, you can choose to share with just a few people, all of your Facebook friends, or publicly with everyone on Facebook. That's why it's so important to understand how your privacy settings work and how to control them.





INSTAGRAM PRIVACY SETTINGS

By default, the photos and videos you share on Instagram are completely public. This means anyone can access whatever you share—even people who don't have an account on Instagram. If you're uncomfortable with the idea of people you don't know viewing your posts, you can make them private. This way, only people you approve will be able to see your posts.



FACEBOOK PRIVACY SETTINGS

Even if you're an experienced Facebook user, modifying your privacy settings for the first time can be a little confusing. And because Facebook can change these options without much notice, it's important to review your privacy settings periodically.

However you use Facebook, it's important to choose the privacy settings that will work best for you.

Facebook offers two main ways to control your privacy:

1. You can apply privacy settings that set general rules about who can contact you and view your information.
2. You can control who sees every individual thing you share.



TWITTER PRIVACY SETTINGS

Looking to make your Twitter profile a bit more personal or make your tweets more secure? Twitter has several options for customizing your account.

By default, everything you share on Twitter is public. This means anyone can see the things you tweet, even if they don't follow you on Twitter.



LINKEDIN PRIVACY SETTINGS

As with any online service, it's important to learn about the various settings and options you have on LinkedIn. While you can change some settings to help you be more comfortable or productive, you can also adjust your privacy settings to control how much of your information is available for everyone to see.

There are a fair number of advertisements on LinkedIn. However, many of them use information from your profile to send you targeted ads based on your location, interests, and education. Luckily, you can change how you interact with these personalized ads. To limit what advertisers learn about you, click the Ads tab at the top of the Settings menu, and adjust each setting however you want. Keep in mind that even if you deactivate everything on this tab, you'll still see ads on LinkedIn. However, they will no longer be based on your personal information.



PINTEREST PRIVACY SETTINGS

It's important to realize that with the exception of your secret boards, anything you pin on Pinterest is completely public. This is why we recommend always using your best judgment when pinning things to Pinterest. Also note that pinning something obscene or overtly offensive can result in the termination of your Pinterest account.

SOURCES

<https://edu.gcfglobal.org>



Erasmus+

CYBER SECURITY IN SCHOOLS

HIDDEN DANGERS IN SOCIAL MEDIA



**KEŞAN
TİCARET VE
SANAYİ ODASI
MTAL**

EDİRNE/TURKEY





HIDDEN DANGERS IN SOCIAL MEDIA



How to Protect Your Child from the Top 7 Dangers of Online Gaming

Cyber bullying
Privacy Problems
Personal Information on Consoles, Computers and Devices
Webcam Worries
Online Predators
Hidden Fees
Malware





What are the hidden dangers on social media?

youtube

online games

tiktok

marketing on social media

Monitor your child's Internet activities closely.

If we spend time with our children and stand by them, they will survive with little damage even if they encounter such content.

HIDDEN DANGERS IN SOCIAL MEDIA

Why Do We Use Social Media So Intensely?

We are exposed to an
endless stream on
social media.

Advertisements,
phenomena, trends,
shares, news and
information content,
photos, videos...

Although we are not
aware of it,
researches say that
we use the internet
for an average of 7
hours a day, and we
spend 3 hours of
these 7 hours using
social media.

Social media is one of
the tools we use
most, especially with
the effect of mobile
phones.



The risks you need to be aware of are:

cyberbullying (bullying
using digital technology)
invasion of privacy.
identity theft.

your child seeing
offensive images and
messages.

the presence of strangers
who may be there to
'groom' other members.



Talk to your child about underlying issues. Problems with social media use can often mask deeper issues. Is your child having problems fitting in at school? Are they suffering from shyness or social anxiety? Are problems at home causing them stress?



Enforce “social media” breaks. For example, you could ban social media until your child has completed their homework in the evening, not allow phones at the dinner table or in their bedroom, and plan family activities that preclude the use of phones or other devices. To prevent sleep problems, always insist phones are turned off at least one hour before bed.

Encourage exercise and offline interests. Get your child away from social media by encouraging them to pursue physical activities and hobbies that involve real-world interaction.





Erasmus+

Rules

**we should pay attention to
when communicating
on social media**

**We have to
communicate
with people in
a sweet
language.**

**We should
stay away from
lies in our
conversations.**

**We must not
give up on
honesty.**

**We should
not share
our personal
information.**

**We should not
interfere in the
private life of
others.**



SIGNS THAT SOCIAL MEDIA IS IMPACTING YOUR MENTAL HEALTH



SPENDING MORE TIME ON SOCIAL MEDIA
THAN WITH REAL WORLD FRIENDS.



COMPARING YOURSELF UNFAVORABLY
WITH OTHERS ON SOCIAL MEDIA.



EXPERIENCING CYBERBULLYING.



BEING DISTRACTED AT SCHOOL OR
WORK.



SUFFERING FROM SLEEP PROBLEMS.



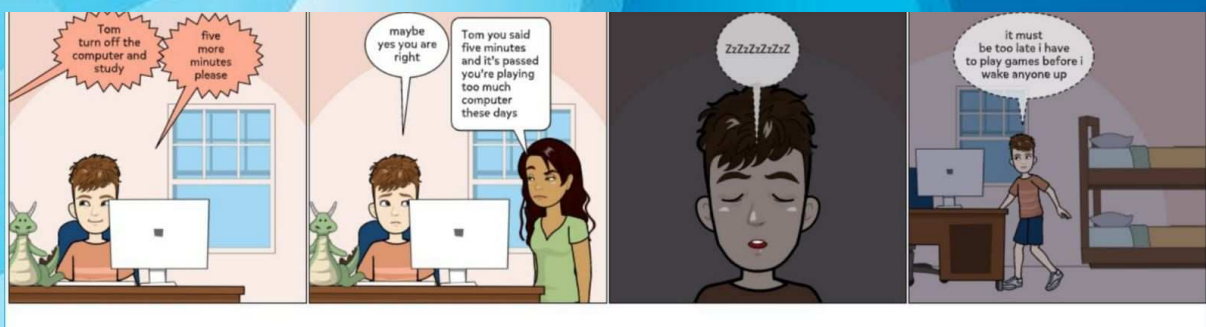
HAVING NO TIME FOR SELF-REFLECTION.



ENGAGING IN RISKY BEHAVIOR IN ORDER
TO GAIN LIKES, SHARES, OR POSITIVE
REACTIONS ON SOCIAL MEDIA.



WORSENING SYMPTOMS OF ANXIETY OR
DEPRESSION.

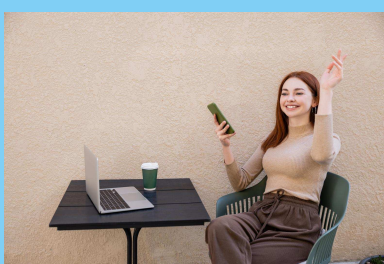
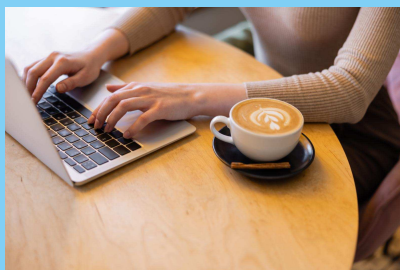
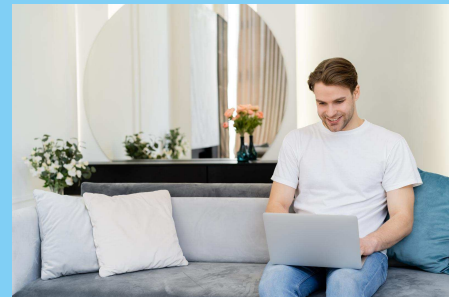
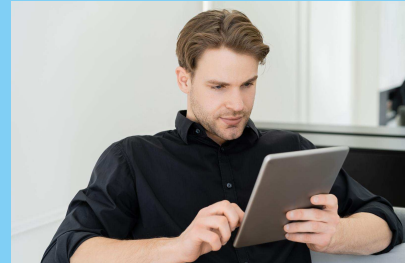
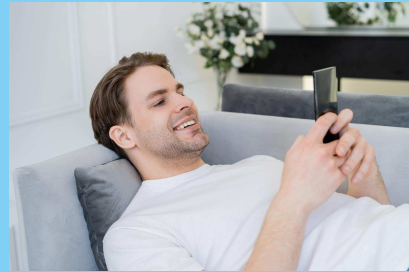


How to avoid the dangers of social media

There are two main things that you can do to avoid the dangers of social media:

Reduce your use of social media, or eliminate it entirely.

- To achieve this, you can use various techniques, such as implementing software-based solutions to limit your access, reducing the visibility of social media on your digital devices, and finding alternative activities to engage in.



Focus on using social media in a positive way.

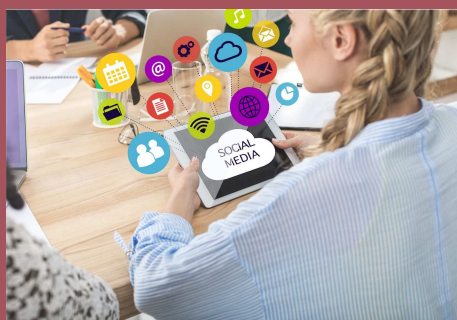
- For example, this can involve using media to actively communicate with people that you care about, rather than using it as a passive way to consume information.



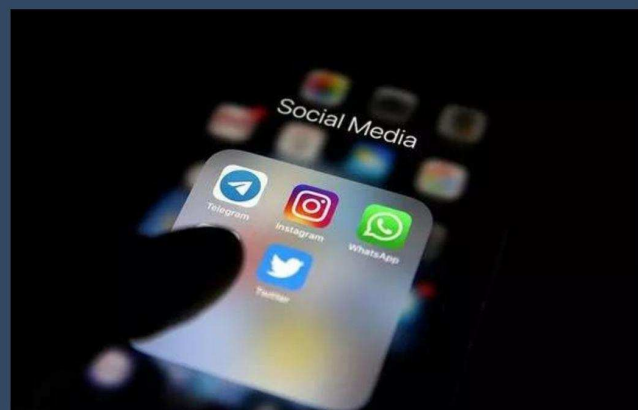
HOW TO TELL IF SOCIAL MEDIA IS AFFECTING YOU NEGATIVELY



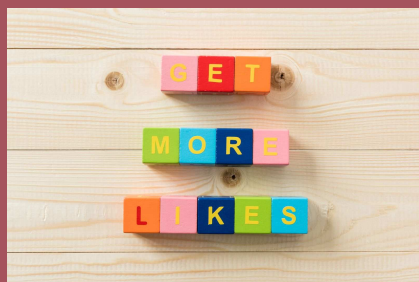
- **Preoccupation.** have you regularly found that you can't think of anything else but the moment that you will be able to use social media again?
- **Tolerance.** Have you regularly felt dissatisfied because you wanted to spend more time on social media?
- **Withdrawal.** Have you often felt bad when you could not use social media?
- **Persistence.** Have you tried to spend less time on social media, but failed?



- **Displacement.** Have you regularly neglected other activities (e.g. hobbies, sport) because you wanted to use social media?
- **Problem.** Have you regularly had arguments with others because of your use of social media?
- **Deception.** Have you regularly lied to your family, friends, or partner about the amount of time you spend on social media?
- **Escape.** Have you often used social media to escape from negative feelings?
- **Conflict.** Have you had serious conflicts with your family, friends, or partner because of your use of social media?



The more issues you've experienced due to your social media use, and the more severe these issues are, the more problematic your use with social media likely is. However, note that this questionnaire revolves only around some aspects of problematic social media use, but doesn't cover all the issues that social media can lead to, meaning that you might have a problematic relationship with social media, even if you haven't experienced these issues in particular.



Finally, it's important to note that you might not be able to accurately judge yourself whether social media is problematic for you. Accordingly, you might benefit from using self-distancing techniques, which will help you assess your situation, or from asking for feedback from someone whose opinion you trust.



Who is most vulnerable to the dangers of social media?

Certain factors are associated with an increased tendency to use social media in a problematic manner, or to suffer from issues as a result of using social media. These factors include:

Suffering from depression.

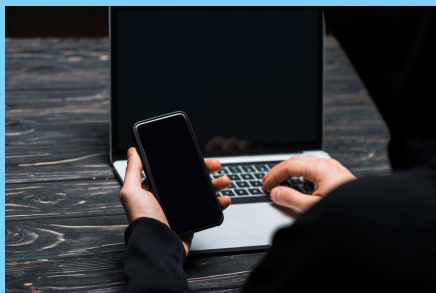
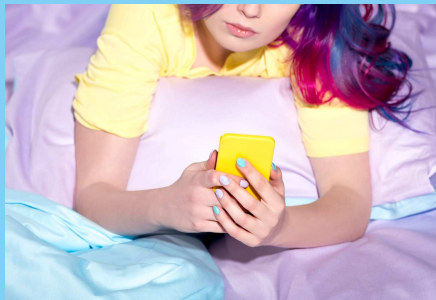
Having low self-esteem.

Being unsatisfied with life.

Having high levels of neuroticism.

Having high levels of narcissism.

Being prone to social comparisons.

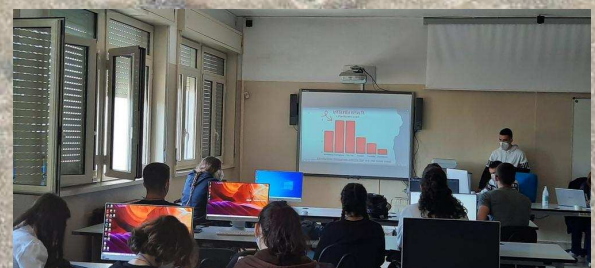


In addition, when it comes to specific certain specific dangers of social media, other factors can increase people's vulnerability. For example, when it comes to cyberbullying of children, factors such as psychological difficulties, lack of parental support, and peer norms can make children more vulnerable.

Finally, the way in which people use social media can also make them more vulnerable to its dangers. For example, people who use social media in a way that does not reflect their true self, for example by trying to reinvent themselves online, tend to experience more issues as a result of social media use, such as loneliness.



ACTIVITY PHOTOS ON MOBILITY TO ITALY



ACTIVITY VIDEOS ON MOBILITY TO ITALY

Video for mobility to Italy



Conference Video on mobility to Italy



Presentation of IT teacher of host school

