

# THE DANGER OF BOT MANIPULATION ON SOCIAL MEDIA



**Dr. Nimet Özgül ÜNSAL**

Ankara Üniversitesi



Funded by  
the European Union



# Presentation Flow



**What is Bot Manipulation?**

**Bot Manipulation Activities**

**What are the Objectives of Bot Attacks?**

**How Does It Work?**  
**The Mechanism of Botnets in Social Media**

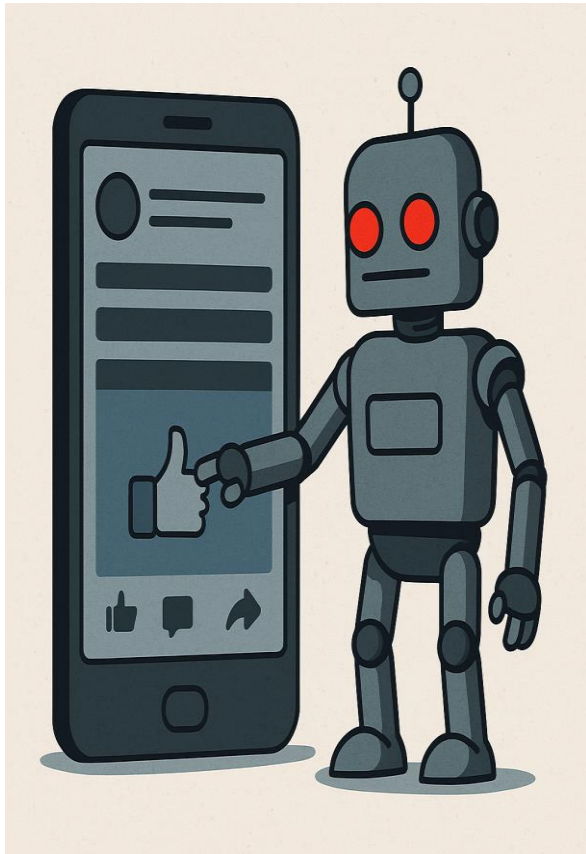
**Examples of Botnet Attacks**

**We are social's World statistics on social media**

**Social Network Security**

**References**

# What is Bot Manipulation?



**Bots** are software-developed accounts that are designed to behave like humans.

# What is Bot Manipulation?



**Bots** and botnet attacks are organized by networks of compromised devices, which are hijacked through malicious software to carry out coordinated, automated, and often malicious activities on social media platforms. While the term “bot” refers to software agents controlled from a central point, “botnet” (robot network) defines the collective network formed by these agents.

# Bot Manipulation Activities

Resharing or  
Reposting  
Existing Content

Commenting  
on and liking  
posts

Meaningful  
posts

Sending  
connection  
requests



# Bot Manipulation Activities

They may be well-intentioned.



They may be malicious.

# What are the Objectives of Bot Attacks?

## Disinformation

- Spreading false news, creating political manipulation.

## Perception Management

- Creating a false positive/negative image about a specific person, company, or country.

## Cyber Harassment (Harassment)

- Harassing or intimidating targeted users.

## Fake Popularity

- Promoting content, users, or campaigns with fake interactions.

## Phishing and Malware

- Redirecting users to malicious software through harmful links.

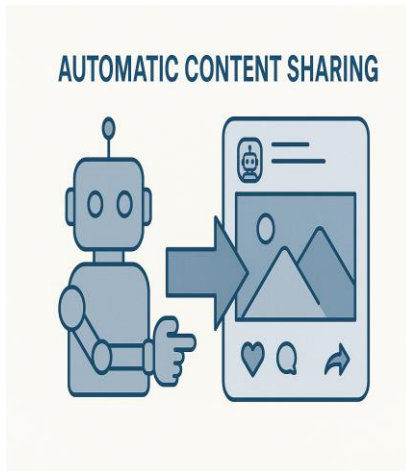
# How Does It Work?

## The Mechanism of Botnets in Social Media

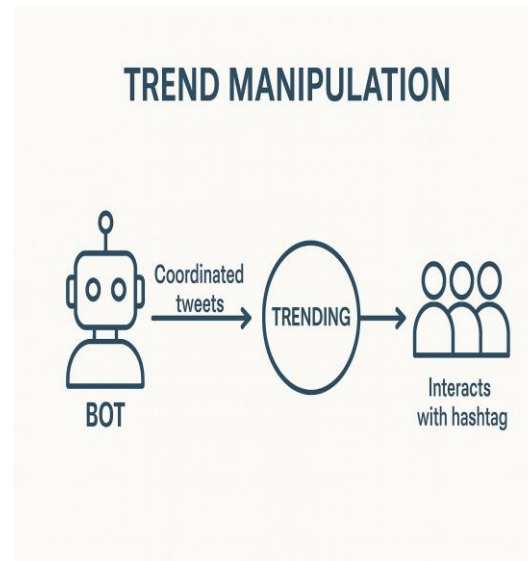


### 1. The Creation of Bots

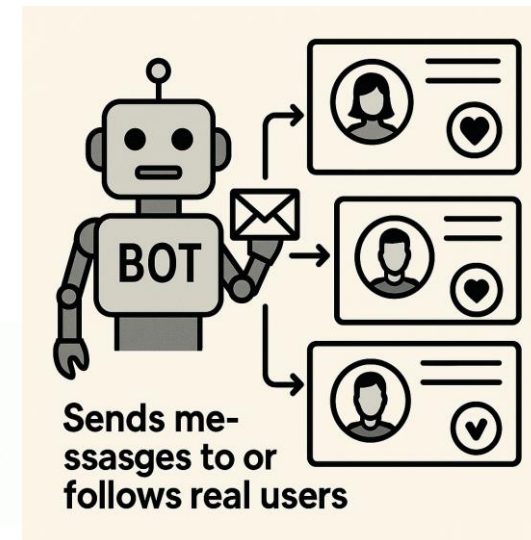
1



2



3





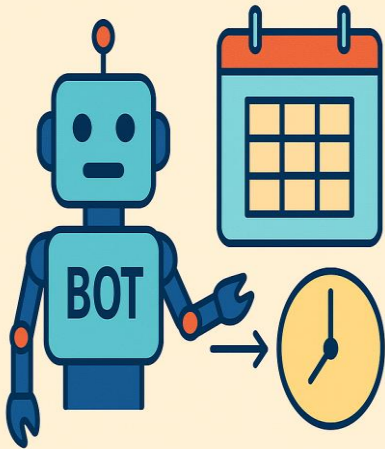


# How Does It Work?

## The Mechanism of Botnets in Social Media

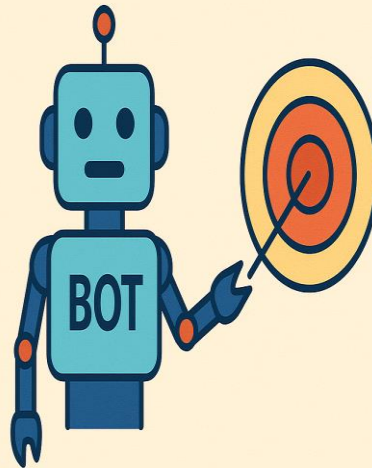
### 2. Command-and-Control (C&C) Mechanism

1



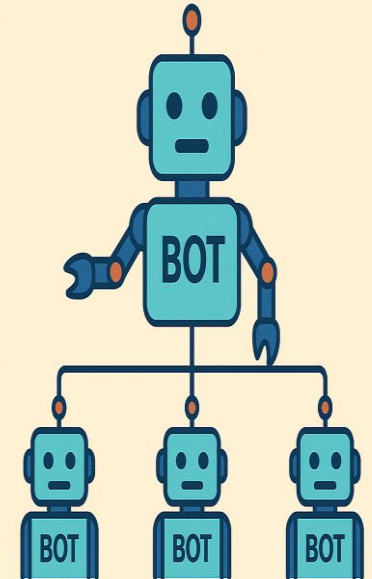
Determines when  
and what to share

2



Directs which targets  
to attack

3



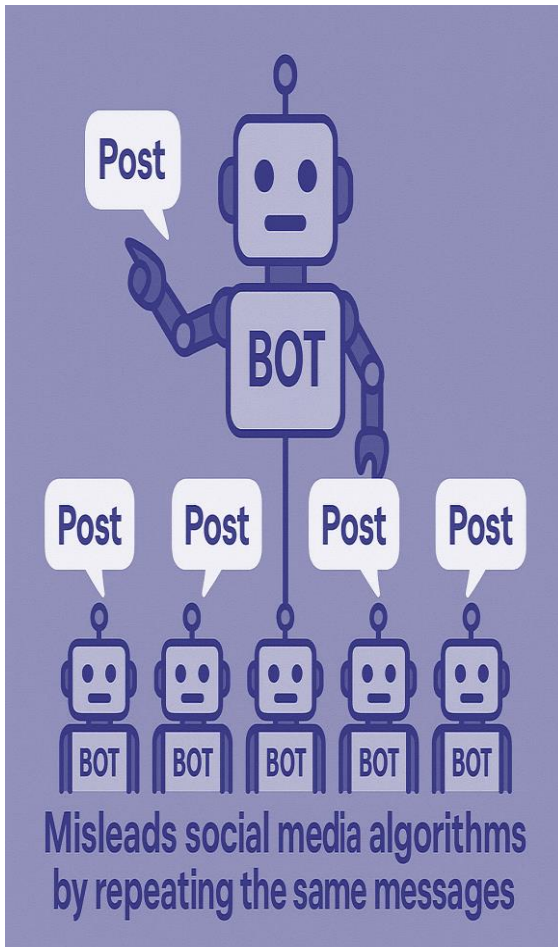
Coordinates bots  
simultaneously



# How Does It Work?

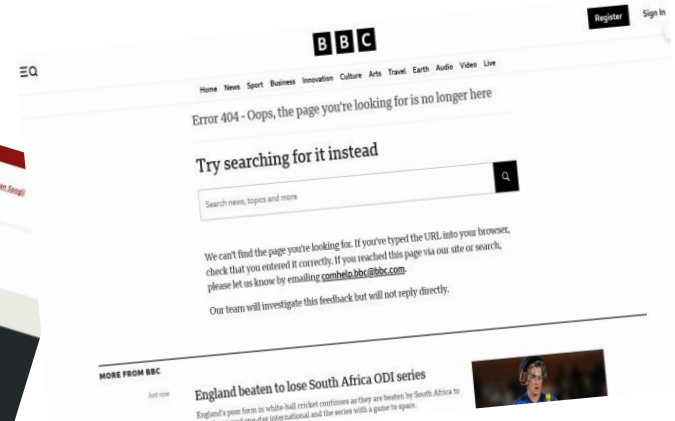
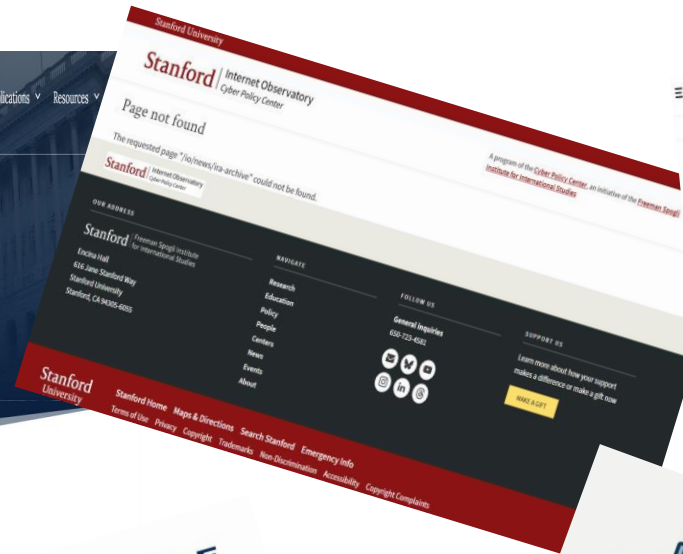
## The Mechanism of Botnets in Social Media

### 3. Coordinated Influence



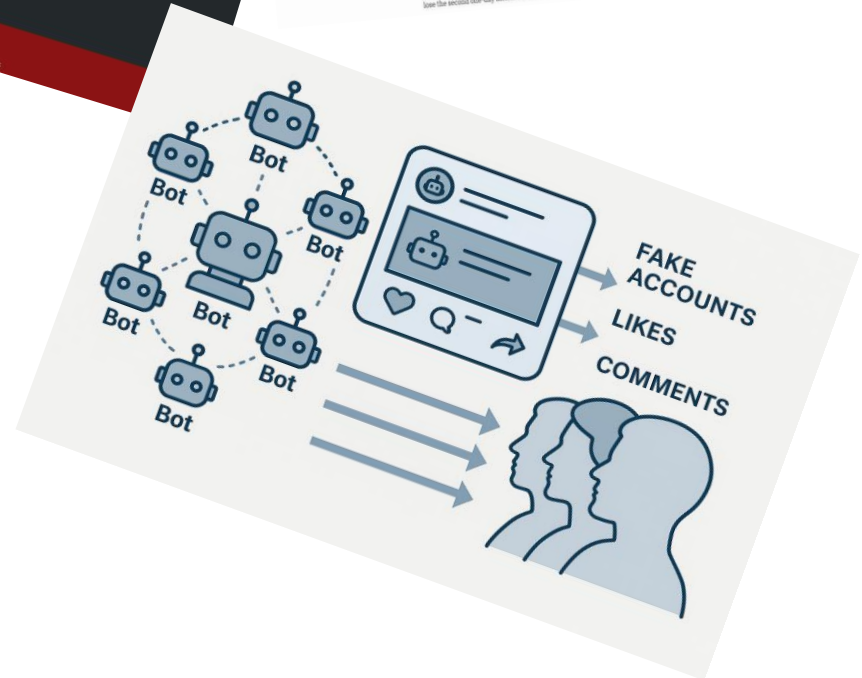
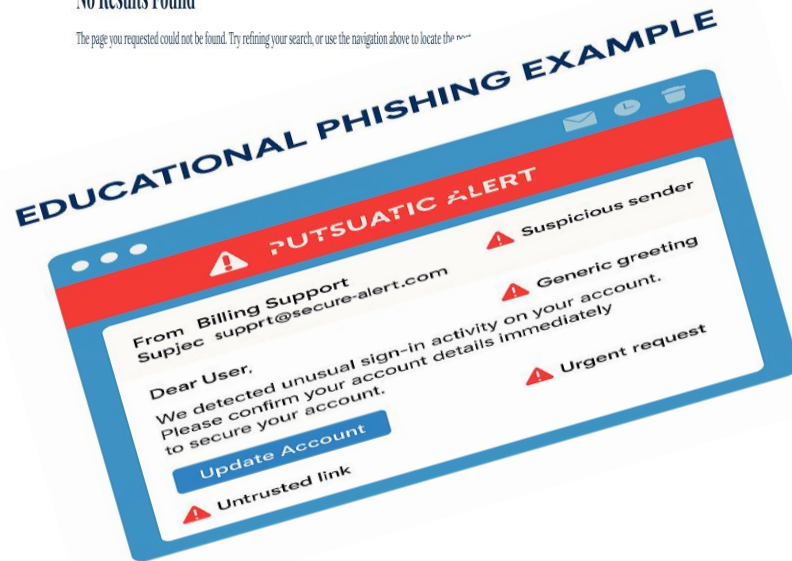
- Messages can become trending topics
- Misleading content can reach broad audiences
- Algorithms may interpret this as genuine user interest

# Examples of Botnet Attacks



No Results Found

The page you requested could not be found. Try refining your search, or use the navigation above to locate the page.



# Examples of Botnet Attacks

## 1. Trend Manipulation (Astroturfing)

**Purpose:** To create artificial popularity.

**Explanation:** Bots rapidly share specific hashtags within a short time to push them onto the “Trending Topic” (TT) list. As real users begin to participate in the trend, the influence grows significantly.

**Example:**

- In Turkey, political hashtags such as #HodriMeydanErdoğan were pushed onto the TT list within hours by bot activity. Subsequently, the content was deleted, leading users to believe that the trend had emerged organically.

## 2. Disinformation-Spreading Bots

**Purpose:** To disseminate misleading or false information.

**Explanation:** Such bots generate and distribute fake content on sensitive issues like health, economy, or war in order to mislead the public.

**Example:**

- During the COVID-19 pandemic, false claims such as “5G spreads the virus” were circulated on Twitter and YouTube through fake accounts. Bots amplified these posts by engaging with them, thereby creating an information environment that appeared credible.

# Examples of Botnet Attacks

## 3. Impersonation Bots (Fake Identity Bots)

**Purpose:** To gain trust and deceive users.

**Explanation:** Fraudsters create fake accounts by imitating well-known individuals or organizations, tricking users into scams.

**Example:**

- Fake accounts created under the name of Elon Musk promised “If you send me crypto, I will return double the amount”, leading to Bitcoin scams worth thousands of dollars (Twitter’s 2020 bot scandal).

## 4. Spam and Link Bombardment

**Purpose:** To redirect users to malicious websites or promote advertisements.

**Explanation:** Bots encourage users to click on fraudulent links through automated comments and private messages.

**Example:**

- On Instagram, messages such as “Someone who follows you has reported you, click the link” are mostly spread by bot accounts. These links typically redirect users to phishing pages with fake login screens.



# Examples of Botnet Attacks

## 5. Emotional Amplification Bots

**Purpose:** To trigger emotions such as anger, fear, or disgust in order to create viral content.

**Explanation:** During social events, bots are often used to spread discrimination, conspiracy theories, or a sense of panic.

**Example:**

- Hate-filled hashtags about refugees (such as #IDontWantRefugeesInMyCountry) were disseminated by bot armies, which subsequently led certain groups to organize street protests.

## 6. Political Pressure and Cyber Harassment

**Purpose:** To silence or intimidate dissenting voices.

**Explanation:** Individuals or journalists expressing opposing views are targeted by bots, which exert pressure through comments and private messages.

**Example:**

- In 2021, journalist Ceren Sözeri was targeted by thousands of bot accounts after sharing news posts. As a result of mass spam reports, her account was temporarily suspended (a domestic example – directly linked to a bot network).

# Examples of Botnet Attacks

## 7. Engagement Inflation and Fake Popularity

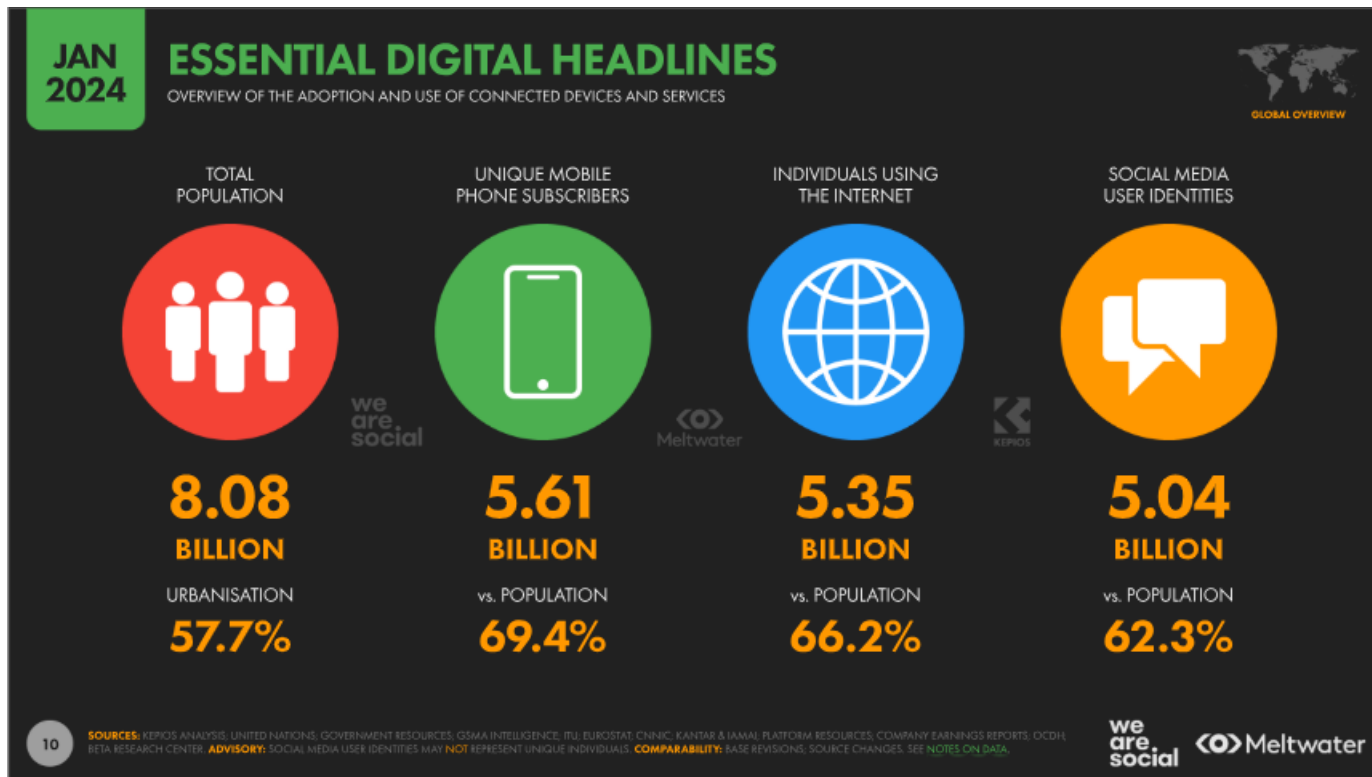
**Purpose:** To artificially boost the growth of content or accounts.

**Explanation:** Bots artificially increase metrics such as likes, shares, and comments. This method is especially used in product marketing, political propaganda, and the creation of influencer accounts.

**Example:**

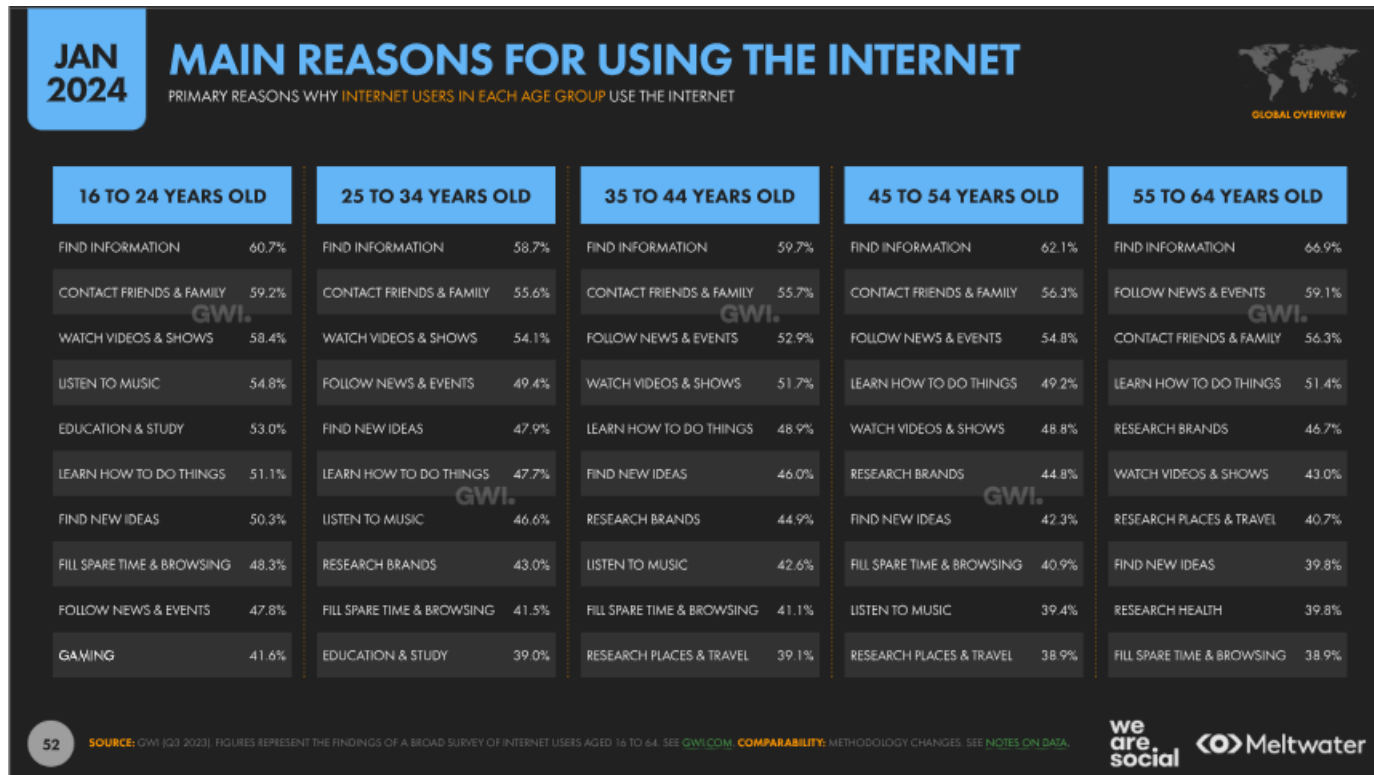
- On Instagram, some users known as “influencers” have created millions of fake followers and interactions using follower and engagement bots. In some cases, brands were deceived by these inflated metrics and entered into sponsorship agreements.

# Social Media Usage Rates in the World

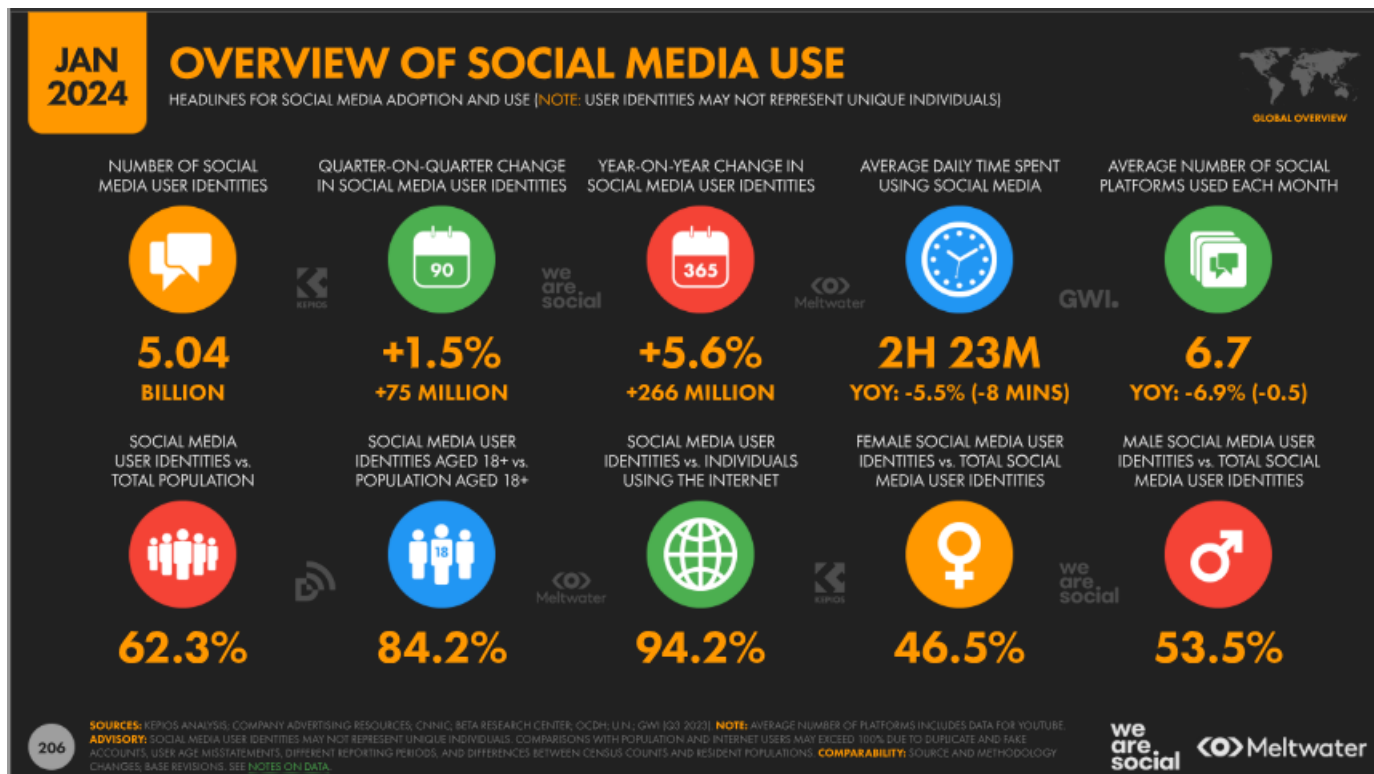




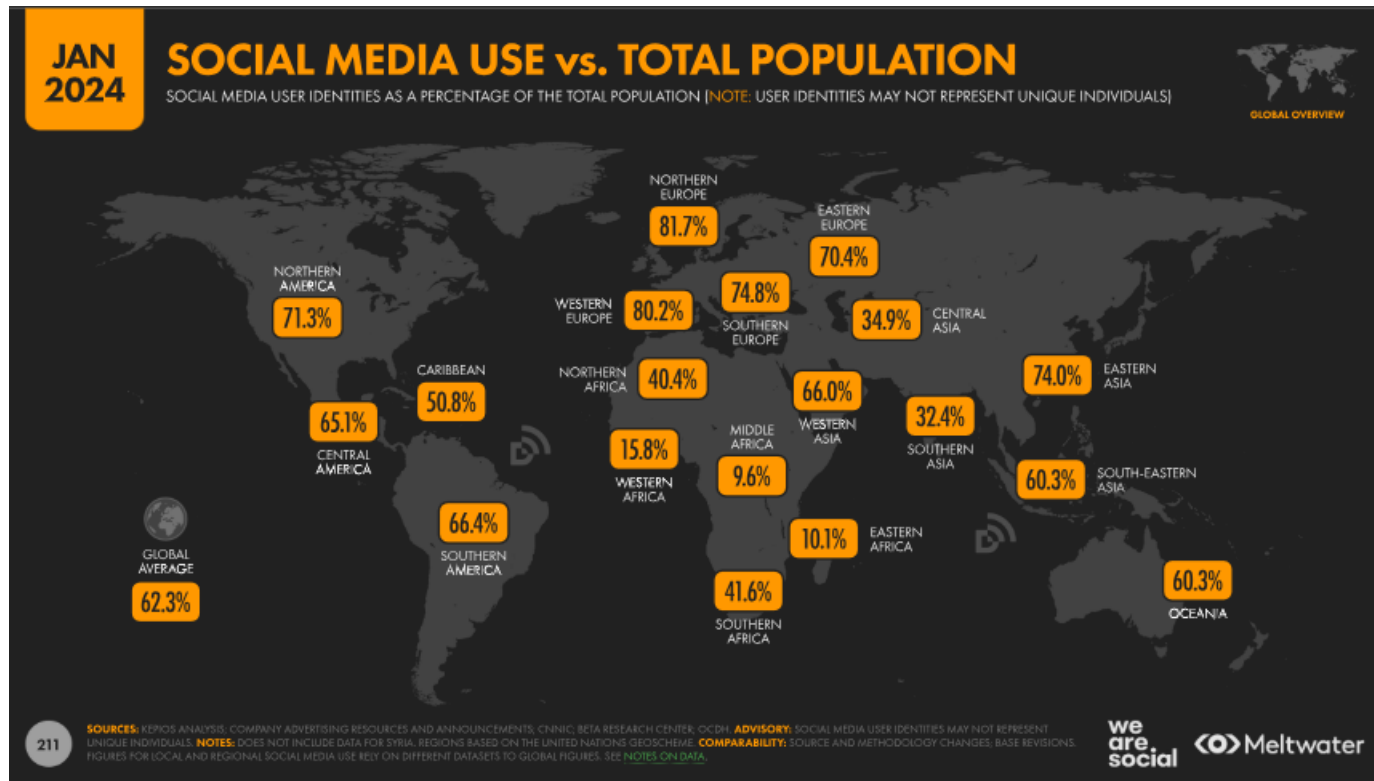
# Ages and Purposes of Internet Use in the World



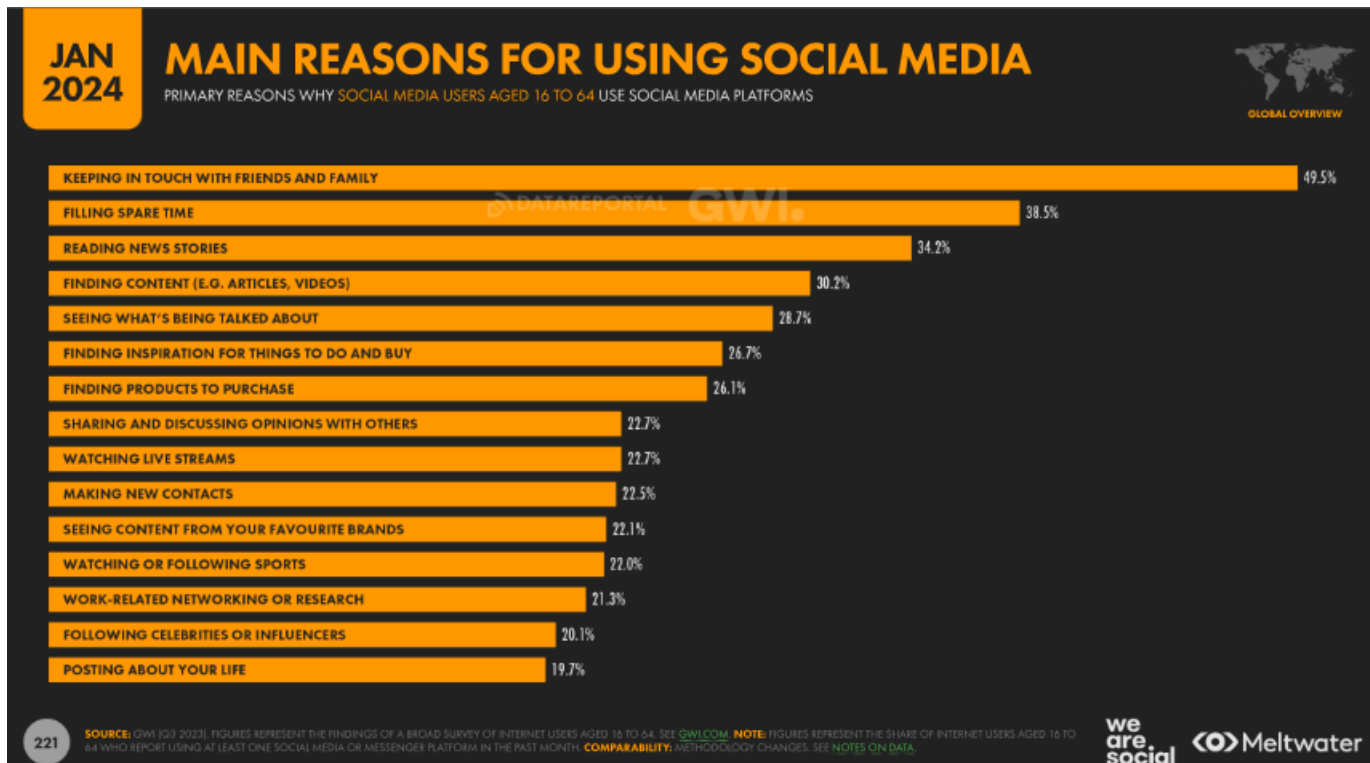
# Social Media Usage Rates in the World



# Social Media Usage Rates by Country



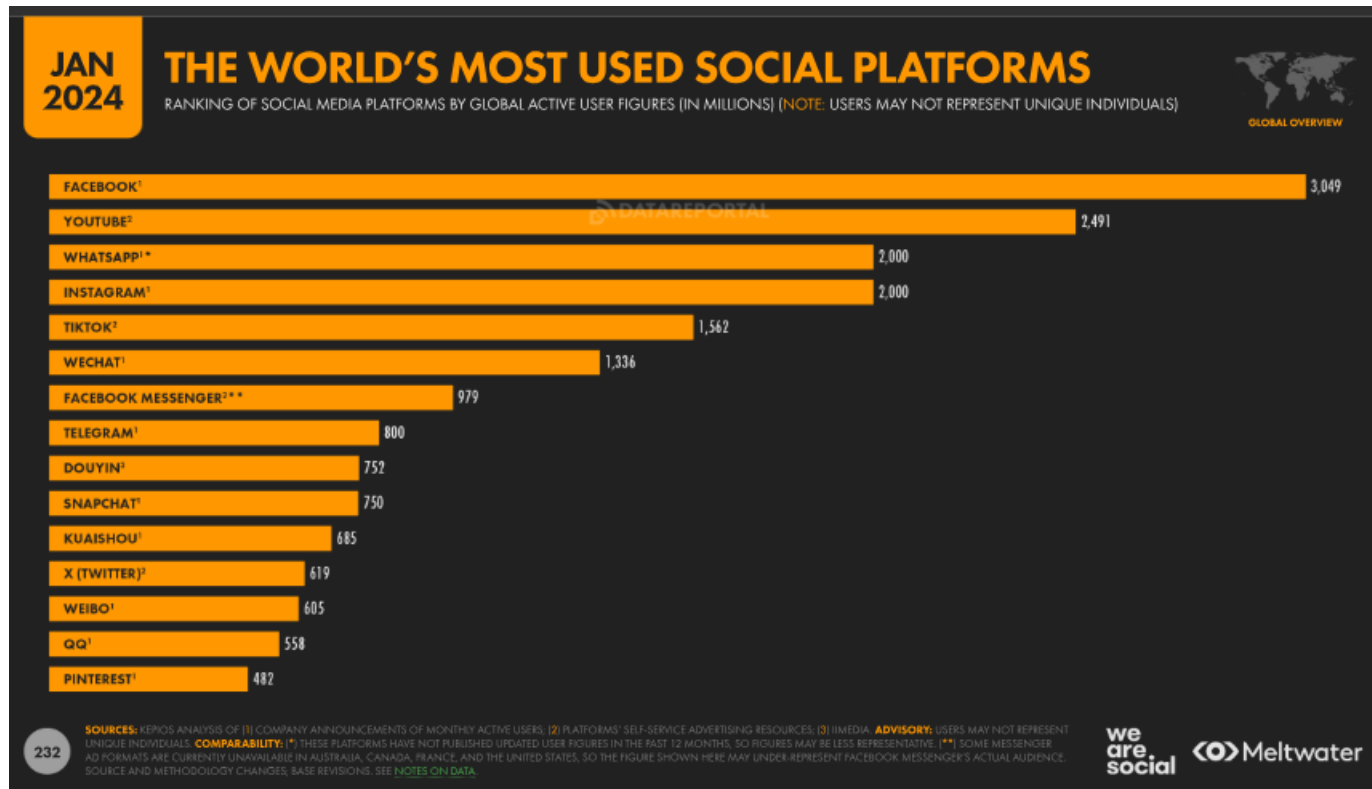
# Social Media Usage Purposes by Country



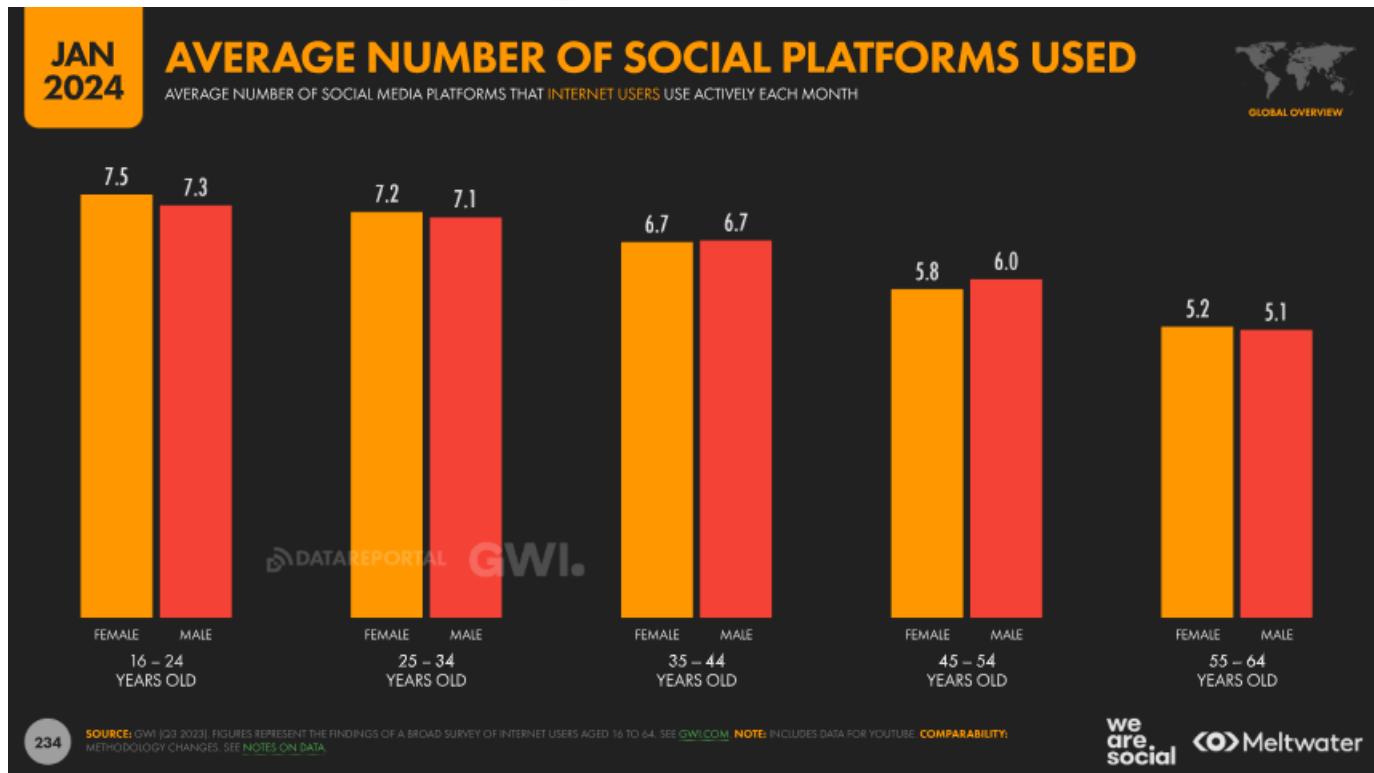
# Social Media Usage Purpose by Country and Age



# The Most Used Social Media Platforms in the World



# Distribution of Social Media Usage Rates by Gender and Age in the World



# Social Network Security





# Social Network Security

Phone number

Home, school, and work addresses

Date of birth

National identification number (e.g., ID number)

E-mail address

Salary information

E-government (e-Devlet) credentials

Driver's license and passport details







Username and password

Do Not Share!



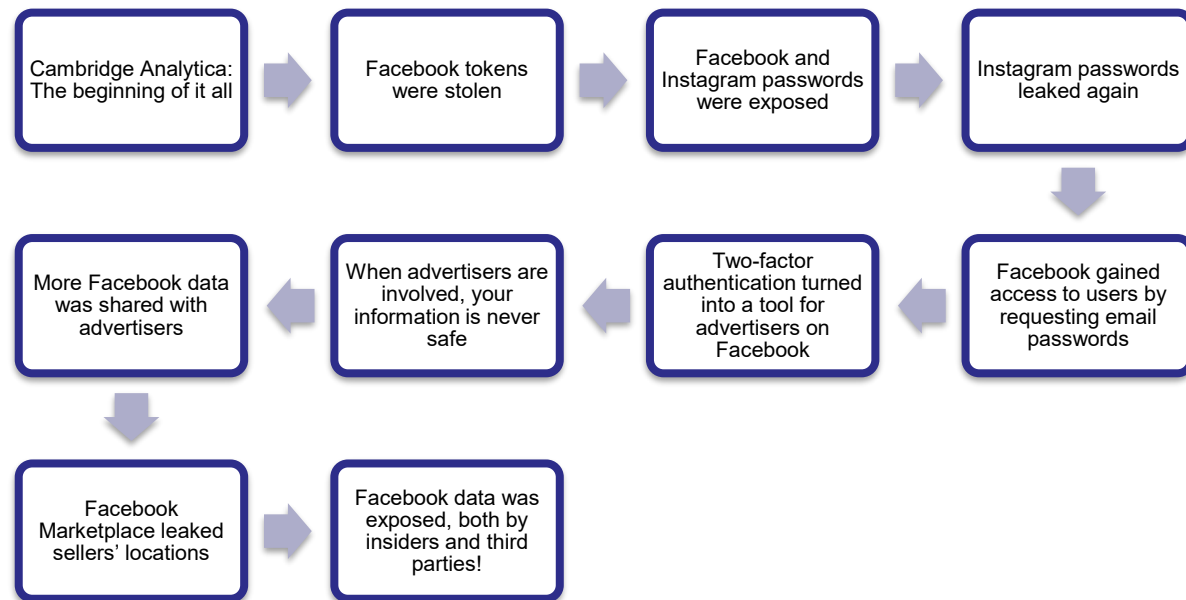
# Social Network Security

Users are also required to act responsibly with regard to copyright (Ocak ve Gökçearslan, 2014).

	Attribution	CC BY	Alıntı
	Attribution-ShareAlike	CC BY-SA	Alıntı-LisansDevam
	Attribution-NoDerivs	CC BY-ND	Alıntı-Türetilemez
	Attribution-NonCommercial	CC BY-NC	Alıntı-Gayriticari
	Attribution-NonCommercial-ShareAlike	CC BY-NC-SA	Alıntı-Gayriticari-LisansDevam
	Attribution-NonCommercial-NoDerivs	CC BY-NC-ND	Alıntı-Gayriticari-Türetilemez

# Social Network Security

## The 10 Most Epic Facebook and Instagram Fails



<https://www.kaspersky.com.tr/blog/facebook-10-fails/6058/>

# Social Network Security

## Security and Privacy Criteria for Messaging Applications

1. Are the data transmitted in an encrypted form?
2. If the data are encrypted, can the service provider still read them?
3. Can you verify the true identities of your contacts?
4. Does the service provider ensure perfect forward secrecy? That is, even if the encryption keys are temporary and compromised, is it still impossible to decrypt past communications with them?
5. Are the source codes of the service open and visible to everyone?
6. Have the cryptographic application procedures and processes been properly documented?
7. Has the application undergone independent security audits within the past 12 months?

	1		2
	1		2
	2		2

<https://www.kaspersky.com.tr/blog/guvenli-olmayan-11-mobil-ve-internet-mesajlasma-uygulamasi/1812/>

# Social Network Security

## How to Prevent Websites from Sending Data to Facebook

1. Go to Settings → Your Facebook Information → Off-Facebook Activity → Manage Your Off-Facebook Activity.
2. From the list, click or tap on the name of the website, and in the pop-up window select Turn off future activity from [website name].

## How to Stop Facebook from Showing You Targeted Ads Based on the Websites and Apps You Use

**1. On the Manage Your Off-Facebook Activity page, which displays the list of services sharing your data with Facebook, click or tap Manage Future Activity.**

On the web version, this option can be found on the right side of the screen.

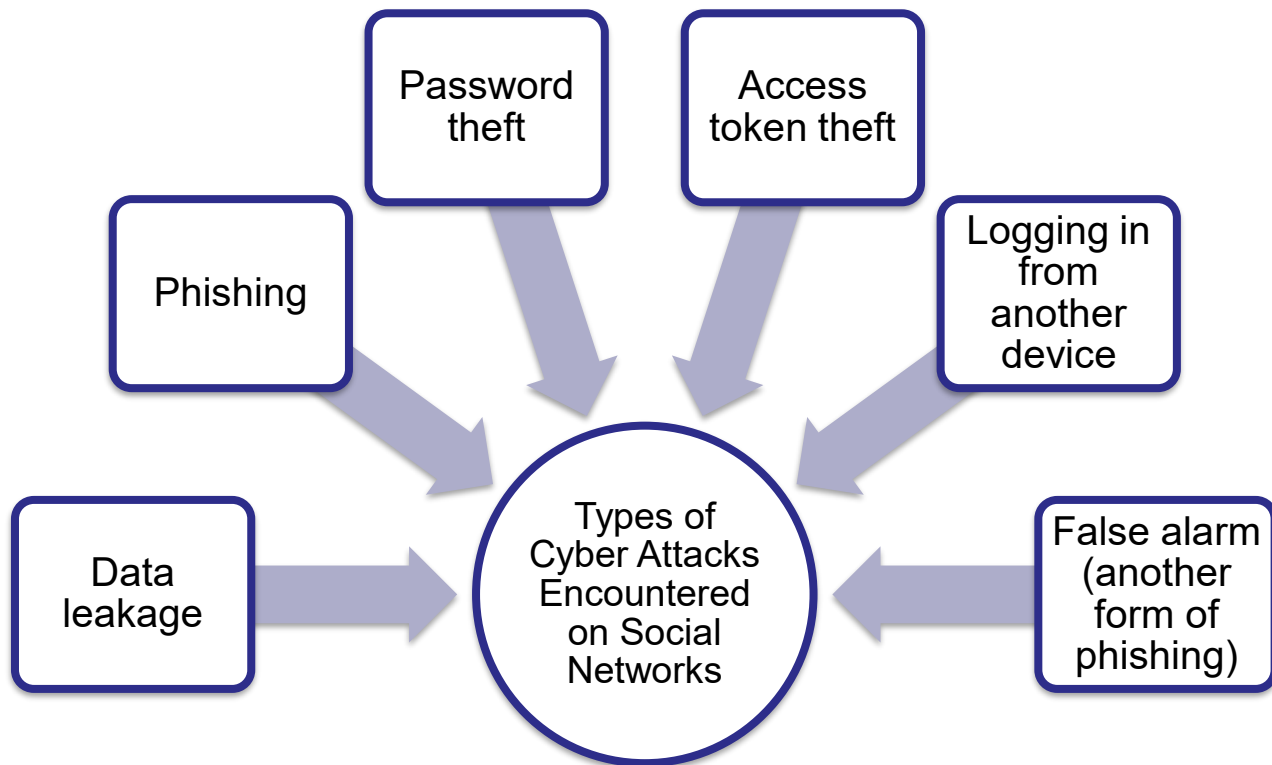
On the mobile version, it can be accessed through the three-dot menu.

**2. Click or tap Manage Future Activity.**

**3. Disable the option Future Off-Facebook Activity.**

<https://www.kaspersky.com.tr/blog/what-is-off-facebook-activity/9359/>

# Social Network Security



<https://www.kaspersky.com.tr/blog/suspicious-login-attempt-facebook-instagram/9386/>

# Social Network Security



## Social Network Users:

(in the USA, Canada, UK, France, Germany, Italy, Spain, Turkey, Russia, Brazil, Mexico, and Japan)

- ✓ **78%** are considering quitting social media.
- ✓ They are tired of spending time on it **(39%)**.
- ✓ They dislike being tracked by big tech companies **(30%)**.
- ✓ They want to stay in touch with friends and family **(62%)**.
- ✓ They are open to a solution that allows them to control their digital memories **(28%)**.

<https://www.kaspersky.com.tr/blog/suspicious-login-attempt-facebook-instagram/9386/>

# Social Network Security



## Necessary Precautions

Antivirus  
software

Software updates

Permissions  
granted during  
app installation

Strong password

Wi-Fi, Bluetooth,  
and infrared  
should not be  
made publicly  
accessible

Avoid links from  
unknown sources

Confidentiality of  
personal data

Security scanning  
of downloaded  
applications

Automatic screen  
lock

Avoid connecting  
to public/open  
wireless networks





# References

- BD Emerson. (2025). Small business cybersecurity statistics: Costs, risks, and survival rates. Retrieved from <https://www.bdemerson.com>
- Exploding Topics. (2025). Cybersecurity statistics: How many cyber attacks happen per day? Retrieved from <https://explodingtopics.com>
- Fortinet. (2025). Fortinet threat landscape report. Retrieved from <https://www.fortinet.com/resources/reports/threat-landscape-report>
- IBM. (2025). Threat intelligence index 2025. IBM Institute for Business Value. Retrieved from <https://www.ibm.com>
- VikingCloud. (2025). Cybersecurity statistics 2025: Costs, attacks, and market trends. Retrieved from <https://www.vikingcloud.com>
- Wikipedia. (2025). 2025 St. Paul cyberattack. In Wikipedia. Retrieved from [https://en.wikipedia.org/wiki/2025\\_St.\\_Paul\\_cyberattack](https://en.wikipedia.org/wiki/2025_St._Paul_cyberattack)
- Wikipedia. (2025). Lazarus Group. In Wikipedia. Retrieved from [https://en.wikipedia.org/wiki/Lazarus\\_Group](https://en.wikipedia.org/wiki/Lazarus_Group)
- IBM. (2025). *IBM X-Force Threat Intelligence Index 2025*. IBM Institute for Business Value. Retrieved from <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index>
- Check Point Research. (2025). *Q1 2025 Global Cyber Attack Report*. Check Point Software. Retrieved from <https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks>
- VikingCloud. (2025). *Cybersecurity statistics 2025: Costs, attacks, and market trends*. Retrieved from <https://www.vikingcloud.com>
- CyberScoop. (2025). *IBM report: Cost of a data breach rises to \$4.44M globally, \$10.22M in U.S.* Retrieved from <https://cyberscoop.com/ibm-cost-data-breach-2025>
- Deepstrike. (2025). *Top industries targeted by hackers in 2025*. Retrieved from <https://deepstrike.io/blog/top-industries-targeted-by-hackers-2025>
- ITPro. (2025). *AI-related breaches are happening in real life, adding \$670k per incident*. Retrieved from <https://www.itpro.com/security/data-breaches/ai-breaches-arent-just-a-scare-story-any-more-theyre-happening-in-real-life>

# THANK YOU!



Funded by  
the European Union



**Dr. Nimet Özgöl ÜNSAL**