

D5.2 Digital Marketing Channels & Tools

Project website and partner channels

Contents

About the Digital4Security project.....	4
The Digital4Security Consortium	6
Document Control Information.....	8
Introduction	9
Social Media Channels	11
Social Media Engagement Strategy	11
LinkedIn	12
YouTube	12
Email Newsletter	13
Direct Mailing.....	13
Instagram and Facebook	14
Communication Channels & Tools.....	15
Project Website	16
Website Domain	17
Technologies Used	17
Website Administration.....	18
Website Pages.....	18
Hosting.....	28
SSL	31
Support.....	32
Dedicated support team	33
Monthly support report	33
Partner Webpage	34
Partner Webpage Assets	36

Table of Figures

Figure 1 Digital4Security LinkedIn Page	12
Figure 2 Digital4Security YouTube Channel	13
Figure 3 Email Newsletter Sign Up on Website.....	13
Figure 4 Digital4Security Website.....	17
Figure 5 Digital4Security Homepage	18
Figure 6 Digital4Security About Page.....	19
Figure 7 Our Partners Page	20
Figure 8 Example of partner page from website	21
Figure 9 News & Events Page	22
Figure 10 Contact Us page	23
Figure 11 Website Footer	24
Figure 12 Hosting platform for digital4security.eu web site	29
Figure 13 Latest software configuration of the hosting server.....	30
Figure 14 Overview of the visits from robots.....	31
Figure 15 HTTP status codes.....	31
Figure 16 Connecting to digital4security.eu sources.	31
Figure 17 Overview of the Let's encrypt certificate used on digital4security.eu.....	32
Figure 18 Sample Partner Page.....	36
Figure 19 Sample visual assets 1.....	36
Figure 20 Sample visual assets 2	37
Figure 21 Sample visual assets 3	37
Figure 22 Banner for partner page	38



About the Digital4Security project

Digital4Security is a ground-breaking pan-European master's program aimed at addressing the escalating challenges posed by cybersecurity threats and data privacy concerns across all industries. This €20m industry-led Master's is supported by funding from the DIGITAL Europe Programme. It has garnered support from a Consortium comprising 35 partners spanning 14 countries. This industry-driven program will provide comprehensive knowledge of cybersecurity management, regulatory compliance, and technical expertise to European SMEs and companies.

Digital Marketing Tools and Channels (D5.2)

This deliverable, D5.2, falls under Work Package 5 (WP5), which concentrates on dissemination and European impact. WP5 focuses on developing a dynamic pan-European Cybersecurity stakeholder ecosystem and supporting the implementation of a European Master's Programme in Cybersecurity Management. The main activities within WP5 include:

- Creation of communications strategy, branding, and communications materials (T5.1) in collaboration with various Partners.
- Setup and management of digital marketing channels, tools, and website (T5.2).
- Launch of Digital4Security EU-wide communications campaign to promote the Digital4Security programme, targeting potential students and industry Partners (T5.3).
- Collaborating with the Digital Skills and Jobs Platform with the goal of publishing online learning resources (T5.4).
- Establishing a Partnership development programme to build a pan-European ecosystem of industry and education Partners and strengthen the network of contributors and host companies involved in the programme (T5.5).
- Conducting surveys and interviews to develop case studies and good practice examples to promote the programme's results (T5.6).
- Implementing an Industry and Education Campaign to encourage the adoption of the programme format by industry and education providers (T5.7).
- Setting up a monitoring tool to collect data on communication actions and campaigns' performance to provide recommendations for improvement (T5.8).

Overall, WP5 aims to establish a robust communication strategy, promote the Digital4Security programme, build Partnerships, and monitor communication performance to ensure the successful implementation and adoption of the European Master's Programme in Cybersecurity Management.

The goal of D5.2 is to outline the setup and management of digital marketing channels, tools, and the project's website. This includes the creation and maintenance of a robust digital presence to ensure the visibility and promotion of the Digital4Security programme among all relevant stakeholders.

Specifically, D5.2 aims to:

- Establish and manage digital marketing channels such as social media accounts, email marketing platforms, and online advertising campaigns.
- Develop and maintain a user-friendly and informative project website.
- Utilise targeted digital marketing tools to reach potential students, industry partners, and other stakeholders.
- Monitor and analyse the performance of digital marketing efforts to optimise strategies and maximise impact.

The digital marketing strategy for Digital4Security is a collaborative effort between Matrix, DIGITAL Europe, and Indiepics, ensuring a comprehensive and coordinated approach. By leveraging the capacities and networks of the project partners, we aim to create a dynamic and effective digital marketing ecosystem that supports the successful implementation and adoption of the European Master's Programme in Cybersecurity Management.

In summary, D5.2 is a critical component of WP5, dedicated to enhancing the visibility and impact of the Digital4Security project through effective digital marketing tools and channels. By fostering a strong online presence and engaging with a broad audience, we aim to promote the innovative approaches of the programme, build valuable partnerships, and support the development of a robust pan-European cybersecurity stakeholder ecosystem.

The Digital4Security Consortium

The Digital4Security Consortium is a dynamic pan-European partnership of innovators in the field of cybersecurity. It comprises higher education institutions, industry partners, training providers and cybersecurity clusters, working together to design, promote and deliver a transformative cybersecurity management programme, developed and delivered by the best cybersecurity talent from Europe and worldwide.

No.	Role	Short name	Partner	Country
1	COO	POLITEHNICA BUCHAREST	NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST	RO
2	BEN	SA	SCHUMAN ASSOCIATES SCRL	BE
3	BEN	Ataya	ATAYA & PARTNERS	BE
4	BEN	POLIMI	POLITECNICO DI MILANO	IT
5	BEN	CMIP	POLSKI KLASTER CYBERBEZPIECZENSTWA CYBERMADEINPOLAND SP. Z O. O.	PL
6	BEN	Contrader	CONTRADER SRL	IT
7	BEN	DTSL	DIGITAL TECHNOLOGY SKILLS LIMITED	IE
8	BEN	indiepics	INDEPENDENT PICTURES LIMITED	IE
9	BEN	MATRIX	MATRIX INTERNET APPLICATIONS LIMITED	IE
10	BEN	PROFIL KLETT	PROFIL KLETT D.O.O.	HR
11	BEN	ServiceNow	SERVICENOW IRELAND LIMITED	IE
12	BEN	UNIBS	UNIVERSITA DEGLI STUDI DI BRESCIA	IT
13	BEN	UDS	UNIVERSITY OF DIGITAL SCIENCE GGMBH	DE
14	BEN	SKILLNET	SKILLNET IRELAND COMPANY LIMITED BY GUARANTEE	IE
15	BEN	IT@CORK	IT@CORK ASSOCIATION LIMITED LBG	IE
16	BEN	ADECCO TRAINING	ADECCO FORMAZIONE SRL	IT
17	BEN	UNI KO	UNIVERSITAT KOBLENZ	DE
18	BEN	BRNO UNIVERSITY	VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ	CZ
19	BEN	MTU	MUNSTER TECHNOLOGICAL UNIVERSITY	IE

20	BEN	DIGITAL SME	EUROPEAN DIGITAL SME ALLIANCE	BE
21	BEN	DIGITALEUROPE	DIGITALEUROPE AISBL*	BE
22	BEN	MRU	MYKOLO ROMERIO UNIVERSITETAS	LT
23	BEN	UNIRI	SVEUCILISTE U RIJECI	HR
24	BEN	NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	PL
25	BEN	UNIR	UNIVERSIDAD INTERNACIONAL DE LA RIOJA SA	ES
26	BEN	NCI	NATIONAL COLLEGE OF IRELAND	IE
27	BEN	TERAWE	TERAWE TECHNOLOGIES LIMITED	IE
28	BEN	CY CERGY PARIS	CY CERGY PARIS UNIVERSITE	FR
29	BEN	BANCO SANTAN DER	BANCO SANTANDER SA	ES
30	BEN	CYBER RANGES	CYBER RANGES LTD	CY
31	BEN	RED OPEN S.R.L .	RED OPEN S.R.L.	IT
32	BEN	VMU	VYTAUTO DIDZIOJO UNIVERSITETAS	LT
33	AP	FHG	FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV	DE
34	AP	Pearson Benelux	Pearson Benelux BV	NL

Document Control Information

Project	Digital4Security
Document Title	D5.2 Digital Marketing Channels & Tools
Work Package Number	WP5
Deliverable Number	D5.2
Lead Beneficiary	Matrix Internet
Project Coordinator:	National University of Science and Technology Politehnica of Bucharest (NUSTPB)
Dissemination Level	Sensitive — limited under the conditions of the Grant Agreement
Authors	Aoife O'Driscoll (MATRIX), Fionnuala Mahon (MATRIX), Bogdan-Costel Mocanu (National University of Science and Technology Politehnica of Bucharest)
Reviewers	Diarmaid Mac Mathúna, Indiepics
Description	Digital Marketing Channels & Tools
Status	Final
Delivery Date	31.03.2024
Due date	31.03.2024
Approval Date:	31.03.2024

Revision history

Version	Date	Modified by	Comments
1	08.03.2024	Aoife O'Driscoll, Fionnuala Mahon, Bogdan-Costel Mocanu	First Draft
2	15.03.2024	Diarmaid Mac Mathúna , Indiepics	QA



Introduction

The project website and marketing channels will disseminate and leverage the strengths and networks of the project partners and encourage close collaboration among the Consortium team with the goal of achieving the following best practices:

Develop a Pan-European Cybersecurity Stakeholder Ecosystem:

- Engage higher education institutions (HEIs), industry partners, training providers, and cybersecurity clusters.
- Enhance and deliver an innovative Cybersecurity Management Programme led by top experts from Europe and worldwide.

Support European SMEs and Companies:

- Assist in recruiting and upskilling their workforce in cybersecurity roles.
- Integrate them into the Master's programme and help identify cybersecurity risks, skills gaps, and European Cybersecurity Skills Framework (ECSF) occupational profiles.

Create a 'Best Practice' Model for Cybersecurity Education:

- Develop a Master's Programme in Cybersecurity Management that can be adopted by mid-size European HEIs and EUIs.
- Expand the availability and accessibility of cybersecurity education across Europe.

The Digital Marketing Channels and Tools will establish a model for cybersecurity education that can be easily adopted and effectively implemented by educational institutions across Europe, enhancing the accessibility and quality of cybersecurity education for learners. Developing a pan-European cybersecurity network involving higher education institutions, industry partners, non-profits, and educational technology clusters to enhance, develop, and deliver innovative cybersecurity educational content led by top experts from Europe and beyond.

- Showcase transformative cybersecurity practices through case studies and testimonials.
- Drive visitors to the project website and encourage potential candidates to explore the Master's programme.

- Raise awareness and usage of cybersecurity educational tools.
- Collect feedback to refine and improve project offerings continuously.
- Identify and recruit additional educational and industry partners.
- Leverage influencers and multipliers to extend the project's reach.
- Raise brand awareness and reinforce the Digital4Security Project identity.
- Promote success stories and case studies to illustrate the project's impact and inspire prospective students.
- Foster partnerships and community involvement.
- Build widespread awareness of the Digital4Security Project's objectives and available resources.
- Encourage the integration of Digital4Security tools into educational and corporate settings.
- Engage potential candidates through targeted content, guiding them to sign up for the Master's programme.
- Support enrolled students through their studies with engaging and informative content.
- Encourage graduates to become advocates for Digital4Security, sharing their success stories and experiences.
- Share content to celebrate achievements and insights from ongoing research and implementation phases.



Social Media Channels

The Digital4Security project will leverage the existing social media channels of its partners for outreach, supplemented by the project's own LinkedIn page and YouTube channel. This approach ensures a wide reach and engagement through established networks, with a particular emphasis on LinkedIn for professional engagement.

Social Media Engagement Strategy

To create an active community and promote the Digital4Security project via partner channels and its LinkedIn page, the following actions will be undertaken:

- Regular publication and interaction with the project's ecosystem.
- Promotion through project newsletters and partner email newsletters.
- Targeted sponsored content to reach specific audiences.
- Use of relevant hashtags such as #Cybersecurity, #CyberManagement, and #Digital4Security.
- Utilise partners' channels to share stories, infographics, and key outcomes from the project.

WP5 Leaders Will Provide

- Pre-designed posts and graphics highlighting key successes.
- Scheduled plan for posting across various partners' platforms including LinkedIn, Twitter, Facebook, and Instagram.
- Hashtags specifically created for tracking campaign engagement, e.g., #D4SSuccess, #CyberEducation.

LinkedIn

The Digital4Security LinkedIn page (<https://www.linkedin.com/company/digital4security/>) will play a crucial role in the dissemination strategy, focusing on professional engagement and industry connections. Regular updates, success stories, and project outcomes will be shared to engage and attract potential candidates, partners, and stakeholders. The posting style blends informative articles with visually appealing graphics and videos. The content aims to strike a balance between thought leadership and actionable insights, catering to a wide range of professionals interested in the digital skills sphere. Interactive posts, including thought-provoking questions and engaging polls, intend to foster a sense of community and encourage meaningful discussions among followers.



Figure 1 Digital4Security LinkedIn Page

YouTube

The Digital4Security YouTube channel (www.youtube.com/@Digital4Security) will be utilised for sharing video content such as webinars, project updates, and success stories to support the overall dissemination strategy.



Figure 2 Digital4Security YouTube Channel

Email Newsletter

Brevo has been selected as the Digital4Security Project email newsletter solution based on its service offerings and EU GDPR compliance. The official Digital4Security newsletter, managed via Brevo, will be issued in line with the communications strategy and on an ad-hoc basis as needed. It will communicate project progress, results, and key related topics. Partners are encouraged to contribute content, including their own and third-party material relevant to the project's target audiences. Subscribers can sign up via an embedded form on the project's website homepage.

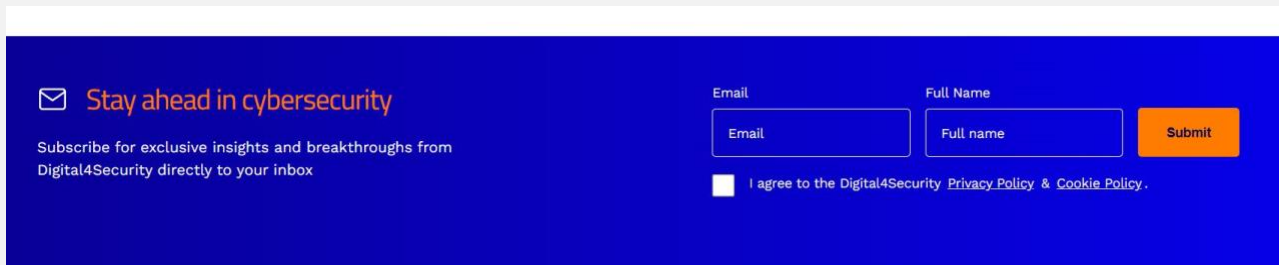


Figure 3 Email Newsletter Sign Up on Website

Direct Mailing

For specific outreach purposes, consortium partners will use direct mailing, leveraging their mailing lists while adhering to GDPR norms. This includes:

- **Sending emails to targeted individuals and organisations.**
- **Using partners' contacts to reach specific audiences.**

By integrating these digital communication strategies, the Digital4Security project ensures consistent and effective dissemination of information, fostering engagement and support across all stakeholder groups.

Promotional email templates will be created for different stages of dissemination campaigns, tailored to various segments of the email list.

Website visitors can subscribe to the newsletter via an embedded form on the footer of all pages of the project website www.digital4security.eu.

By utilising these comprehensive strategies, the Digital4Security project aims to build a robust online presence, effectively engaging and supporting its community through well-coordinated digital marketing efforts.

WP5 leaders manages the Digital4Security newsletter editorial line to ensure consistency. Partners are encouraged to submit interesting and related content directly to admin@digital4security to be promoted in the newsletter. This includes:

- Partners' own content related to the topics of the project
- Third-party content that partners find suitable and interesting for our target audiences (e.g. evergreen content, hot topics content)

All partners can already subscribe to the Digital4Security Project newsletter. To promote the newsletter, partners are encouraged to share it with their network. GDPR norms will be respected while handling all mailing lists.

Instagram and Facebook

A suite of design assets sized for Instagram and Facebook are available to all partners to allow for sharing on partner accounts.

Communication Channels & Tools

The table below provides an overview of the main communication tools that will be used for the dissemination and outreach activities of the Digital4Security Project, as well as their respective characteristics of communication:

Tool	Channel	Characteristic / Tone of voice
Digital4Security Project Website	Portal for LMS	Official, informative, welcoming
	Blog articles	Semi-formal, informative, narrative, engaging
Social media	LinkedIn*	Professional, informative, visual, engaging, interactive
	Twitter **	Semi-formal, informative, interactive
	Facebook**	Informal, informative, visual, engaging
	Instagram**	
Mailing	Project email newsletter	Official, informative, narrative, promotional
	Partners' email newsletter	
	Direct mailing/message	Informal, informative, promotional
Press & media	Press releases	Official, informative, storytelling
	Press articles	
Events/Webinars	Project events	Official, informative, storytelling, promotional
	External representations	
Visual assets	Online and offline communications	Official, informative, visual, engaging
Partner communication channels	Social media, websites and email newsletters.	Official, informative, narrative, promotional

*Dissemination on both project page and partner platforms

** Dissemination will be on partner platforms.

We are continually creating evergreen and thematic content for the project website and partner communication channels, scheduled and planned in a content calendar.



Project Website

A dedicated project website has been set up to support the promotion of expert guidance and provide access to resources on cybersecurity education, management, and technological advancements. It is a user-friendly website with comprehensive information for each user type. The Digital4Security project website is available at www.digital4security.eu.

The website has two main purposes:

- **Informative:** It informs stakeholders about the project through a narrative-based user experience, making all public project results available.
- **Collaborative:** It hosts and links to the Digital4Security teaching resources for educators and students and will link to the Learning Management System (LMS) and provide a section on modules in future versions.

Initially, we had a holding page created at the start of the project with key project details, and the full website was launched on 27/03/2024. As the project progresses, the website will feature detailed reports, data, and testimonials from the project.

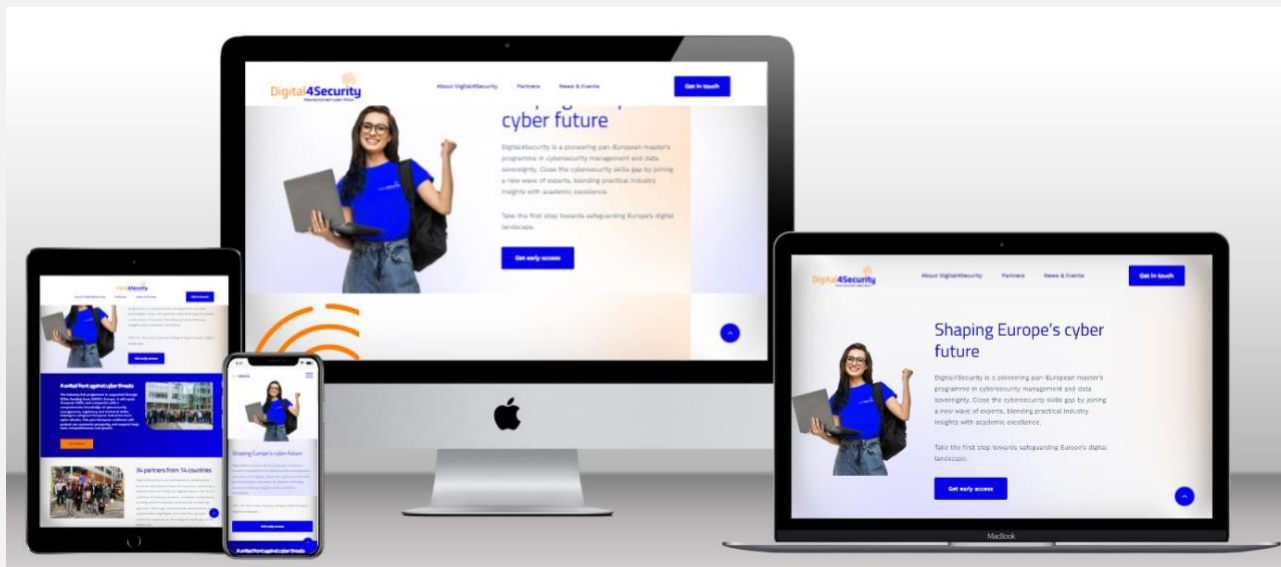


Figure 4 Digital4Security Website

Website Domain

We nominated and purchased the following domain name for the Digital4Security project website: www.digital4security.eu

Technologies Used

The selected website platform for the project website is the WordPress content management system (CMS).

WP1 leaders, POLITEHNICA BUCHAREST, manage the hosting for the website.

WordPress is the world's most widely used and capable CMS. It allows role-based access and administration and is fully extensible to facilitate advanced feature development and custom integrations, in line with the processes of the organisation. WordPress provides a rich and easy-to-follow experience when creating and editing content. Our main criteria for choosing a content management system for this specific project include:

- **Security**
- **Reliability**
- **Ease of operation**
- **Scalability for the future**
- **Cost**

WordPress is used on over 450 million websites, ensuring it will remain a popular CMS for many years. Future scoping indicates that WordPress has a vast range of external plugins designed to meet the functional needs of most businesses, thus reducing development time and costs. Plugins are also built in a manner that enables the creation of custom modules tailored to precise requirements, ensuring seamless integration of potential functionalities if needed later.

Website Administration

WP5 leaders, MATRIX and DIGITAL Europe, are the administrators of the website. Additional user accounts with relevant access will be set up in the future so that consortium partners can contribute to the website content and moderate or process user registration if necessary.

Website Pages

Homepage

The homepage introduces the Digital4Security project and the main navigation links to:

1. Home
2. About Digital4Security
3. Partners
4. News & Events
5. Contact Us

The homepage content is a quick introduction, with a shortcut to a summary about the project, which links to the latest news and events. It highlights the number of partners involved and their respective countries. The homepage displays the latest news and events and photographs of real people related to the project. There is a call to action to contact the consortium if users have any questions. It contains the email newsletter signup with GDPR opt-in.



Figure 5 Digital4Security Homepage

About Digital4Security

This page offers a detailed overview of the Digital4Security project and highlights our mission, values, and methods. These images will be updated as the project progresses to include photos of the partners, making the content relatable and real. www.digital4security.eu/about

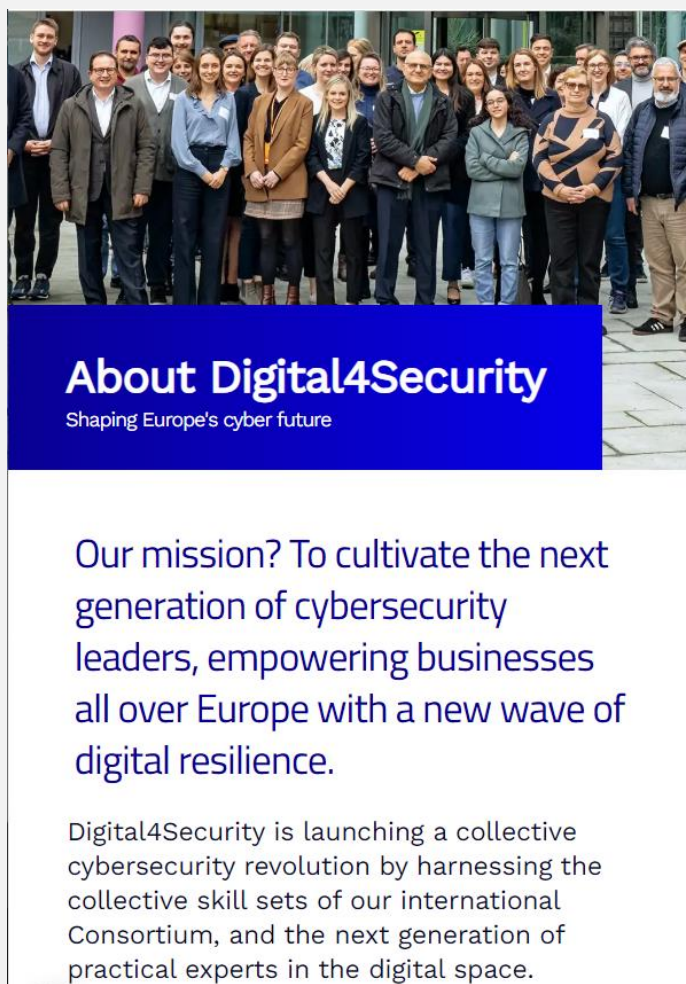


Figure 6 Digital4Security About Page

Our Partners

This page lists all consortium partner and associated partner logos in alphabetical order. The logos link to a dedicated page for each partner on the project website.

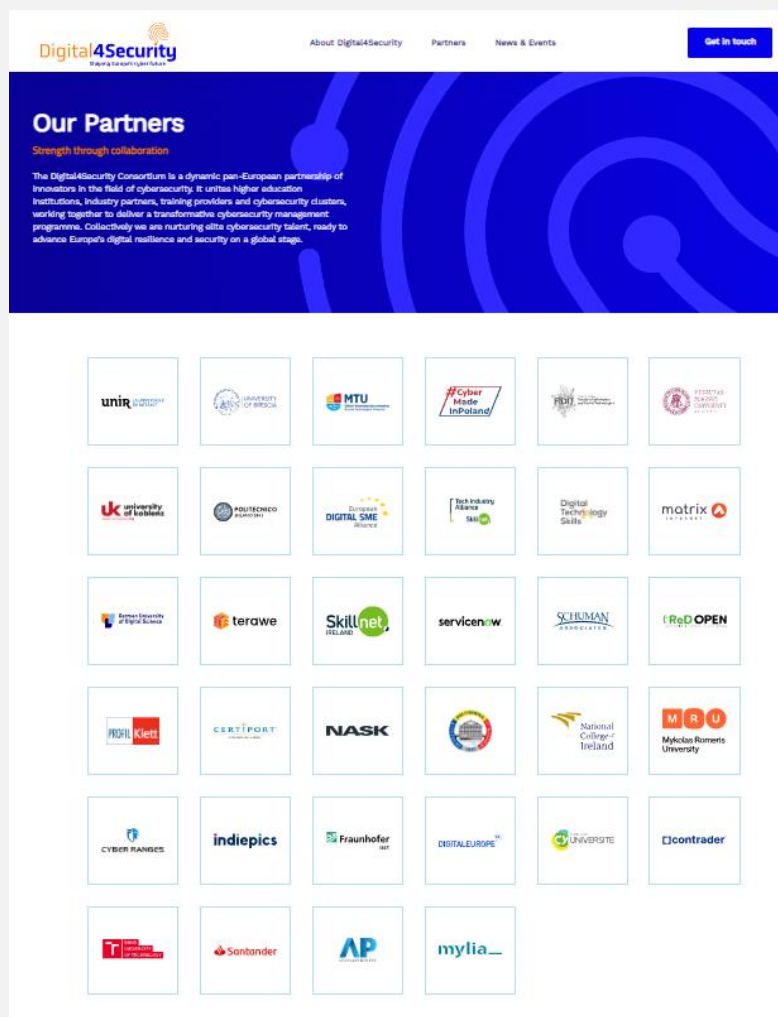


Figure 7 Our Partners Page

Dedicated Partner Page on Project Website

The administrators have streamlined the workload for other partners by creating templates, guides, prompts, instructions, graphics, and suggestions. For the dedicated individual partner page on the project website, an initial sample page was created and shared with detailed guidelines: Each partner page contains:

- **Partner tagline:** max 80 characters
- **Partner bio:** 300-800 characters
- **Partner country**
- **Partner contribution to consortium content:** 300-1,500 characters
- **Partner mission tagline:** max 80 characters
- **Partner mission content:** 300-1,500 characters

- Contact details
 - Partner address and Google Maps embed code
 - Nominated partner contact number
 - Nominated partner email for project contact
 - Partner website URL
- Each partner was given guidelines on image dimensions and guidelines for images on their dedicated page. Each partner selected imagery that was on-brand for their organisation, university, agency, or company, and also aligned with the project website.

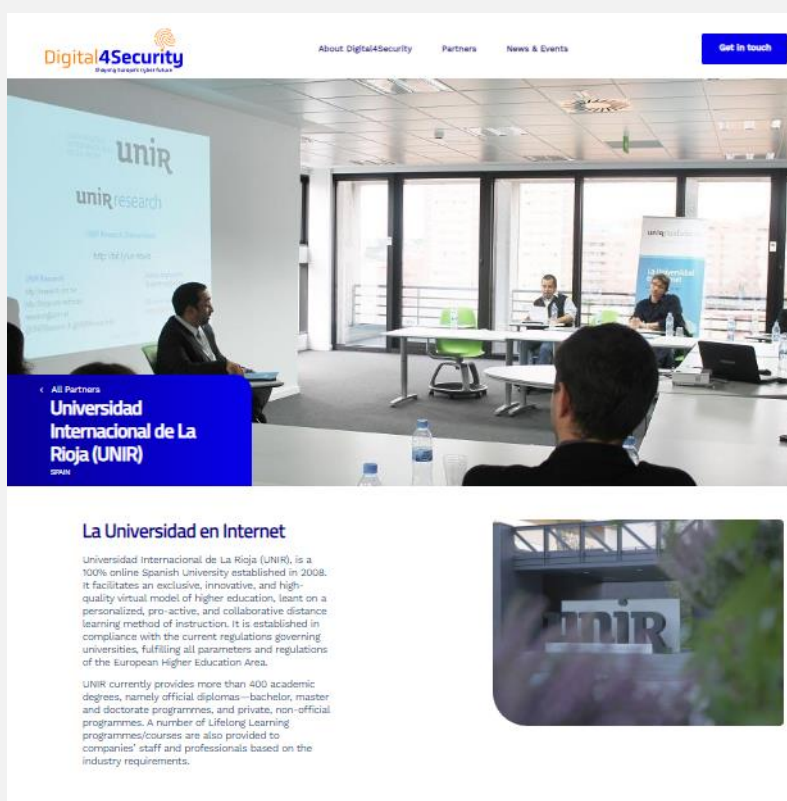


Figure 8 Example of partner page from website

News & Events

The website's blog, titled News & Events, serves as the central hub for updates on the Digital4Security project and related topics, establishing the project as a leader and expert in its field. This section will feature:

- Informative articles on project milestones, progress, and activities.
- News on related European projects and initiatives.
- Announcements of all Digital4Security events.
- Evergreen content and hot topics on cybersecurity education, management, and technological advancements. www.digital4security.eu/news-events

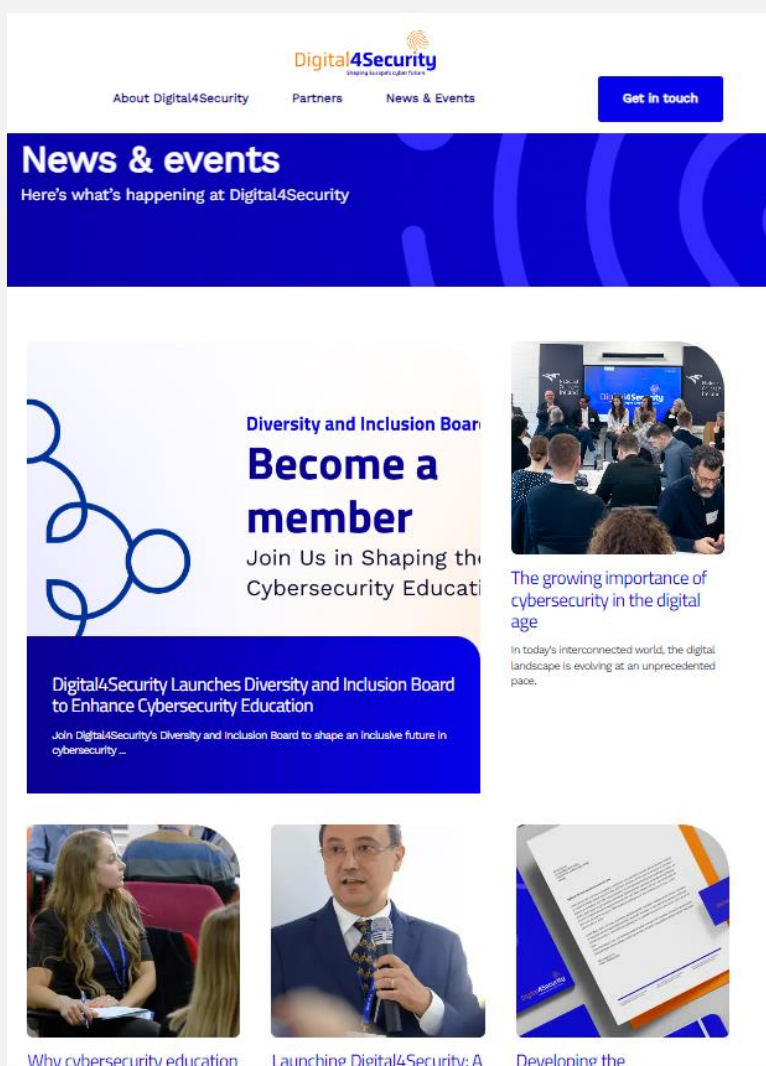
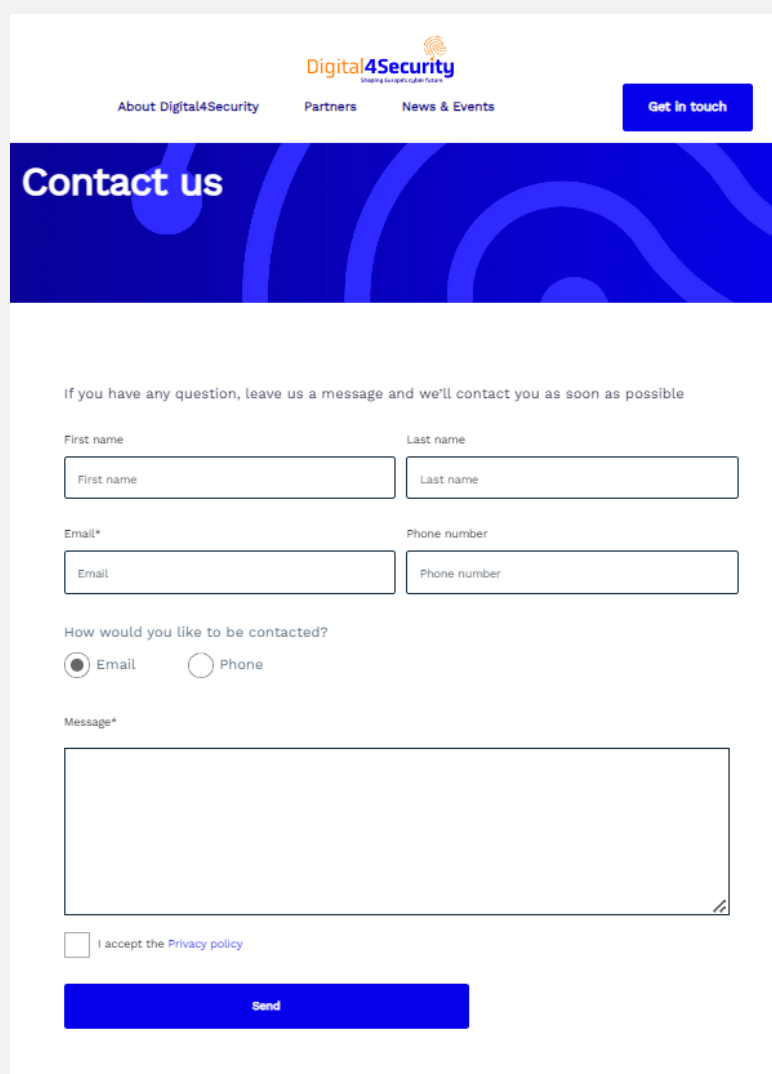


Figure 9 News & Events Page

Contact Us

Website visitors can contact the Digital4Security project consortium through a contact form, which is accessible on all pages via a main navigation link. This reassures users that

Digital4Security is available to respond to any queries. It encourages visitors to get in touch with our team or register for upcoming events. The form is GDPR compliant with an obligatory opt-in to our privacy policy so we can collect responses and respond accordingly. The relevant fields are set to obligatory, so we capture the details we need to reply. Input field titles must be visible on all states. Any obligatory field must have (*) at the end of the input field title. reCAPTCHA v3 verification is set up as a SPAM filter. All submissions to the form are sent to admin@digital4security.eu, which is monitored and responded to accordingly by WP5 leaders. www.digital4security.eu/contact-us



If you have any question, leave us a message and we'll contact you as soon as possible

First name

Last name

Email*

Phone number

How would you like to be contacted?

☒ Email ☐ Phone

Message*

☐ I accept the [Privacy policy](#)

Figure 10 Contact Us page

Footer

The footer appears on all pages of the Digital4Security website. It prominently displays the "Co-funded by the European Union" logo, as required for all related materials of co-funded projects. The footer includes links to the Contact Us page, as well as the Cookie Policy, Privacy Policy, and Sitemap, ensuring easy navigation and compliance with relevant regulations.

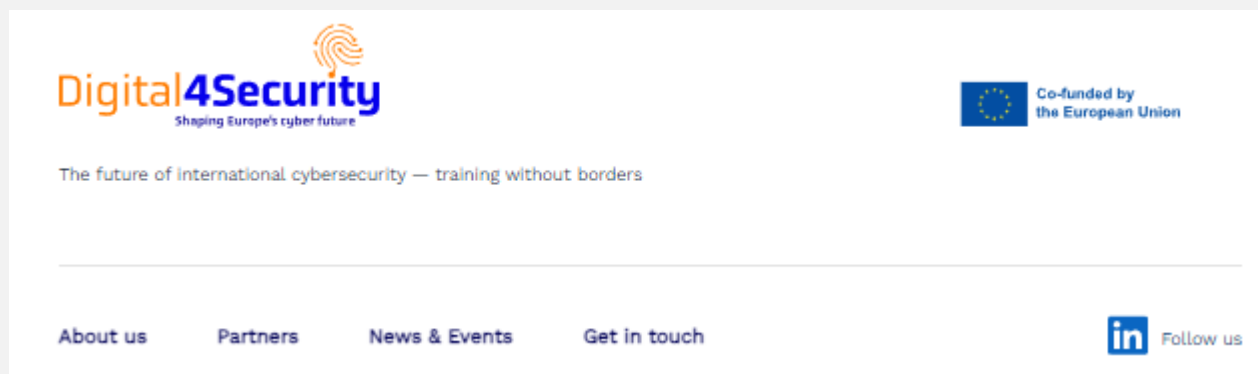


Figure 11 Website Footer

Privacy Policy

The Privacy Policy page displays the website's privacy policy, outlining how we collect, use, and protect users' personal data in compliance with GDPR regulations. You can view the full privacy policy here: [Privacy Policy](#).

Cookie Policy

This page details the website's cookie policy, explaining which cookies are active (automatically updated by Cookiebot) and allowing users to view and update their cookie preferences. You can manage your cookie settings and view the full policy here: [Cookie Policy](#).

Sitemap

The Sitemap page lists all the website pages and the relationships between them, providing a clear structure of the site. This helps search engines crawl the website more efficiently for indexing and ranking on their related search engine platforms. You can access the sitemap here: [Sitemap](#).

Cookie Script

In line with GDPR requirements, a cookie script has been installed on the Digital4Security website.

Cookiebot

We have selected Cookiebot as our cookie script solution to assist with GDPR compliance. The first time a user visits <https://www.digital4security.eu>, they encounter a cookie popup enabling them to select their cookie preferences.

The Cookiebot icon is always readily available in the bottom left corner of all pages, allowing users to update their cookie preferences at any time.

When users click on the Cookiebot update icon, they are presented with their current preferences and the following options:

- Cookiebot automatically scans to monitor and report all types of cookies and similar tracking on the project website and updates the cookie policy page accordingly. Our cookie policy is automatically updated and is available to read at <https://www.digital4security.eu/cookie-policy>.

Why Cookiebot?

Cookiebot Consent Management Platform (CMP) is a plug-and-play compliance solution built around an unrivalled scanning technology that detects and controls all cookies and trackers used on a website, and automatically manages end-user consents. It is a market leader in the field of CMP. Cookiebot CMP is a self-serve cloud service provided by the e-privacy company Usercentrics, enabling automated compliance with global data privacy laws, particularly EU GDPR. Cookiebot will enable the Digital4Security project to collect, manage, and document user consents on the project website, achieving full compliance with global privacy regulations while facilitating high consent rates and building trust with our website users.

Website Analytics

Monitoring website usage is crucial for achieving the overall project mission and goals. We needed to set up tracking goals with real-time data monitoring and location tracking of the various users who visit the project website, and we selected the best solution.

Matomo

Matomo was chosen for the project as it provides a customisable dashboard, allowing personalised views and can be used without consent while still being GDPR-compliant.

Why We Chose Matomo

- User-privacy protection: 100% GDPR-compliant
- 100% ownership of the data
- Displays different search engines and keywords used to arrive at a page
- Helps determine pages with high traffic volume and which pages are underperforming
- Provides heatmaps with the premium subscription
- Ability to import historical Universal Analytics data
- Open source, enabling high customisation of functionalities
- No data sampling

How Matomo Tracks

- Matomo offers cookie-less tracking by using visitor `config_id` – a randomly-seeded, privacy-enabled, time-limited hash of a limited set of the visitor's settings and attributes.

The config_id or config hash is a string calculated for a visitor based on their operating system, browser, browser plugins, IP address, and browser language.

- Tracks pageviews, events, downloaded files, clicks on external links, and user session duration.

For example, we can track:

- **How many users downloaded a document**
- **How many users watched a video**
- **How many users clicked on a link from an external website**

Matomo provides video analytics and heatmaps (premium subscription) that show how users interact with different pages via color-coded splotches. Matomo has its own Google Tag Manager called Matomo Tag Manager.

Matomo Setup

We installed the WP-Matomo Integration (WP-Piwik), which supports WordPress networks and manages multiple sites and their tracking codes as well as Matomo (Cloud). A Matomo account has been set up and paired with the website to collect relevant and anonymised data from visitors. The data collected will then be centralised and analysed by the WP5 leader.

Matomo Weekly Report

Weekly reports are sent to the WP5 leader to keep us constantly informed of website activity. The weekly report for the Digital4Security project includes:

- **Visits Summary**
 - Country
 - Region
 - City
 - Language code
 - Device type
 - Browsers
 - Visits by day of the week
 - Actions - Main metrics
 - Referrers Overview
 - Channel Type
 - All Channels
 - Search Engines

- **Visits Summary**
 - Visits
 - Actions
 - Maximum actions in one visit
 - Actions per Visit
 - Avg. Visit Duration (in seconds)
 - Bounce Rate
- **Country**
- **Region**
- **City**
- **Language code**
- **Device type**
 - Desktop
 - Smartphone
 - Phablet
 - Tablet
- **Browsers**
- **Visits by day of the week**
- **Actions - Main metrics**
- **Pageviews**
 - Unique Pageviews
 - Downloads
 - Unique Downloads
 - Outlinks
 - Unique Outlinks
 - Searches
 - Unique Keywords
- **Referrers Overview**
 - Visitors from Search Engines

- Visitors from Social Networks
 - Visitors from Direct Entry
 - Visitors from Websites
 - Visitors from Campaigns
 - Distinct search engines
 - Distinct social networks
 - Distinct keywords
 - Distinct websites
 - Distinct campaigns
 - Percent of Visitors from Direct Entry
 - Percent of Visitors from Search Engines
 - Percent of Visitors from Campaigns
 - Percent of Visitors from Social Networks
 - Percent of Visitors from Websites
- **Channel Type**
 - Direct Entry
 - Websites
 - Search Engines

Hosting

The project's website is hosted by Politehnica Bucharest, on their own servers using specialised hosting services and software that ensures high availability, redundancy and security of the hosted website. The **hosting.upb.ro** platform (see **Error! Reference source not found.**) is an ISPConfig¹ open-source solution that offers a hosting control panel designed to manage multiple servers from a single interface, making it an efficient solution for web hosting companies and IT professionals. It supports the management of Apache and Nginx web servers, allowing users to handle a variety of web hosting needs. Key features include multi-server management, which enables the control of multiple servers from one central panel, and a highly customizable user interface that caters to administrators, resellers, and clients. ISPConfig also offers robust security features, including SSL certificate management, and extensive support for email hosting, including Postfix and

¹ <https://www.ispconfig.org/>

Dovecot integration. Additionally, it provides DNS management, file management through FTP and web-based file managers, and database management with MySQL. Its modular architecture ensures scalability and flexibility, accommodating a wide range of hosting environments and configurations.

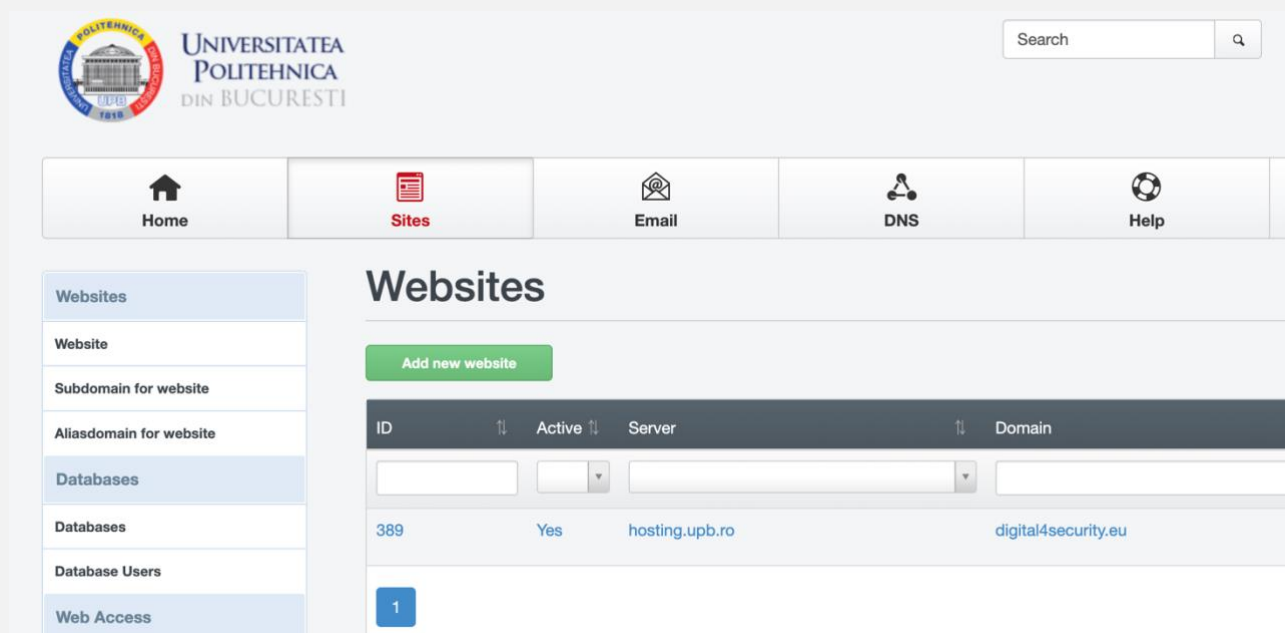


Figure 12 Hosting platform for digital4security.eu web site

Hosting configurations

The hosting service provides a versatile and user-friendly interface for managing all aspects of web hosting, from server setup to website maintenance as follows:

- Public IPv4 address: 141.85.241.222;
- Public IPv6 address: 2001:b30:800:f010:215:5dff:fe14:502;
- Domain name: digital4security.eu;
- PHP version: PHP-FPM version php8.2;
- Automatically redirect HTTP to HTTPS;
- SSL: Let's Encrypt Certificate;
- MySQL database;
- Mailing lists;
- Backup service: The website is configured to automatically backup once a month. Also, backups are performed as required by the Politehnica Bucharest team.

Hosting service software inventory

The hosting service is running on a Debian 12 server and is composed of the following services:

- ISPConfig 3.2.12 - last updated 20.06.2024;
- ISPConfig Migration Toolkit 2.2.7 - last updated 15.03.2024.

The software components of the hosting service are always kept updated according to the latest releases as shown in Figure 13 Latest software configuration of the hosting server..

Statistics of the hosting

In this subsection we present the statistics of the resource usage of the digital4security.eu website:

- Website Harddisk Quota: 8825.8 MB;
- Database Quota: 83.1 MB;
- Number of email domains: 1;
- Number of mailing lists: 10;
- Number of web domains: 1;
- Number of FTP users: 2 (one for the Politehnica Bucharest team and one for the Matrix team);
- Number of databases: 1.

Latest news
2024-06-20 ISPConfig 3.2.12 Released
2024-03-15 ISPConfig Migration Toolkit 2.2.7 Released
2024-02-09 ISPConfig 3.2.11p2 Released
2023-10-26 ISPConfig 3.2.11p1 Released
2023-10-03 ISPConfig Autoinstaller Script Updated
2023-09-08 Update the ISPConfig Perfect Server from Debian 11 to Debian 12
2023-08-08

Figure 13 Latest software configuration of the hosting server.

Website monitoring

In this section we present the monitoring figures for the project's website. The hosting service is using AWStats², an open-source tool for server monitoring and statistics, that outputs data in graphically and easy to understand manner. This log analyser works as a CGI or from command line and shows you all the information your log contains in a few graphical web pages. It uses a partial information file to be able to process large log files, often and quickly. In terms of security aspects, AWStats shows you the following information:

² <https://awstats.sourceforge.io>

- Visits of robots: 15 different robots (Figure 14);
- Worms attacks: none;
- HTTP status codes as shown in Figure 15.

Robots/Spiders visitors (Top 10) - Full list - Last visit			
15 different robots*			
	Hits	Bandwidth	Last visit
wordpress	180	815.13 KB	24 Jun 2024 - 23:12
nbot	67+3	4.42 MB	24 Jun 2024 - 12:58
link	42	2.22 MB	24 Jun 2024 - 08:04
Unknown robot identified by bot*	5+14	190.87 KB	24 Jun 2024 - 23:12
AhrefsBot	11+2	315.30 KB	24 Jun 2024 - 18:51
facebookexternalhit	10+1	1.26 MB	24 Jun 2024 - 21:10
bingbot	9+2	167.20 KB	24 Jun 2024 - 23:23
CFNetwork	7	369.01 KB	24 Jun 2024 - 14:14
empty user agent string	5	320.15 KB	24 Jun 2024 - 14:08
Googlebot	2+2	63.81 KB	23 Jun 2024 - 04:26
Others	3+3	156.40 KB	

* Robots shown here gave hits or traffic "not viewed" by visitors, so they are not included in other charts. Numbers after + are successful hits on "robots.txt" files.

Figure 14 Overview of the visits from robots.

HTTP Status codes			
HTTP Status codes*			
	Hits	Percent	Bandwidth
301 Moved permanently (redirect)	1,220	92.4 %	1.01 MB
404 Document Not Found (hits on favicon excluded)	45	3.4 %	395.54 KB
401 Unauthorized	41	3.1 %	191.98 KB
403 Forbidden	8	0.6 %	9.63 KB
500 Internal server Error	3	0.2 %	15.72 KB
503 Server busy	2	0.1 %	16.26 KB
421 Unknown error	1	0 %	7.08 KB

* Codes shown here gave hits or traffic "not viewed" by visitors, so they are not included in other charts.

Figure 15 HTTP status codes.

Focusing on the way users reach our website we have the following statistics (Figure 16):

- Direct access: 1531 pages with 1622 hits, resulting 99.3%;
- link from Google.com: 3 pages with 3 hits, resulting 100%;
- link from LinkedIn: 7 pages with 7 hits, resulting 100%;
- link from <https://www.skillnetireland.ie/>: 3 pages with 3 hits, resulting 100%;
- link from facebook.com: 1 pages with 1 hits, resulting 100%;

Connect to site from			
Origin			
	Pages	Percent	Hits
Direct address / Bookmark / Link in email...	1,531	99.3 %	1,622
Links from an Internet Search Engine - Full list	3	0.1 %	3
- Google .com 3 / 3			
Links from an external page (other web sites except search engines) - Full list	7	0.4 %	7
- https://www.linkedin.com 3 3			
- https://www.skillnetireland.ie 3 3			
- http://m.facebook.com 1 1			
Unknown Origin			

Figure 16 Connecting to digital4security.eu sources.

As an overall conclusion, the monitoring of the web hosting indicated that the availability of the services is above 95%. In terms of security, the project web site hosting does not indicate any potential vulnerabilities.

SSL

A Let's Encrypt SSL certificate was installed on the server as part of the go-live process. Let's Encrypt is a free, automated, and open certificate authority provided by the nonprofit Internet Security Research Group (ISRG). The details of the certificate are presented in

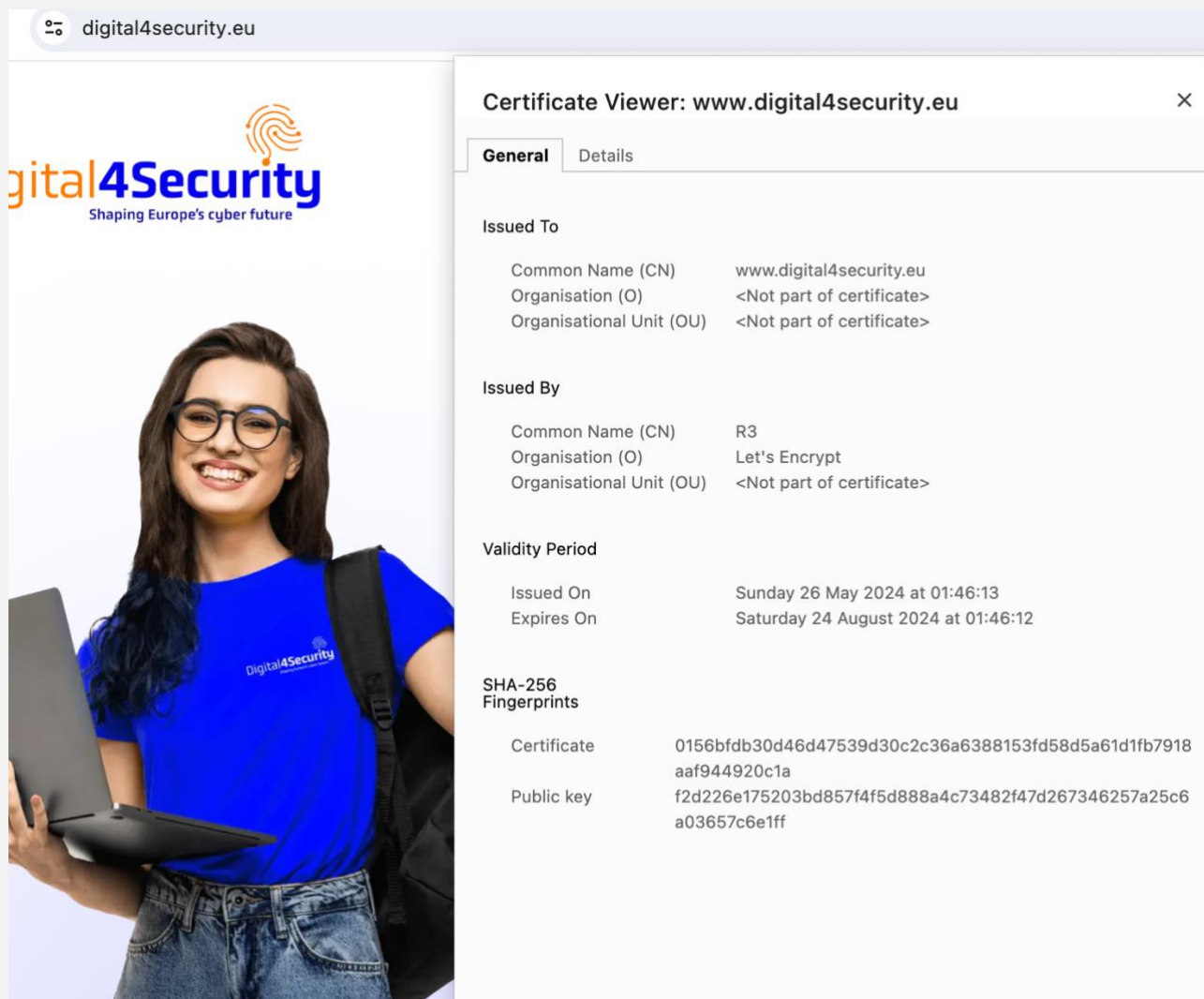


Figure 17 Overview of the Let's encrypt certificate used on digital4security.eu.

Support

To ensure the project website is kept fully up-to-date and secure and to optimise long-term website performance the website was added to Matrix Internet dedicated support, where technical support and maintenance will be provided for the agreed duration of the project.

CMS and all plugin updates are performed within a month of new releases. Backups are regularly taken to act as website recovery in case of minor or major data loss.

A monthly report detailing current website performance status is sent to nominated people (WP5 working leaders and co-leaders).

Dedicated support team

The WP5 leaders have access to a dedicated support team with rapid response times by emailing support@matrixinternet.ie:

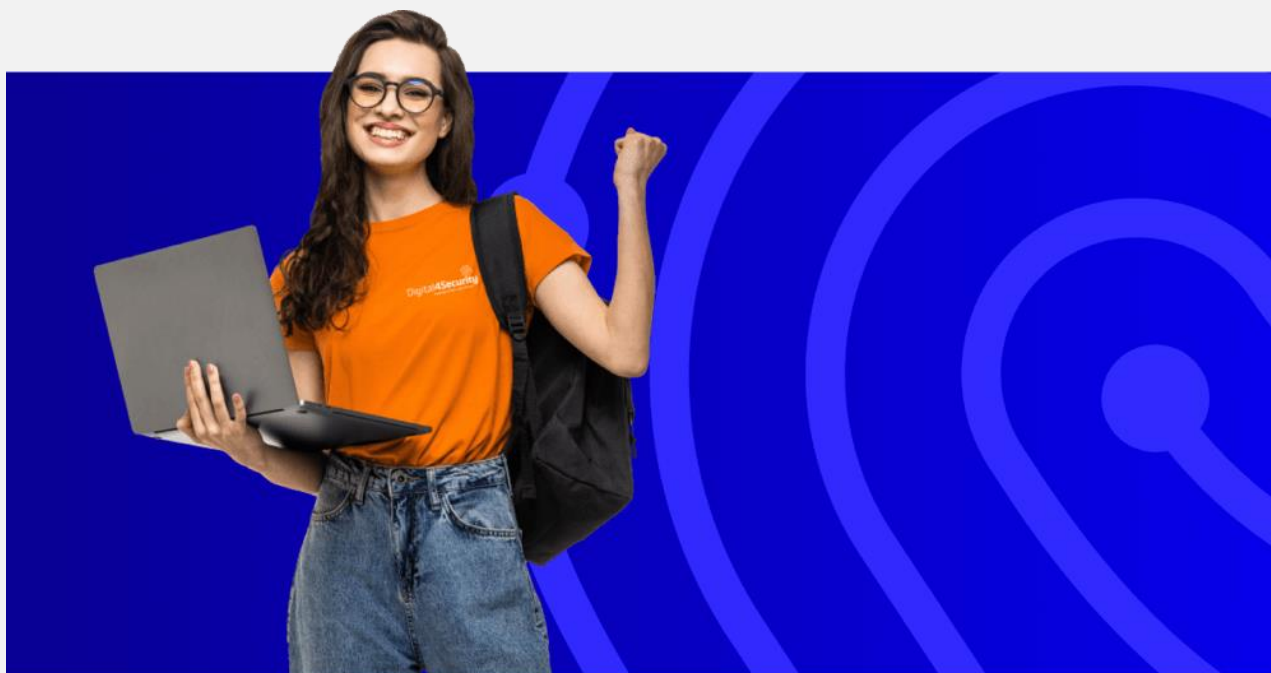
- Within 2 hours during office hours (Monday to Friday).
- Within 4 hours outside office hours on weekdays (Monday to Friday).
- Within 24 hours on weekends or holidays.

Monthly support report

Technical support and maintenance are carried out monthly. To minimise downtime while ensuring the website is fully up-to-date and secure, a dedicated support developer completes the following steps once a month:

- A full copy of the live website files and database are taken.
- This is then used to create a fully independent clone of the website and testing environment.
- All appropriate updates are performed in appropriate areas and WordPress Core
- Full QA/QC is performed on this cloned website.
- Once verified and tested, these updates are pushed to the live site.
- Web server updates are also processed where appropriate.
- The live site is also tested to ensure no issues have presented.

A full monthly report is generated and shared with the WP5 working leaders and co-leaders



Partner Webpage

Each Consortium Partner was tasked with creating a dedicated project page on their respective website. To facilitate this, MATRIX created its own Partner landing page first, to serve as a working illustrative example, and then created a detailed brief for all partners to follow.

Partner Webpage Content Guide

Webpage Creation

- **Brief:** Each partner is requested to create a page on their website showcasing the Digital4Security Project.
- **Page Template:** Partners may use an existing page template such as news items, case studies, or project pages. Ensure that the design aligns with your organisation's website style while maintaining a focus on the Digital4Security Project.
- **Banner and Localisation:** Include a banner specific to the Digital4Security Project and localise the content provided to reflect your organisation's role and perspective within the consortium.
- **Assets:** Utilise the range of assets prepared by the coordinating partner to enhance the page visually and informatively. These assets include logos, infographics, and photographs relevant to the project. [Link to assets in SharePoint] Please remember to display the co-funded by European Union logo which is on the banners provided.
- **Project Link:** Ensure the page includes a direct link to the Digital4Security project's main website for visitors seeking more detailed information: www.digital4security.eu

Content Requirements (please localise)

- **Page Title:** Use 'Digital4Security Project' as the page title to maintain consistency across all partner websites.
- **Introductory Section:** Introduce the Digital4Security Project, mentioning the launch year (2024), the funding information (€20 million from the European Union), and the project's mission to create a comprehensive Master's Programme in Cybersecurity Management & Data Sovereignty.
- **Detailed Description:** Expand on the consortium's composition, the roles of different partners, and specific contributions your organisation is making to the project.
- **Master Programme:** Describe the approach to building the curriculum based on needs analysis involving all consortium partners. Emphasise the programme will combine theoretical knowledge with practical, job-ready skills that are essential for immediate and effective application in the workforce.

Visibility and Promotion

- **Prominent Display:** Position the Digital4Security Project page in a prominent part of your website, such as in recent news, featured projects, or other high-visibility areas.
- **Call to Action:** Encourage visitors to learn more about the project, participate in events, or apply to the program through clear call-to-action buttons.

Update and Reporting

- **URL Submission:** Once the page is live, submit the URL to the consortium's central coordination team via the provided SharePoint link for inclusion in the overall project directory.
- **Continuous Updates:** Regularly update the page with new developments, upcoming events, and additional resources as the project progresses.

Sample Page

- **Matrix Internet page:** <https://www.matrixinternet.ie/digital4security>

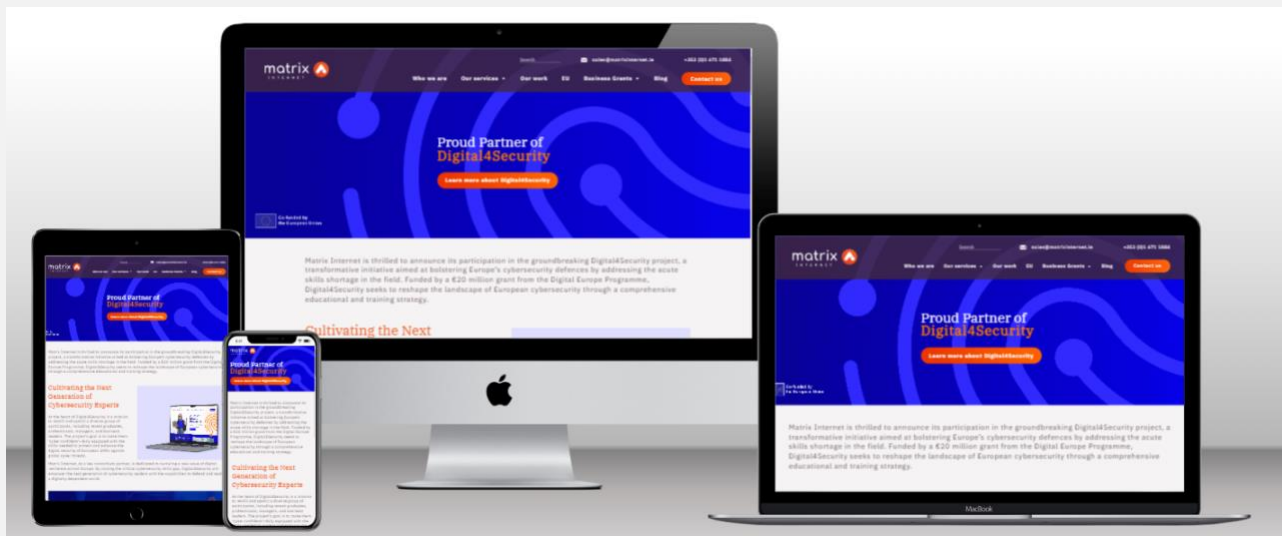


Figure 18 Sample Partner Page

Partner Webpage Assets

A range of assets were provided to support the partners in the creation of their dedicated page, ensuring consistency and high-quality presentation across all consortium partner websites.



Figure 19 Sample visual assets 1



Figure 20 Sample visual assets 2

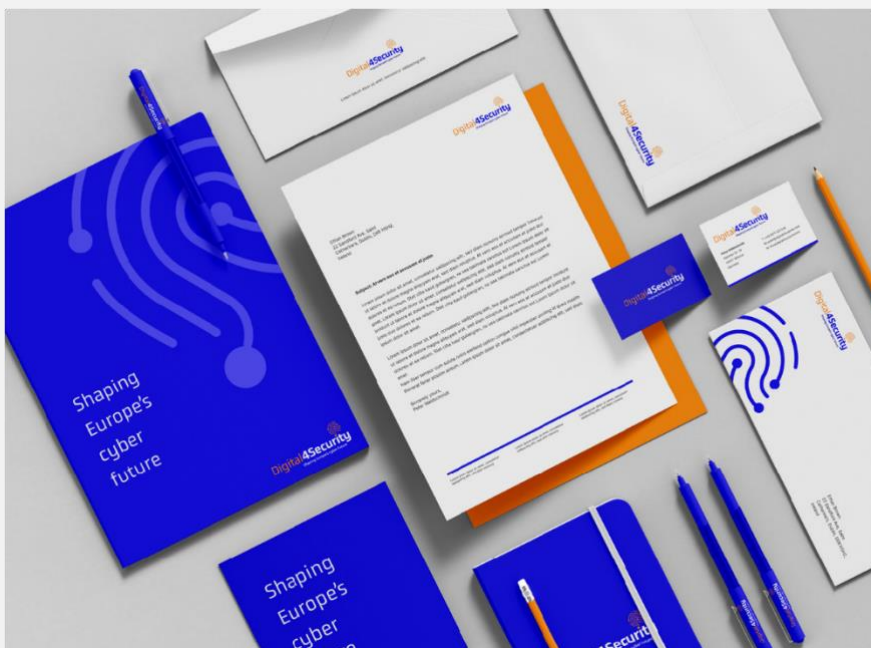


Figure 21 Sample visual assets 3



Figure 22 Banner for partner page

Legal Disclaimer

The European Commission's support to produce this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project 101123430 — Digital4Security — DIGITAL-2022-SKILLS-03

Copyright © 2024 by Digital4Security Consortium



Digital4Security

Shaping Europe's cyber future

