



# AKTUALNE KIBERNETSKE GROŽNJE KAKO KRMARITI MED ZAUP LJIVOSTJO ZAPOSLENIH IN PRETKANOSTJO NAPADALCEV?

dr. Aleš Zupan, CISA, CISSP, C|CISO, CGEIT, CRISC, CSX-P | Svetla zvezda, svetovanje, d.o.o.  
David Rozman, MBA, MOS Master, ECDL CTP | B2 IT d.o.o.

26. – 28. september 2022

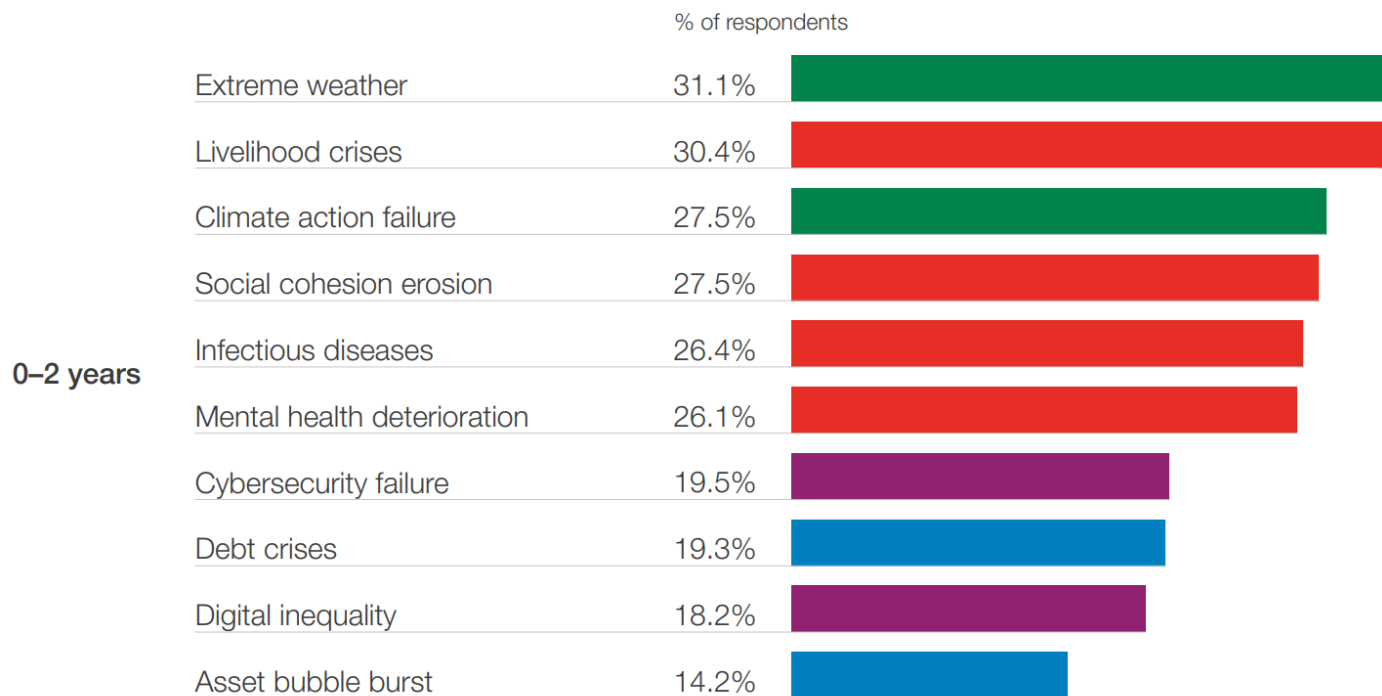
#ntk22

# WEF THE GLOBAL RISKS REPORT

## Global Risks Horizon

When will risks become a critical threat to the world?

■ Economic ■ Environmental ■ Geopolitical ■ Societal ■ Technological



0-2 years

### 435%

porast izsiljevalske programske opreme v letu 2020

### 3 milijonski

primanjkljaj strokovnjakov za kibernetiko varnost

### 95%

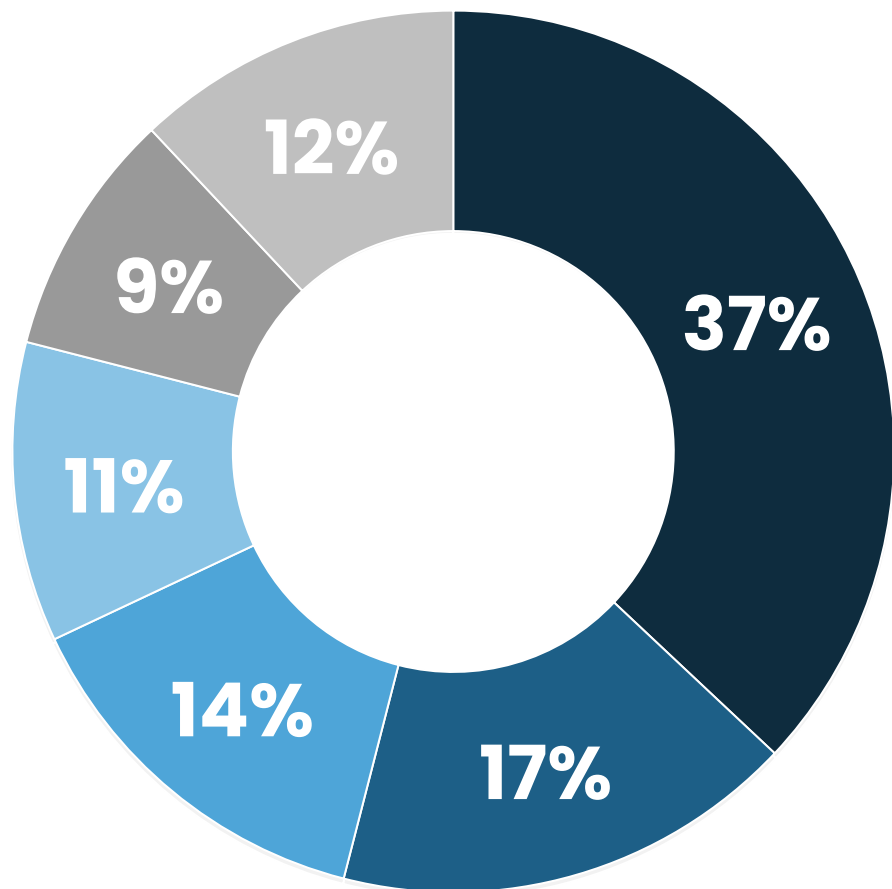
kršitev kibernetike varnosti je posledica človeške napake

World Economic Forum: [The Global Risks Report 2022](#)



KIBERNETSKA NEVARNOST  
JE TUKAJ IN ZDAJ

# VSTOPNE POTI (2021)



Mandiant special report: [M-TRENDS 2022](#)

- IZKORIŠČANJE RANLJIVOSTI  
(»exploits«)
- KOMPROMITIRANJE DOBAVNE VERIGE  
(»supply chain compromise«)
- PREJŠNJA KOMPROMITIRANJA  
(»prior compromise«)
- PHISHING
- KRAJA POVERILNIC  
(»stolen credentials«)
- OSTALO

# VEDNO BOLJ PREFINJENI POSKUSI



**SMISHING**  
SMS phishing

**SOCIALNI INŽENIRING**



**VISHING**  
Glasovni phishing



**MFA FATIGUE**

**ZLORABA TEHNOLOGIJ**

# ZLORABA OT TEHNOLOGIJE, KI LAHKO VODI DO IZGUBE ČLOVEŠKIH ŽIVLJENJ

STAMFORD, Conn., July 21, 2021

**Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans**

Gartner: [povezava](#)

# ZLORABA OT TEHNOLOGIJE, KI LAHKO VODI DO IZGUBE ČLOVEŠKIH ŽIVLJENJ



## Questions and Considerations from Alleged Ukraine Chemical Plant Event



By Joe Slowik 07.16.18

On 11 July 2018, Interfax-Ukraine released a short, somewhat ambiguous, but very concerning press release from the Security Service of Ukraine (SBU) on a thwarted attack on a chlorine production plant. The plant itself appears to produce chlorine for water and wastewater treatment applications. Chlorine is a dangerous chemical, especially in industrial application concentrations, making such an attack extremely alarming.

Before proceeding further, the following statement is necessary: targeting such infrastructure, which could cause immediate harm to personnel onsite or nearby and potential longer-term civilian harm by impacting water treatment capability, represents an indefensible action. Whether applying various permutations of the Laws of War or Just War

# NAJŠIBKEJŠI ČLEN? ČLOVEK

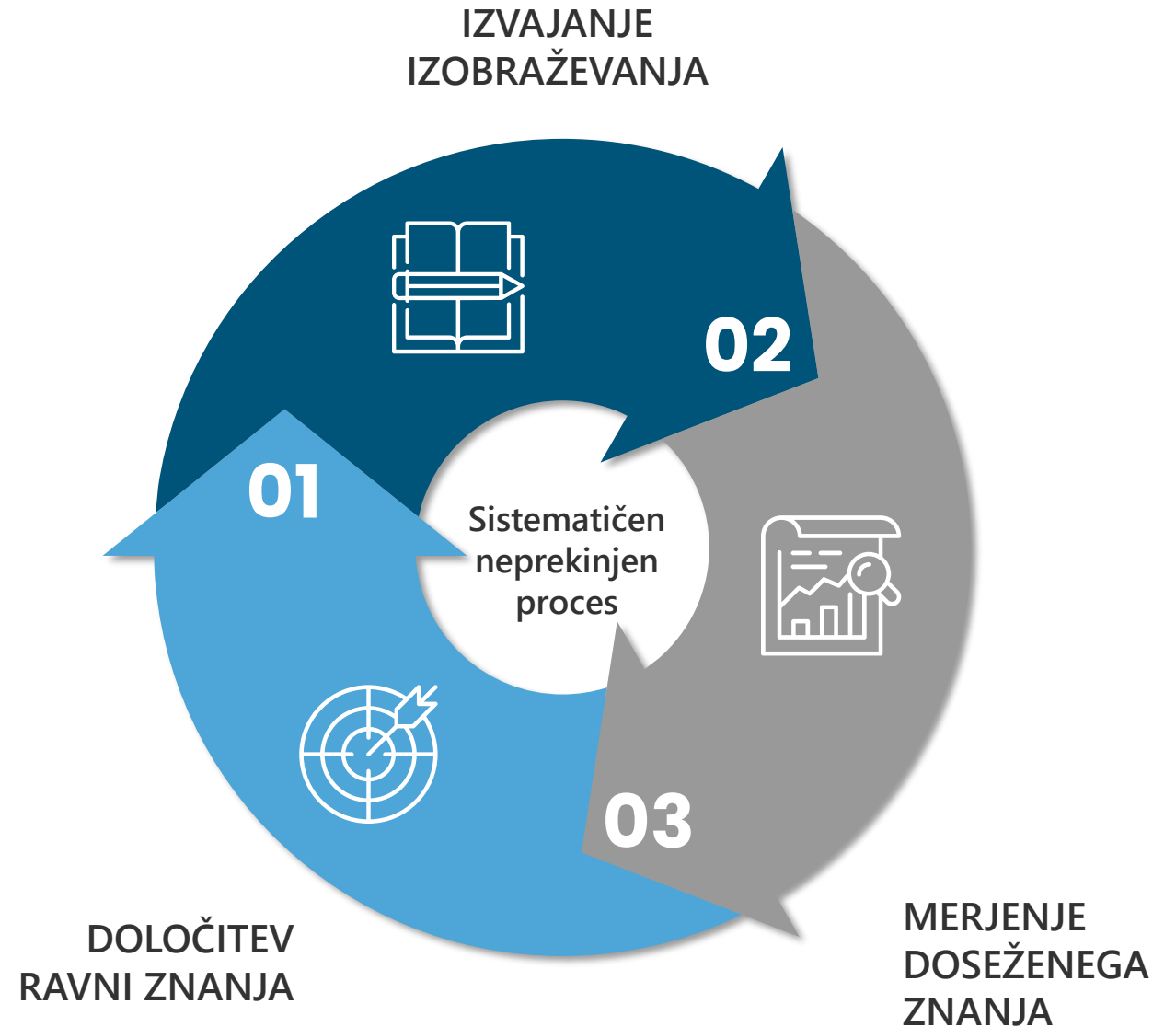
- Dostop do zaupnih podatkov in sistemov.
- Z **neznanjem** ali **malomarnostjo** omogoča uresničitev informacijskih groženj.



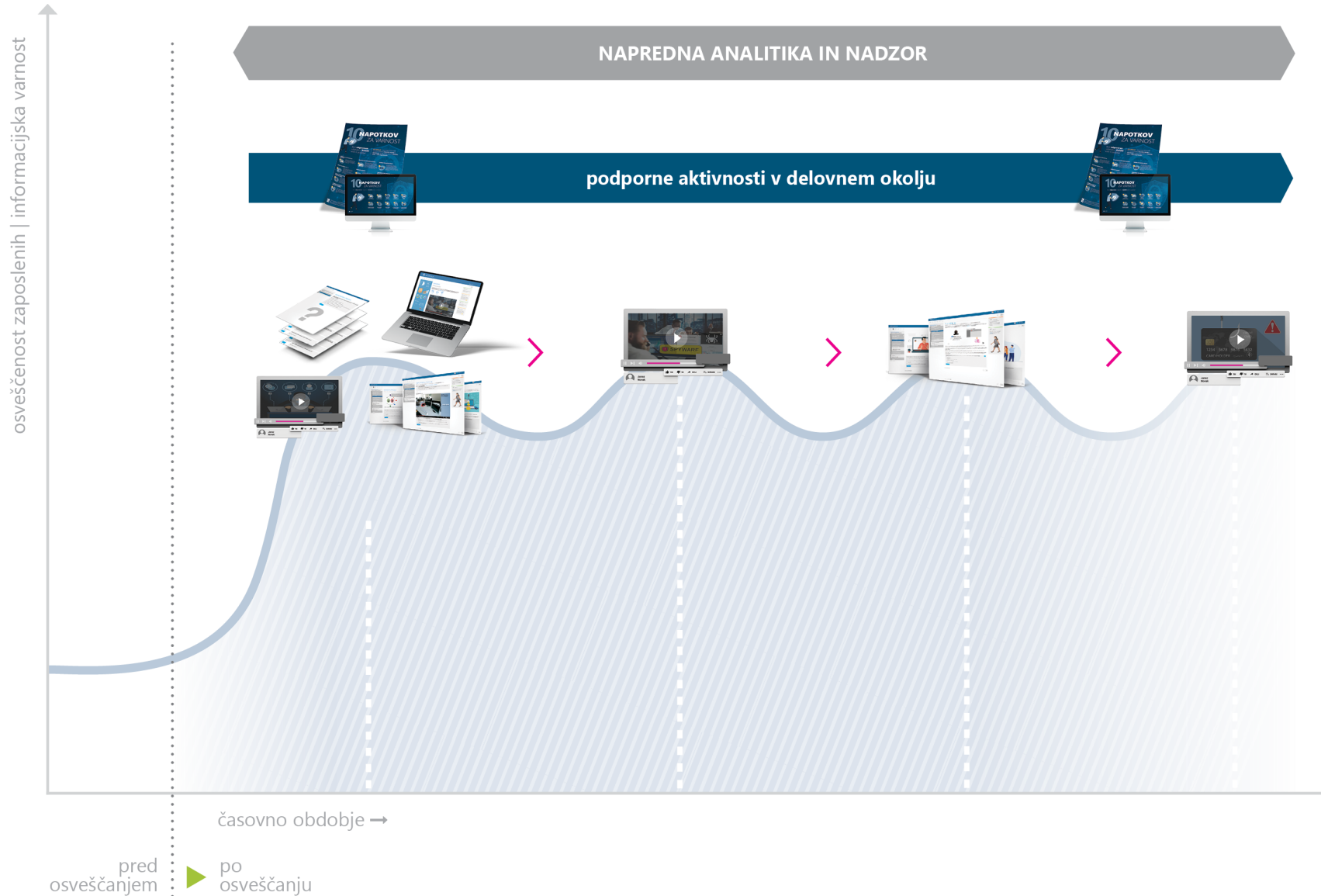


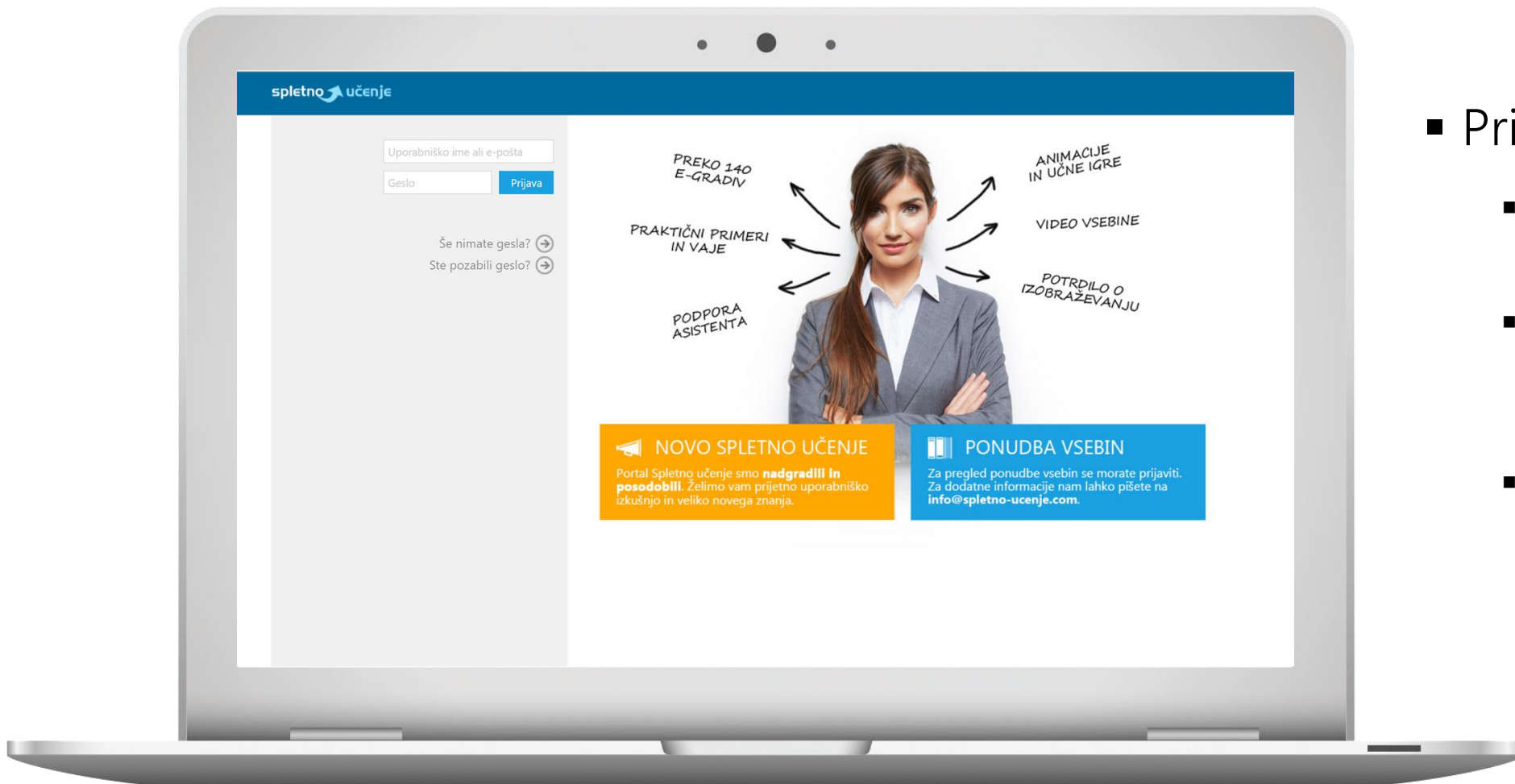
# KAJ LAHKO STORIMO?

- Vpeljava preventivnih programov izobraževanja in ozaveščanja:
  - Načrtujemo jih vnaprej.
  - Vključimo vse zaposlene.
  - Upoštevamo različne komunikacijske kanale.
  - Dolgoročno merimo iste kazalnike (PDCA).



# SISTEMATSKO OZAVEŠČANJE IN IZOBRAŽEVANJE





## Princip valov:

- Standardni moduli usposabljanja
- Specifične vsebine posamezne organizacije
- Osvežitveni in interaktivni moduli usposabljanja

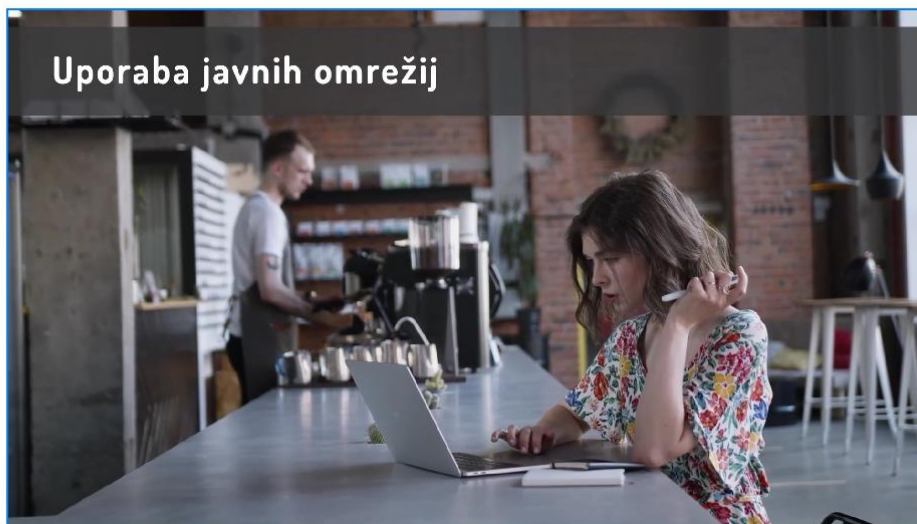


INFORMACIJSKA VARNOST (DODATNO)  
NEVARNOSTI DELA OD DOMA (I.  
DEL)

	Naslovnica
+	Uporaba lastnih naprav
+	Uporaba službene opreme
+	Fizična varnost naprav in informacij
-	Uporaba javnih omrežij
	<b>Uporaba javnih omrežij - video</b>
	Zaključni test

Poišči v e-gradivu

## UPORABA JAVNIH OMREŽIJ - VIDEO



KRATKI VIDEOI

### ■ Princip valov:

- Standardni moduli usposabljanja
- Lastni moduli strank
- Osvežitveni in interaktivni moduli usposabljanja



INFORMACIJSKA VARNOST (DODATNO)  
NEVARNOSTI DELA OD DOMA (I.  
DEL)

-	Naslovnica
+	Uporaba lastnih naprav
-	<b>Uporaba službene opreme</b>
-	Uporaba službene opreme video
+	Fizična varnost naprav in informacij
+	Uporaba javnih omrežij
-	Zaključni test

Poišči v e-gradivu

## UPORABA SLUŽBENE OPREME

▶ **Ana želi na služben telefon, na katerem se nahajajo strogo zaupni službeni podatki, namestiti priljubljeno mobilno aplikacijo Facebook.** **NAPREJ**

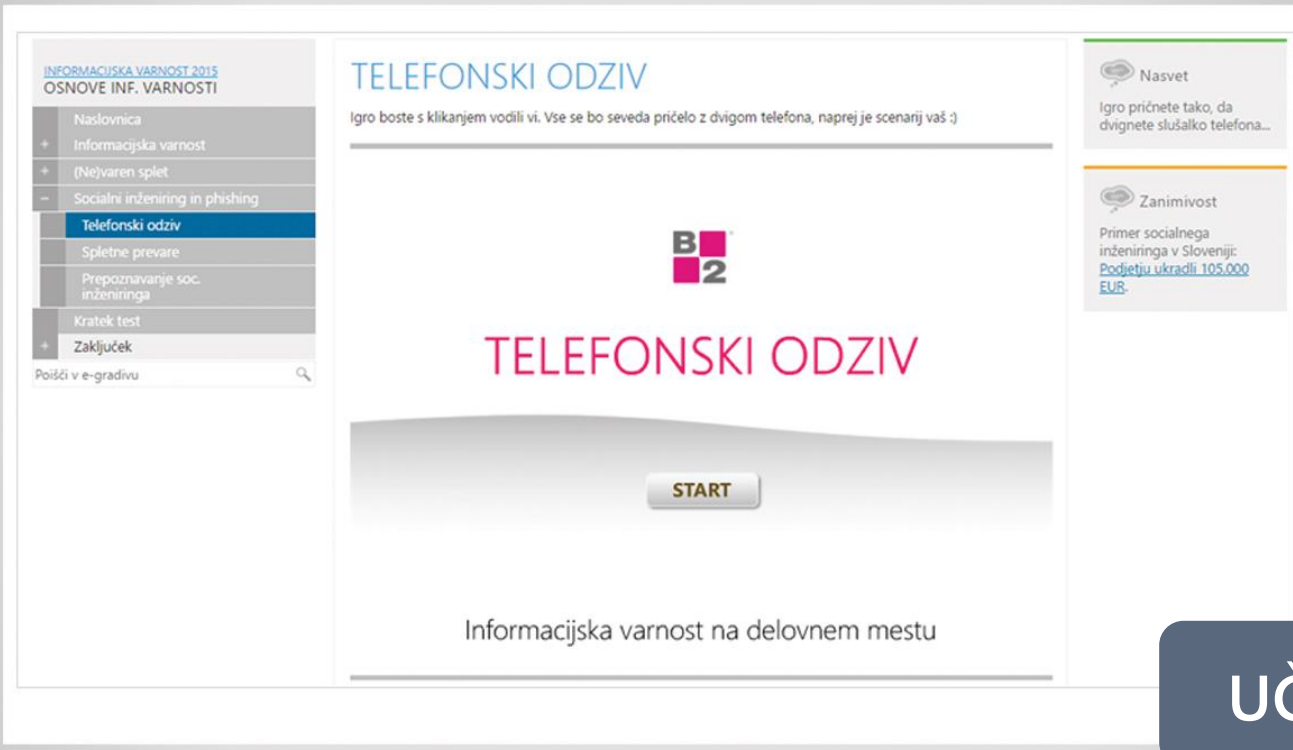


ANIMACIJE

## Princip valov:

- Standardni moduli usposabljanja
- Lastni moduli strank
- Osvežitveni in interaktivni moduli usposabljanja





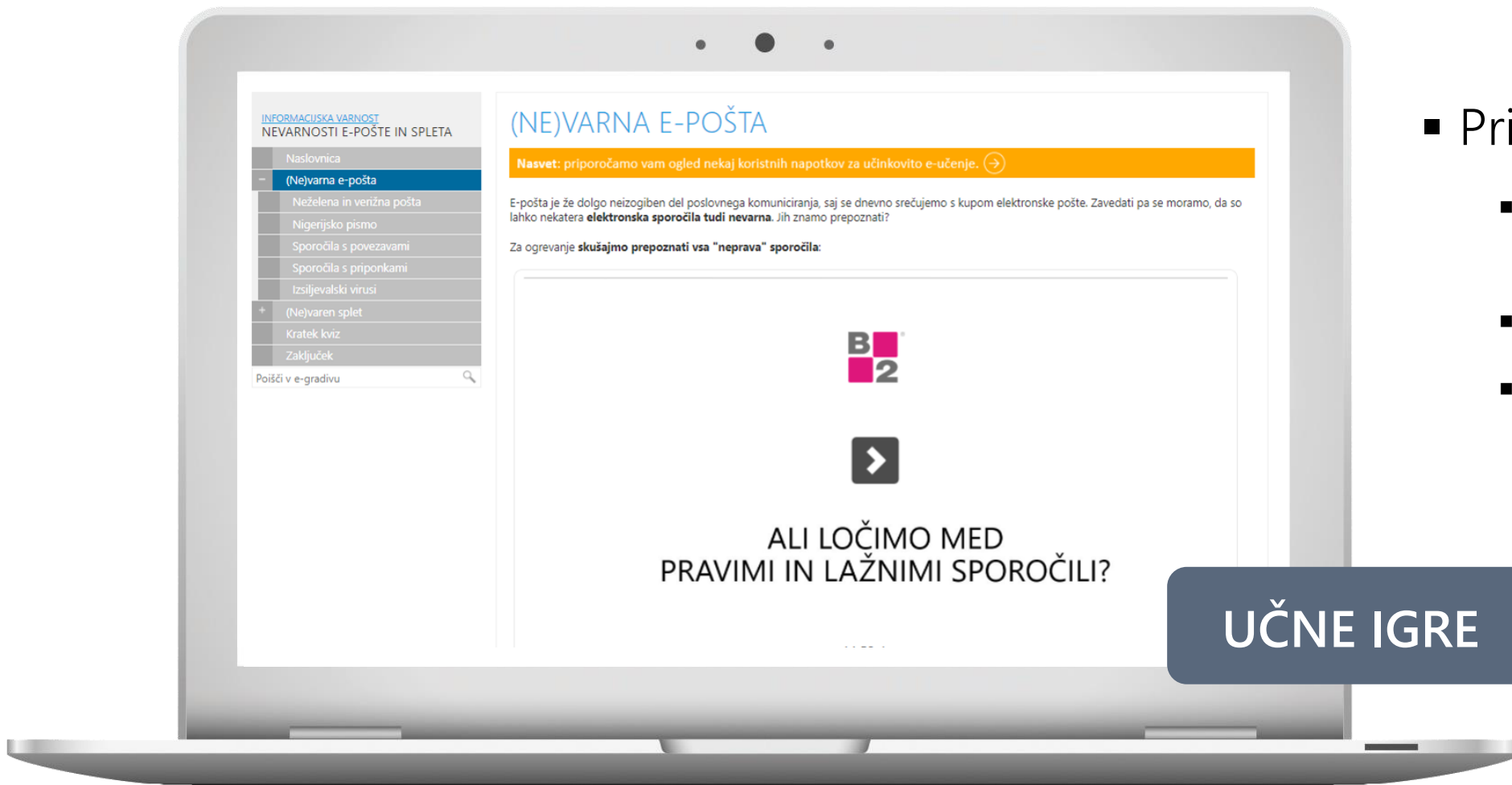
## UČNE IGRE

- Princip valov:
  - Standardni moduli usposabljanja
  - Lastni moduli strank
  - Osvežitveni in interaktivni moduli usposabljanja

osveženost zaposlenih



#ntk22



## ■ Princip valov:

- Standardni moduli usposabljanja
- Lastni moduli strank
- Osvežitveni in interaktivni moduli usposabljanja



**INFORMACIJSKA VARNOST  
GESLA IN DOSTOPI**

- Naslovnica
- + Dostop do informacijskih sistemov
- + Močna gesla
- Varovanje gesel
- Metode za pridobivanje gesel**
- Nivoji zaščite
- Kratek kviz
- Zaključek

Poišči v e-gradivu

## METODE ZA PRIDOBIVANJE GESEL

Spletni kriminalci so venomer na preži in skušajo pridobiti gesla predvsem tistih, ki so **slabo izobraženi** glede internetne varnosti. Zato je pomembno osnovno poznavanje metod za pridobivanje oziroma prestrezanje gesel, ki jih uporabljajo hekerji. V osnovi ločimo **dva načina pridobivanja gesel**:

**Socialni inženiring** **Tehnične metode** **Primer razbijanja gesla**

V skrajnih primerih se **hekerji** lotijo razbijanja gesel tako, da **preverjajo vse možne kombinacije** črk in števil (brute-force metoda). Iz tega vidika je zelo pomembno, da je **naše geslo kvalitetno**, kar pomeni, da je **dovolj dolgo** ter da je **sestavljeno iz raznolikih znakov** (male in velike črke, števila, posebni znaki).

Za grob občutek, koliko časa potrebuje heker za razbijanje gesla, v spodnji tabeli določite elemente vašega gesla ter kliknite gumb "Razbij geslo".

Koliko časa potrebuje 'heker', da ugotovi vaše geslo?

Število znakov v geslu: 4 5 6 7 8 9 10 11 12

Nabor znakov v geslu: male črke male in velike črke črke in številke črke, številke in znaki

Razbij geslo

Različnih variacij gesel:  
Ocenjeni čas:

**Nasvet**  
Dobro geslo ima vsaj 12 znakov, male in velike črke, številke (npr. Moj3Pes1kec).

**Opozorilo**  
Ne vpisujte gesel na straneh, za katere niste prepričani, da so verodostojne.

**Zanimivost**  
Zlikovci ponavadi izkoristijo aktualne dogodke za napad na uporabnike. Tako se je ob pričetku pandemije korona virusa pojavilo **lažno sporočilo NIJZ** glede nabave zaščitne opreme, ki je vsebovalo priponko z virusom.

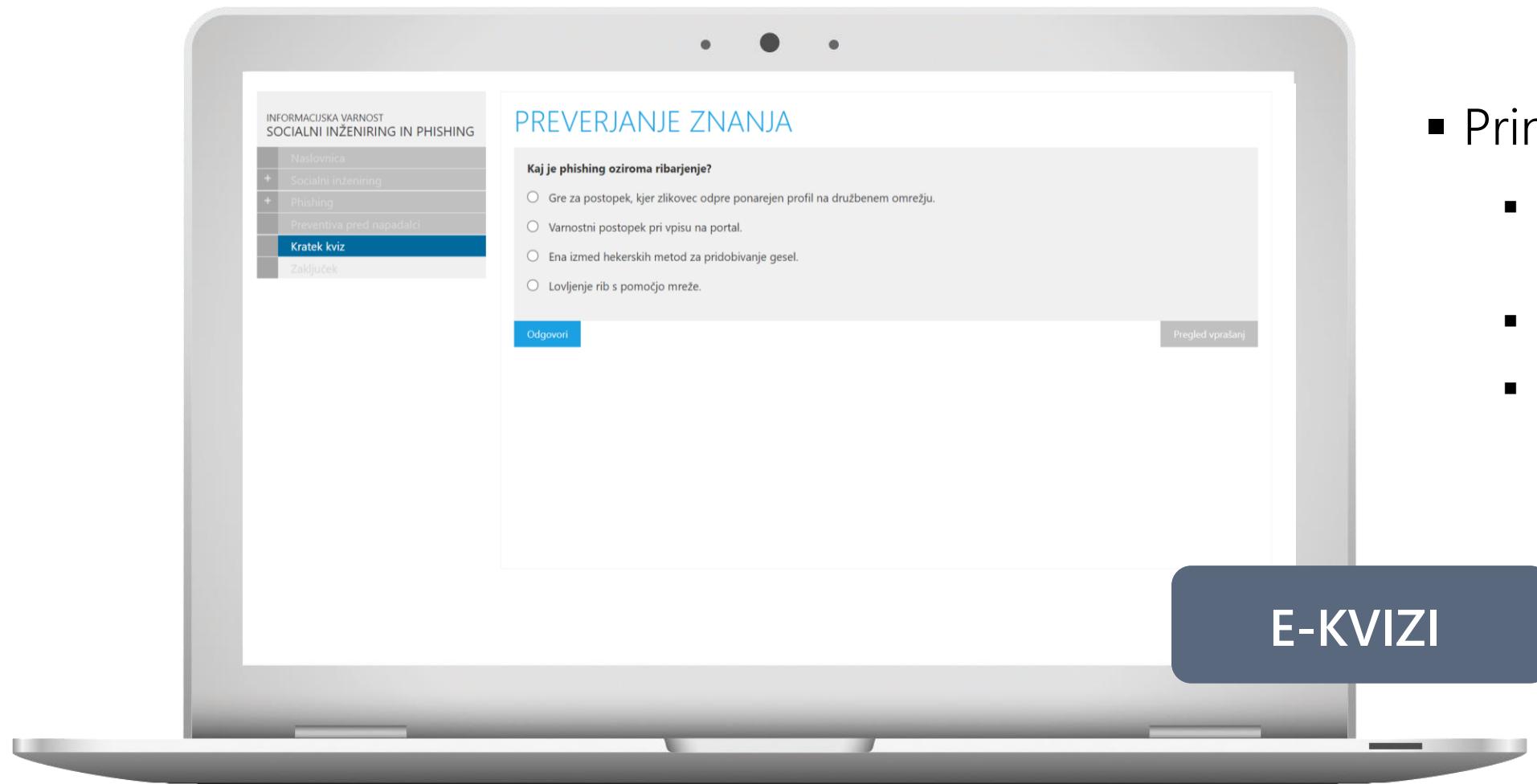
UČNE IGRE

## Princip valov:

- Standardni moduli usposabljanja
- Lastni moduli strank
- Osvežitveni in interaktivni moduli usposabljanja







## E-KVIZI

- Princip valov:
  - Standardni moduli usposabljanja
  - Lastni moduli strank
  - Osvežitveni in interaktivni moduli usposabljanja



# STANDARDNI MODULI

Osnove informacijske varnosti

Gesla in dostopi

Nevarnosti e-pošte in spleta

Socialni inženiring in phishing

Mobilna izpostavljenost

Varnost podatkov in naprav



# OSVEŽITVENI MODULI

- Periodično obnavljanje znanja na zabaven in poučen način iz različnih tematik:

Phishing

Preprečimo socialni inženiring

Varno kreiranje gesel

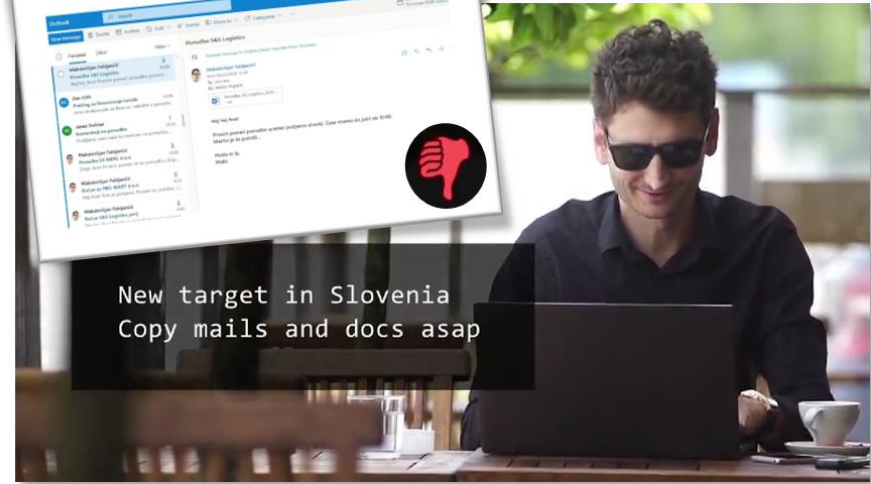
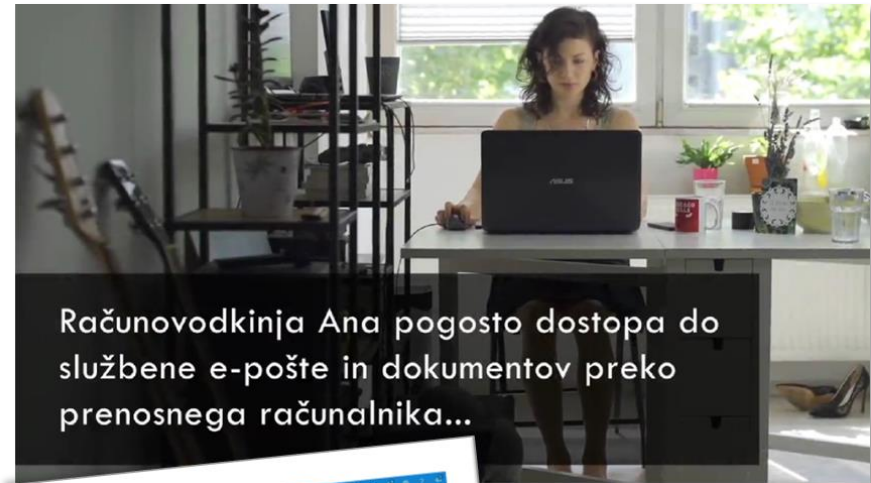
Nevarnosti dela od doma

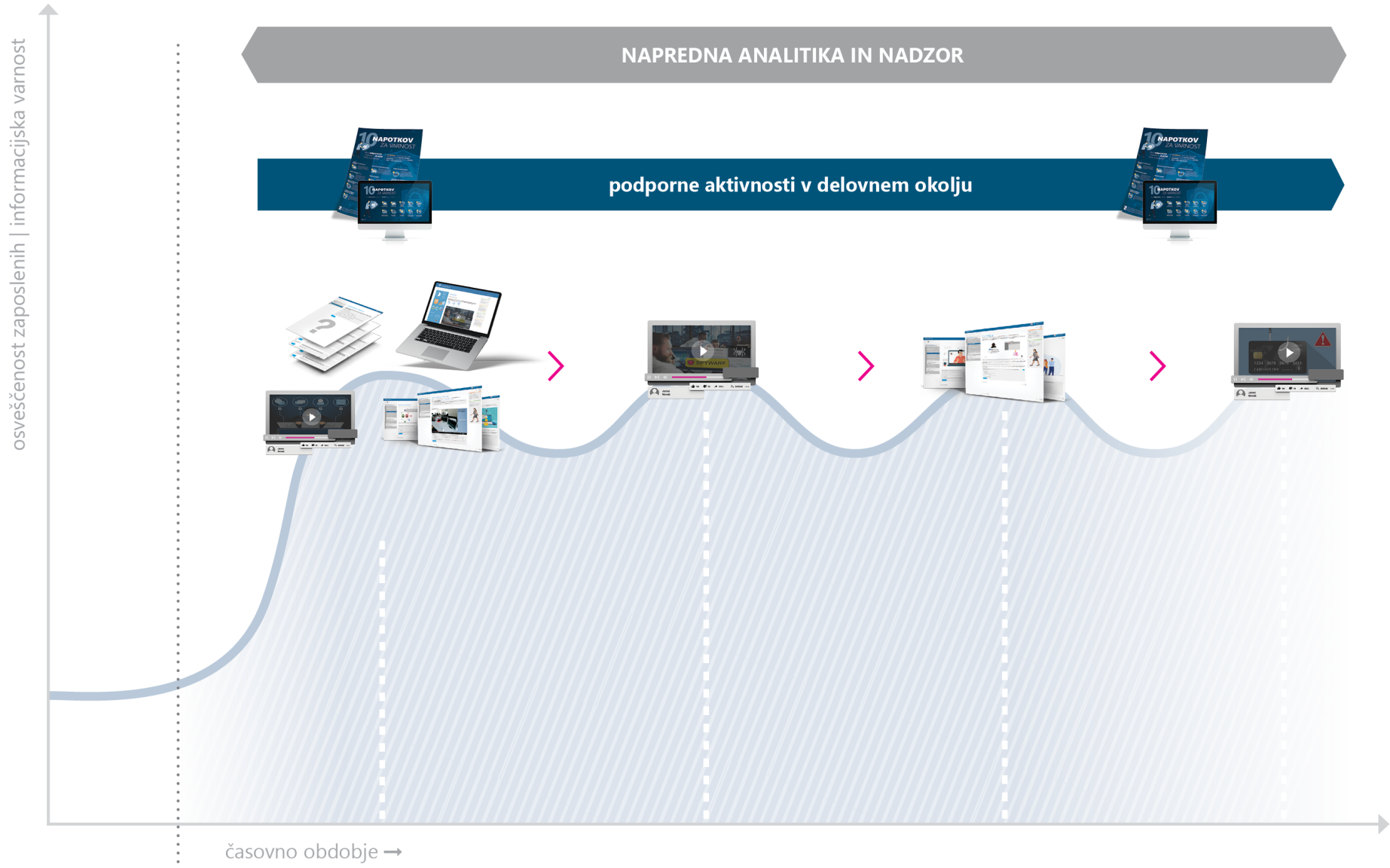
Mobilni spyware



# OSVEŽITVENI MODULI

- Periodično obnavljanje znanja na zabaven in poučen način iz različnih tematik:
- Inovativni pristopi
  - Ključki pred vhomom
  - Šotor pred jedilnico / učne igre in kvizi
- Bite-size learning





pred osveščanjem

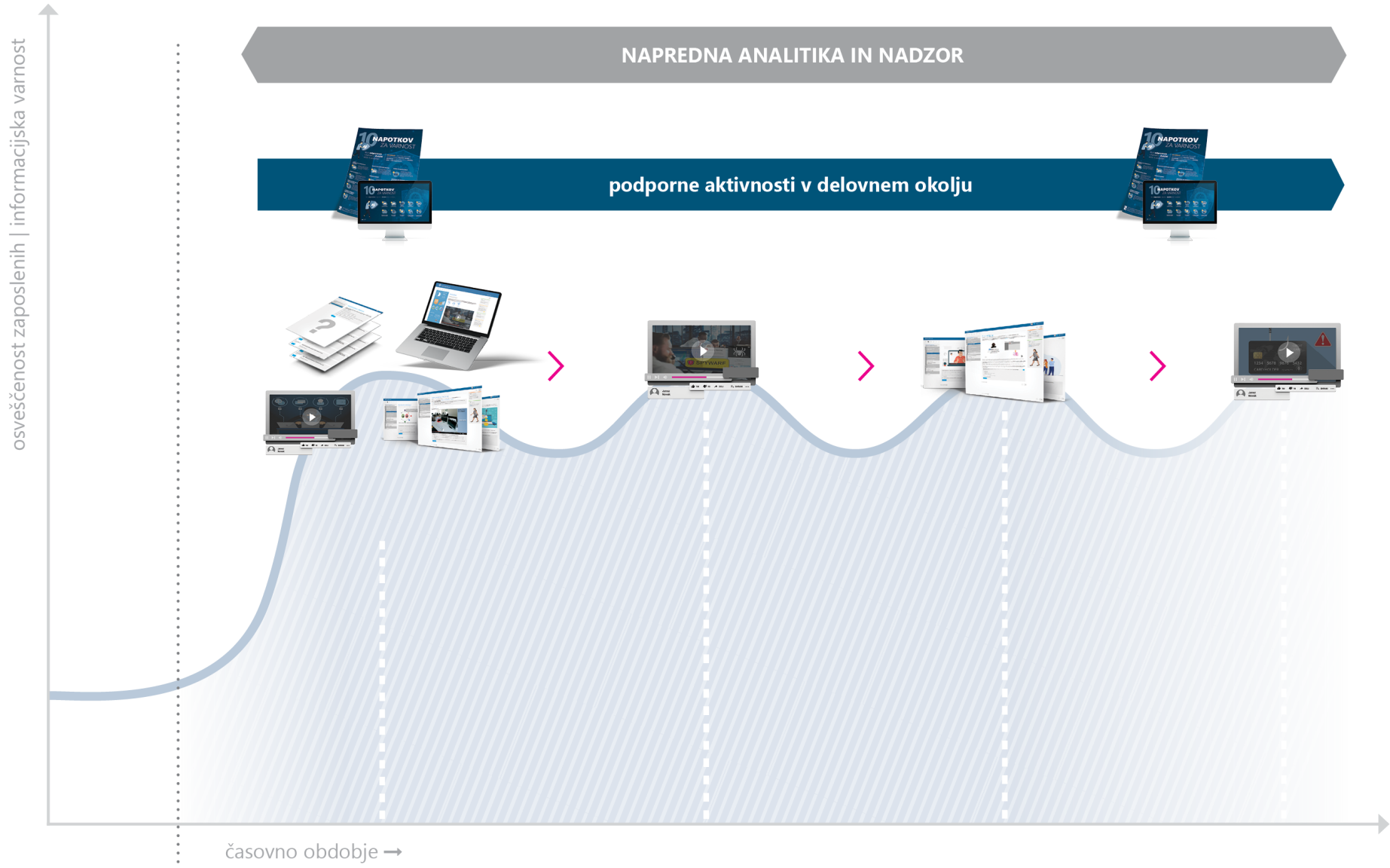
▶ po osveščanju

# NAPREDNA ANALITIKA IN NADZOR



- Omogoča hiter in pregleden nadzor nad razvojem zaposlenih in učnimi aktivnostmi.
- Preprosta priprava poročil.
- Za potrebe spodbujanja in motiviranja zaposlenih.





## podporne aktivnosti v delovnem okolju



- Podporne aktivnosti:
  - ohranjevalniki zaslona
  - plakati
  - certifikati
  - novičke

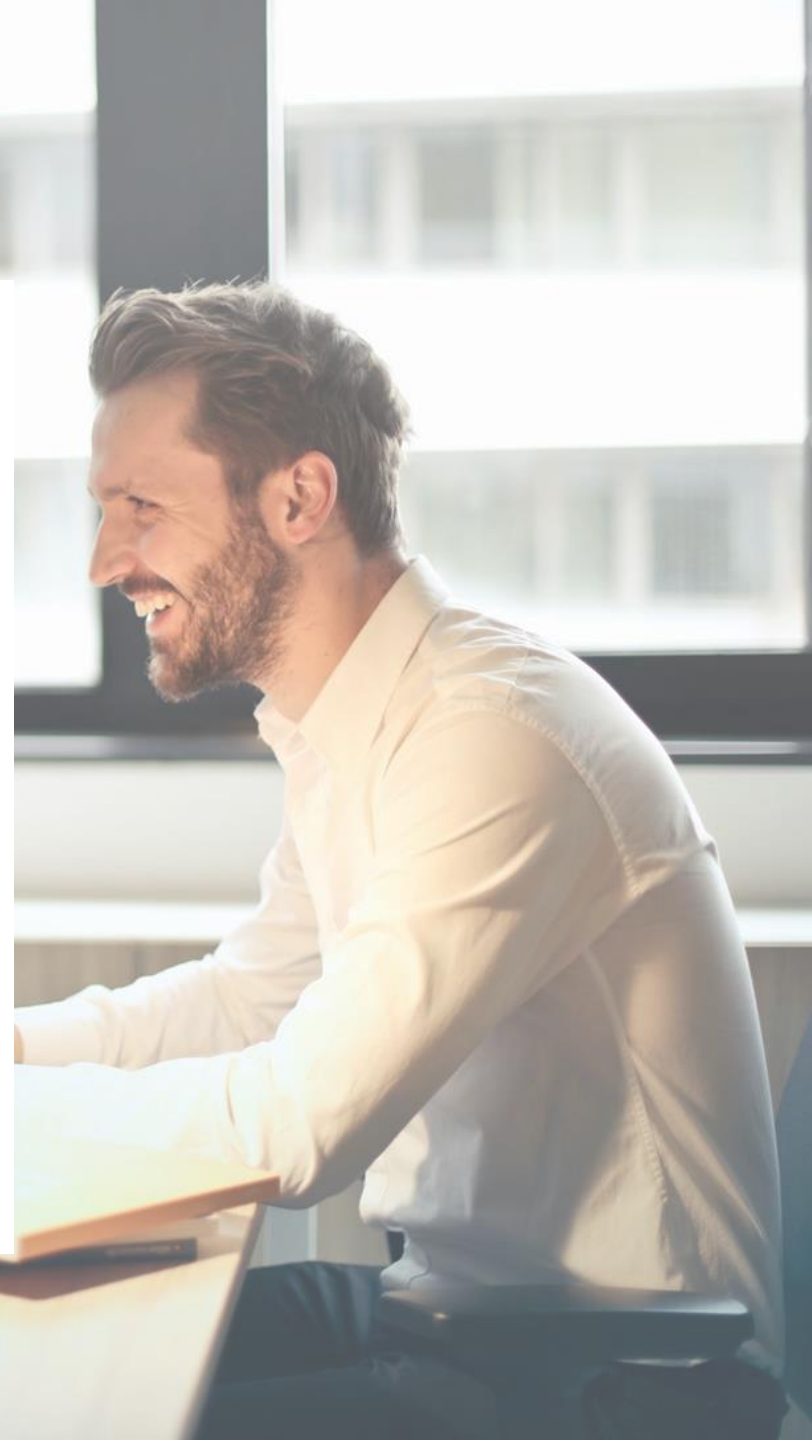
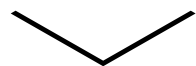


# VTISI NAŠIH STRANK

“

Navdušil nas je online program usposabljanja podjetja B2 IT, saj je obsegal **ključene vsebine**, ki jih mora poznati sleherni zaposleni.

”

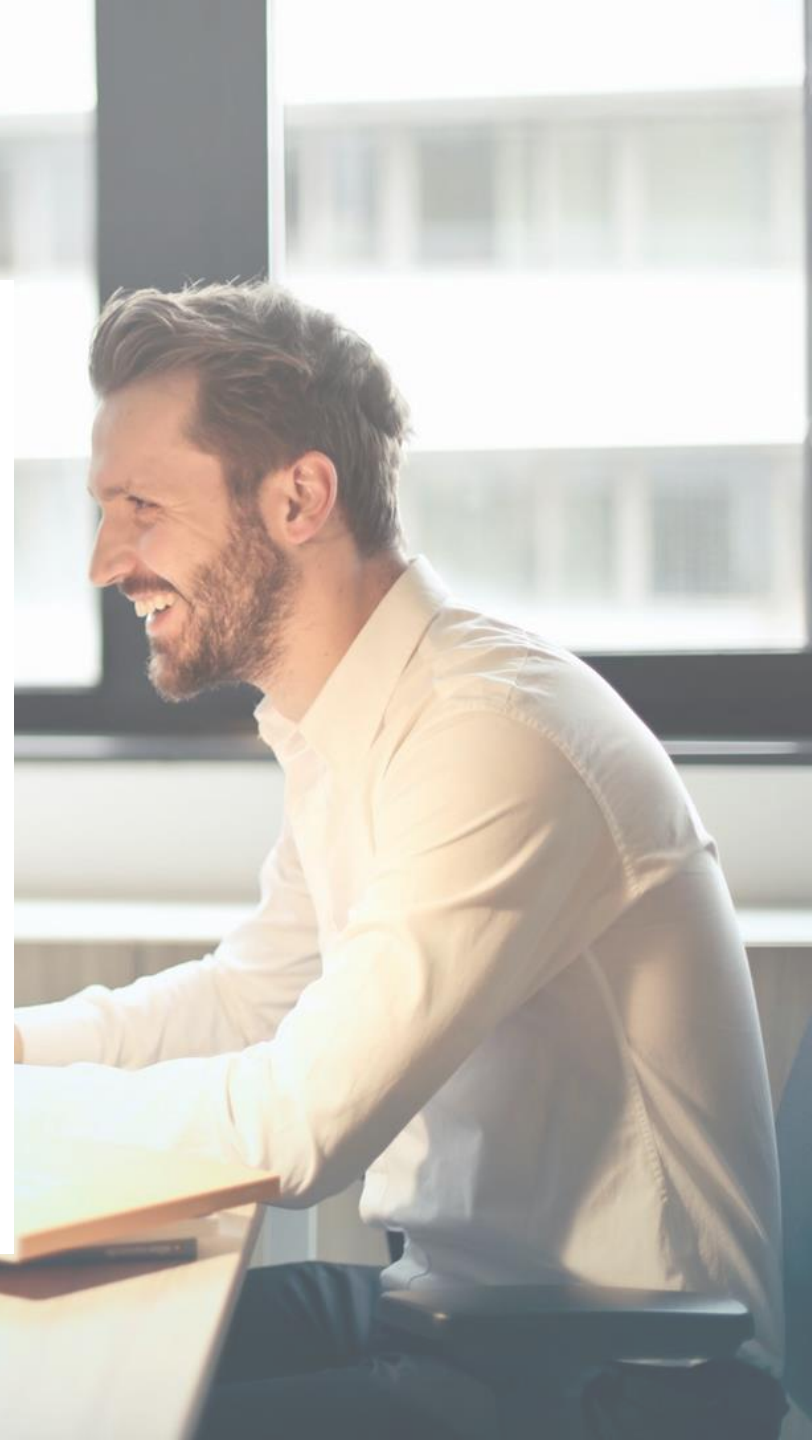
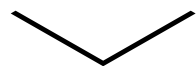


# VTISI NAŠIH STRANK

“

Izkazalo se je, da je e-izobraževanje za nas zelo primerno, zaradi **lokacijske razpršenosti** naših sodelavcev. Pomembno vlogo igra tudi **čas**, ki so si ga udeleženci **razporedili sami**, glede na njihove zadolžitve.

”

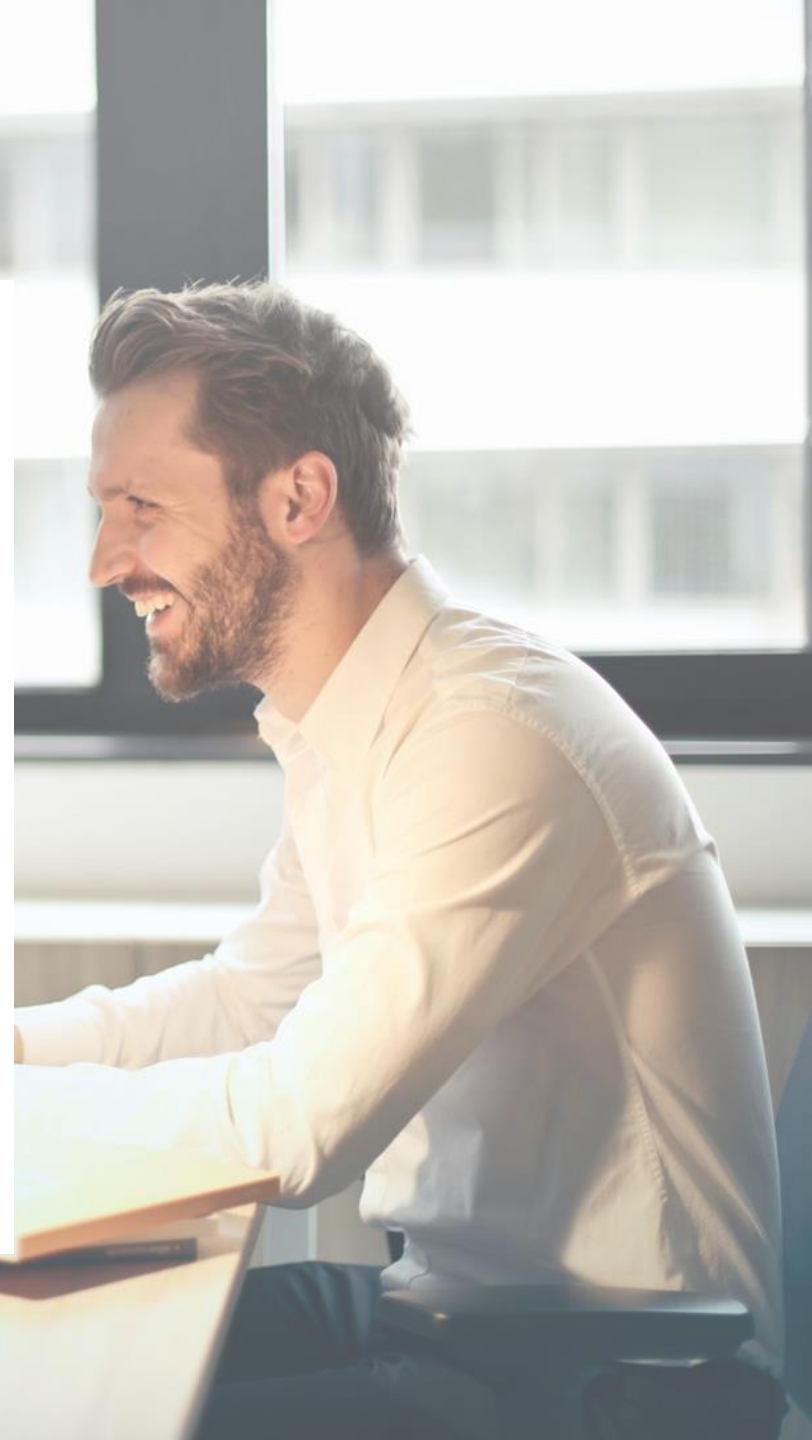
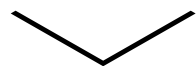


# VTISI NAŠIH STRANK

“

Odlična lastnost spletne učilnice je, da **mentor lahko spremlja napredovanje** udeležencev, **končno poročilo** pa prikaže: **čas**, ki so ga posamezni zaposleni porabili za učenje, rezultate učenja in **rezultate ankete** o izvedenem izobraževanju, gradivu, željah in predlogih udeležencev.

”

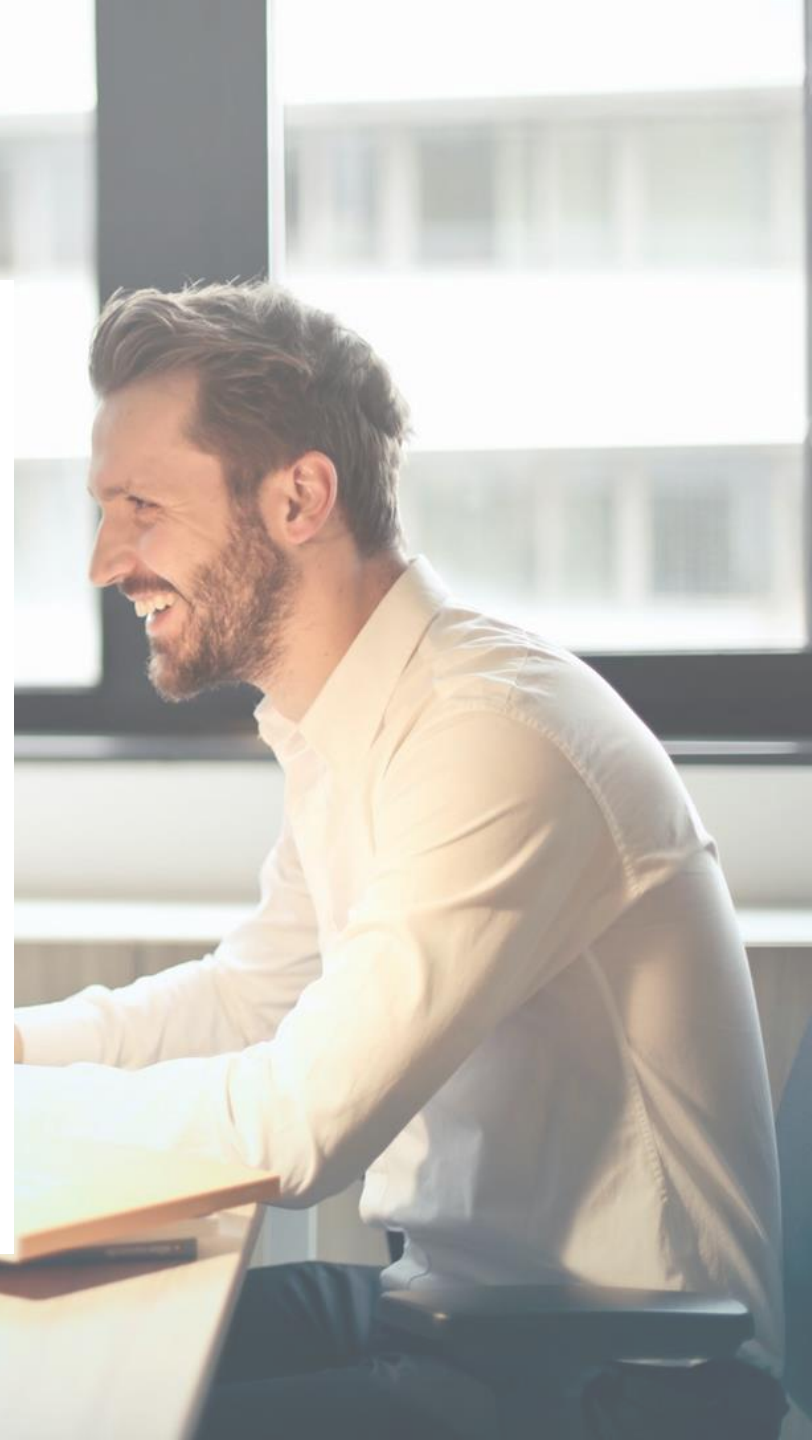
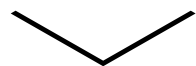


# VTISI NAŠIH STRANK

“

Dodano vrednost nam predstavljajo **osvežitveni moduli**, saj verjamemo, da moramo skrbeti za redno osveščanje svojih zaposlenih iz aktualnih kibernetских napadov in s sodelovanjem na tem področju z B2 IT tudi v prihodnje nadaljujemo.

”

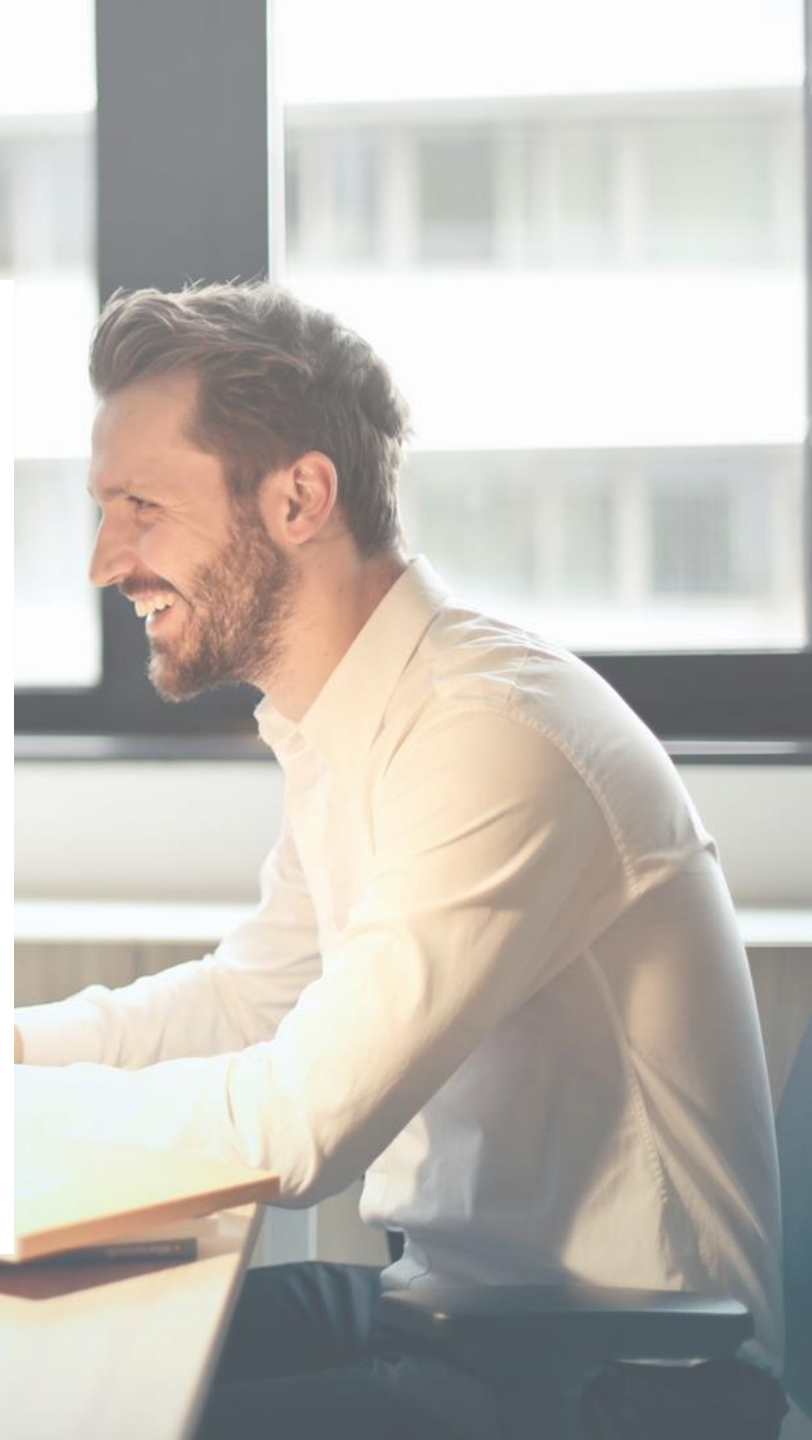
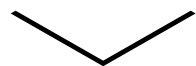


# VTISI NAŠIH STRANK

“

Priznam, da sem bil »jezen« po napovedi službe za informatike, da se bomo morali e-izobraževati. Vtisi zdaj, po opravljenem izobraževanju, pa so povsem drugačni. **HVALA - sem bogatejši in pametnejši** se za tisti del, ki me do sedaj ni preveč zanimal, brigal, sedaj pa..... **...bom le bolj previden in pazljiv.**

”



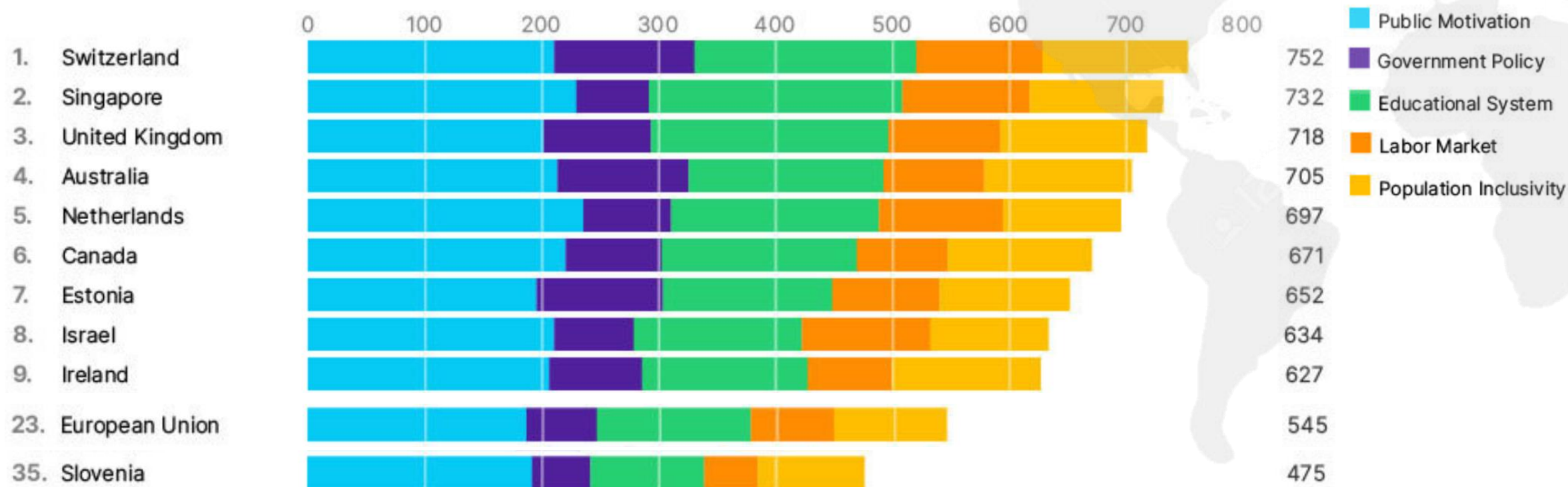
# ZAKLJUČEK

CYBERSECURITY

**After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk**

## Cyber Risk Literacy And Education Index Rankings

Five major drivers constitute the Index underpinned by key pillars related to population cyber risk literacy and education



# INT KONFE RENCA 2022

Inovativni pristopi,  
predvsem pa sistematika,  
odzivnost, avtomatizacija  
in analitika.



"MAYBE WE SHOULD TRY A DIFFERENT  
SECURITY APPROACH THIS YEAR."