TEACHING THE NECESSITY TO USE DMARC IN UKRAINIAN EDUCATIONAL INSTITUTIONS

Daria Kononova
Ph.D. in Linguistics, Assistant Professor,
National Academy of the Security Service of Ukraine, Ukraine
e-mail: kdv_ed@ukr.net, orcid.org/0000-0003-3804-2356

Olena Kobus
Ph.D. in Physics and Mathematical Science, Assistant Professor,
National Academy of the Security Service of Ukraine, Ukraine
e-mail: kobus_olena@ukr.net, orcid.org/0000-0003-3130-6515

Summary

In today's interconnected world, email remains a cornerstone of communication for businesses, government agencies, and individuals alike. However, this ubiquitousness also makes it a prime target for cybercriminals. Phishing, spoofing, and other email-borne attacks can have devastating consequences, ranging from financial losses and data breaches to reputational damage and disruption of critical services. In Ukraine, amidst the backdrop of ongoing conflict and heightened cyber activity, the importance of robust email security measures like DMARC (Domain-based Message Authentication, Reporting & Conformance) cannot be overstated. This article explores the importance of DMARC in safeguarding Ukraine's digital landscape and why its widespread adoption is essential.

Ukrainian educational institutions face increasing cyber threats, particularly email spoofing and phishing attacks. Implementing DMARC is crucial to protect their email communications. DMARC helps to verify that emails claiming to be from an institution are genuinely sent from their authorized servers. This prevents malicious actors from impersonating the institution, safeguarding sensitive data like student or staff records and research information. By adopting DMARC, Ukrainian educational institutions can enhance their cybersecurity posture, maintain trust in their email communications, and ensure a safer online environment for students, faculty, and staff.

Key words: online learning and communication, Ukraine's digital infrastructure and digital technologies, email security and data protection from cyberattacks, the country's IT infrastructure and cybersecurity landscape, cloud-based solutions, cybercrimes, Legal and Regulatory Landscape.

DOI https://doi.org/10.23856/6809

1. Introduction

The aim of the article is to promote and facilitate the effective implementation of DMARC *(What is DMARC? 2024)* within Ukrainian educational institutions, enhancing email security and protecting the educational ecosystem from cyber threats.

The tasks are:

1. Raise Awareness: Conduct comprehensive awareness campaigns about the importance of DMARC and its benefits for educational institutions in Ukraine. This includes targeting

administrators, IT staff, teachers, students, and parents. These campaigns should explain what DMARC is, how it works, and why it's crucial for protecting against phishing, spoofing, and other email-borne attacks.

2. Provide Training and Support: Offer practical training and technical support to educational institutions on how to implement DMARC effectively. This involves workshops, online resources, and access to expert consultants. Training should cover DNS record configuration *(Incorrect DNS entry, 2023),* policy selection (none, quarantine, reject), report analysis, and ongoing maintenance.

3. Develop Educational Resources: Create Ukrainian-language educational materials, including guides, tutorials, and FAQs, to support DMARC implementation and ongoing management. These resources should be tailored to the specific needs and technical capabilities of Ukrainian educational institutions.

4. Foster Collaboration: Encourage collaboration and information sharing among educational institutions, IT professionals, cybersecurity experts, and government agencies regarding DMARC implementation and best practices. This can be achieved through forums, conferences, and online communities.

5. Advocate for Policy Support: Advocate for policies and regulations that promote the adoption of DMARC in the education sector in Ukraine. This includes working with government agencies and educational organizations to raise awareness and encourage the implementation of email security standards.

Methodology. So, as the goal is to measure and understand the overall level of DMARC knowledge in Ukrainian educational institutions, the quantitative method can be used, especially gathering and analyzing the information. Also qualitative method is also used focusing on exploring the challenges of implementing DMARC in Ukrainian educational institutions through in-depth understanding of experiences, perspectives, and meanings. Meta-analysis is used for synthesizing the findings of multiple studies to draw broader conclusions.

Actuality of this topic. Nowadays it is very important. Ukrainian educational institutions are increasingly targeted by cyberattacks, including phishing, spoofing, and malware distribution via email. DMARC is a critical defense against these threats. We know that educational institutions handle vast amounts of sensitive student and staff data, making them prime targets for data breaches. DMARC helps protect this data by securing email communications. In modern situation in Ukraine and ongoing war Email can be used to spread disinformation and propaganda, undermining trust in educational institutions. DMARC helps ensure the authenticity of email communications.

So, in general, cyberattacks can damage the reputation and erode trust in educational institutions. DMARC helps maintain trust by demonstrating a commitment to email security. Many educational institutions are subject to data privacy regulations that require them to implement appropriate security measures. DMARC can contribute to meeting these requirements. As Ukrainian education increasingly relies on digital technologies, robust email security is essential for ensuring the integrity and reliability of online learning and communication. Also we should take into consideration that in the context of post-war recovery, strengthening cybersecurity in education is crucial for rebuilding and ensuring the continuity of educational services.

Speaking about objectives, we should take into consideration:

1. Increased DMARC Adoption. Increase the number of Ukrainian educational institutions that have successfully implemented DMARC. This can be measured by the number of institutions with published DMARC records and the percentage of their email traffic that is authenticated.

2. Improved Email Security. Reduce the number of successful phishing and spoofing attacks targeting Ukrainian educational institutions. This can be measured by tracking reported incidents and analyzing email traffic data.

3. Enhanced Data Protection. Minimize the risk of data breaches resulting from email-borne attacks in Ukrainian educational institutions. This can be measured by tracking reported data breaches and assessing the effectiveness of implemented security measures.

4. Greater Awareness. Raise awareness among Ukrainian educational stakeholders about the importance of email security and the benefits of DMARC. This can be measured through surveys, website traffic, and social media engagement.

5. Improved Technical Capacity. Enhance the technical capacity of Ukrainian educational institutions to implement and manage DMARC effectively. This can be measured by the number of IT staff trained in DMARC implementation and the availability of technical support resources.

6. Stronger Cybersecurity Posture. Strengthen the overall cybersecurity posture of Ukrainian educational institutions by implementing DMARC as a key component of their email security strategy.

By achieving these objectives, the initiative aims to create a safer and more secure digital learning environment for students, teachers, and staff in Ukraine.

2. Landscape threats in Ukraine

Ukraine has become a focal point for cyber warfare, with both state-sponsored actors and cybercriminals actively targeting its infrastructure, businesses, and government institutions. The ongoing conflict has amplified these threats, making Ukrainian organizations and individuals even more vulnerable to email-based attacks.

Let's analyze thhe landscape threats in Ukraine. Here we should pay attention to increased Phishing and Spoofing. Phishing campaigns, often disguised as legitimate communications from banks, government agencies, or even humanitarian organizations, are rampant. These attacks aim to steal sensitive information such as login credentials, financial details, or personal data. Spoofing, where attackers forge email headers to make it appear as though emails are from trusted sources, is also on the rise *(Slavin, 2024).* Email remains a primary vector for malware distribution. Malicious attachments or links in phishing emails can infect devices with ransomware, spyware, or other harmful software, disrupting operations and potentially crippling critical infrastructure *(Malware, 2021).* Email can be used to spread disinformation and propaganda, undermining trust in institutions and creating social unrest. Spoofed emails can be used to spread false narratives or manipulate public opinion *(Lenaerts-Bergmans, 2025).* Cyberattacks targeting critical infrastructure, such as power grids, telecommunications networks, and financial institutions, can have a devastating impact on essential services and the overall economy. Email can be used as an entry point for these attacks. Email breaches can lead to the loss of sensitive data, including personal information, financial records, and intellectual property. This can result in significant financial losses, reputational damage, and legal liabilities *(Email Security Breaches, 2025).*

Given the unique cybersecurity challenges facing Ukraine, DMARC implementation is particularly crucial for several reasons:

a) Protecting Critical Infrastructure. DMARC can help protect critical infrastructure from email-borne attacks by preventing attackers from spoofing email addresses and distributing malware. By ensuring that only legitimate emails are delivered, DMARC can help maintain the integrity and availability of essential services.

b) Combating Disinformation. DMARC can play a role in combating disinformation campaigns by making it more difficult for attackers to spoof email addresses and spread false narratives. By verifying the authenticity of emails, DMARC can help build trust in legitimate sources of information.

c) Safeguarding Government Communications. Government agencies rely heavily on email for communication. DMARC can help protect these communications from spoofing and phishing attacks, ensuring that sensitive information is not compromised.

d) Protecting Businesses and Individuals. DMARC can help protect businesses and individuals from phishing attacks, malware distribution, and other email-borne threats. This is particularly important in Ukraine, where cybercriminals are actively targeting businesses and individuals.

e) Building Trust in Digital Communications. By verifying the authenticity of emails, DMARC helps build trust in digital communications. This is essential for fostering a healthy digital economy and encouraging online interactions.

f) Enhancing International Cooperation. DMARC is an internationally recognized standard for email authentication. By adopting DMARC, Ukrainian organizations can demonstrate their commitment to cybersecurity and facilitate international cooperation in combating cybercrime.

g) Supporting Ukraine's Cybersecurity Resilience. Implementing DMARC is a proactive step that organizations can take to strengthen their cybersecurity resilience. By protecting against email-borne threats, DMARC helps organizations maintain business continuity and minimize the impact of cyberattacks.

h) Reducing the Impact of Cyber Warfare. In the context of ongoing cyber warfare, DMARC can play a vital role in protecting Ukraine's digital infrastructure and preventing attackers from exploiting email as a vector for attacks.

3. Domain-based Message Authentication, Reporting & Conformance

So, DMARC *(Fortinet, 2025)* (Domain-based Message Authentication, Reporting & Conformance) is an email authentication system designed to protect email senders and recipients from spam, phishing, and other malicious email activities. It allows a sender to indicate that their emails are authenticated by **SPF** (Sender Policy Framework) and **DKIM** (DomainKeys Identified Mail), and tells the recipient's mail server what to do with messages that fail authentication checks. While **DMARC** offers significant security benefits, its implementation and effectiveness in Ukraine, like many other regions, face a variety of challenges. This article explores these problems, covering technical, cultural, and legal aspects.

1. Understanding DMARC Fundamentals *(DMARC Fundamentals, 2025)*

DMARC acts as a powerful defense against these email-borne threats by building upon two existing email authentication mechanisms: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). Before diving into the problems, it's crucial to understand the basics of DMARC. It works by aligning the "From" address in an email with the domain used for SPF and DKIM authentication.

SPF: Allows a domain owner to specify which mail servers are authorized to send email on their behalf. It publishes a list of authorized IP addresses in a DNS TXT record.

DKIM: Adds a digital signature to the email header, which can be verified by the recipient's mail server. This ensures that the message content hasn't been tampered with during transit.

DMARC: Builds upon SPF and DKIM by allowing the domain owner to specify a policy for handling emails that fail authentication. This policy can be:

– None: (Monitor mode) Collects reports on authentication failures without taking action.

– Quarantine: Instructs the recipient's mail server to place failing messages in the spam or junk folder.

– Reject: Instructs the recipient's mail server to block failing messages entirely.

2. Technical Challenges in Ukraine:

Many organizations in Ukraine, particularly smaller businesses and government institutions as well as educational ones, still rely on older email systems that may not fully support or be easily configurable for SPF, DKIM, and DMARC. There is also a general lack of awareness about the importance of email authentication and the benefits of DMARC. This leads to slow adoption rates and inconsistent implementation.

Incorrect DNS Configuration *(Cloudflare Community, 2022):* Implementing DMARC requires accurate configuration of DNS records. Common mistakes include:

SPF record limitations: SPF has a 10-lookup limit, which can be easily exceeded by organizations using multiple email sending services. This can lead to SPF failures and DMARC issues.

DKIM key management: Rotating DKIM keys is essential for security, but many organizations fail to do so regularly, potentially invalidating legitimate emails.

Misconfigured DMARC policies: Setting a "reject" policy prematurely without thoroughly analyzing reports can lead to legitimate emails being blocked. Similarly, a "none" policy indefinitely provides no real protection.

Missing or incorrect reporting addresses: DMARC relies on reports being sent to designated email addresses. If these are missing or misconfigured, the sender won't receive valuable feedback on authentication failures.

Complexities with Email Forwarding *(Common Problems When Forwarding Email, 2023; Email Forwarding, 2025)*: Email forwarding can break SPF authentication, as the receiving server's IP address will differ from the authorized IP in the sender's SPF record. While there are mechanisms like ARC (Authenticated Received Chain) to address this, they are not universally adopted, causing issues with DMARC for forwarded emails. This is a significant problem in Ukraine, where email forwarding is still common.

Involving economic situation in Ukraine nowadays it’s obvious to pay attention to such issue as money. Implementing DMARC may involve costs for technical expertise, software, and infrastructure upgrades. Some organizations may be hesitant to invest in DMARC, especially if they have limited resources. Also, some organizations may still be using older email systems that are not compatible with DMARC. Upgrading these systems can be costly and time-consuming.

Another problem can appear that there may be a lack of enforcement of email security standards in Ukraine, which can reduce the incentive for organizations to implement DMARC.

Different email providers and mail servers may have varying levels of DMARC compliance and enforcement. This can lead to inconsistent handling of emails, even if DMARC is correctly configured.

Setting up and maintaining DMARC requires a certain level of technical expertise. Many organizations in Ukraine, especially SMEs, may lack the in-house skills to implement DMARC effectively. Outsourcing to specialized providers can be costly, further hindering adoption.

3. Cultural and Socioeconomic Factors:

Cybersecurity, including email security, may not be a top priority for many organizations in Ukraine, particularly those facing economic hardship or focusing on other pressing issues. This

can lead to a lack of investment in DMARC implementation. Much of the available documentation and resources on DMARC are in English. This can be a barrier for Ukrainian organizations that primarily operate in Ukrainian. Some organizations may be hesitant to adopt new technologies like DMARC, particularly if they haven't experienced significant email security issues in the past. They may perceive the effort and cost of implementation as outweighing the potential benefits. Implementing DMARC often requires changes to existing email workflows and processes. This can be met with resistance from employees who are accustomed to the old ways of doing things.

4. Legal and Regulatory Landscape:

While Ukraine has data protection laws, the specific requirements for email security and authentication may not be explicitly defined. This can create uncertainty for organizations regarding their obligations. The evolving landscape of GDPR and other international regulations also adds complexity. Even if regulations exist, the level of enforcement regarding email security practices may be limited. This can reduce the incentive for organizations to implement DMARC. Email often crosses international borders, making it challenging to enforce DMARC policies and address email security issues that originate outside of Ukraine. International cooperation and harmonization of email security standards are crucial but often difficult to achieve.

5. Impact of the War:

The ongoing war in Ukraine has significantly impacted the country's IT infrastructure and cybersecurity landscape. This has introduced new challenges for DMARC implementation:

Disrupted Communication Channels *(Bandouil, 2025).* The war has disrupted communication channels and internet connectivity, making it difficult for some organizations to manage their email systems and DNS records.

Increased Cyberattacks *(Artemchuk, 2025).* The conflict has led to a surge in cyberattacks, including phishing and spam campaigns targeting Ukrainian organizations and individuals. This makes DMARC even more critical, but also more challenging to implement due to the heightened threat environment.

Focus on Immediate Security Needs. Organizations may be prioritizing other immediate security needs over long-term email security measures like DMARC.

Displacement of IT Staff. The war has led to the displacement of IT staff, making it difficult for some organizations to maintain their email systems and implement DMARC.

6. Addressing the Challenges:

To overcome these challenges and promote widespread DMARC adoption in Ukraine, the following recommendations are proposed:

– Education and Awareness Campaigns. Launch public awareness campaigns to educate organizations and individuals about the importance of email authentication and the benefits of DMARC. These campaigns should be tailored to different audiences and delivered through various channels, including online resources, workshops, and seminars.

– Education and Awareness. Raising awareness about the importance of email authentication and the benefits of DMARC is crucial. This can be done through workshops, seminars, online resources, and public awareness campaigns. Translating resources into Ukrainian and Russian is essential.

– Technical Assistance and Support. Providing technical assistance and support to organizations implementing DMARC is vital. This can include offering training, developing easy-to-use tools, and providing access to expert consultants.

– Incentivizing Adoption. Offer incentives for DMARC adoption, such as tax breaks, grants, or recognition programs. This can encourage more organizations to invest in DMARC implementation.

– Promoting Collaboration and Information Sharing. Foster collaboration and information sharing between organizations, ISPs, and government agencies on email security best practices. This can help improve email security practices across the board.

– Strengthening Regulatory Framework. Develop a clear and comprehensive regulatory framework for email security, including specific requirements for email authentication. This can provide organizations with greater clarity and encourage compliance.

– International Cooperation. Collaborate with international organizations and other countries to address cross-border email security issues and promote the adoption of global email security standards.

– Simplifying DMARC Implementation. Develop simplified tools and processes for DMARC implementation to make it easier for organizations, especially smaller businesses, to adopt this technology.

– Leveraging Cloud-Based Solutions. Cloud-based email providers often offer built-in DMARC support, which can simplify implementation for organizations that use these services

4. Enhancing email security in educational settings

DMARC is a powerful email authentication system that can significantly enhance email security in educational settings. Here are the ways:

1. Protecting Students and Staff from Phishing Attacks:

DMARC helps prevent cybercriminals from spoofing email addresses of teachers, administrators, or the institution itself. This makes it harder for them to trick students and staff into revealing sensitive information like login credentials, financial details, or personal data through phishing emails. By verifying the authenticity of emails, DMARC helps build trust in official communications from the educational institutions. This ensures that students and staff can confidently rely on emails from their teachers, administrators, and the institution as a whole.

2. Safeguarding Sensitive Data:

Educational institutions store vast amounts of sensitive data, including student records, grades, financial information, and research data. DMARC helps protect this data from falling into the wrong hands by preventing email-borne attacks that can lead to data breaches. Many educational institutions are subject to data privacy regulations like FERPA (Family Educational Rights and Privacy Act) in the US *(What is FERPA? 2025).* DMARC can help these institutions meet compliance requirements by strengthening their email security posture.

3. Preserving Reputation and Trust:

Cybercriminals often target educational institutions to exploit their trusted reputation. DMARC helps protect the institution's brand image by preventing attackers from using its name to send malicious emails. Students, parents, alumni, and donors need to trust that their communications with the institution are secure. DMARC helps maintain this trust by demonstrating a commitment to email security and data protection.

4. Ensuring Effective Communication:

DMARC can help reduce the amount of spam and junk mail that reaches students and staff, allowing them to focus on important communications. By authenticating legitimate emails, DMARC can help improve the deliverability of important communications from the educational institutions, ensuring that they reach the intended recipients.

5. Promoting Cybersecurity Awareness:

Implementing DMARC can be an opportunity to educate students and staff about the importance of email security and how to identify phishing attempts. By taking proactive steps

to protect its email systems, the educational institution can demonstrate its commitment to cybersecurity and foster a culture of security awareness among its stakeholders.

Overall, DMARC is a valuable tool for educational institutions to protect themselves from email-borne threats, safeguard sensitive data, preserve their reputation, and ensure effective communication. By implementing DMARC and educating their stakeholders about email security best practices, educational institutions can create a safer and more secure digital environment for everyone.

5. Conclusions

DMARC is a critical tool for combating email fraud and improving email security. While its implementation in Ukraine faces numerous challenges, including technical complexities, cultural barriers, and the impact of the war, these challenges can be addressed through a concerted effort involving education, technical support, incentivization, collaboration, and regulatory improvements. By working together, Ukrainian organizations, educational institutions, ISPs, government agencies, and international partners can create a more secure email environment for everyone. Overcoming these challenges is not only essential for protecting individuals and organizations from cyber threats but also for fostering trust in digital communications and supporting the growth of the digital economy in Ukraine.

While challenges to DMARC adoption exist, these can be overcome through concerted efforts involving education, technical assistance, incentivization, collaboration, and regulatory improvements. Promoting widespread DMARC adoption is not only essential for strengthening Ukraine's cybersecurity resilience but also for fostering trust in digital communications and supporting the growth of the digital economy. By prioritizing email security and embracing DMARC, Ukraine can take a significant step towards creating a safer and more secure digital environment for all.

Government and educational organizations can play a key role in promoting and encouraging the implementation of email security standards. This can involve incentives, mandates, or simply raising the profile of DMARC as a best practice. Ultimately, a coordinated effort will be most effective in securing email communications within the Ukrainian educational system.

References

1. Artemchuk O. (2025). Number of cyberattacks on Ukraine increased by 70% in past year. URL: https://www.pravda.com.ua/eng/news/2025/01/9/7492671/ (date of access: 18.02.2025).
2. Bandouil S. (2025). Ukraine's military intelligence reportedly disrupts Gazprom's digital services. URL: https://kyivindependent.com/ukrainian-military-intelligence-disrupts-gazproms-digital-services/ (date of access: 18.02.2025).
3. Cloudflare Community. (2022) DNS settings incorrect/not active. URL: https://community.cloudflare.com/t/dns-settings-incorrect-not-active/343551 (date of access: 19.02.2025).
4. Common Problems When Forwarding Email. (2023) URL: https://support.wharton.upenn.edu/help/forwarding-email-problem (date of access: 18.02.2025).
5. DMARC Fundamentals: Everything You Need to Know About Email Authentication Protocols. (2025). URL: https://dmarcreport.com/courses/dmarc-fundamentals/ (date of access: 18.02.2025).
6. Email Forwarding. (2025). URL: https://www.activecampaign.com/glossary/email-forwarding (date of access: 18.02.2025).

7. Email Security Breaches: Common Causes and 7 Recent Breaches to Learn From. (2025). URL: https://perception-point.io/guides/email-security/email-security-breaches/ (date of access: 18.02.2025).
8. Fortinet (2025). What Is DMARC (Domain-based Message Authentication, Reporting, And Conformance)? Understand the benefits and descriptions of DMARC records and DMARC reports. URL: https://www.fortinet.com/resources/cyberglossary/dmarc (date of access: 18.02.2025).
9. Lenaerts-Bergmans B. (2025). Disinformation Campaign. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/disinformation-campaign/ (date of access: 18.02.2025).
10. Malware. (2021). URL: https://www.vectra.ai/topics/malware (date of access: 18.02.2025).
11. Slavin B. (2024). Phishing and Spoofing– Two emerging cyberattack trends in 2024. URL: https://dmarcreport.com/blog/phishing-and-spoofing-two-emerging-cyberattack-trends-in-2024/ (date of access: 18.02.2025).
12. Spiceworks Community. Incorrect DNS entry for Windows Server. (2023) URL: https://community.spiceworks.com/t/incorrect-dns-entry-for-windows-server/955183 (date of access: 19.02.2025).
13. What is DMARC? (2024) URL: https://dmarc.org/ (date of access: 17.02.2025).
14. What is FERPA? (2025) URL: https://studentprivacy.ed.gov/faq/what-ferpa (date of access: 19.02.2025).