



# RAISING AWARENESS AND CYBER HYGIENE IN SMEs

KNOW CYBER GRANTS FOR THE WESTERN BALKANS CIVIL SOCIETY ORGANISATIONS



Project duration:  
**12 months**



Location:  
**Montenegro**

[ivona@visionevent.me](mailto:ivona@visionevent.me) 



# Strengthening SMEs' Resilience



- SMEs are **not only a statistical majority**, but **the economic foundation of our societies**.
- The **digital transformation** of SMEs has accelerated, but **their awareness of cybersecurity and defense has not evolved** accordingly.
- The **economic implications** of cyber insecurity for SMEs are **profound**.
- The **end users** of our project are **the citizens of Montenegro**.

# Project phases



## Quantitative research

Quantitative research on current level of cyber hygiene skills and capacities in small and medium-sized enterprises.



## Training sessions

Training sessions held by expert for employees and management personnel in small and medium-sized enterprises.



## Educational material

Creating educational material about cyber hygiene skills and tools, which will be distributed through different channels.



## Awareness and education campaign

Cyber hygiene raising awareness and education campaign aimed at the general public, SMEs and intuitions of the system.



# Exposed: The Security Gaps Within SMEs



**Low awareness of cyber hygiene**

**76,5%**

are not familiar with the concept of cyber hygiene, indicating a serious lack of basic knowledge about digital security.



**Insufficient implementation of cybersecurity measures**

**1,7%**

achieve a high level of protection through practicing moderate cyber hygiene measures.



**Weak incident reporting and policy enforcement**

**67,5%**

of companies have some form of cyber hygiene policies, but they are neither sufficiently clear nor consistently enforced.



**Insufficient investment in cybersecurity**

**23,2%**

of companies allocate adequate resources to cybersecurity, while 13.9% invest significantly less than necessary.



# The Critical Need for Cyber Training



**Rare software and password updates**

**61%**

of employees update software only when prompted by the system, while 21.9% rarely or never update their business devices, creating opportunities for cyber-attacks.



**Greatest interest in data protection**

**42,7%**

want to improve the protection of personal and business data, while aspects such as device security and recognizing cyber-attacks are lower priorities.



**Potential of training to reduce risks**

**87,4%**

of respondents believe that additional training would help reduce the risk of cyber incidents.



**Cybersecurity training is rare and underdeveloped**

**85,4%**

of respondents have never undergone cybersecurity training. which clearly justifies the need for project implementation.



# Training sessions

**1**

## Management-Level Training

- Strategic planning
- Cyber risk assessment
- Organizational policies
- The key leadership role in fostering a culture of cyber hygiene

**2**

## Technical Staff Training

- Training on security tools
- Incident response protocols
- Data protection techniques
- Regulatory compliance

**3**

## Gender-Focused Training

- General cyber security skills
- Specific threats and challenges
- Gender diversity and inclusion in the cyber security sector

# Outputs & outcomes:

**Conducted research among 350 SMEs' employees in Montenegro**

Gathered data on the current level of cyber hygiene awareness, skills and capacities in SMEs in Montenegro, identifying their key challenges and areas for improvement.

**3 cycles of training sessions, each consisting of 2-day workshop**

Educated employees in SMEs will contribute to the stability and cyber security of SMEs, which will have a long-term positive effect on the economy of Montenegro.

**Raised awareness through social media and outdoor - more than 120.000**

Higher level of cyber hygiene awareness among SMEs, relevant institutions and general public will increase the security of our state system in the future.

# Impact left behind

Views

26,842

71.5% from ads

## "ZAŠTO JE SAJBER HIGIJENA VAŽNA"

- 76,5% zaposlenih u malim i srednjim preduzećima u Crnoj Gori nije upoznato sa sajber higijenom, što je proporcionalno nivou rizika po bezbjednost poslovanja, ličnih i korporativnih podataka i digitalnih sistema.
- Sajber higijena stoga nije opcija, već neophodnost za kontinuitet i sigurnost poslovanja.
- Čak 60% malih i srednjih preduzeća u Evropi je primorano da se zatvori u roku od 6 mjeseci nakon sajber napada.
- Prosječan finansijski gubitak od ovih napada iznosi 70.000-130.000 EUR.
- Izgubljeno povjerenje = izgubljeno poslovanje/dobit.

## "7 DOBRIH NAVIKA" "Sajber higijena je stvar mentaliteta koliko i alata"

7 osnovnih navika sajber higijene za mala i srednja preduzeća:

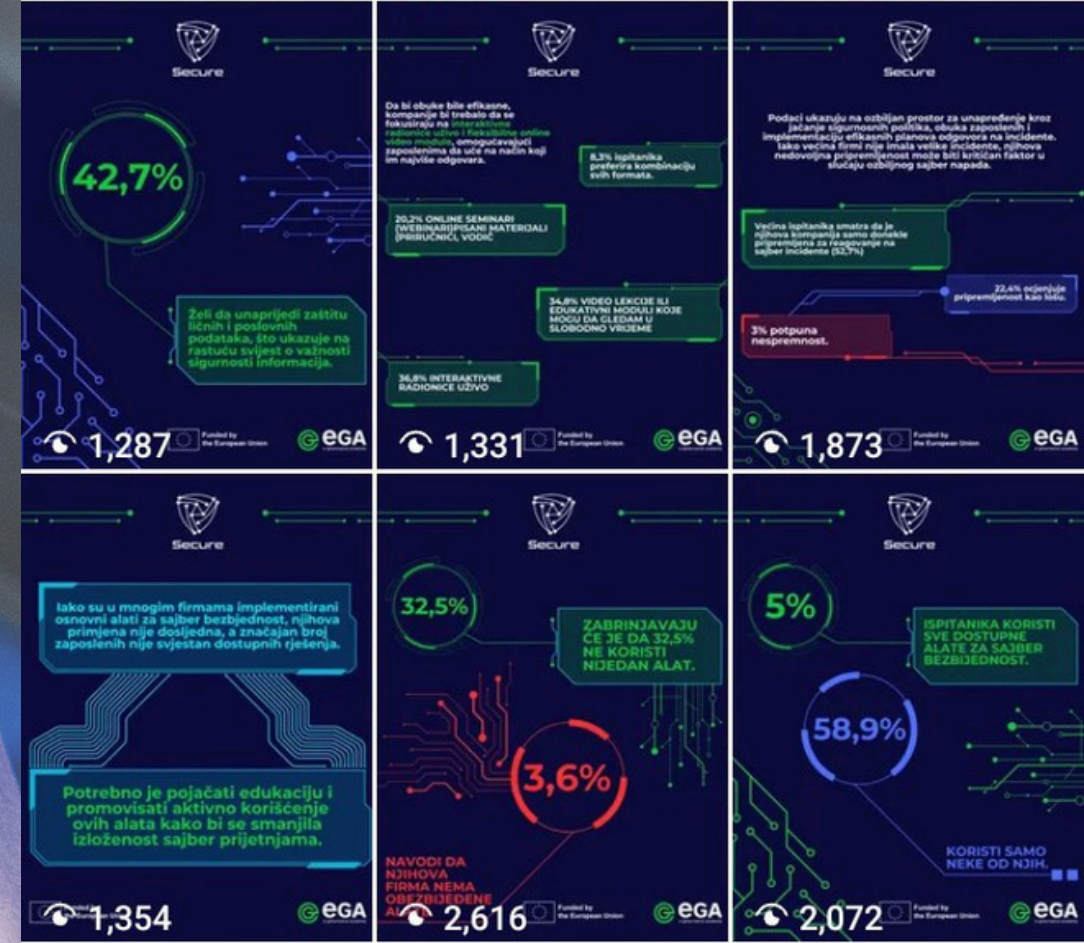
- Koristite jake lozinke**  
Koristite jedinstvene, složene lozinke. Implementirajte automatizovano upravljanje lozinkama.
- Omogućite višefaktorsku autentifikaciju (MFA).** Dodajte dodatni sloj zaštite pored lozinke.
- Redovno ažurirajte softvere**  
Održavajte sisteme, aplikacije i antivirusne programe ažurnim.
- Često pravite bezbjednosne kopije podataka.** Koristite sigurne, automatizovane bezbjednosne kopije u Cloud-u ili offline.
- Ograničite pristup**  
Omogućite zaposlenima pristup samo onome što im je potrebno. Klasifikujte korisnička prava na sistemu.
- Edukujte svoj tim**  
Naučite zaposlene da prepoznaju sumnjivo ponašanje i događaje u digitalnom domenu i da pravovremeno obavijeste odgovornu osobu. Organizujte obuku o korišćenju novih alata za zaposlene, prilikom kupovine uređaja i digitalnih alata.
- Osigurajte svoj Wi-Fi**  
Koristite snažnu enkripciju i odvojene mreže za goste.

## "KAKO ZAPOČETI" "Učinite sajber higijenu svakodnevnom rutinom"

67% malih i srednjih preduzeća u Crnoj Gori ima neku vrstu sajber politike, ali one obično nisu dovoljno jasne korisnicima ili nisu adekvatno implementirane.

Ne morate biti tehnički obrazovani da biste zaštitili svoje poslovanje od sajber prijetnji, samo trebate osigurati da svaki član tima ima dobre digitalne navike:

- ✓ Kreirajte jednostavne politike za svakodnevnu primjenu.
- ✓ Uključite cijeli svoj tim - edukujte svakog zaposlenog o sajber prijetnjama i kako da se zaštiti u digitalnom svijetu.
- ✓ Svi uređaji organizacije su ažurirani.
- ✓ Antivirus je aktivan i radi na svim sistemima.
- ✓ Bezbjednosne kopije su testirane i rade.
- ✓ Prava pristupa su pregledana (ko može pristupiti čemu).
- ✓ Zaposleni dobijaju redovne podsjetnike o phishingu.
- ✓ Wi-Fi mreže su zaštićene lozinkom.
- ✓ Višefaktorska lozinka je postavljena na svim (kritičnim) računarima.
- ✓ Stari računari i nalozi (bivši zaposleni, nekorišćene usluge/uređaji) su uklonjeni.
- ✓ Mobilni uređaji (USB, laptop itd.) su sigurni i šifrovani.
- ✓ Odštampajte ovu listu. Postavite je na zid kancelarije. Neka vam to postane navika.





# The Difference We Made

	BEFORE (1-5)	AFTER (1-5)	PROGRESS
Average self-rated cyber hygiene	3.44	4.76	+ 38.37%
Phishing recognition	3.75	4.72	+ 25.87%
Password strength and regular change	3.92	4.93	+ 25.77%
Incident reporting awareness	2.89	4.79	+ 65.74%
Cyber hygiene awareness	3.30	4.71	+ 42.73%

Usefulness of training





Secure

# THANK YOU

## GET TO KNOW US

More info at:

 [www.ngosecure.me](http://www.ngosecure.me)

 +382 69 010 014

 [ivona@visionevent.me](mailto:ivona@visionevent.me)

