

»59. srečanje mladih raziskovalcev Slovenije 2025«

Obraz, prst in koda: Biometrija v času umetne inteligence

Interdisciplinarno raziskovalno področje

Računalništvo ali telekomunikacije in psihologija ali pedagogika

Raziskovalna naloga

Avtor: Blaž Jesenik

Mentor: Mirko Pešec, prof.

Šola: II. gimnazija Maribor

Maribor, april 2025

KAZALO VSEBINE

Povzetek.....	iv
Abstract.....	v
Zahvala.....	vi
1 uvod.....	7
1.1 Hipoteze naloge	8
2 teoretični del.....	9
2.1 Psihološki del.....	9
2.1.1 Zasebnost	9
2.1.2 Lažne informacije in tehnologije globokih ponaredkov	9
2.1.3 Socialni inženiring	12
2.1.4 Digitalni sledovi.....	12
2.1.5 Uporabniška izkušnja.....	13
2.2 Računalniški del.....	13
2.2.1 Umetna inteligenca (UI)	13
2.2.2 Biometrija in biometrični sistemi.....	14
2.2.3 Etične dileme	14
2.2.4 Proces prijavljanja.....	15
2.2.5 Metode prijave	16
2.2.6 Večstopenjsko preverjanje (2FA)	17
2.2.7 Statična avtentikacija	17
2.2.8 Strojno učenje	17
3 metodologija	19
3.1 Opis vzorca	19
3.2 Uporabljeni programi in orodja	19
3.2.1 ChatGPT	19

3.2.2	Dall-E.....	20
3.2.3	ElevenLabs.....	20
4	Rezultati	21
4.1	Rezultati ankete.....	21
4.2	Udeležba na konferenci CIOSEC 2024	24
4.3	Intervju.....	25
5	Razprava	26
5.1	H1: Primerjava biometričnih in tradicionalnih gesel.....	26
5.2	H2: Uporabniška izkušnja in zanesljivost biometričnih sistemov	27
5.3	H3: Uporaba biometričnih gesel med dijaki in študenti	28
6	Družbena odgovornost.....	29
7	sklep.....	30
8	viri in literatura	31
	priloge	1

KAZALO SLIK, TABEL IN GRAFOV

Slika 1: Generirana fotografija 1 (Dall-E)	10
Slika 2: Generirana fotografija 2 (Dall-E)	10
Slika 3: Generirana fotografija 3 (Dall-E)	11
Slika 4: Resnična fotografija (Getty Images).....	11
Slika 5: Biometrične lastnosti	14
Slika 6: Proces avtentikacije (lasten arhiv).....	15
Tabela 1: Prednosti in slabosti biometričnih gesel	13
Graf 1: Zanesljivost metod.....	21
Graf 2: Najpogostejša metoda prijavljanja	22
Graf 3: Ferkvenčnost menjave gesel.....	22
Graf 4: Uporaba enakih gesel	23
Graf 5: Dvostopenjsko preverjanje	23

POVZETEK

Ta raziskovalna naloga obravnava vpliv umetne inteligence na razvoj in uporabo biometričnih sistemov tako z vidika računalništva kot psihologije. Analizira, kako algoritmi za prepoznavo obraza, glasu in prstnih odtisov prispevajo k večji kibernetiski varnosti ter kako nove metode, kot so globoki ponaredki (»deepfakes«), predstavljajo izziv za zanesljivost avtentikacije. Psihološki vidik raziskave se osredotoča na dožemanje različnih biometričnih metod med srednješolci in študenti ter njihovo zaupanje v varnost in zasebnost teh sistemov.

Raziskava ugotavlja, da mladi dojemajo biometrične metode kot enostavnejše in bolj zanesljive, vendar digitalna varnost močno vpliva na psihološko doživljanje uporabnikov. Nezaupanje in občutek izgube nadzora nad lastnimi podatki sta pogosti posledici kibernetiskih napadov ali uhajanja podatkov. V ospredje so postavljene tudi številne aktualne etične dileme ter pomen digitalne varnosti v sodobni družbi.

Ključne besede: umetna inteligenca, biometrični sistemi, kibernetiska varnost, globoki ponaredki, dvostopenjska avtentikacija, kraja identitete, kršitev zasebnosti

ABSTRACT

This research thesis examines the impact of artificial intelligence on the development and use of biometric systems from both a computer science and a psychology perspective. It analyses how facial, voice and fingerprint recognition algorithms contribute to increased cyber security and how new methods such as deepfakes challenge the reliability of authentication. The psychological aspect of the research focuses on the perception of different biometric methods among high school and university students and their trust in the security and privacy of these systems.

The research finds that young people perceive biometric methods as simpler and more reliable, but that digital security has a strong impact on the psychological experience of users. Mistrust and a sense of loss of control over one's own data are common consequences of cyber-attacks or data leaks. It also highlights a number of current ethical dilemmas and the importance of digital security in modern society.

Keywords: artificial intelligence, biometric systems, cybersecurity, deep forgeries, two-factor authentication, identity theft, privacy breaches.

ZAHVALA

Zahvaljujem se mentorju za pomoč in svetovanje pri nalogi ter šolski koordinatorici za odlično organizacijo. Posebna zahvala gre tudi dr. Srđanu Škrbiću za strokovne odgovore na zastavljena vprašanja in moji družini ter prijateljem za podporo ob pisanju naloge.

1 UVOD

“Biometrija je tehnologija zbiranja in obdelave podatkov o posameznikovih merljivih telesnih in vedenjskih lastnosti, po katerih ga je mogoče preveriti in prepoznati” (Fran/iskanje/biometrija, 2024). Razširjeno se uporablja vse od zadnjega desetletja 20. stoletja, temeljno zasnovano pa so postavili že antični Egipčani, ki so na podlagi opisa videza prepoznavali zaupanja vredne trgovce. Leta 1892 je britanski znanstvenik Frances Galton objavil knjigo o klasifikaciji prstnih odtisov, ki je imela pomemben vpliv na razvoj policijskih sistemov za identifikacijo oseb. Danes se biometrični sistemi uporabljajo tudi v bančništvu z namenom preprečevanja prevar in vdorov, saj navadna gesla in PIN-kode pogosto niso dovolj zanesljivi (Britannica Library, 2024). Hiter napredek umetne inteligence (v nadaljevanju UI) je še dodatno okrepil varnost, vendar je hkrati hekerjem omogočil uporabo bolj prefinjenih orodij.

Še posebej skrb vzbujajoča je tehnologija globokih ponaredkov (t. i. »deepfakes«), ki omogoča ustvarjanje lažnih video-zvočnih vsebin, ki posebljajo vedenje ali govor posameznika. Propaganda lažnih informacij (»fake news«) v medijih in na socialnih omrežjih bi lahko posledično povzročila veliko zmedo v družbi (Waizel, 2024). Za zaščito osebnih podatkov lahko veliko storimo tudi uporabniki, saj z izbiro varnega gesla zmanjšamo verjetnost za vdor v svoje račune. Odklepanje s prstnim odtisom ali prepoznavo obraza je videti kot varnejša rešitev, vendar s posredovanjem naših unikatnih (težko zamenljivih) podatkov oblačnim storitvam, kjer so shranjeni, postanemo ranljivi. Dodatno plast varnosti predstavlja tudi dvostopenjsko preverjanje (2FA), kjer gre za potrjevanje identitete z nečim, kar imamo (npr. fizični ključ USB ali SMS koda) ali/in uporaba generatorjev varnih gesel. Predavanji na temo umetne inteligence in vse pogostejše pojavljanje novic o hekerskih vdorih v medijih sta me spodbudili, da še sam raziščem področje biometrije in primerjam različne vrste klasičnih gesel (npr. PIN-kode) z biometričnimi (npr. prepoznavna prstnega odtisa) ter drugimi alternativnimi metodami prijave.

1.1 Hipoteze naloge

Pred raziskovanjem sem si zastavil naslednja raziskovalna vprašanja (RV) in hipoteze (H):

RV1: Kako se biometrična in tradicionalna gesla razlikujejo v varnosti in možnostih menjave v primeru kraje?

H1: Uporaba biometričnih gesel je varnejša kot uporaba tradicionalnih metod prijavljanja, vendar so le ta težje zamenljiva v primeru kraje.

RV2: Ali uporabniška izkušnja vpliva na mnenje uporabnikov glede zanesljivosti biometričnih sistemov?

H2: Uporabniki biometrične sisteme ocenjujejo kot bolj varne in zanesljive, če je dobra tudi uporabniška izkušnja.

RV3: Ali študentje in dijaki menijo, da so biometrična gesla varnejša v primerjavi z drugimi načini prijavljanja?

H3: Študentje in dijaki pogosteje uporabljajo biometrična gesla, saj jih ocenjujejo kot bolj varna v primerjavi s tradicionalnimi načini prijave (npr. gesli, PIN-kodami).

2 TEORETIČNI DEL

2.1 Psihološki del

2.1.1 Zasebnost

Zaradi unikatnosti biometričnih podatkov je pomembno, da so le ti varno hranjeni. Kljub vsem protokolom in varnostnim slojem vdorov v podatkovne baze nikoli ni mogoče v celoti preprečiti. S tehnološkim napredkom so vse spretnjši tudi napadalci, ki uporabljajo vedno bolj prefinjene metode. V letu 2015 je bilo zaradi napada na Ameriški urad za upravljanje z osebjem ogroženih kar 5.6 milijonov prstnih odtisov. V primeru takšnih incidentov je možna menjava tradicionalnih gesel (npr. PIN-kod), ne pa tudi biometričnih, ki jih je bistveno težje nadomestiti. Posledice kraje so lahko dosmrtno. V kljub navidezno močnejši varnosti se je pokazala ranljivost s hujšimi posledicami kot pri geslih z manj močno varnostjo (Gabriel Vigariu & Marin, 2024).

2.1.2 Lažne informacije in tehnologije globokih ponaredkov

Včasih je ta tehnologija bila na voljo le naprednim tehnološkim laboratorijem, danes pa je že cenovno dostopna uporabnikom po vsem svetu (*The Social Impact of Deepfakes*, 2024). Na videz sicer neškodljiva oblika video in fotomontaže lahko ima negativne posledice na družbo, saj omogoča hitro širjenje lažnih (pogosto spornih) novic.

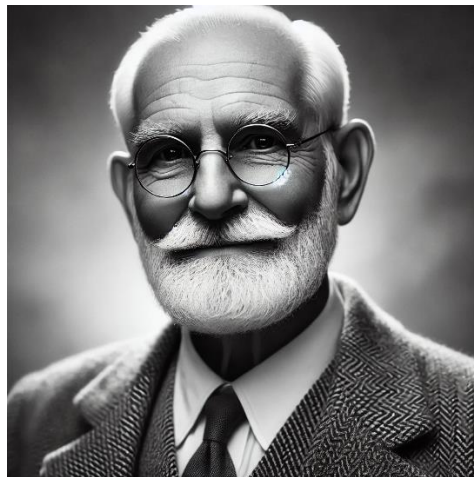
Pozabiti ne smemo deljenih ponaredkov na posameznika, katerega identiteta je bila ukradena. Poleg javnega poniževanja, sovražnega govora in ostrih kritik lahko celo pride do tožb in protestov ter gospodarskih posledic, sploh če je žrtev vplivna osebnost.

Ljudje smo večinsko neracionalna bitja, ki pogosto sklepamo na podlagi premajhnega števila znanih dejstev. Verjamemo v predvsem to, v kar želimo verjeti, pri čemer ne podvomimo o obstoječem znanju. Kombinacija prehitrega sklepanja in nezanesljivih informacij lahko ima velike posledice za družbo, sploh če informacija pride iz dokaj zanesljivega medija.

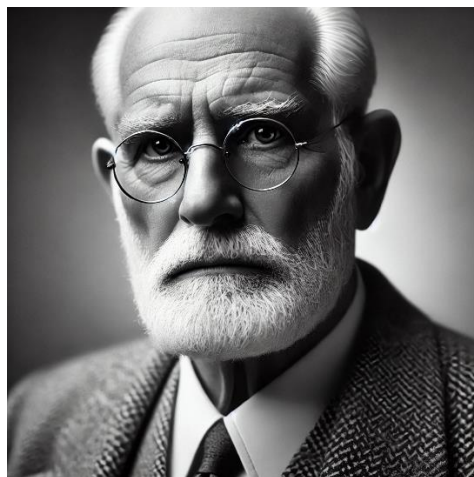
Namen ustvarjanja lažnih vsebin ni nujno škodoželjen; posamezniki lahko zaradi radovednosti eksperimentirajo s tehnologijo ponarejanja za lastno zabavo, kar nato delijo s prijatelji. Na tak

način sicer nenamerno lažni posnetki in slike delijo naprej in postanejo viralni (zelo gledani) na družbenih omrežjih.

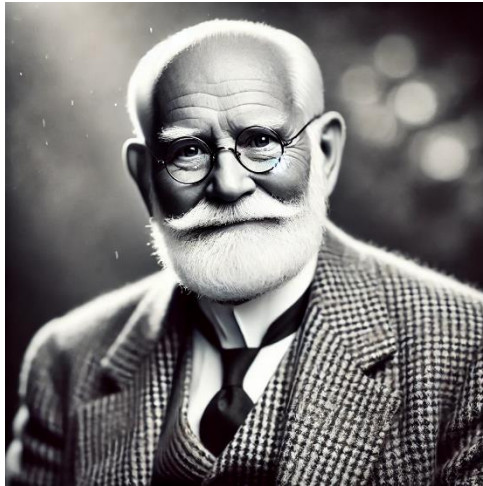
Za namen ponazarjanja, kako lahko umetna inteligenca ustvarja digitalne vsebine, sem s pomočjo orodja ChatGPT Dall-E ustvaril podobno fotografijo znanega nevrologa Sigmund Freuda. Na ukaz »Generate a realistic picture of an Austrian neurologist, Sigmund Freud« je orodje zavrnilo izdelavo fotografije, saj ni v skladu z načeli podjetja, vendar je ponudilo možnost, da ustvari fotografijo podobnega človeka.



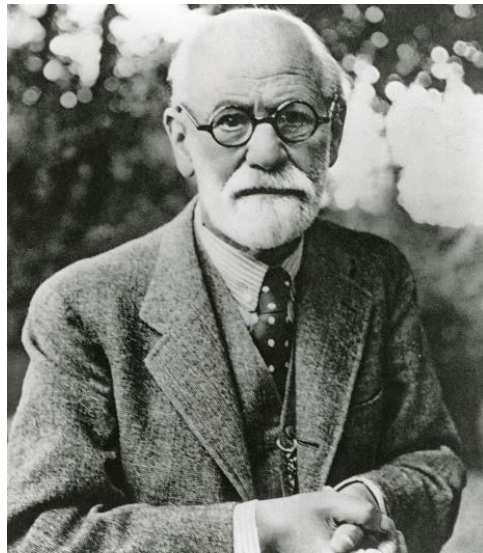
Slika 1: Generirana fotografija 1 (Dall-E)



Slika 2: Generirana fotografija 2 (Dall-E)



Slika 3: Generirana fotografija 3 (Dall-E)



Slika 4: Resnična fotografija (Getty Images)

Kljub nekaterim kazalnikom, ki nakazujejo na prisotnost umetne inteligence, lahko s primerjavo generiranih slik z resničnim portretom opazimo podobnosti. V primeru, da bi na generirano sliko naleteli na spletu in prave ne bi poznali, bi bilo določanje, ali gre za ponaredek težje. Kljub skrb vzbujajočim napovedim je treba poudariti, da so tovrstne tehnologije in umetna inteligenca šele v fazi razvoja, zato posledice še niso tako očitne.

2.1.3 Socialni inženiring

Iz vidika kibernetске varnosti socialni inženiring pomeni manipulacije, pri katerih napadalci uporabljajo psihološke trike, s pomočjo katerih izkoriščajo človeško radovednost, strah ali željo, saj lahko tako pridobijo dostop do občutljivih informacij (npr. podatke o geslih, kreditnih karticah in številkah bančnih računov).

V času hitrega življenjskega sloga pogosto nismo pozorni na podrobnosti in poskušamo v tem krajšem času opraviti največ dela. Napadalci nepozornost pogosto zlorabijo in se s pomočjo lažnih identitet – vse pogosteje ustvarjenih z umetno inteligenco – predstavljajo kot nekdo drug. Med bolj znane primere spada t. i. »CEO fraud«, prevara pri kateri se napadalec izdaja za vodjo podjetja, ki od zaposlenega nemudoma zahteva občutljive podatke. Drugi pogosti incidenti vključujejo phishing (»ribarjenje«), prevare s telefonskimi klici in lažnimi e-poštnimi sporočili, vsebina katerih se pogosto navezuje na obvestila o vdoru v račun, sumljivih dejavnostih na bančnem računu ali nujni menjavi gesla. Napadalci se pogosto predstavljajo kot zaposleni dostavnih služb, v podpori tehnoloških podjetij, bančnih in zavarovalniških podjetjih. Natančno kopirane spletne strani in podobne e-poštne naslove ter URL povezave žrtve pogosto spregledajo, saj napadalci z njimi tudi čustveno manipulirajo (IEEE, 2024). V stiski žrtve pogosto občutijo strah in anksioznost, sploh ko gre za probleme ki pomembno vplivajo na življenje (npr. varnost, denar in zaposlitev).

2.1.4 Digitalni sledovi

Pod pojem digitalni sledovi si pogosto razlagamo kakršnekoli zapise in podatke o dejavnosti na digitalnih napravah. Najpogosteje je to zgodovina brskanja na spletu. Spletne strani pogosto uporabljajo t. i. piškotke, ki omogočajo pridobivanje analitičnih podatkov. Uporabnik se lahko z zbiranjem podatkov strinja ali ne strinja, pri čemer jih veliko sploh ne prebere pogojev, ter tako niso posledično seznanjeni z vsemi podatki, ki jih spletna stran zbira. Analitična podjetja takšne podatke uporabljajo za namen marketinga ter prilagajanja uporabniške izkušnje, saj tako kujejo dobiček.

Nekateri brskalniki omogočajo tudi shranjevanje gesel, ne samo za spletne strani, ampak tudi podatke o bančnih karticah in naslovih. Ob ponovni uporabi spletne strani se podatki vpišejo že samodejno, kar uporabniku prihrani čas. Vdor v npr. Googlov račun, ki ima shranjena gesla za druge platforme, bi pomenil veliko škode in izgube.

2.1.5 Uporabniška izkušnja

Uporabniki biometrične sisteme pogosto ocenjujejo kot varnejše od tradicionalnih gesel, saj se zavedajo unikatnosti biometričnih podatkov, vendar se le redko vprašajo po shranjevanju in uporabi teh podatkov.

Tabela 1: Prednosti in slabosti biometričnih gesel

Prednosti	Slabosti
<ul style="list-style-type: none">▪ enostavnejša in hitrejša uporaba (ni potrebe po vnosu gesla)	<ul style="list-style-type: none">▪ jih je težje menjati v primeru kraje (mehanizmi so kompleksni in niso brezhibni)
<ul style="list-style-type: none">▪ izboljšana varnost	<ul style="list-style-type: none">▪ možnost sistemske napake (slabo pozicioniranje prsta, nejasna slika pri prepoznavi obraza)
<ul style="list-style-type: none">▪ pomnjenje ni potrebno	<ul style="list-style-type: none">▪ nelagodje ob deljenju občutljivih informacij

Potencial za izboljšavo uporabniške izkušnje se kaže predvsem z razvojem alternativnih metod preverjanja, kot so fizični varnostni ključi in enkratne generirane geselske kode (one-time token oziroma OTP). Gre za metode, ki ne zahtevajo tako občutljivih podatkov, kot so biometrični, vendar so zanesljive in varne. Njihova pomanjkljivost (predvsem fizičnih ključev) je potreba po fizični prisotnosti, torej, da jih imamo pri sebi vsakič, ko se želimo prijaviti. Seveda se s tem do določene mere poveča tudi možnost kraje, če naprave uporabljamo na javnih mestih.

2.2 Računalniški del

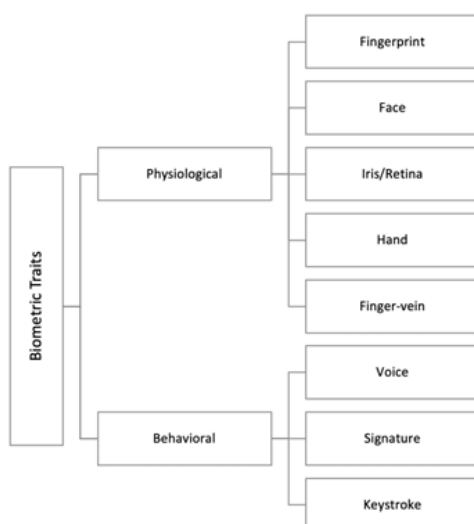
2.2.1 Umetna inteligenca (UI)

Na zastavljeno vprašanje »kaj je umetna inteligenca in kaj je njen namen?« je umetno inteligenčno orodje OpenAI ChatGPT generiralo naslednji odgovor: »Umetna inteligenca (UI) je področje računalništva, ki se ukvarja z razvojem sistemov, ki lahko izvajajo naloge, za katere običajno potrebujemo človeško inteligenco. To vključuje razumevanje jezika, prepoznavanje vzorcev, učenje iz podatkov, reševanje problemov, odločanje in celo ustvarjalno delo.«

2.2.2 Biometrija in biometrični sistemi

“Biometrija je tehnologija zbiranja in obdelave podatkov o posameznikovi merljivih telesnih in vedenjskih lastnosti, po katerih ga je mogoče preveriti in prepoznati” (Fran/iskanje/biometrija, 2024). Temelji na prepoznavanju prstnih odtisov, obrazov, šarenic, glasu, dlani in celo vzorcev hoje ali tipkanja. Uporaba biometrije se je v zadnjih desetletjih močno razširila in se pogosto uporablja za namen:

- nadzorovanja (varnostne kamere)
- biometričnega bančništva
- odklepanje naprav
- preverjanje identitete na letališčih in državnih prehodih
- marketinga



Slika 5: Biometrične lastnosti

2.2.3 Etične dileme

Naše potrebe, želje in prepričanja močno vplivajo na naš pogled na vedno večjo vlogo umetne inteligence v družbi. Biometrične sisteme lahko razumemo kot tehnološki napredek, ki izboljšuje varnost in omogoča hitrejšo identifikacijo, ali pa kot potencialno grožnjo za svojo zasebnost in varstvo podatkov.

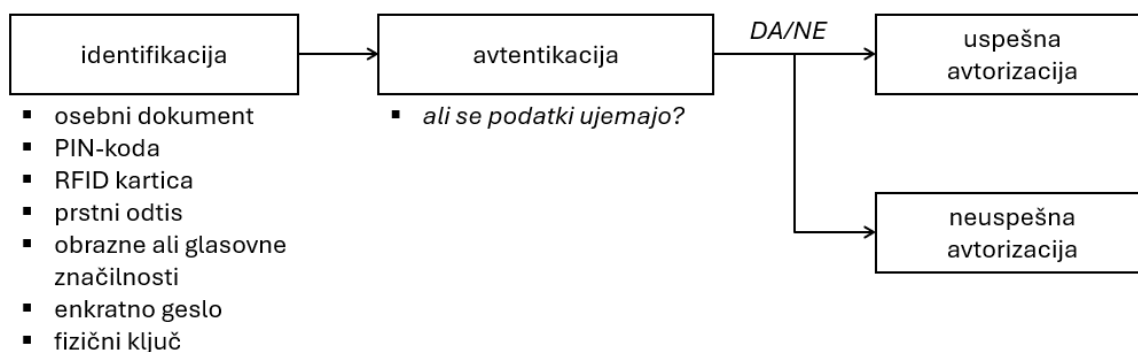
Eden izmed glavnih izzivov biometričnih sistemov je hramba podatkov, ki ključna za varnost uporabnikov. Pomembno je, da platforme s podatki ravnajo odgovorno, v skladu s protokoli in trenutno zakonodajo. Vprašljive so predvsem »third-party« platforme oziroma platforme

neznanega izvora, za katere pogosto ne vemo, kdo podatke upravlja in kakšne varnostne protokole uporabljajo. S tem se poveča tveganje za krajo identitete ali nepooblaščen dostop.

S tehnološkim napredkom hitro zastara tudi zakonodaja na tem področju, kar še dodatno oslabi varnost.

2.2.4 Proces prijavljanja

Po podatkih nekaterih raziskav je na internetu prisotnih že več kot 2,4 milijarde uporabnikov. Z množično digitalizacijo in vse večjim zanašanjem na digitalno infrastrukturo se je povečalo tudi število spletnih napadov in kraj podatkov, ki imajo pogosto tudi gospodarske posledice. Za zaščito podatkov tako organizacij kot uporabnikov se je pokazala potreba po boljši zaščiti.



Slika 6: Proces avtentikacije (lasten arhiv)

Preverjanje bi lahko razdelili v naslednje stopnje: identifikacija, avtentikacija, avtorizacija.

V stopnji identifikacije uporabnik ali informacijski sistem (IS) predloži dokaz, ki potrjuje njegovo identiteto. Dokaze oziroma dejavnike avtentikacije lahko razdelimo v naslednje kategorije:

- Nekaj, kar uporabnik ve (geslo, PIN-kodo)
- nekaj, kar opisuje značilnosti uporabnika (obrazne značilnosti, glasovne značilnosti)
- nekaj, kar uporabnik ima (fizični ključ, RFID kartico)
- nekaj, kar uporabnik lahko naredi (se podpiše, hodi, tipka na tipkovnico)
- tam, kjer se uporabnik je (lokacija, ura in datum)*

*primer: Če prehodna vratca na smučišču zaznajo isto smučarsko karto v krajšem časovnem intervalu, smučarja ne bodo spustila skozenj, saj se tako zmanjša možnost zlorabe (npr. deljenje iste karte med smučarji)

Najpogostejše metode za prijavljanje sta kombinacija uporabniškega imena ter gesla ali kartice (npr. bančne) in PIN-kode. Kategorije se lahko med seboj prepletajo, pogosto je metoda preverjanja odvisna od statusa uporabnika. Če gre za skrbnika sistema, bo v večini primerov tudi več slojev zaščite, saj gre za pomembnejšo vlogo v omrežju.

2.2.5 Metode prijave

Poglavitna razlika med biometričnimi in tradicionalnimi gesli je ta, da biometrična temeljijo na zasnovi tega, kar opisuje značilnosti uporabnika, tradicionalna pa na tem, kar uporabnik ve.

Biometrična gesla:

- glasovna prepoznavna
- obrazna prepoznavna
- prepoznavna prstnega odtisa
- prepoznavna mrežnice

Tradicionalna gesla:

- navadno geslo
- PIN-koda
- vzorec odklepanja
- fizični ključi (RFID, USB)

Ena izmed prednosti biometričnih gesel je, da ne zahtevajo kognitivne obremenitve oz. pomnjenja. Kako bi pa lahko tudi uveljavili tudi na področju tradicionalnih gesel? Na Švedskem so se domislili novega načina, kako lahko zaposlenim omogočajo dostop v službene prostore. *»V visokotehnološki poslovni zgradbi Epicenter v Stockholmu za dostop do posameznih prostorov namesto elektronskih kartic preizkušajo novo tehnologijo. Zaposlenim v roko vstavijo čip, ki jim za zdaj omogoča le dostop do pisarn in uporabo fotokopirnega stroja, a možnosti njegove uporabe so precej večje. Za fotokopiranje morajo zaposleni roko zgolj približati napravi in identifikacija je opravljena.«* (David Kos, 2015)

Glavni razvijalec Hannes Sjobland največjo prednost čipiranja ljudi vidi v tem, da ne bo potrebe po PIN-kodah in geslih, prav tako pa meni, da je *»bolj intuitivno približati roko z vgrajenim čipom«*. Ta primer prakse ponuja rešitev za potrebo po kognitivni obremenitvi, prav tako predstavlja varnejši način kot prijave. Hkrati vzbuja številne dileme in moralne zadržke zaradi vstavljanja tehnologije v človeka in pod vprašaj postavlja možne zlorabe z npr. bralnikom čipov/kartic.

2.2.6 Večstopenjsko preverjanje (2FA)

Vse pogostejša je uporaba metode dvostopenjske avtentikacije oziroma dvostopenjskega preverjanja (2-factor authentication). Gre za varnostni mehanizem, ki zahteva dve različni metodi preverjanja identitete uporabnika. Običajno gre za kombinacijo gesla in kode, ki jo uporabnik prejme na mobilno napravo. To dodatno varnostno plast povečuje zaščito računov in sistemov pred nepooblaščenim dostopom (Microsoft Corporation, 2023)

Primer nadgrajene prakse metode 2FA so »Google Passkeys«, Tako imenovani "Passkeys" je nova tehnologija avtentikacije brez gesla, ki jo razvijajo Google in druga velika tehnološka podjetja. Gre za varnejši način prijavljanja v napravo ali storitev, saj gesla "Passkeys" uporabljajo kombinacijo biometričnih podatkov in kriptografije, kar omogoča varno preverjanje uporabnikov (Google, 2023). Čeprav druge varnostne tehnologije, kot so dvostopenjska avtentikacija in upravitelji gesel, lahko pripomorejo k varnosti, še vedno predstavljajo tarčo hekerjem. Prednost te tehnologije je tudi, da si nam ni treba zapomniti gesla, vendar lahko preprosto uporabimo prstni odtis ali prepoznavo obraza, kar je vseeno boljše od kratkih, preprostih gesel. Tehnološki gigant Google si prizadeva, da bi »Passkeys« postal primaren način prijave za Googlove storitve.

2.2.7 Statična avtentikacija

Statična avtentikacija velja za gesla in PIN-kode; torej za nekaj, kar uporabnik ve. Pomanjkljivost takšne avtentikacije je visoka dovzetnost za krajo na naslednje načine:

- Beležnik tipkanja (»keylogger«): preprosta naprava, ki zabeleži zaporedja pritisnjenih tipk, kar napadalcem omogoči odkrivanje gesel
- Ugibanje gesla: poskušanje različnih pogostih kombinacij, zaporedij, letnic
- Napad z grobo silo (»brute-force attack«): pristop, pri katerem napadalec s pomočjo namigov ob neuspehi avtorizaciji poskuša uganiti pravo geslo

2.2.8 Strojno učenje

Med raziskovanjem sem ugotovil, da ne poznam razlike med strojnimi učenjem in umetno inteligenco, zato sem odgovor poiskal kar s pomočjo orodja ChatGPT, ki je na poziv »V

kratkem odstavku pojasni razliko med umetno inteligenco in strojnimi učenjem” odgovorilo naslednje: *Umetna inteligenca (UI) in strojno učenje (SU) sta povezana, vendar različna pojma. UI je širši koncept, ki vključuje razvoj sistemov, ki lahko posnemajo človeško inteligenco pri opravljanju nalog, kot so prepoznavanje vzorcev, razumevanje jezika in sprejemanje odločitev. Strojno učenje je podskupina UI, ki omogoča računalnikom, da se učijo iz podatkov brez eksplicitnega programiranja. Medtem ko UI zajema različne metode, vključno s pravili in ekspertnimi sistemi, SU temelji na algoritmih, ki s pomočjo podatkov izboljšujejo svoje delovanje in napovedi.*

3 METODOLOGIJA

3.1 Opis vzorca

V raziskavi je sodelovalo 135 dijakov »šole 1« in 24 študentov »šole 2« (skupaj 159). Nanj so odgovorile večinoma ženske (65,4 %). Vzorec je bil izbran ciljno, saj sem želel analizirati specifično populacijo mladih, ki pogosteje uporabljajo digitalne tehnologije. Anketa je bila anonimna in zasnova za preverjanje na hipotezo H3, ali študentje in dijaki pogosteje uporabljajo biometrična gesla, saj jih ocenjujejo kot bolj zanesljiva v primerjavi z gesli/PIN-kodami. Poleg ankete je bil izveden tudi strukturiran intervju s strokovnjakom s področja kibernetike, dr. Srđanom Škrbićem, v katerem sem se osredotočil na razlike med biometričnimi in tradicionalnimi gesli ter na postopke menjave biometričnih podatkov in alternativne možnosti prijave. Za dodatno poglobitev razumevanja o trendih in izzivih na področju kibernetike sem se udeležil spletne konference CIOSEC 2024, na kateri so govorniki predstavili primere kibernetičnih napak in seznanili poslušalce z obstoječimi regulativami in zakonodajo na tem področju. Zapiski konference ter rezultati ankete so priloženi v poglavju Priloga.

3.2 Uporabljeni programi in orodja

3.2.1 ChatGPT

Za namen generiranja idej in predlogov besedila je bilo uporabljeno umetno-inteligenčno orodje OpenAI ChatGPT. Podatki, ki jih je zagotovilo orodje so bili pregledani in prilagojeni ter preverjeni s strani avtorja.¹

Povezave za dostop do orodij
¹ <https://chatgpt.com/>

3.2.2 Dall-E

Orodje Dall-E je model umetne inteligence, ki ga je razvilo podjetje OpenAI za generiranja fotografij na podlagi besedilnih opisov. V raziskavi je uporabljen za namen prikazovanja zmožnosti umetne inteligence in primerjavo realističnih fotografij z umetno generiranimi.²

3.2.3 ElevenLabs

ElevenLabs je orodje za generiranje govora, ki uporablja umetno inteligenco za ustvarjanje naravno zvenceh glasov. Temelji na nevronskih mrežah, ki analizirajo glasovne značilnosti, kot sta intonacija in naglas.³

² <https://openai.com/index/dall-e-2/>

³ <https://elevenlabs.io/>

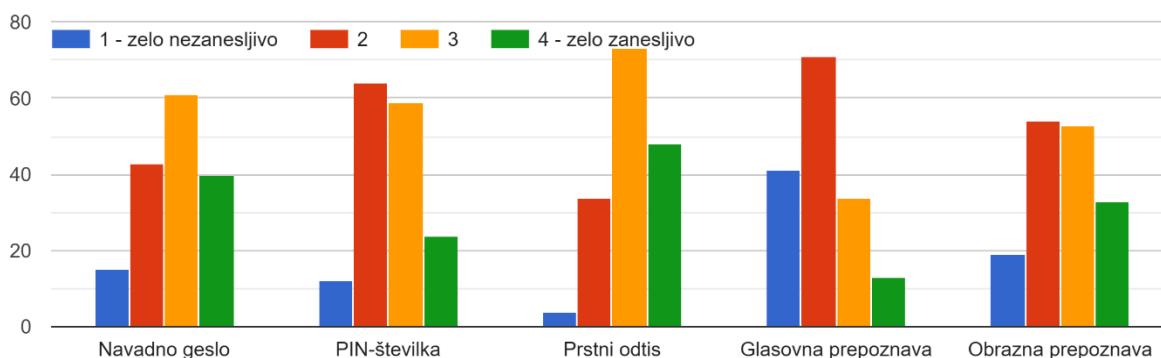
4 REZULTATI

4.1 Rezultati ankete

V tem podpoglavju so izpostavljene pomembnejše ugotovitve iz ankete. Vsi rezultati in vzorec ankete so priloženi v poglavju Priloge.

Na vprašanje »Kako ocenjujete svojo digitalno varnost?« na lestvici 1-4 niti en uporabnik ni odgovoril, da svojo digitalno varnost ocenjuje kot slabo. Odziv me je presenetil, saj kaže na trdno prepričanje uporabnikov, da je njihova digitalna varnost vsaj zadostna kljub temu, da jih skoraj polovica uporablja enaka gesla za več storitev (*Graf 4: Uporaba enakih gesel*).

Ocenite zanesljivost naslednjih metod prijavljanja



Graf 1: Zanesljivost metod

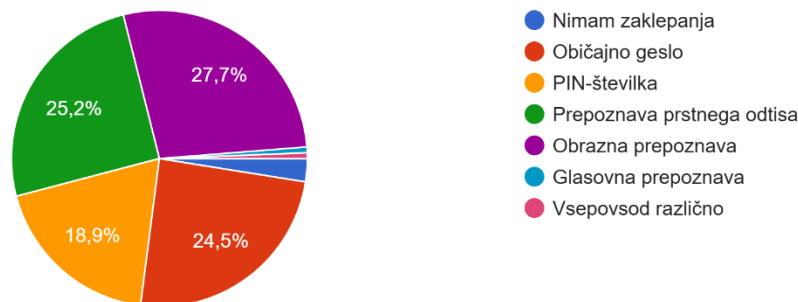
Vprašani so zanesljivost metod prijavljanja ocenili po naslednjem vrstnem redu (od najbolj zanesljive do najmanj zanesljive):

1. Prstni odtis
2. Navadno geslo
3. Obrazna prepoznavna
4. PIN-koda
5. Glasovna prepoznavna

Presenetilo me je, da so vprašani v povprečju navadno geslo ocenili kot bolj zanesljivo kot obrazno prepoznavo. Predvidevam, da zaradi težav pri prepoznavi, do katerih lahko pride zaradi okoljskih dejavnikov (npr. nošenje maske, očal ali slaba svetloba).

Katero metodo prijavljanja najpogosteje uporabljate za svoje naprave?

159 odgovorov

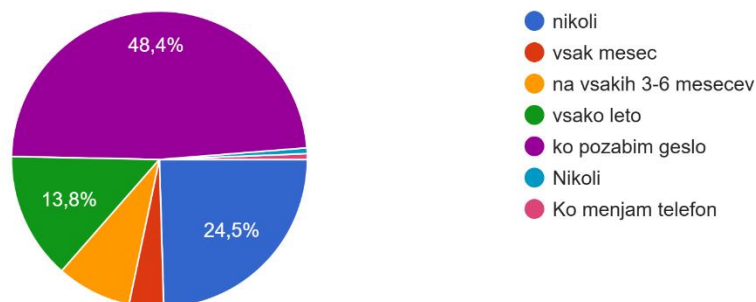


Graf 2: Najpogostejša metoda prijavljanja

Največ uporabnikov se v svoje naprave prijavlja z biometričnimi gesli (več kot polovica). Presenetila me je razširjenost navadnih gesel, saj sem pričakoval, da bo zaradi lažjega in hitrejšega vnosa več vprašanih uporabljajo PIN-kodo.

Kako pogosto menjate svoja gesla?

159 odgovorov

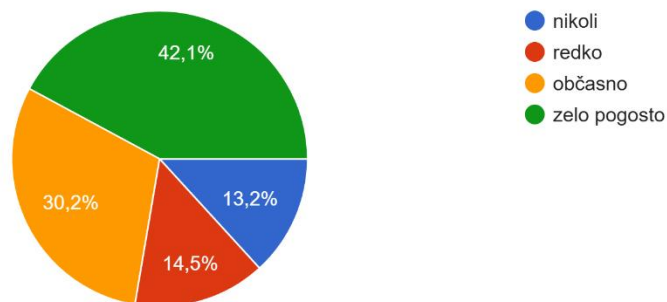


Graf 3: Ferkvenčnost menjave gesel

Skrb vzbujajoč je podatek, da skoraj polovica anketirancev geslo menja šele, ko pozabijo geslo. Iz tega lahko sklepam, da le ti ne vodijo evidence o svojih geslih oziroma jih ne hranijo na primernih mestih. V času, ko vse več storitev zahteva račun, je pomembno voditi evidenco svojih gesel ter jih tudi hraniti na varen način.

Kako pogosto uporabljate enaka gesla za različne račune?

159 odgovorov

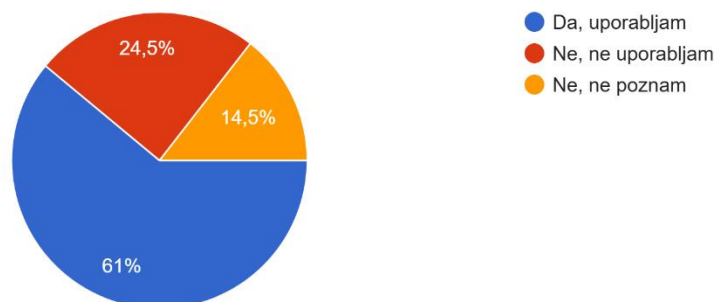


Graf 4: Uporaba enakih gesel

Več kot 2/3 vprašanih uporabljata enaka gesla za iste račune zelo pogosto ali občasno, kar predstavlja resno varnostno tveganje. Uporaba enakega gesla na več platformah pomeni, da lahko uspešen vdor v en račun napadalcem omogoči dostop do več drugih računov, npr. e-pošte, družbenih omrežij, spletnega bančništva ali drugih zaupnih informacij. V literaturi takšno serijo vdorov pogosto imenujemo napad veriženja gesel, ko napadalci pridobijo eno geslo in ga preizkušajo na drugih spletnih mestih. Mogočo rešitev za ta problem predstavljajo upravitelji gesel, ki so koristni predvsem za shranjevanje večjega števila gesel.

Ali uporabljate dvostopenjsko preverjanje (2FA)?

159 odgovorov



Graf 5: Dvostopenjsko preverjanje

Večina vprašanih uporablja dvostopenjsko preverjanje, kar kaže na vedno večje zavedanje o pomenu dodatne varnosti v prijavi v spletne storitve. Nekatera podjetja metodo že uvajajo kot obvezno pri registraciji v storitev. Le manjši delež le teh z metodo 2FA ni seznanjen.

- Tisti, ki so na vprašanje o vdoru v njihov račun odgovorili z »da«, so na podvprašanje *»Kaj je po vašem mnenju bil vzrok za uspešen napad?«* večinsko navedli naslednje vzroke:
- uporaba istih gesel za več računov
- slabo (uganljivo) geslo
- »phising« ali ribarjenje oz. klik na nevarno povezavo

4.2 Udeležba na konferenci CIOSEC 2024

Povzetek konference je priložen v poglavju Priloge.

Kljub dobrim zaščitnim ukrepom vedno obstaja tveganje za napad na velike sisteme, posledice katerih imajo velik vpliv na organizacije in posameznika. Gre za t. i. zasnova "črnega laboda"; nepričakovani dogodki so redki vendar imajo velik vpliv na družbo in gospodarstvo. V zadnjih letih trend vedno bolj prefinjenih napadov na večje organizacije narašča. Razvoj novih tehnologij za preprečevanje tveganj pa bo zahteval znanje, zato je aktualen problem na to temo tudi digitalna pismenost in izobraževanje. Kdo bo izobraževal organizacije in posameznike za ravnanje v primeru napada in izvajanje zaščitnih ukrepov? Izobraževanja strokovnjakov in skrbnikov sistema na tem področju ne bodo zadostovala, saj je najpomembnejši akter takoj za napadom uporabnik sam.

Ker tveganja tudi zaradi človeškega dejavnika nikoli ni mogoče v celoti preprečiti, je pomembno učinkovito obvladovanje položaja z hitrim obveščanjem vseh vpletenih in analiza šibkih točk.

Z razvojem se spreminja tudi vloga strokovnjakov za informacijske tehnologije (IT), ki so v prejšnjih desetletjih imeli vlogo predlaganja inovativnih rešitev, danes pa morajo pogosto kritično oceniti, ali je nadgradnja / posodobitev sistema po najnovejši tehnologiji sploh smiselna in varna za uporabnike.

Zavedati se moramo, da umetna inteligenca ne more nadomestiti človeka, saj mi odločamo o uporabi in vlogi, ki jih lahko ima UI v družbi. Omenjeni govorniki poudarjajo, da je ključnega pomena tudi prenašanje znanja na naslednje generacije; zavedanja, da se ne smemo povsem zanesti na UI.

4.3 Intervju

Da bi izvedel več o biometričnih geslih in vlogi umetne inteligence na področju kibernetike sem 15. novembra 2024, sem opravil pisni intervju z dr. Srdanom Škrbićem. Celoten intervju je priložen v poglavju Priloge.

“Glavna razlika med biometričnimi in tradicionalnimi gesli je način avtentikacije”. Biometrična gesla so unikatna, saj temeljijo na težko spremenljivih vedenjskih lastnostih posameznika, medtem ko si tradicionalna gesla izmislimo sami in jih je zato mogoče lažje okrasti ali uganiti.

Menjava ukradenih gesel (sploh biometričnih) je zapleten postopek, ki prinaša določena tveganja. Ključnega pomena je takojšnje ukrepanje uporabnika.

Dodaten sloj zaščite je tudi t. i. 2-stopenjsko preverjanje (2FA), ki pa ga ni mogoče zagotoviti v nekaterih okoljih, kjer je uporaba telefona prepovedana (npr. šolah). Kot mogočo rešitev dr. Škrbić predlaga vzpostavitev politik kibernetске varnosti, redna usposabljanja zaposlenih (in učencev) ter redno ocenjevanje tveganj.

Zaradi razvoja umetne inteligence in strojnega učenja bodo kibernetски napadi v prihodnosti postali še bolj prefinjeni. Umetna inteligenca bo imela pomembno vlogo pri preprečevanju in zmanjševanju tveganj. Napredek odpira številna vprašanja tudi o problematiki zasebnosti, ki je ob vse večjem pretoku informacij vedno bolj ogrožena.

5 RAZPRAVA

5.1 H1: Primerjava biometričnih in tradicionalnih gesel

Hipoteza: *Uporaba biometričnih gesel je varnejša kot uporaba tradicionalnih metod prijavljanja, vendar so le ta težje zamenljiva v primeru kraje.*

Biometrična gesla so naprednejša oblika avtentikacije, saj zagotavljajo večjo varnost v primerjavi s tradicionalnimi gesli, saj predstavljajo unikatne fizične ali psihološke značilnosti posameznika. Pomembno vlogo ima varnost samega sistema, saj lahko slab sistem poveča možnost kraje in zlorabe.

Največja pomanjkljivost biometričnih gesel je njihova nezamenljivost v primeru kraje. Njihova unikatnost sicer nudi dodaten sloj zaščite, vendar hkrati predstavlja veliko tveganje. Ponarejanje biometričnih vzorcev s pomočjo umetnih odtisov ali 3D-modelov obraza napadalcem omogoča nepooblaščen dostop do občutljivih informacij.

Poudariti je treba tudi zakonodajne in etične vidike v zvezi z varovanjem biometričnih podatkov. Kljub dobri varnosti se pojavljajo vprašanja zasebnosti in omejenost nadzora nad lastnimi podatki. Uporabniki imajo pogosto pomisleke glede tega, kdo ima dostop do njihovih podatkov, zato morajo storitve zagotoviti preglednost ter izvajati stroge varnostne protokole pri upravljanju z le temi.

5.2 H2: Uporabniška izkušnja in zanesljivost biometričnih sistemov

Hipoteza: *Uporabniki biometrične sisteme ocenjujejo kot bolj varne in zanesljive, če je dobra tudi uporabniška izkušnja.*

Uspešnost biometričnih sistemov ni odvisna le od njihovih tehničnih značilnosti, temveč tudi od zaznavanja uporabnikov. Raziskave so pokazale, da ljudje s pozitivno uporabniško izkušnjo pogosteje verjamejo, da so biometrična gesla varnejša in bolj zanesljiva. Za dobro uporabniško izkušnjo sta ključni preprosta uporaba, hitra prepoznavna, majhna potreba po pomnjenju gesla in nizka stopnja napak, povezanih s prepoznavo (RISKY OR).

Vzrok, da je med dijaki in študenti najbolj pogost način prijave obrazna prepoznavna, bi lahko pripisali dejstvu, da gre za najhitrejšo in najbolj enostavno metodo prijave. Pri branju prstnih odtisov lahko namreč pride do napak zaradi napačnega pozicioniranja prstov. Nošenje mask ali očal ter poškodbe na delih telesa, ki so ključni za biometrično prepoznavo po navedbah uporabnikov pogosto povzročajo težave pri prijavljanju, kar posledično vpliva na zadovoljstvo.

Uporabniška izkušnja je subjektivna in je odvisna od vsakega posameznika. Pogosto je tesno povezana z varnostjo in zasebnostjo. Prepričanja in mnenja zaradi kulturnih, religioznih ali drugih vzrokov prav tako vplivajo na mnenje glede uporabe in shranjevanja posameznikovih unikatnih lastnosti v podatkovne baze. Uporabniki, ki imajo občutek nadzora nad svojimi biometričnimi podatki, so bolj naklonjeni uporabi le teh, vendar se v primeru zlorabe ali neprimerne hrambe pojavi nezaupanje do podjetij, ki upravljajo takšne sisteme.

Da bi zagotovili večje zaupanje v biometrične sisteme je pomembno razviti rešitve, ki upoštevajo potrebe uporabnikov. Izboljšanje natančnosti sistemov ter ponujanje več metod prijavljanja za različne položaje ter zagotavljanje natančnih informacij kako se podatki shranjujejo in uporabljajo so ključni dejavniki, ki prispevajo k preglednosti in pozitivnemu javnemu mnenju.

5.3 H3: Uporaba biometričnih gesel med dijaki in študenti

Hipoteza: *Študentje in dijaki pogosteje uporabljajo biometrična gesla, saj jih ocenjujejo kot bolj varna v primerjavi z drugimi načini prijave.*

Rezultati opravljene ankete in analiza strokovne literature potrjujeta to hipotezo. Raziskava o uporabi biometričnih metod prijavljanja med dijaki in študenti je pokazala, da večina mladih uporabnikov uporablja odklepanje naprave s prstnim odtisom ali obrazom. Biometrične metode dojemajo kot varnejše in bolj zanesljive ter enostavnejše za uporabo, saj ni potrebe po vnosu gesla, a se hkrati zavedajo, da umetna inteligenca tudi ogroža njihovo digitalno varnost.

Zaupanje v biometrične podatke temelji na prepričanju, da so le ti unikatni in zato bolj varni od npr. navadnih gesel. Uporabniki se prednosti biometričnih gesel dobro zavedajo, vendar le redko pomislijo, kako se ti podatki obdelujejo in shranjujejo, saj nimajo dovolj dobrega pogleda v to oziroma ker digitalno varnost dojemajo kot samoumevno vrednoto. Podjetja za svoja orodja nenehno izboljšujejo uporabniško izkušnjo, da bi uporabnikom zagotovila čim enostavnejšo uporabo.

Na drugi strani obstajajo pomisleki glede zasebnosti in varnosti shranjenih biometričnih podatkov, saj so nekatere študije pokazale, da kljub priljubljenosti biometričnih gesel veliko uporabnikov ne ve, kako se njihovi podatki uporabljajo in shranjujejo, saj ne preberejo pogojev.

6 DRUŽBENA ODGOVORNOST

Uporabnik mora biti odgovoren posameznik, ki kritično presodi, ali bo neki storitvi zaupal svoje podatke. Preden se registrira, se mora seznaniti s pogoji. Organizacije in podjetja morajo zagotoviti varno shrambo podatkov ter v primeru incidenta v čim krajšem času obvestiti vse vpletene in ravnati preudarno. Prav tako morajo ob zbiranju vseh vrst podatkov jasno nakazati uporabniku, katere podatke zbirajo in s kakšnim namenom ter kako jih hranijo. Vloga zakonodajalcev je redno posodabljanje zakonodaje na področju biometrije in varovanja podatkov ter dosledno kaznovanje kršiteljev. Za blaginjo vseh bi bila koristna redna izobraževanja učencev in dijakov ter delavcev, sistemskih skrbnikov sistemov in nasploh organizacij.

Ta raziskovalna naloga je družbeno odgovorna, saj obravnava ključne etične, psihološke in varnostne vidike uporabe biometričnih sistemov v času umetne inteligence. Z ozaveščanjem o tveganjih uporabe le teh opozarja na pomanjkljivosti in dejavnike tveganja ter ponuja vpogled v uporabniško izkušnjo. Glavna vloga te raziskave je izobraževanje lokalne skupnosti, za namen krepitev zaupanja v tehnologijo, ki igra vse večjo vlogo v našem vsakdanjem življenju.

Da bi izsledki naloge dobili praktično vrednost, sem naredil naslednje:

- izvedel krajšo učno uro v 1. letniku informatike
- predstavil raziskovalno nalogo in uporabo orodja ElevenLabs na informativnih dnevnikih
- izdelal plakat s koraki do izboljšave lastne digitalne varnosti (priložen v poglavju Priloga)

Izvedeno bom natančneje predstavil na zagovoru naloge.

7 SKLEP

Biometrična gesla so med dijaki in študenti postala priljubljena alternativa tradicionalnim načinom avtentikacije, saj gre za hitrejši in enostavnejši način prijave, ki je hkrati varnejši zaradi unikatnih fizičnih in psiholoških lastnosti posameznika. Kljub prednostim, ki jih prinašajo, se še vedno pojavljajo etične dileme in zadržki glede zasebnosti ter varovanja podatkov, pa tudi pomisleki glede posledic v primeru zlorabe.

Raziskava je pokazala tesno povezanost uporabniške izkušnje z dojemanjem biometričnih sistemov. Če sistem ne deluje natančno, torej pogosto zavrne uporabnika, bo le ta najverjetneje v zvezi z biometričnim načinom prijave imel negativno mnenje. Na kakovost prepoznave lahko vplivajo tudi drugi dejavniki, kot so svetloba ali poškodbe na ključnih delih telesa.

Zaključim lahko, da so biometrična gesla bistven prispevek k področju kibernetike varnosti, vendar niso popolna rešitev. Nadaljnji razvoj umetne inteligence, kvantnega računalništva in strojnega učenja bodo doprinesel številne nove izboljšane alternative, vendar se moramo zavedati, da vdorov nikoli ni mogoče zagotovo preprečiti. Uporabniki in podjetja, ki upravljajo podatke morajo stremeti k minimaliziranju kibernetičnih tveganj, za kar bo pomembno ozaveščanje o digitalni varnosti, kjer bodo ključno vlogo imele tudi izobraževalne institucije in zakonodajalci.

Največji osebni izziv mi je predstavljala časovna razporeditev, saj je to področje, na katerem se še moram precej izboljšati. Odlaganje s pisanjem na kratki rok nima večjih posledic, problem nastane šele, ko se nevarno približuje rok oddaje. Sprotno pisanje je na kratki rok morda manj prijetno, vendar ne predstavlja tolikšnega stresa. Pridobljeno lekcijo sem si dobro zapomnil in jo bom upošteval v svoji naslednji raziskovalni nalogi.

Predlog za nadgradnjo: Nalogo bi lahko v prihodnje še dodatno izboljšal tako, da bi raziskal vpliv digitalne varnosti na psihološko percepcijo uporabnika.

8 VIRI IN LITERATURA

- Adegbenle, A., Nzenwata, U., Rotimi, O., Oreoluwa, A., & James, A. (2020). *ETHICS IN BIOMETRICS AUTHENTICATION*. 8(9).
- Britannica Library. (2024). *Biometrics*. <https://library-eb-co-uk.eviri.ook.sik.si/levels/adult/article/biometrics/641923>
- Fran (2024). *Fran/iskanje/biometrija*. <https://fran.si/iskanje?View=1&Query=biometrija>
- Gabriel Vigariu, M., & Marin, C.-A. (2024, januar 1). *The cyberpsychology of biometric information ecosystems. Sustainability or digital totalitarianism? | EBSCOhost*. <https://doi.org/10.33727/JRISS.2024.1.10:83-87>
- Google (2024). *Passwordless by default: Make the switch to passkeys*. <https://blog.google/technology/safety-security/passkeys-default-google-accounts/>
- IEEE Journals & Magazine / *IEEE Xplore*. (b. d.). *Biometrics: Trust, But Verify*. Pridobljeno 12. februar 2025, s <https://ieeexplore.ieee.org/abstract/document/9581287>
- Kos, David (januar 2015). *Ali bi dovolili svojemu delodajalci, da vam pod kožo vgradi čip?* Pridobljeno 10. februar 2025, s <https://siol.net/novice/posel-danes/ali-bi-svojemu-delodajalcu-dovolili-da-vam-pod-kozo-vgradi-cip-35736>
- [Microsoft Security. (2024). *What Is Two-Factor Authentication (2FA)?* Pridobljeno 12. februar 2025, s <https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa>
- Syed Idrus, S. Z., Cherrier, E., Rosenberger, C., & Schwartzmann, J.-J. (2013). A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, 7(5), 95–107.
- The Social Impact of Deepfakes*. (b. d.). <https://doi.org/10.1089/cyber.2021.29208.jth>
- Waizel, G. (2024). Bridging the AI divide: The evolving arms race between AI- driven cyber attacks and AI-powered cybersecurity defenses. *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings, 1*, 141–156.

PRILOGE

Anketni vprašalnik

Obraz, prst in koda: Umetna inteligenca in biometrija

Pozdravljeni! V sklopu projekta *Mladi za napredek Maribora* pišem raziskovalno nalogo *Obraz, prst in koda* v kateri bom ugotavljal zanesljivost različnih vrst gesel in preučeval vlogo umetne inteligence na področju kibernetne varnosti.

Prosim te, da mi pomagaš tako, da rešiš kratko anketo. Sodelovanje je **anonimno**.
Hvala za tvoj čas!

* Nakazuje obvezno vprašanje

1. Vaš biološki spol *

Označite samo en oval.

Moški

Ženski

2. Šolanje *

Označite samo en oval.

dijak

študent

3. Kako ocenjujete svojo digitalno varnost? *

Označite samo en oval.

1 2 3 4

slabo odlično

4. Katero metodo prijavljanja najpogosteje uporabljate za svoje naprave? *

Označite samo en oval.

- Nimam zaklepanja
- Običajno geslo
- PIN-številka
- Prepoznavna prstnega odtisa
- Obrazna prepoznavna
- Glasovna prepoznavna
- Drugo:

5. Ocenite zanesljivost naslednjih metod prijavljanja *

Označite samo en oval na vrstico.

	1 - zelo nezanesljivo	2	3	4 - zelo zanesljivo
Navadno geslo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PIN-številka	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prstni odtis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Glasovna prepoznavna	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Obrazna prepoznavna	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. Kako pogosto menjate svoja gesla? *

Označite samo en oval.

- nikoli
- vsak mesec na vsakih 3-
- 6 mesecev
- vsako leto
- ko pozabim geslo
- Drugo:

7. Kako pogosto uporabljate enaka gesla za različne račune? *

Označite samo en oval.

- nikoli
- redko
- občasno
- zelo pogosto

8. Ali umetna inteligenca (UI) izboljšuje ali ogroža varnost uporabnikov? *

Označite samo en oval.

- izboljšuje
- ogroža
- oboje hkrati

Dvostopenjsko preverjanje 2FA (oz. avtentikacija)

Metoda prijavljanja, ki vključuje uporabo dodatne naprave ali kode (npr. QR koda ali SMS).

Primer:

- QR koda, ki jo skeniramo, da se prijavimo koda, ki jo
- prejmemo v SMS-u (koda za preverjanje)

9. Ali uporabljate dvostopenjsko preverjanje (2FA)? *

Označite samo en oval.

- Da, uporabljam
- Ne, ne uporabljam
- Ne, ne poznam

10. Ali ste že bili tarča kibernetkega napada / vdora v račun? *

Označite samo en oval.

- Da *Preskočite na vprašanje 10.1*
- Ne *Preskočite na vprašanje 11*

10.1 Kaj je po vašem mnenju bil vzrok za uspešen napad? *

Označite samo en oval.

- Slabo geslo
- Phising ("ribarjenje")
- Uporaba istega gesla za več računov
- Nisem se odjavil/-a iz naprave
- Drugo:

11. Ali menite da so biometrični podatki (npr. prstni odtisi) unikatni? *

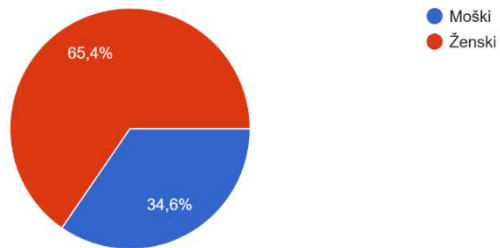
Označite samo en oval.

- Da
- Ne

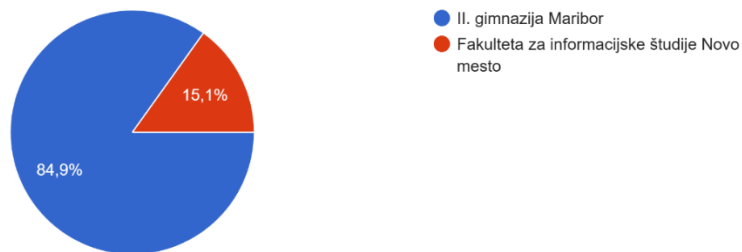
NEOBVEZNO: Če bi želeli prejeti rezultate raziskave, vnesite svoj e-mail.

Rezultati ankete

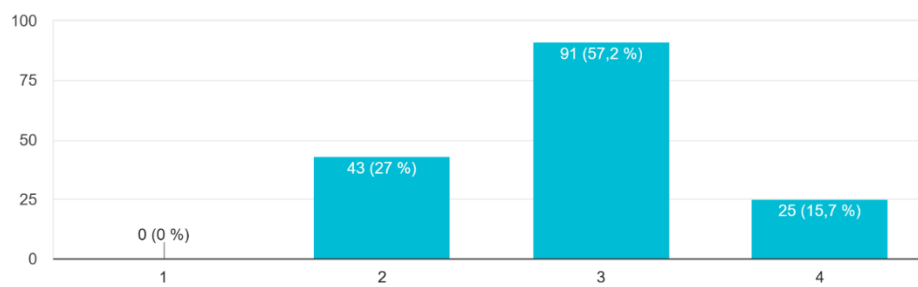
Vaš biološki spol
159 odgovorov



Šola
159 odgovorov

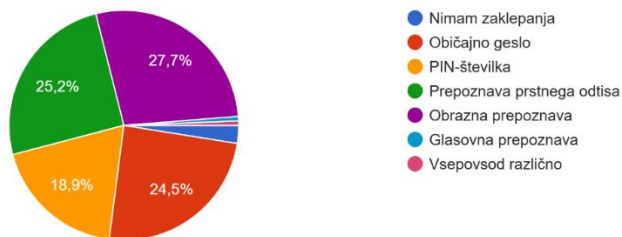


Kako ocenjujete svojo digitalno varnost?
159 odgovorov

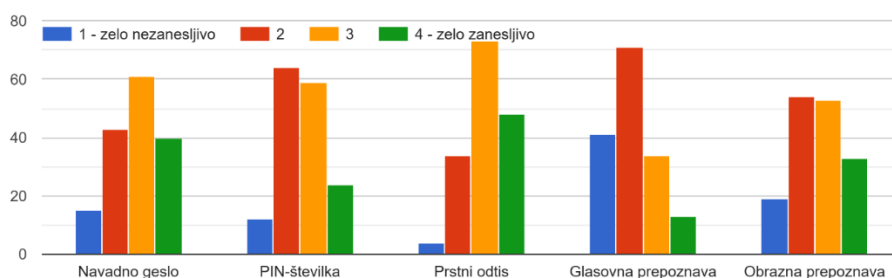


Katero metodo prijavljanja najpogosteje uporabljate za svoje naprave?

159 odgovorov

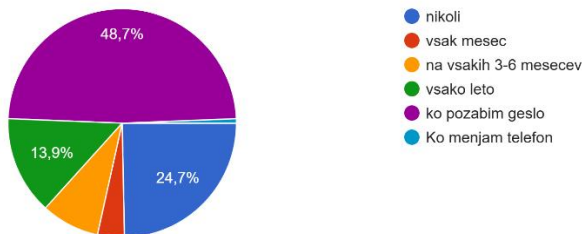


Ocenite zanesljivost naslednjih metod prijavljanja



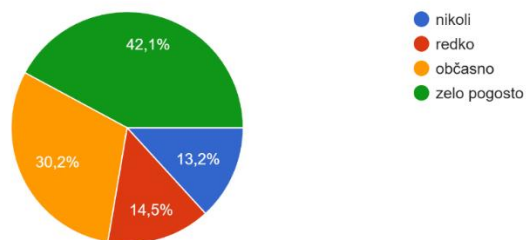
Kako pogosto menjate svoja gesla?

158 odgovorov



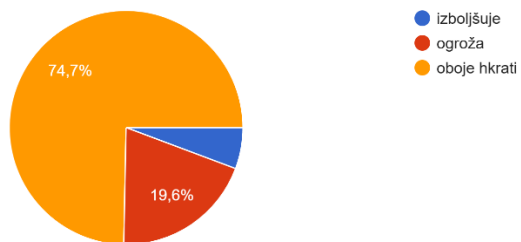
Kako pogosto uporabljate enaka gesla za različne račune?

159 odgovorov



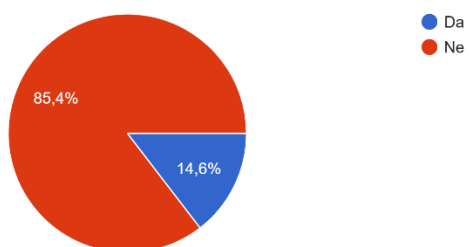
Ali umetna inteligenca (UI) izboljšuje ali ogroža varnost uporabnikov?

158 odgovorov



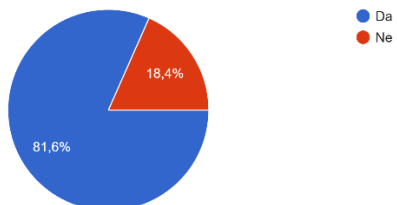
Ali ste že bili tarča kibernetnega napada / vdora v račun?

158 odgovorov



11. Ali menite da so biometrični podatki (npr. prstni odtisi) unikatni?

158 odgovorov



Celoten intervju

1. V čem se biometrična gesla po varnosti razlikujejo od tradicionalnih? Ali obstajajo situacije, v katerih je tradicionalno geslo varnejše kot biometrično?

Glavna razlika med biometričnimi in tradicionalnimi gesli je v načinu avtentikacije. Medtem ko so tradicionalna gesla odvisna od uporabnika, ki vnese kombinacijo znakov za pridobitev dostopa, biometrija za preverjanje pristnosti uporablja edinstvene fizične ali vedenjske lastnosti, kot so prstni odtisi ali poteze obraza. Torej, biometrična gesla in tradicionalna gesla predstavljajo dva različna pristopa k avtentikaciji uporabnikov, od katerih ima vsak svoje varnostne posledice.

Posledično, biometrična gesla je težko posnemati ali ukrasti. Nasprotno pa tradicionalna gesla pogosto temeljijo na znanju in jih je mogoče uganiti, deliti ali ukrasti. Biometrične sisteme bi torej ocenil kot na splošno bolj odporne na običajne metode napada.

Medtem ko biometričnih lastnosti ni lahko spremeniti, je tradicionalna gesla enostavno posodobiti. To možnost lahko razumemo kot prednost tradicionalnih gesel. V situacijah, ko biometrični sistemi odpovejo (na primer mokri ali premrzli prsti), so tradicionalna gesla zanesljiva rezervna metoda. Poleg tega shranjevanje biometričnih podatkov povzroča precejšnja vprašanja zasebnosti.

2. Kaj lahko storimo v primeru, da so bili naši biometrični podatki ukradeni? Kako učinkoviti so postopki menjave biometričnih podatkov (npr. zamenjava prstnega odtisa)? Kakšne so dolgoročne posledice takšne kraje podatkov?

Če so biometrični podatki ukradeni, jih ni mogoče spremeniti tako kot gesla, ali pa ni tako enostavno. Čeprav obstajajo mehanizmi za zamenjavo ukradenih biometričnih podatkov, niso brezhibni in prinašajo tveganja. Postopek zamenjave je v bistvu zajemanje novih biometričnih vzorcev in njihovo preverjanje glede na obstoječe zapise. Dolgoročne posledice takšne kraje so hude in zahtevajo stroge zaščitne ukrepe in pravne okvire za zaščito biometričnih podatkov posameznikov.

V primeru kraje biometričnih podatkov je zelo pomembno takojšnje ukrepanje. Na primer, obrnemo se na ustrezne organe in pozorno spremljamo svoje račune za morebitne

nepooblaščne transakcije. Zavarujemo svoje naprave s posodobitvijo načinov prijave in gesel ter preverjanjem zlonamerne programske opreme.

3. Kakšne alternative za 2FA (dvostopenjsko preverjanje) bi lahko uporabili v okoljih, kjer uporaba telefona ni dovoljena (npr. šolah)? Kako lahko izobraževalne ustanove pomagajo pri zagotavljanju digitalne varnosti?

Teoretično gledano dvostopenjsko preverjanje oziroma avtentikacija temelji na nečem, kar imamo ali nečem, kar smo. Mobilni telefon je torej običajno prva izbira za preverjanje, ne glede na to, ali uporabljamo storitev SMS, authenticator aplikacijo ali podobno. Alternativne metode so biometrično preverjanje, uporaba email-a za pošiljanje enkratnega ključa, uporaba fizičnih kartič, uporaba strojnih varnostnih ključev in podobno.

Kar zadeva izboljšanje in zagotavljanje digitalne varnosti v izobraževalnih ustanovah, bi lahko predlagal naslednje: vzpostavitev politik kibernetске varnosti, redni programi usposabljanja za učence in osebje, vlaganje v napredna varnostna orodja (firewall, 2FA), ter izvajanje rednih ocen tveganja.

4. Kako se trenutno razvijajo trendi v kibernetски varnosti? Kako se bo to področje razvijalo v prihodnjih letih in kako bo to vplivalo na posameznike in podjetja?

To vprašanje je zelo široko in težko, saj je težko podati pravilen odgovor o prihodnjih trendih. V prvi vrsti trenutni trendi vsekakor vključujejo uporabo umetne inteligence in strojnega učenja za odkrivanje in ublažitev groženj. Kot drugi trend, bi morda omenil vprašanje zasebnosti na spletu (privacy issues) in razvoj različnih tehnologij za izboljšanje zasebnosti (privacy enhancing). S preходом na oblačne storitve (cloud services) je tudi zagotavljanje varnosti oblačnih okolij postalo ena glavnih skrbi.

Kako se bo področje razvijalo v prihodnosti? Daljši razvoj področja bo poganjal napredek v umetni inteligenci in strojnem učenju, ki bo še povečal zmožnosti odkrivanja groženj in odzivanja. Težko je napovedati, kako se bo razvijalo, vendar kvantno računalništvo predstavlja tako priložnosti za večjo varnost kot izzive, saj ogroža obstoječe metode šifriranja. Na splošno, ko bodo kibernetске grožnje postajale bolj sofisticirane (z uporabo AI, ML in morda kvantnega računalništva), bodo morala podjetja in posamezniki biti pripravljeni sprejeti nove varnostne ukrepe in vlagati v zaščito svojih podatkov in operacij.

Zapiski konference CIOSEC 2024

ZAPISKI KONFERENCE CIOSEC 2024

predavanja na temo kibernetске varnosti

Janko Kersnik: Prepoznavanje kibernetских tveganj

- kibernetско tveganje: napadalec sproži grožnjo, ki izrabi pomanjkljivost (ranljivost) sistema → sledijo posledice za uporabnike in organizacije
- primer vektorjev napada: »phising«
- kibernetска sredstva: omrežja 5G, uporabniška imena in gesla, oblačne storitve
- **protokol ASMR**: za učinkovito proaktivno varnost je potrebno:
 - hitro razkrivanje površin napada
 - zmanjševanje tveganja z preventivnimi ukrepi
 - ocenjevanje in prioritizacija tveganj
- protokol omogoča lažjo vidljivost, jasnost in avtomatizacijo varnostnih protokolov
- indeks izpostavljenosti tveganju se izračuna na podlagi strežnikov, oblačnih storitev, internetnih sistemov in storitev za uporabnike izven organizacije
- kibernetско tveganje predstavlja tudi **poslovno tveganje**
- vloga UI: lažja in hitrejša diagnostika (prepoznavanje tveganj in napadov) ter predlogi za izboljšave sistema

mag. Miha Ozmek: zakonodaja o informacijski varnosti

- trenutna zakonodaja na področju informacijske varnosti sistemov v EU:
 - DORA regulacija
 - NIS 2 direktiva
 - CRA
- kljub majhnim tveganjem vedno obstaja verjetnost za napad na velike sisteme, ki imajo velik vpliv in posledice na ljudi in organizacije
- koncept črnega laboda: nepričakovani dogodki so redki vendar imajo velik vpliv na družbo in gospodarstvo
- v zadnjih letih **trend napadanja večjih organizacij narašča**; napadi so hitrejši, pogostejši in bolj sofisticirani zaradi pojava novih tehnologij in uporabe »machine learninga« in umetne inteligence
- odpornost varnostnih sistemov: nenehna pripravljenost da gre »vse po zlu« in rezervni načrti za krizne situacije ki omogočajo neprekinjeno poslovanje

- tveganja ni mogoče v celoti preprečiti → pomembno je učinkovito obvladovanje situacije (hitro obveščanje vseh vpletenih in analiza šibkih točk)

Okrogla miza o prihodnosti kibernetike, poklicev in UI

pojavljanje novih tehnologij: napadalci vedno korak odspredaj

- pomembnost izobraževanja posameznikov in organizacij
- **PROBLEM:** Kdo bo izobraževal posameznike in organizacije o kibernetiki varnosti?
- razvoj bo vplival na iznajdbo novih načinov napada; nepridipravi bi lahko podtikali napačne informacije novejšim strojnimi modelom učenja → dezinformacije («fake news»)!
- spreminjanje vloge zaposlenih v IT
 - prejšnje desetletje: predlaganje inovativnih rešitev
 - danes: kritično ocenjevanje smiselnosti uporabe najnovejših tehnologije (premišljeno sprejemanje novih varnostnih tehnologij)
- **spremembe poklicev in razvoj novih področij;** porast strokovnjakov na področju upravljanja s podatki in zmanjšanje št. sistemskih strokovnjakov in razvijalcev aplikacij
- UI nas ne bo nadomestila → mi odločamo o uporabi in se vedno znova prilagajamo
- nasvet za prihodnje generacije: zavedanje, da se ne smemo povsem zanašati na UI

Hekerji ne počivajo!



6 preprostih korakov za lastno varnost na internetu

Uporaba varnih gesel 01



Uporabljaljaj močna gesla, nikoli enakih za več računov!

02 Zaščitni ukrepi

Uporabljaljaj 2-stopenjsko preverjanje (2FA).



Kritična presoja 03



Če je predobro, da bi bilo res, ne zaupaj lažnim sporočilom.

04 Digitalne sledi

Redno briši piškotke spletnih strani in ne shranjuj gesel v brskalnikih.



Zavedanje posledic 05



Razmisli, kakšne bi bile posledice, če bi bilo tvoje geslo ukradeno.

06 Redno posodabljanje

Uporabljaljaj požarni zid in programe za zaščito (antivirus).



Skeniraj QR kodo in preveri, kako varen/varna si!

