SPLOŠNI NEFORMALNI IZOBRAŽEVALNI PROGRAM

KO KLIK NI VEČ NEDOLŽEN: KIBERNETSKA TVEGANJA V IZOBRAŽEVANJU ODRASLIH

Pripravila: Zveza ljudskih univerz Slovenije

April, 2026

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VZGOJO IN IZOBRAŽEVANJE

Vsebina

1. Ime programa

Ko klik ni več nedolžen: kibernetska tveganja v izobraževanju odraslih

2. Vrsta programa

Program splošnega neformalnega izobraževanja odraslih.

Program je namenjen izboljšanju splošne izobraženosti odraslih ter krepitvi digitalnih, varnostnih in odgovornih ravnanj v delovnem in vsakdanjem digitalnem okolju.

3. Utemeljitev in namen programa

Zaposleni v izobraževanju odraslih se pri vsakodnevnem delu srečujejo z elektronsko pošto, spletnimi storitvami, deljenjem dokumentov, uporabo informacijskih sistemov, obdelavo osebnih podatkov in komunikacijo na daljavo. Zaradi tega so izpostavljeni različnim kibernetskim tveganjem, kot so phishing, zlonamerna programska oprema, kraja identitete, neustrezna raba naprav, nepravilno ravnanje z osebnimi podatki in šibki odzivi ob incidentih. Izhodišča naloge posebej izpostavljajo, da so zaposleni pogosto najbolj ranljiv del organizacije in da lahko pomanjkanje znanja povzroči krajo podatkov, finančno škodo, prekinitev delovanja storitev in izgubo zaupanja uporabnikov.

Namen programa je okrepiti varno, odgovorno in kritično ravnanje zaposlenih v organizacijah za izobraževanje odraslih v digitalnem okolju. Program udeležencem omogoča, da:

- razumejo osnovna načela kibernetske varnosti,
- prepoznajo najpogostejše oblike digitalnih groženj,
- varneje uporabljajo naprave, omrežja in digitalna orodja,
- ustrezno ravnajo z osebnimi podatki v skladu z delovnim kontekstom,
- znajo ob incidentu ukrepati mirno, pravočasno in po dogovorjenih poteh,
- prenašajo pridobljeno znanje v svoje delovno okolje.

Program je zasnovan praktično, problemsko in andragoško, s poudarkom na prenosu znanja v prakso, reševanju primerov iz delovnega okolja, mentorski podpori, obrnjeni učni zasnovi, sprotnem preverjanju razumevanja in učenju med vrstniki.

4. Ciljna skupina

Ciljna skupina so odrasli, zaposleni v organizacijah za izobraževanje odraslih, zlasti:

- organizatorji izobraževanja odraslih,
- učitelji in drugi izobraževalci odraslih,
- strokovni delavci,
- administrativni delavci,
- vodstveni kader,
- drugi zaposleni, ki pri delu uporabljajo informacijsko-komunikacijsko tehnologijo ali obdelujejo osebne podatke.

Program je primarno namenjen zaposlenim v izobraževanju odraslih. Pri zasnovi programa se upošteva, da imajo udeleženci različno predznanje, različne delovne vloge in različno stopnjo digitalne samozavesti. Zato program omogoča diferenciranje aktivnosti glede na predznanje in delovno vlogo.

5. Vključitveni pogoji

Za vključitev v program ni formalnih izobrazbenih ali drugih pogojev.

Priporočljivo je:

- da je udeleženec zaposlen ali aktiven na področju izobraževanja odraslih oziroma podpornih dejavnosti,
- da uporablja računalnik, elektronsko pošto ali pametni telefon,
- da ima osnovno uporabniško izkušnjo z delom v digitalnem okolju.

6. Temeljne zmožnosti, ki jih program razvija

Program smiselno razvija predvsem te temeljne zmožnosti:

- digitalno zmožnost,
- zmožnost učenja in samouravnavanja učenja,
- osebnostne in socialne zmožnosti,
- državljanske zmožnosti,
- sporazumevalne zmožnosti.

Program smiselno vključuje tudi temeljne spretnosti:

- branje in razumevanje digitalnih sporočil, opozoril, navodil in pravilnikov,
- pisanje kratkih strokovnih odzivov, prijav incidenta in varnostnih obvestil,
- osnovno računanje in presojanje pri varnostnih nastavitvah, časovnih rokih, stopnji tveganja in verjetnosti,
- digitalne spretnosti pri varni rabi naprav, računov, aplikacij in omrežij.

7. Splošni cilji programa

Udeleženec v programu:

- razume pomen kibernetske varnosti v delovanju organizacije za izobraževanje odraslih;
- prepozna najpogostejše digitalne grožnje in tveganja;
- razvija odgovoren odnos do varovanja podatkov, naprav, dostopov in digitalne komunikacije;
- uporablja osnovne varnostne prakse pri delu;
- zna ravnati ob zaznavi varnostnega incidenta;
- razume osnovne obveznosti pri ravnanju z osebnimi podatki v delovnem okolju;
- uporablja priporočila in gradiva SI-CERT kot podporo pri vsakodnevnem delu;
- reflektira lastne vrzeli v znanju ter pripravi osebni načrt izboljšanja varnostnih ravnanj.

8. Operativni cilji programa

Po zaključku programa udeleženec:

- opiše osnovne pojme s področja kibernetske varnosti;
- razlikuje med najpogostejšimi vrstami napadov;
- prepozna sumljivo elektronsko sporočilo, povezavo ali priponko;
- oblikuje in uporablja močnejša gesla ter razume pomen večfaktorske avtentikacije;
- varneje uporablja službeni računalnik, mobilno napravo in omrežja;
- pojasni osnovne korake ukrepanja ob incidentu;
- pravilno odreagira ob sumu na phishing, izgubo naprave ali nepooblaščen dostop;
- pozna osnovna načela varnega ravnanja z osebnimi podatki;
- presodi primernost ravnanja v konkretnih primerih iz prakse;
- pripravi predlog ene izboljšave za svoje delovno okolje.

9. Trajanje programa

Skupni obseg programa je **20 pedagoških ur**.

Program se izvede v **štirih srečanjih po 5 pedagoških ur**

10. Struktura in vsebinska zasnova programa

Za neformalni program je najprimernejša **enovita zasnova po vsebinskih sklopih**, ker je program kratek in izrazito praktično usmerjen.

Pregled vsebinskih sklopov

Vsebinski sklop	Obseg
1. Uvod v kibernetsko varnost	2 uri
2. Najpogostejše grožnje	4 ure
3. Fizična in dostopovna varnost	2 uri
4. Varno delo z napravami in omrežji	2 uri
5. Varnostni incidenti in odzivi	2 uri
6. Delavnica: simulacija vdora prek klika na e-sporočilo	2 uri
7. ZVOP-2 in varstvo osebnih podatkov	4 ure
8. Delavnica: ravnanje z osebnimi podatki v praksi	2 uri
Skupaj	**20 ur**

11. Katalog znanja oziroma vsebina programa

Vsebinski sklop 1: Uvod v kibernetsko varnost

Obseg: 2 pedagoški uri

Priporočene vsebine:

- kaj je kibernetska varnost,
- zakaj je pomembna,
- digitalne grožnje danes,
- vloga posameznika pri zagotavljanju varnosti.

Znanje:
Udeleženec:

- pojasni pojem kibernetske varnosti;
- razume povezavo med ravnanjem posameznika in varnostjo organizacije;
- opiše osnovne vrste tveganj v digitalnem okolju.

Spretnosti:
Udeleženec:

- prepozna varnostno občutljive situacije pri svojem delu;
- poimenuje lastna tveganja v delovnem procesu;
- oblikuje seznam svojih vsakodnevnih digitalnih navad in jih kritično ovrednoti.

Vsebinski sklop 2: Najpogostejše grožnje

Obseg: 4 pedagoške ure

Priporočene vsebine:

- virusi in zlonamerna programska oprema,
- phishing,
- hekerski vdori,
- trojanci,
- ransomware,
- kraja identitete.

Znanje:
Udeleženec:

- razlikuje med posameznimi vrstami digitalnih groženj;
- razume značilne znake phishing napadov;
- pozna osnovne posledice okužbe sistema ali zlorabe dostopa.

Spretnosti:
Udeleženec:

- analizira elektronsko sporočilo z vidika tveganja;
- prepozna sumljive povezave, priponke in zahteve po razkritju podatkov;
- presodi verodostojnost pošiljatelja in vsebine.

Vsebinski sklop 3: Fizična in dostopovna varnost

Obseg: 2 pedagoški uri

Priporočene vsebine:

- politika gesel,
- oblikovanje močnih gesel,
- večfaktorska avtentikacija,
- zaklepanje naprav in prostorov.

Znanje:
Udeleženec:

- razume pomen močnih gesel in MFA;
- pozna osnovna načela fizične zaščite dostopa do naprav in dokumentacije.

Spretnosti:
Udeleženec:

- oblikuje primer varnejšega gesla oziroma geselne strategije;
- nastavi osnovne zaščitne mehanizme na napravi;
- uporablja dobre navade pri zaklepanju naprav in delovnega prostora.

Vsebinski sklop 4: Varno delo z napravami in omrežji

Obseg: 2 pedagoški uri

Priporočene vsebine:

- varna raba računalnikov in mobilnih naprav,
- javna Wi-Fi omrežja,
- posodabljanje sistemov in aplikacij,
- protivirusna zaščita in požarni zid.

Znanje:
Udeleženec:

- pojasni pomen posodobitev in osnovne zaščite naprav;
- razume tveganja uporabe nezavarovanih omrežij;
- pozna osnovna priporočila za delo na daljavo.

Spretnosti:
Udeleženec:

- preveri osnovne varnostne nastavitve naprave;
- presodi primernost uporabe določenega omrežja;
- pripravi kontrolni seznam za varnejše delo od doma ali na terenu.

Vsebinski sklop 5: Varnostni incidenti in odzivi

Obseg: 2 pedagoški uri

Priporočene vsebine:

- politika informacijske varnosti v zavodu,
- kaj je varnostni incident,
- osnovni koraki ukrepanja,
- komu in kako poročamo.

Znanje:
Udeleženec:

- opredeli, kaj šteje za varnostni incident;
- razume pomen hitrega in pravilnega notranjega obveščanja;
- pozna osnovne odzivne korake v organizaciji.

Spretnosti:
Udeleženec:

- opiše ustrezen prvi odziv ob incidentu;
- izpolni osnutek prijave incidenta;
- razlikuje med tem, kaj sme narediti sam in kdaj mora vključiti odgovorno osebo ali IT podporo.

Vsebinski sklop 6: Delavnica: simulacija vdora prek klika na e-sporočilo

Obseg: 2 pedagoški uri

Priporočene vsebine:

- analiza scenarija,
- prepoznavanje znakov napada,
- odločanje o ustreznih odzivih.

Znanje:
Udeleženec:

- razume zaporedje dogodkov pri tipičnem phishing napadu;
- razloži posledice neustreznega odziva.

Spretnosti:
Udeleženec:

- v simuliranem primeru prepozna tveganje;
- sprejme utemeljeno odločitev;
- utemelji, zakaj je določen odziv primeren ali neprimeren.

Vsebinski sklop 7: ZVOP-2 in varstvo osebnih podatkov

Obseg: 4 pedagoške ure

Priporočene vsebine:

- ključne zahteve ZVOP-2,
- vloga pooblaščene osebe za varstvo podatkov,
- varno delo z osebnimi podatki v praksi,
- evidenca obdelav osebnih podatkov,

- varna hramba,
- dostopi in pooblastila,
- delo na daljavo in varnostna tveganja.

Znanje:
Udeleženec:

- pojasni osnovna načela varnega ravnanja z osebnimi podatki;
- razume pomen dostopov, pooblastil in sledljivosti ravnanj;
- pozna vlogo DPO in osnovne notranje obveznosti organizacije.

Spretnosti:
Udeleženec:

- presodi, katero ravnanje z osebnimi podatki je ustrezno in katero ne;
- pravilno ravna z dokumenti, evidencami in digitalnimi datotekami z osebnimi podatki;
- pripravi predlog izboljšave za varnejšo obdelavo podatkov v svojem delovnem okolju.

Vsebinski sklop 8: Delavnica: ravnanje z osebnimi podatki v praksi

Obseg: 2 pedagoški uri

Priporočene vsebine:

- praktični scenariji,
- presoja pravilnega ravnanja,
- priprava izboljšav za lastno delovno okolje.

Znanje:
Udeleženec:

- razlikuje med dopustnim, tveganim in nedopustnim ravnanjem;
- razume posledice nepravilne obdelave osebnih podatkov.

Spretnosti:
Udeleženec:

- analizira primer iz prakse;
- utemelji pravilno ravnanje;
- pripravi mini-protokol ali priporočilo za svoje delovno mesto.

12. Metode in oblike dela

Program se izvaja po andragoških načelih, s poudarkom na aktivni vlogi udeležencev, prenosu v prakso in sprotni refleksiji. Program vključuje mentorsko podporo, učenje na primerih, obrnjeni model učenja, mikro-učenje, sprotno preverjanje razumevanja, peer learning in uporabo IKT orodij.

Predvidene metode dela:

- kratko interaktivno predavanje,
- vodena razprava,

- študija primera,
- analiza elektronskih sporočil in situacij,
- problemsko učenje,
- delavnica,
- delo v parih in manjših skupinah,
- samoevalvacija,
- mentorski pogovor,
- kratki kvizi in refleksije,
- uporaba spletne učilnice.

Predvidene oblike dela:

- skupinsko delo v živo,
- individualno delo,
- delo na daljavo v spletni učilnici,
- vodeno samostojno delo med srečanji.

13. Organizacija izobraževanja

Program se praviloma izvede v skupini od 10 do 18 udeležencev.

Priporočena organizacija:

- 4 srečanja po 5 pedagoških ur,
- med srečanji kratke samostojne naloge v spletni učilnici,
- kombinacija skupinskega in individualnega dela,
- možnost prilagoditve primerov glede na delovno vlogo udeležencev,
- možnost izvedbe v živo ali v kombinirani obliki.

Priporočeno razmerje oblik dela:

- približno 70 % skupinskega dela,
- približno 30 % individualnega ali samostojnega dela.

Didaktična organizacija:

- uvodna aktivacija predznanja,
- obravnava vsebine,
- praktična vaja ali analiza primera,
- refleksija in prenos v delovno okolje,
- sprotno preverjanje razumevanja.

14. Spremljanje, preverjanje in vrednotenje znanja

Načini preverjanja

Znanje in napredek udeležencev se preverjata:

- z začetnim samoocenjevalnim vprašalnikom,
- s sprotnimi mini kvizi,

- z analizo primerov,
- z opazovanjem sodelovanja pri vajah,
- z reševanjem problemskih nalog,
- s končno praktično nalogo ali izdelkom ali
- s končno refleksijo.

Način izražanja doseganja ciljev

Doseganje ciljev se izrazi opisno:

- dosega cilje programa,
- delno dosega cilje programa,
- še ne dosega ciljev programa.

15. Pogoji za dokončanje programa

Udeleženec program uspešno zaključi, ko izpolni najmanj 80 odstotkov prisotnosti ter aktivno sodeluje pri delavnicah in praktičnih nalogah, ki so del vsebine.

16. Kadrovski pogoji oziroma izvajalci programa

Program izvajajo strokovni delavci oziroma zunanji strokovnjaki z ustreznim znanjem in izkušnjami. Zaželeno je, da program izvajajo strokovnjaki za kibernetsko varnost, predstavniki SI-CERT, pooblaščene osebe za varstvo podatkov ter strokovni delavci z ustreznimi andragoškimi kompetencami. Izvajalci morajo dobro poznati tako vsebino kot didaktične pristope za delo z odraslimi.

Priporočeni profili izvajalcev

Nosilni izvajalec programa

- visokošolska izobrazba ustrezne smeri,
- izkušnje z izobraževanjem odraslih,
- poznavanje andragoških pristopov,
- izkušnje z vodenjem interaktivnih delavnic.

Strokovnjak za kibernetsko varnost

- strokovno znanje s področja informacijske in kibernetske varnosti,
- izkušnje z usposabljanjem zaposlenih,
- sposobnost prevajanja strokovnih vsebin v vsakodnevno delovno prakso.

Strokovnjak za varstvo osebnih podatkov oziroma DPO

- poznavanje ZVOP-2 in praktičnega ravnanja z osebnimi podatki v organizacijah,
- izkušnje s svetovanjem ali izobraževanjem zaposlenih.

Priporočena dodatna usposobljenost izvajalcev

- delo z odraslimi,
- facilitiranje skupinske refleksije,

- uporaba digitalnih učnih okolij,
- izkušnje z delom z raznolikimi skupinami udeležencev.

17. Materialni in prostorski pogoji

Za izvedbo programa izvajalec zagotovi:

- učilnico z internetno povezavo,
- računalnik in projektor,
- dostop do spletne učilnice,
- gradiva za analizo primerov,
- možnost uporabe pametnih telefonov ali računalnikov pri vajah,
- vzorčne scenarije, obrazce in kontrolne sezname.

18. Učna gradiva

Program spremljajo:

- predstavitve izvajalcev,
- učni listi,
- primeri phishing sporočil,
- kontrolni seznami za varno ravnanje,
- kratki kvizi,
- gradiva SI-CERT,
- primeri pravilnega in nepravilnega ravnanja z osebnimi podatki,
- predloge mini-protokolov za organizacijo.

Priprava učnega gradiva je med pričakovanimi rezultati naloge posebej navedena.

19. Potrdilo o udeležbi oziroma potrdilo o uspešno zaključenem programu

Udeleženci, ki uspešno zaključijo program, prejmejo **Potrdilo o uspešno zaključenem neformalnem izobraževalnem programu**, ki vsebuje:

- naziv izvajalca,
- naziv programa,
- obseg programa v pedagoških urah,
- obdobje izvedbe,
- kratko navedbo ključnih vsebin,
- potrditev, da je udeleženec izpolnil obveznosti programa.

20. Spremljanje kakovosti in evalvacija programa

Evalvacija se izvede:

- pred začetkom programa z vprašalnikom o potrebah in pričakovanjih,
- med programom s kratkimi sprotnimi povratnimi informacijami,
- ob zaključku s končnim evalvacijskim vprašalnikom,
- po zaključku z analizo uporabnosti programa v praksi.

Spremljajo se zlasti:

- zadovoljstvo udeležencev,
- doseganje ciljev,
- uporabnost vsebin pri delu,
- kakovost gradiv,
- ustreznost metod dela,
- predlogi za izboljšave.

21. Pričakovani učinki programa

Po izvedbi programa se pričakuje:

- večja ozaveščenost zaposlenih o kibernetskih tveganjih,
- boljša sposobnost prepoznavanja groženj,
- odgovornejše ravnanje z osebnimi podatki,
- bolj dosledna uporaba osnovnih varnostnih praks,
- večja pripravljenost na pravočasen odziv ob incidentu,
- več sodelovanja in izmenjave dobrih praks med zaposlenimi.