

Cybersecurity attacks and defences



INTRODUCTION

🌐 In the age of digitization, cyber security is a key element in protecting data and privacy.

⚠️ Every day there are new threats and attacks that can affect any of us.

🎯 The purpose of this presentation is:

- Introduce the topic of cyber security,
- Discuss the most common attacks,
- Present effective methods of defense.



What is cyber security?

Cyber security is a set of practices, technologies and processes designed to protect computer systems, networks, software and data from unauthorized access, use, disclosure, disruption, modification or destruction.



In other words, cyber security is the protection of our digital assets.



Why is cyber security so important in this day and age?



Growing dependence on technology:

Our lives are becoming increasingly digital. We store data in the cloud, communicate online, work remotely and even control home appliances via the Internet.



Increase in cybercrime:

Cybercriminals are becoming more sophisticated and using new technologies to launch attacks.



Global consequences of the attacks:

Cyber attacks can destabilize economies, disrupt critical infrastructure (e.g., power grids, banking systems) and affect national security.



Key aspects of cyber security:

01

Confidentiality:

Ensure that information is available only to authorized persons.

02

Integrity:

Protecting data from unauthorized modification.

03

Availability:

Ensure continuous access to information and systems for authorized users.

04

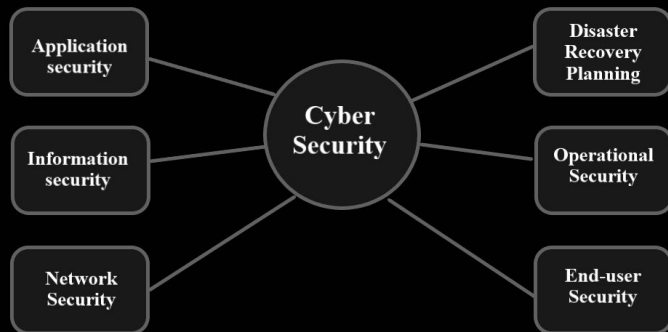
Authentication:

Confirm the identity of users.

05

Unauthorized:

Preventing unauthorized activities.







Security in the Digital World:

- **Computer Systems:** Cyber security protects computers from malware, hacking attacks and unauthorized access.
 - **Example:** Firewalls block malicious network traffic to prevent intrusions into systems.
- **Networks:** Cyber security protects networks from DoS and DDoS attacks, ensuring stability and availability of services.
 - **Example:** Intrusion detection systems (IDS) monitor network traffic, identifying and blocking suspicious activity.
- **Data:** Cyber security protects data from theft, modification and destruction.
 - **Example:** Data encryption prevents unauthorized people from reading information.

Cyber security is not only about technology, but also about **people and processes**:

User awareness: Education and training help reduce the risk of social engineering attacks, such as phishing.

Security policies: Clear procedures and policies help manage risks and respond to incidents.



Security in the Digital Age



Our lives are inextricably **linked to technology**. We store data in the cloud, communicate online, work remotely and use online services on a daily basis. This **growing dependence on technology** makes us more vulnerable to **cyber threats**.



Cyber security is the key to protection:

- **Privacy:** Our personal, financial, medical and other sensitive information is valuable to cyber criminals. Privacy violations can lead to identity theft, blackmail and other serious consequences.

Doxing – the deliberate disclosure of personal information online without consent – is a real threat to our reputation and security



- **Financial Security:** Cyberattacks can cripple companies' operations, cause data loss and lead to huge financial losses

Ransomware – malware that encrypts data and demands a ransom to decrypt it – is a growing threat



Cybercriminals are constantly improving their methods:

- They use advanced techniques such as phishing, social engineering and malware to gain access to our data and systems
- **Malware** takes many forms, from viruses and worms to Trojans and rootkits, each with a different purpose and modus operandi





What is Malware?



Malware is short for “malicious software” and refers to any type of computer program designed to harm computer systems, networks or users.

Malware can come in a variety of forms and purposes, but usually works in secret to avoid detection and maximize its harmful effects.



Types of Malware:

- **Viruses:** Self-replicating code that attaches itself to files or programs and infects other files when the infected file is run.
- **Worms:** Self-replicating malware that does not require a host to spread. Worms can spread through computer networks by exploiting vulnerabilities in software.
- **Trojan horses:** Software that pretends to be a useful tool, but once launched, performs harmful actions such as stealing data or damaging the system.
 - Example: An attacker can create a Trojan horse that looks like a program to play music, but actually steals user passwords.
- **Rootkits:** Software that provides permanent access to a system with administrator privileges while hiding its presence from administrators.
- **Logic bombs:** Code embedded in legitimate programs that is activated when certain conditions are met, such as on a certain day or when a specific user logs in. Once activated, a logical bomb typically damages the system.
- **Spyware:** Spyware that collects information about a user without the user's knowledge. Examples of spyware include keyloggers (keystroke loggers) and screen scrapers (programs that read data from the screen).
- **Scareware:** Software that scares users into taking actions that ultimately compromise their security, such as paying for a fake antivirus program.



YouAreAnIdiot

you are an idiot

YouAreAnIdiot rose to fame between 2009 and 2012, initially as a harmless application. But how did it become an inspiration for malware creators?



Beginnings and transformation:

- **Innocent fun:** The app displayed the message “You are an idiot!” with three smiling emoticons, attracting attention with its humorous form.
- **Return of a legend:** Popularity and nostalgic memories caused people to create copies of it. Unfortunately, some of them have been modified into malware.

Action of the malicious Trojan:

- **Screen chaos:** the Trojan triggered “jumping” browser windows, and attempts to close them caused new, smaller windows to open.
- **System lockdown:** Malicious scripts consumed system resources until it completely crashed.
- **Shutdown attempt:** Alt+F4 shortcut displayed successive “You are an idiot!” messages.

Removal and evolution:

- **Simple solution:** the infected system could be saved by restarting or terminating the process in Task Manager.
- **Evolution of malicious code:** The original scripts were removed in 2012, but alternative versions emerged, often containing harmful or shocking content.

Conclusions:

YouAreAnIdiot is an example of how an innocent application, influenced by legend and user interest, can inspire malware developers, turning a digital joke into a cyber threat.

Watykańczyk: The Polish equivalent of YouAreAnIdiot

Around 2015, there was a program known as Vatican – inspired by the legend YouAreAnIdiot, but based on local cultural references. Its goal was to annoy the user in a humorous, though sometimes controversial, way.

Program operation:

- **Musical surprise:** Barka, a song associated with the Polish Pope, was played in the background.
- **Memes with the Pope:** Various memes with the image of John Paul II were displayed on the screen.
- **DVD drive manipulation:** The program opened and closed the drive, displaying the message “Insert creamer.”
- **Sudden shutdown of the computer:** At 21:37, the system was automatically shut down to symbolize the hour of the Polish Pope's death.

Controversy:

The Vatican was intended only to irritate users, but relying on the image of John Paul II, important to many Poles, stirred mixed emotions. For certain segments of society, especially those of deep faith, such a joke could have been unpleasant and even offensive.



How to protect yourself from Malware:

- Install an antivirus program and update it regularly.
- Do not open suspicious e-mail attachments or click on links from unknown senders.
- Update your operating system and software regularly.
- Use strong passwords and do not use the same password for multiple accounts.
- Be careful when downloading files from the Internet.
- Make regular backups of important data.

Remember!

Cybercriminals are constantly improving their methods, so it's important to stay up-to-date on the latest threats and take the proper precautions to protect your data and systems.





Ransomware: Digital Blackmail in a New Edition

Ransomware is a type of malware that blocks access to a user's computer system or files and then demands a ransom to unlock them. It is a sophisticated form of digital blackmail that poses a growing threat to individuals and organizations around the world.

Mechanism of action:

1. **Infection:** Ransomware can enter a system in a variety of ways, such as through email attachments, infected websites or software vulnerabilities.
2. **Encryption:** Once the system is infected, the ransomware encrypts user files, preventing access to them.
3. **Ransom demand:** A message appears on the victim's screen demanding a ransom, usually in cryptocurrency such as Bitcoin, in exchange for a decryption key.
4. **Time pressure:** Cybercriminals often use time pressure tactics, setting a short deadline for paying the ransom, threatening to permanently delete the data.

Types of Ransomware:

- **Locker ransomware:** Blocks access to the entire operating system.
- **Crypto ransomware:** Encrypts user files.
- **Crypto-trojans:** A variant of the Trojan that encrypts files.





WannaCry: The Global Attack That Shook the World

WannaCry is **ransomware** that spread to hundreds of thousands of computers around the world in May 2017. The attack paralyzed the operations of **hospitals, companies and government institutions**, proving the destructive power of malware in the digital age.

How did WannaCry work?

WannaCry **combined two components**: a worm and ransomware.

- The worm exploited a **security vulnerability in the SMB (Server Message Block) protocol** on Windows systems. The vulnerability, known as ETERNALBLUE, allowed the worm to **spread between** computers on the same LAN.
- Once infected, the ransomware **encrypted user files** and then displayed a ransom demand of \$300 (later raised to \$600) in Bitcoins.

WannaCry also spread through malicious **email attachments**.





Global Chaos:

The WannaCry **attack caused panic** around the world. Hospitals in the UK had to cancel operations, companies lost data and suffered financial losses, and government institutions faced paralyzed systems.

The scale of the damage:

- More than 200,000 computers in 150 countries were infected.
- Financial losses amounted to billions of dollars.

WannaCry revealed:

- **The importance of software updates:** the ETERNALBLUE vulnerability was patched by Microsoft two months before the attack, but many systems had not been updated.
- **Insufficient awareness of cyber threats:** Many attack victims were unaware of how to protect themselves from ransomware.

Ransomware Protection:

WannaCry was an important lesson for the world. The attack underscored the importance of a proactive approach to cybersecurity.

To protect yourself from ransomware, you should:

- Update systems and software regularly.
- Back up your data.
- Be careful when opening e-mail attachments and clicking on links.
- Use strong passwords and multi-component authentication.
- Implement an antivirus program and update it regularly.
- Train employees on cyber security.



Remember: Preventing ransomware attacks is much easier than dealing with their effects.



Who is behind the attack?

Initially, there **was no clear evidence pointing** to a specific perpetrator. However, as the investigation proceeded, circumstantial evidence and suspicions emerged:

- **Lazarus group:** Cybersecurity experts have identified similarities between the WannaCry code and software used by the Lazarus group, which is linked to North Korea.
- **No conclusive confirmation:** Despite circumstantial evidence, there is no hard evidence to unequivocally attribute the attack to North Korea. Other cybercriminals may have copied code snippets or used Lazarus group tools.

Difficulties in identifying the perpetrators:

- **Network anonymity:** Cybercriminals use anonymizing networks and tools to hide their identities.●
- **Complicated investigations:** Cybercrime investigations are complex and require international cooperation.●
- **Lack of incentive to expose perpetrators:** In some cases, governments or organizations may be reluctant to reveal the identity of perpetrators, fearing further attacks or reputational damage.





Sociotechnical Attacks: Manipulation of Man, Key to Data

In the world of cyber security, advanced technologies and sophisticated software are not the only threats. Humans, with their weaknesses and vulnerability to manipulation, often become the weakest link in the security chain. It is on this fact that sociotechnical attacks are based, using psychology and deception to gain access to sensitive data, systems or resources.

The Essence of a Sociotechnical Attack:

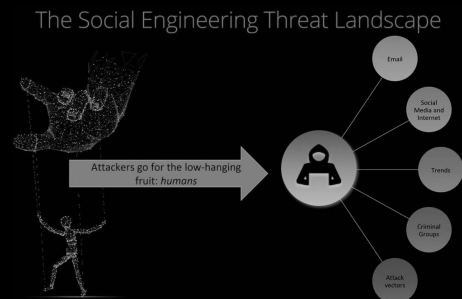
Sociotechnical attacks do not focus on hacking into systems by force, but on exploiting human errors and tendencies to trust. The attacker's goal is to get the victim to take actions that compromise the security of themselves or the organization they work for.

Social engineering attackers use various techniques to manipulate their victims:

- **Phishing:** Sending fake emails or SMS messages that impersonate credible sources, such as banks, government institutions or well-known companies. The purpose of phishing is to extract sensitive data such as logins, passwords, credit card numbers.
- **Pretexting:** creating a false pretext or story to build trust with the victim and phishing for information.
- **Baiting:** Using an enticing offer or gift to entice the victim to click on a link or download a file that contains malware.
- **Quid pro quo:** Offering something in exchange for access to information or systems.
- **Tailgating:** Getting into a secured area by following a person who has the right of entry.

Why are social engineering attacks so effective?

- **They exploit human emotions:** Attackers often appeal to fear, a sense of urgency or a desire to help in order to manipulate their victims.
- **Difficult to detect:** Social engineering attacks do not require advanced technical skills and often go unnoticed by traditional security systems.
- **Constantly evolving:** Cybercriminals are constantly refining their methods and adapting them to current trends.





Phishing Campaign ArmagedOn

Who was ArmagedOn?

Tomasz T., known as ArmagedOn, is a Polish hacker who for years conducted extensive cybercriminal activities, including ransomware and phishing attacks.

Modus operandi:

- **Ransomware:** Encrypted thousands of computers in Poland, demanding a ransom in bitcoins (\$200-400).
- **Phishing:** Impersonated well-known companies, banks, postal operators and institutions, sending out fake messages with viruses (Allegro).
- **Forged wire transfers:** Used viruses to divert money to his accounts by manipulating data on users' clipboards.

Effects of activities:

- Paralyzed systems of many Polish users and companies.
- Criminal proceeds placed on cryptocurrency exchanges.



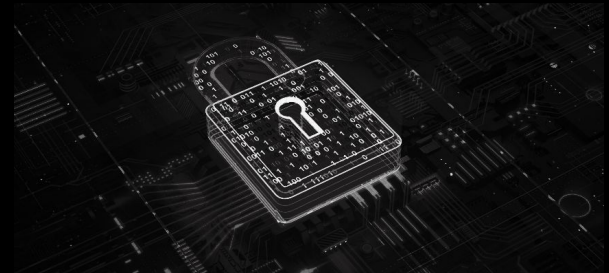
Your Arsenal of Defense in Cyberspace

1. Increased vigilance: best weapons:

- **Always verify the sender:** Pay attention to the sender's e-mail address. Check it for correctness, typos or suspicious domains.
- **Don't click on links from unknown senders:** First hover your cursor over the link to see the exact URL. Make sure it is an authentic site and not a fake site.
- **Be suspicious of requests for confidential data:** No credible institution would ask you for your password, credit card number or other sensitive data via email or SMS.
- **Check for grammatical and spelling errors:** Cybercriminals often make language mistakes. Be wary if the message contains typos or awkward wording.
- **Beware of messages that evoke strong emotions:** Attackers often use fear, a sense of urgency or a desire to help to manipulate their victims.

2. Tools and techniques to increase security:

- Strong passwords and multi-component authentication: Use unique, strong passwords for each account. Enable multi-component authentication wherever possible.
- Up-to-date software: Update your operating system and all applications regularly to patch security vulnerabilities.
- Anti-virus and anti-phishing software: Use anti-virus and anti-phishing software to block known threats.
- Reporting suspicious messages: Report suspicious correspondence to appropriate institutions, such as the IT security team at Two





Doxing: Revealing Secrets, Violating Privacy in the Age of the Internet

Doxing is the malicious act of publicly revealing a person's personal information without their consent. This information, which is often real but obtained illegally, can include name, home address, phone number, financial data and even photos and videos. The purpose of doxing is to invade privacy, intimidate or publicly humiliate the victim.

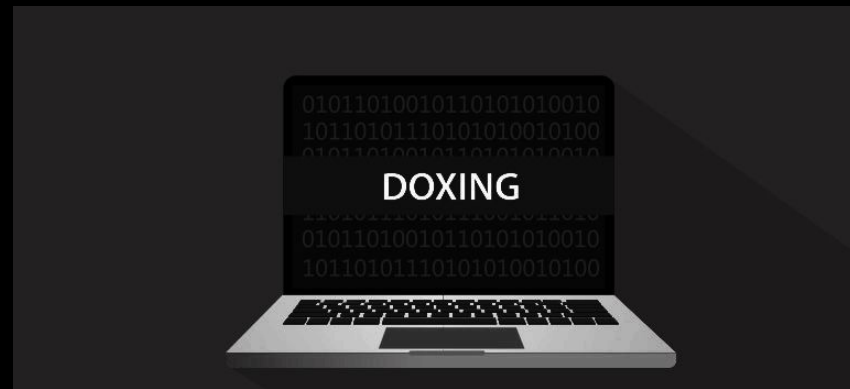
Types of Doxing:

- **Deanonymization:** Revealing the identity of a person who was previously anonymous, such as a person using a pseudonym on the Internet.
- **Targeted doxing:** Revealing specific information about someone to enable contact or locate that person, such as phone number, home address, username and password.
- **Delegitimizing doxing:** Disclosing confidential or intimate information that could damage the victim's reputation or credibility, such as medical, legal, financial data, private messages or photos.

What to do if you fall victim to Doxing?

- Gather evidence of doxing.
- Report the incident to the platform where your data was published.
- Contact law enforcement agencies if necessary.
- Seek support from organizations dedicated to protecting victims of cyberbullying.

Remember: Doxing is a serious crime that can have long-term negative consequences. Be cautious online and protect your personal information.





Doxbin: Controversial Platform

Doxbin is a Dark Web site known for publishing sensitive personal information and materials obtained without the consent of their owners. The platform is controversial due to the unethical and often illegal nature of its published content.

What is Doxbin?

Doxbin is a repository for disclosed personal data and other sensitive information. Users can anonymously upload and publish other people's data without fear of legal consequences.

Content published on Doxbin includes:

- **Personal information:** Names, home addresses, phone numbers, email addresses, dates of birth, etc.
- **Financial information:** Credit card numbers, bank details, transaction history.
- **Login information:** Usernames and passwords for various online services.
- **Compromising material:** Photos, videos, private messages, documents.

Who are Doxbin's users?

- Doxbin users are a diverse group, motivated by different goals:
- Hackers: They often publish data they have stolen through hacking attacks.
- Revenge-seekers: They use Doxbin to take revenge on former partners, employers or others they hold a grudge against.
- Internet trolls: They publish data for entertainment or to sow chaos.
- Activists: They release data on public figures or corporations to expose alleged crimes or activities.

Doxbin controversy:

Doxbin has been widely criticized for invading privacy and promoting illegal activities. The platform facilitates cyberbullying and stalking, and can lead to identity theft and other crimes. Many security experts consider Doxbin a serious threat to Internet security. Despite numerous calls to shut down the site, Doxbin continues to operate, moving between different domains to avoid censorship.

DOXBIN

New Onion (Bookmark it): doxbinrqb7lcs1w.onion

Featured Dox: [Jason Lee Van Dyke a/k/a @MeanTXLawyer](#)

[View the dox archive](#)

Enter a name

DOX go here. This is not your personal slam page, nor is it a page on which to brag about having owned someone, or to complain that they owned you. Post whatever info you have and SHUT UP. There are no limits on what kind of info you can post, so feel free to drop SSNs, financial, medical info, or anything else that is blatantly illegal. We have a strict non-removal policy, so once the dox go up, they stay up unless they are inaccurate, or you didn't include at least a name and address. Asking for dox to be removed is probably the surest way for them to be updated and expanded upon. You have been warned.



A threat that is often overlooked: Fake News

What is fake news?

Fake news – intentionally false information published to mislead. They spread through social media, online portals and communication applications. Often used as a tool for social and political manipulation.

Why is this threat serious?

- **Impact on society**
 - Deepening social divisions.
 - Reinforcement of stereotypes and prejudices.
- **Disinformation at key moments**
 - Elections, health crises (e.g., COVID-19 pandemic), international conflicts.
- **Loss of trust in the media**
 - Decline in the credibility of authentic information.

What are the sources of fake news?

- Internet bots and automated accounts.
- Portals and sites operating to generate sensationalism or financial gain.
- Disinformation campaigns sponsored by states or interest groups.

How to protect yourself from fake news?

- **Verify your sources**
 - Using credible, verified media.
- **Media education**
 - Learning to recognize manipulation and disinformation techniques.
- **Fact-checking tools**
 - Using sites such as Demagog.org.co.uk, Snopes.com and FactCheck.org.





WikiLeaks: what is it and how does it work?

What is WikiLeaks?

- An international non-profit organization founded in 2006 by Julian Assange.
- A platform that publishes secret documents, leaks and information revealed by whistleblowers.
- Main premise: to reveal the truth and ensure transparency of power.

How does WikiLeaks work?

- Anonymous sources
 - Allows whistleblowers to send documents without revealing their identities.
- Data analysis and verification
 - A team of experts assesses the authenticity of documents before they are published.
- Public sharing
 - Publications are open to the public, most often about politics, corporations and government actions.

WikiLeaks vs. fake news

- Debunking fake news
 - Revealing real information that governments or corporations are trying to hide.
 - Example: disclosure of documents related to the wars in Iraq and Afghanistan (the so-called Iraq War Logs and Afghan War Diary).
- Generating fake news?
 - Publication of unverified or manipulated information can lead to disinformation.
- Criticism for the lack of full transparency in the verification process.

Controversy and meaning

- Controversy
 - Accusations of bias, influencing political processes (e.g., the leak of DNC emails during the 2016 US elections).
 - Allegations of collaboration with foreign intelligence.
- Importance in the fight against fake news
 - Allows access to raw, unprocessed data.
 - Contributes to transparency and holding authorities accountable for their actions.

Summary

WikiLeaks is a powerful tool in the fight for truth, which can both refute fake news and become its source. Its activities raise questions about the boundaries between revealing the truth and being responsible for disinformation.



DoS and DDoS: Information flood, network paralysis

Such DoS (Denial of Service) and DDoS (Distributed Denial of Service) are cybercrimes designed to cripple the operation of a server or network, preventing legitimate users from accessing services.

DoS: A lone attack

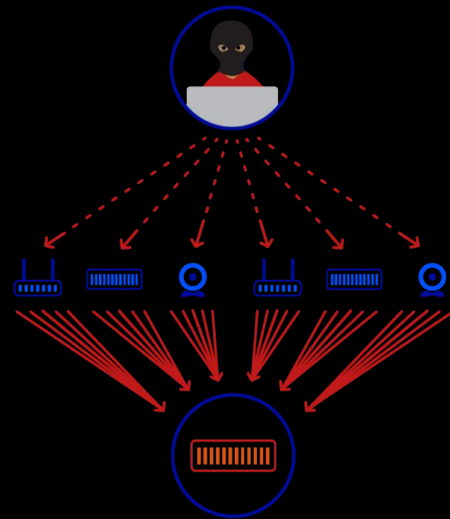
In a DoS attack, a single attacker sends a flood of bogus requests to a server, overloading its resources and blocking access for others. Think of it as trying to enter a store, with one person blocking entry, preventing other customers from shopping.

DDoS: Strength in numbers

DDoS attacks are more sophisticated. Many attackers, often unknowingly controlled zombie computers, simultaneously send a huge number of requests, leading to the paralysis of a server or the entire network. This can be compared to thousands of people trying to enter the same store, causing chaos and preventing normal operations.

Effects of DoS and DDoS attacks:

- Downtime of services and websites.
- Financial losses for companies.
- Loss of reputation and customer trust.
- Disruption of critical infrastructure, e.g. banks, hospitals, power plants.





Intruder detection: IDS

Intrusion detection systems (IDS) play a key role in protecting networks and computer systems, acting like vigilant watchdogs that monitor network traffic, analyze it for suspicious activity and alert when a potential threat is detected.

IDSs fall into two main categories:

Signature-based IDS (signature-based IDS):

- They act like metal detectors, looking for known attack patterns (signatures) in network traffic.
- They are fast and efficient, but ineffective against new, unknown attacks.

Anomaly-based IDS (IDS):

- They learn the “normal” behavior of the network and detect deviations from this pattern, which may indicate an attack.
- They can detect new attacks, but are more complex and prone to false alarms.

IDS can be implemented in two modes:

Network IDS (NIDS):

- Monitors network traffic by analyzing data packets.
- Provides a wide range of visibility, but can be difficult to deploy and configure.

Host IDS (HIDS):

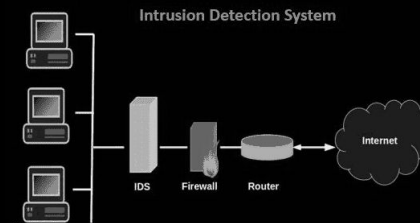
- Monitors activity on a specific computer by analyzing logs, files and processes.
- Focused on protecting a single host, but does not see all network traffic.

Benefits of implementing IDS:

- Early detection of attacks.
- Gathering evidence of security incidents.
- Facilitating incident response.

Limitations of IDS:

- Does not prevent attacks, only detects them.
- Requires regular updates to keep up with new threats.
- Can generate false alarms, putting a strain on security teams.





False Sense of Security: Silk Road and AlphaBay

Silk Road and AlphaBay are two examples of **seemingly super-secure platforms** on the Dark Net that **eventually collapsed**, exposing the false sense of anonymity of their users. Despite the advanced security features and anonymous Bitcoin currency, investigators identified and captured the individuals responsible for these platforms, proving that on the web, everyone leaves traces.

Silk Road, a drug market operating between 2011 and 2013, was considered off-limits to law enforcement. However, the FBI managed to infiltrate the platform and track down its administrator, **Ross Ulbricht**. He was sentenced to life imprisonment.

AlphaBay, which was established after the collapse of Silk Road, became an even larger marketplace for illegal products and services. In 2017, a joint FBI and Europol operation led to the closure of AlphaBay and the arrest of its founder, **Alexander Cza**.

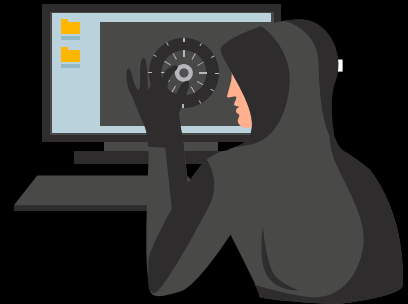
The collapse of Silk Road and AlphaBay shows that even the most advanced security measures do not guarantee complete anonymity online.

Factors that contributed to the collapse of these platforms:

- **Human error:** Administrators made mistakes that revealed their identity or location.
- **Cooperation with informants:** Investigators obtained informants who gave them valuable information.
- **New investigative techniques:** Law enforcement agencies are constantly developing new methods to track online crime.

Let's remember that every activity on the Internet leaves traces.

Even on the Dark Net, we are not completely anonymous. Let's be careful about what information we share and who we contact.





CONCLUSIONS

Our journey through the dark corners of cyberspace has revealed the **existence of platforms like Doxbin, where privacy is mercilessly violated.** The collapse of Silk Road and AlphaBay **debunked the myth of a false sense of anonymity,** showing that even on the Dark Net, everyone leaves traces. **DoS and DDoS attacks** pose a real threat, crippling servers and networks. In the fight against cybercrime, intrusion **detection systems (IDS)** act as vigilant watchdogs, monitoring network traffic and alerting on suspicious activity.

Let's remember:

Cybercriminals are constantly improving their methods.

Awareness of threats is the basis of online security.

Online, we are not completely anonymous.

Let's take care of our personal information, use strong passwords and be cautious online.



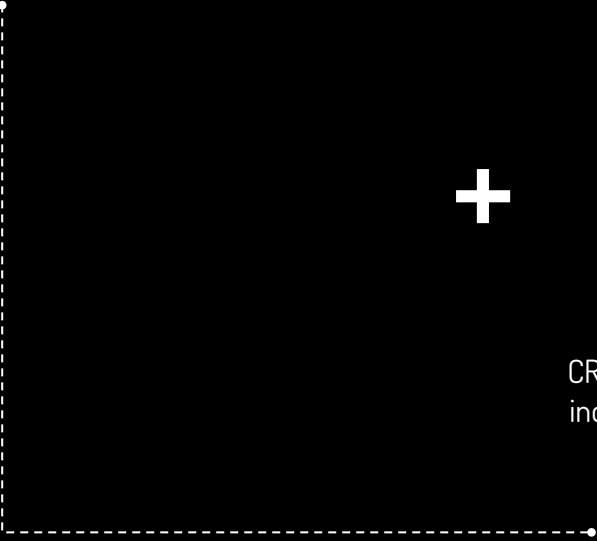
Bibliography

- **Bertrand, N.** (2015). *Homeland security officer: How I busted the web's biggest illegal marketplace*. Business Insider. Dostępne na: [businessinsider.in](https://www.businessinsider.in).
- **Dittrich, David.** (1999). *The DoS Project's "trinoo" Distributed Denial of Service Attack Tool*. University of Washington. Dostępne na: staff.washington.edu.
- **Dittrich, David.** (1999). *The "Tribe Flood Network" Distributed Denial of Service Attack Tool*. University of Washington. Dostępne na: staff.washington.edu.
- **Dittrich, David.** (1999). *The "stacheldraht" Distributed Denial of Service Attack Tool*. University of Washington. Dostępne na: staff.washington.edu.
- **Gibson, Steve.** (2002). *The Strange Tale of the Denial of Service Attacks Against GRC.com*. Gibson Research Corporation. Dostępne na: [grc.com](https://www.grc.com).
- **Karig, David i Ruby Lee.** (2001). *Remote Denial of Service Attacks and Countermeasures*. Princeton University Department of Electrical Engineering Technical Report CE-L2001-002.
- **Kargl, Frank, Maier, Joern, i Weber, Michael.** (2001). *Protecting Web Servers from Distributed Denial of Service Attacks*. WWW'0, Hong Kong, ACM 1-58113-348-0/01/0005.
- **Poznański, U. i Strobel, A.** (brak daty). *Darknet*.
- **Ormsby, E.** (brak daty). *Darknet*.
- **Stein, Lincoln.** (2002). *The World Wide Web Security FAQ, Version 3.1.2*. Dostępne na: [s3.org](https://www.s3.org).
- **Daniels, Thomas E. i Spafford, Eugene H.** (2001). *Network Traffic Tracking Systems: Folly in the Large?* Center for Education and Research in Information Assurance and Security (CERIAS). Lafayette, IN.
- *WannaCry*. Wikipedia. Dostępne na: pl.wikipedia.org.
- *Silk Road (marketplace)*. Wikipedia. Dostępne na: en.wikipedia.org.
- *Doxbin (darknet)*. Wikipedia. Dostępne na: en.wikipedia.org.
- *Antiphishing.org*. Dostępne na: antiphishing.org.
- *FraudWatch International - Phishing Alerts*. Dostępne na: fraudwatchinternational.com.
- *PhishMe.com*. Dostępne na: phishme.com.
- *OnGuardOnline - Phishing*. Dostępne na: onguardonline.gov.
- *Federal Trade Commission: Phone Scams*. Dostępne na: consumer.ftc.gov.
- *FBI - Scams & Safety: Fraud*. Dostępne na: fbi.gov.
- *PhishMe.com - Phishing on Social Media Infographic*. Dostępne na: phishme.com.
- *Phishing*. Wikipedia. Dostępne na: en.wikipedia.org.



THANKS!

Tymoteusz Maj



CREDITS: This presentation template was created by **Slidesgo**,
including icons by **Flaticon**, infographics & images by **Freepik**.