Dofinansowane przez Unię Europejską

THE CREDIBILITY OF INFORMATION IN THE AGE OF FAKE NEWS

WHAT IS DISINFORMATION?

Disinformation is the deliberate spread of false or misleading information with the intent to manipulate public opinion or create confusion. It can take various forms, such as manipulated images and videos, false articles, or social media posts. How can we combat it, and what are the key skills needed to fight disinformation in the digital age?

Firstly, *CRITICAL THINKING*: Ask questions like, Who is the author? What other sources confirm this information?

Secondly, *FACT-CHECKING SKILLS*: Use tools like FactCheck.org and Snopes to verify the accuracy of the information. It's also important to check the publication dates to ensure the information is current.

Thirdly, *SOURCE ANALYSIS*: This is a key skill—make sure the source is recognized as credible and reliable.

Fourthly, *MANIPULATION MECHANISMS*: Be aware of manipulation techniques, such as selective presentation of facts.

Dofinansowane przez Unię Europejską

TOOLS FOR COMBATING DISINFORMATION

To effectively fight disinformation, it's useful to employ several helpful tools.

Image verification tools, such as Google Reverse Image Search, allow you to check if a particular image has been used in different contexts or if it has been manipulated.

Browser plugins and extensions like NewsGuard or Media Bias/Fact Check help assess the credibility of websites and articles by providing information about their reliability.

Fake news monitoring platforms like FactCheck.org or The Poynter Institute offer up-to-date information on the spread of false news, enabling you to track and verify suspicious content in real time.

Media literacy is equally important—online courses and workshops on identifying disinformation help develop critical thinking and fact-checking skills, strengthening the ability to recognize and avoid false information.

Dofinansowane przez Unię Europejską

HOW TO RECOGNIZE AND COUNTER THREATS?

In the era of the digital revolution, alongside the increasing number of false information, modern forms of fraud and identity theft have also emerged and are becoming increasingly common.

Understanding how to recognize these threats and protect yourself from them is crucial for maintaining personal and financial security. What are the latest scams and identity theft tactics, and how can you effectively deal with them?

BLIK Scams and Other Money Fraud Tactics
BLIK, the mobile payment system that has gained immense popularity in Poland, has also become a target for various types of scams. Fraudsters use several techniques to steal money

Phishing: Scammers may impersonate banks or financial institutions and request your BLIK code or login details. They might do this through fake emails, SMS messages, or even phone calls.

Fake Apps: Fraudsters create apps that mimic legitimate BLIK applications. Once installed, these apps can steal users' data or expose them to other types of fraud.

Dofinansowane przez Unię Europejską

HOW TO PROTECT YOURSELF?

Never share your BLIK code or login details over the phone, email, or SMS. Banks and financial institutions will never ask for such information this way. Use phone security features such as passwords, fingerprints, or facial recognition to make it harder for third parties to gain access. Regularly update your software and apps to protect against known security vulnerabilities.

KRADZIEŻ TOŻSAMOŚCI

Identity theft is a serious threat that can lead to financial and personal problems. Fraudsters may use various methods to obtain personal data, such as PESEL numbers, credit card numbers, or bank account details.

How does identity theft occur? For example, through skimming, which involves installing devices on card readers at terminals or ATMs to copy credit card data. Another method is information phishing, where scammers pose as bank representatives over the phone to extract personal information.

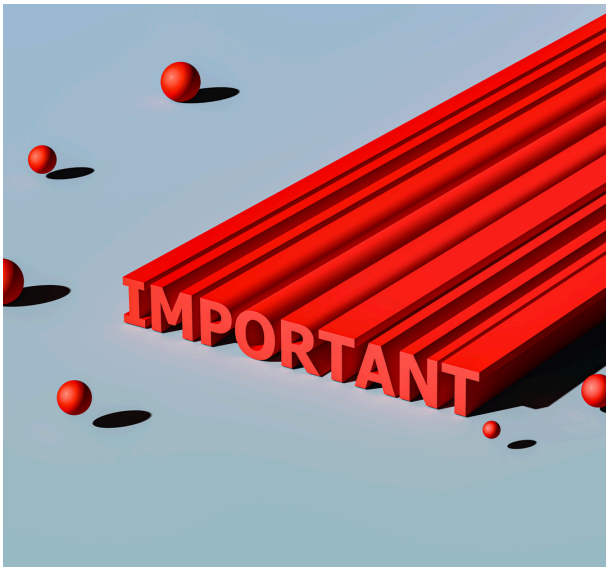
WHAT TO DO?

First and foremost, avoid sharing personal information over the phone or email if you are not sure of the identity of the person on the other end. Regularly check your bank account to quickly detect any unauthorized transactions or account openings in your name. Use antivirus software and keep your operating system updated. Set strong passwords and change them regularly.

Dofinansowane przez Unię Europejską

REMEMBER!

Firstly, educate yourself and others about disinformation and scams. Knowledge of the latest techniques and security tools can help protect against false information and fraud. Secondly, be cautious with emails and messages from unknown senders. Do not click on suspicious links or download attachments that could be phishing attempts. Thirdly, and importantly, use strong passwords and security features on your devices. Regularly change your passwords and use two-factor authentication whenever possible.



Fourth, verify the sources of information before believing or sharing them. Use fact-checking tools and make sure the information comes from reliable sources. Fifth, NEVER share your BLIK code or login details over the phone, email, or SMS. Banks never ask for such information in this way. Lastly, but no less important, install and update antivirus software to protect your devices from threats and malware.

Dofinansowane przez Unię Europejską

SHARE YOUR KNOWLEDGE!

We encourage you to share this article with your family, friends, and colleagues. Disinformation is a serious threat that can affect every one of us, and collective education is the key to building a more informed society.

This article is based on our own experiences and active participation in the mobilities of the project "Information Credibility in the Age of Fake News," funded by the EU. With the knowledge and practice we have gained, we hope to provide you with tools and tips that will help you recognize and combat false information.

Share this article to help others understand the threats of disinformation and learn how to protect themselves effectively. Together, we can create a community that is more resilient to false information!

„Projekt sfinansowany ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności."