DIGITALNA SAMOOBRAMBA

VARNOST IN ZAŠČITA V INFORMATIKI

Roman Herlah, mag. inž. inf. in tehnol. kom.
roman.herlah@gmail.com

MojeZnanje.si

INFORMACIJSKA VARNOST

Informacijska varnost je veda, ki se ukvarja z zaščito informacij in podatkov.

Informacijska varnost se nanaša na zaščito informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo, razkritjem, spreminjanjem ali uničenjem.

MojeZnanje.si

STROKOVNJAK ZA VARNOST

Strokovnjak, ki skrbi za informacijsko varnost je ključna oseba, odgovorna za zaščito informacijskih sistemov, podatkov in omrežij pred kibernetskimi grožnjami, ranljivostmi in napadi. Opravlja eno ali več od naslednjih aktivnosti:

- načrtovanje, izvedba, nadgrajevanje in upravljanje varnostnih rešitev,
- krpanje varnostnih lukenj,
- detekcija in odziv na kibernetske napade in druge varnostne grožnje,
- odpravljanje posledic napadov,
- opravljanje varnostnih pregledov in testov,
- osveščanje uporabnikov.

VAROVANJE PODATKOV

Zaščita osebnih informacij
Varovanje osebnih podatkov, kot so številke kreditnih kartic, osebni podatki in zdravstveni podatki, preprečuje krajo identitete in finančne goljufije.

Zagotavljanje poslovne kontinuitete
Varovanje podatkov pomaga preprečiti izpade storitev in poslovne motnje, ki lahko nastanejo zaradi napadov, izgube podatkov ali okvar sistemov.

Izpolnjevanje zakonskih in regulativnih zahtev
Mnoge države imajo zakonodajo, ki zahteva zaščito osebnih podatkov (npr. GDPR v Evropski uniji). Neupoštevanje teh zahtev lahko vodi do visokih kazni in pravnih težav.

Zaščita poslovnega ugleda
Škoda, ki nastane zaradi varnostnega incidenta ali izgube podatkov, lahko močno vpliva na zaupanje strank in ugled podjetja.

VAROVANJE PODATKOV

Preprečevanje finančne škode
Kibernetski napadi, kraje podatkov in drugi varnostni incidenti lahko povzročijo znatno finančno škodo.

Zaščita intelektualne lastnine
Podjetja pogosto hranijo dragoceno intelektualno lastnino, kot so poslovne skrivnosti, raziskave in razvojni podatki. Njihova zaščita je ključna za ohranjanje konkurenčne prednosti.

Etika in Zakonodaja
Varovanje podatkov odraža etično zavezo, da se spoštuje pravica posameznikov do zasebnosti in varnosti njihovih informacij.

ZAŠČITA DIGITALNIH PODATKOV

Varovati je potrebno predvsem podatke. Varovanje podatkov se začne (a ne konča!) z varovanjem fizične opreme, kjer so podatki nameščeni ali preko katere se do njih dostopa.

Informacijska zaščita podatkov obsega izpolnjevanje naslednjih varnostnih zahtev:

- **zaupnost** (ang. confidentiality) – Zagotavljanje, da informacije niso dostopne nepooblaščenim osebam.
- **celovitost** (ang. integrity) – Zagotavljanje, da se podatki ne spremenijo ali uničijo brez dovoljenja.
- **razpoložljivost** oz. dostopnost (ang. availibity) – Zagotavljanje, da so informacije dostopne, ko so potrebne.

KIBERNETSKI NAPADI

Kibernetski napad (ang. cyber attack) je kaznivo dejanje kot npr. poskus kraje, razkrivanja, spreminjanja, onemogočanja ali uničenja informacij z nepooblaščenim dostopom do računalniških sistemov.

Kibernetska grožnja je možnost, da se zgodi določen kibernetski napad.

Kibernetsko tveganje je možnost, da pride do incidenta, ki bo negativno vplival na varnost, zasebnost ali delovanje informacijskih sistemov.

Kibernetski vdor je nepooblaščeno dejanje, ki se izvede mimo varnostnih mehanizmov omrežja ali inf. sistema

https://www.varninainternetu.si/

RAČUNALNIŠKI VIRUSI IN ČRVI

RAČUNALNIŠKI VIRUS

Računalniški virus je zlonamerna programska koda, ki potrebuje gostitelja. Računalniški virus se širi podobno kot naravni (biološki) virus, torej tako, da okuži zdrave datoteke v računalniku in se z njihovo pomočjo razširja na ostale računalnike. Običajno v računalniku povzroča škodo ali pa vsaj motnje. Virusi so pogosto skriti v izvršljivih datotekah – programih ali v neizvršljivih datotekah kot so npr. Wordovi dokumenti ali slikovne datoteke.

RAČUNALNIŠKI ČRV

Računalniški črv je zlonamerni program, ki se razširja v računalniških omrežjih in se pri tem samodejno razmnožuje. Za svoje širjenje ne potrebuje gostitelja. Je samostojen program, ki se brez našega posredovanja samodejno širi na računalnike v omrežju.

ZNAKI OKUŽBE

- **Upočasnjeno delovanje računalnika**: Sistemi in programi delujejo počasneje kot običajno.
- **Pogosta sesutja ali zamrznitev sistema**: Računalnik se nepričakovano sesuva ali neodzivno zamrzne.
- **Nenavadna pojavna okna**: Pojav nepričakovanih oglasov ali opozoril, tudi ko ne uporabljate interneta.
- **Spremembe na domači strani brskalnika**: Domača stran brskalnika je spremenjena brez vaše odobritve.
- **Neavtorizirane spremembe sistemskih nastavitev:** Spremenjene nastavitve varnosti ali onemogočeni varnostni programi.
- **Povečana uporaba diska ali CPU**: Visoka poraba sistemskih virov tudi, ko računalnik ni aktiven.
- **Nepričakovana elektronska pošta:** Vaš e-poštni račun pošilja sporočila brez vašega vedenja.
- **Neobičajni programi ali procesi**: Na računalniku se pojavijo neznani programi ali se zaženejo neznani procesi.
- **Onemogočeni antivirusni ali varnostni programi**: Vaša varnostna programska oprema je nenadoma onemogočena ali ne deluje pravilno.

MojeZnanje.si

ZAŠČITA

Zaščita pred računalniškimi virusi je nujno potrebna v vsakem računalniškem sistemu. Uporabljati je treba zaupanja vredno protivirusno programsko opremo in jo redno posodabljati. Žal pa nas to ne varuje pred vsemi virusi.

Zato je potrebno še:

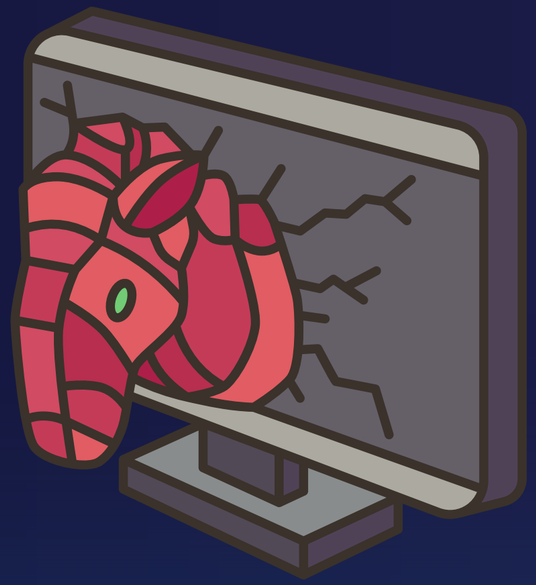
- redno izdelovati varnostne kopije podatkov,
- izogibanje klikanju na pojavne oglase,
- preverjanje e-poštnih prilog pred odpiranjem,
- pazljivost pri klikih na povezave v socialnih omrežjih ali na drugih spletnih straneh.

Poštni strežniki običajno preprečujejo sprejem prilog, ki imajo programske končnice. Ne morejo pa npr. preprečiti sprejema dokumenta (npr. v formatu .DOCX), ki ima vgrajen makro s škodljivo kodo.

TROJANSKI KONJI

Trojanski konj ali trojanec je vrsta virusa, ki se zažene s pomočjo prevare uporabnika. Uporabnik npr. misli, da je naložil koristen program. Zlonamerna programska koda je lahko:

- skrita v programih, ki jih uporabnik naloži iz interneta,
- skrita na spletnih straneh, ki jih uporabnik obišče,
- pripeta elektronski pošti,



Pogosto izkorišča ranljivosti programske opreme, s katero dostopamo do spleta

Trojanski konji ne delujejo samostojno, kot to počnejo virusi ali črvi, temveč potrebujejo, da jih uporabnik sam zažene.

ZNAKI OKUŽBE

- **Neznane aplikacije**: Na računalniku opazite nameščene programe, ki jih niste sami namestili.
- **Povečan promet v omrežju**: Velika aktivnost v omrežju brez vaše vednosti.
- **Povečana uporaba sistemskih virov**: Nenavadno visoka poraba CPU-ja, pomnilnika ali diska.
- **Pojav skrivnih datotek**: Na disku se pojavijo neznane, pogosto skrite ali zakodirane datoteke.
- **Onemogočeni varnostni programi**: Vaš antivirusni ali protivirusni program je izklopljen ali onemogočen brez vašega dovoljenja.
- **Nepojasnjene spremembe v nastavitvah**: Sistem nastavitve se samodejno spremenijo.
- **Neznani procesi v ozadju**: Sumljivi procesi delujejo v ozadju, kar lahko opazite preko upravitelja opravil.
- **Kraja gesel in osebnih podatkov:** Nepojasnjene prijave v vaše spletne račune ali sumljiva dejavnost v teh računih.
- **Preusmeritve brskalnika**: Vaš spletni brskalnik je preusmerjen na neznane spletne strani.
- **Počasno delovanje naprave**: Računalnik ali naprava deluje počasneje kot običajno brez očitnega razloga.

MojeZnanje.si

ZAŠČITA

- **Redno posodabljanje programske opreme**: Poskrbite, da so vaš operacijski sistem in vsi programi posodobljeni, saj tako preprečite izkoriščanje ranljivosti.
- **Uporaba zaupanja vrednega protivirusnega programa**: Uporabljajte zanesljiv antivirusni program, ki zaznava in odstranjuje trojanske konje.
- **Izogibanje odpiranju sumljivih e-poštnih priponk:** Ne odpirajte priponk ali povezav v e-poštnih sporočilih od neznanih pošiljateljev.
- **Prenos programske opreme le iz zaupanja vrednih virov:** Prenesite in nameščajte programe samo iz uradnih spletnih strani ali zaupanja vrednih virov.
- **Uporaba požarnega zidu**: Vklopite požarni zid, ki lahko prepreči nepooblaščen dostop do vašega sistema.
- **Redno varnostno kopiranje podatkov:** Redno varnostno kopirajte pomembne datoteke, da zmanjšate škodo v primeru okužbe.
- **Previdnost pri prenosu datotek:** Izogibajte se prenosu piratske programske opreme ali drugih datotek s sumljivih spletnih mest, ki so pogosto nosilci trojanskih konjev.

IZSILJEVALSKA ŠKODLJIVA KODA

Izsiljevalski programi (ang. ransomware) so ena večjih groženj na področju informacijske varnosti. Podjetjem povzročijo ogromno škode. Najpogosteje jih prenesejo uporabniki sami. Pred njimi se s protivirusno programsko opremo ne moremo ubraniti.

Današnjih izsiljevalski virusi uporabljajo zelo zapletena šifriranja. Zato imajo žrtve le dve možnosti: plačajo ali pa morajo vse okužene podatke izbrisati in jih nato na novo naložiti iz arhivov.

Po okužbi se na žrtvinem računalniku začne proces kodiranja oziroma kriptiranja vseh datotek, kot so tekstovne datoteke, slikovne datoteke in videodatoteke, elektronska pošta, baze podatkov itd. To pomeni, da se uporabniku zakriptira (zaklene) vse, razen nameščenih programov in bližnjic. Ob okužbi izsiljevalski virus ne zakriptira datotek samo na računalniku, ampak tudi na vseh drugih, v računalnik povezanih medijih, kot so mrežni in zunanji diski, USB...

https://www.nomoreransom.org/sl/index.html

ZAŠČITA

Najboljša obramba je backup oz. varnostna kopija vseh dokumentov!

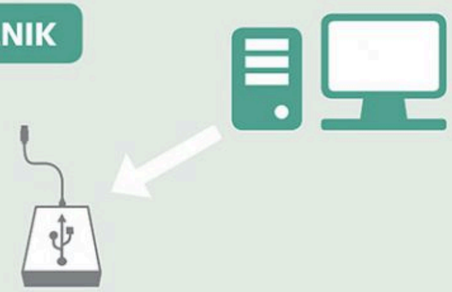
www.varninainternetu.si

VARNI NA INTERNETU

DANES JE DAN ZA BACKUP!

Ustvari varnostno kopijo pomembnih dokumentov, ki jih hraniš na osebnem računalniku, pametnem telefonu ali tablici. Upoštevaj dve pravili. **Vedno kopiraj podatke na dve ločeni lokaciji**, npr. eno kopijo na zunanji disk, drugo v oblak. Drugo pravilo pravi, da **ni dovolj le enkrat letno poskrbeti za kopije**, poskušaj jih izdelovati sproti, ko ustvarjaš nove vsebine (dokumente, fotografije).

1. RAČUNALNIK



ZUNANJI DISK

Backup podatkov na zunanji disk je najhitrejši in najenostavnejši način, tudi diski so cenovno že zelo dostopni. Po izdelavi backupa disk obvezno iztakneš iz računalnika.

OBLAK

Druga varnostna kopija naj bo v oblak, npr. Dropbox, Google Drive, OneDrive, SugarSync, Wuala, SpiderOak.

2. PAMETNI TELEFON ALI TABLICA

Android

GOOGLE RAČUN

Kontakti in koledar se sinhronizirajo z Google računom, za backup SMS sporočil si naloži eno od aplikacij za backup.

RAČUNALNIK

Vsaj dvakrat letno še poveži napravo z računalnikom in iz nje skopiraj fotografije in video posnetke.

OBLAK

Nastavi avtomatsko shranjevanje fotografij na Google+ ali drugo oblačno storitev, npr. Dropbox, OneDrive, Flickr.

iPad ali iPhone

iCLOUD

Če ne uporabljaš pogosto osebnega računalnika, sinhroniziraj iOS naprave v iCloud. Nasprotno, če pogosto uporabljaš osebni računalnik, želiš lokalno hrambo varnostnih kopij ali še dodatno backup lokacijo, shrani podatke s pomočjo iTunes.

RAČUNALNIK

Vsaj dvakrat letno še poveži napravo z računalnikom in shrani fotografije in video posnetke.

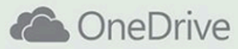
Windows telefon ali tablica

MICROSOFT RAČUN

Aplikacije, nastavitve, SMS sporočila, fotografije in video posnetki se sinhronizirajo z Microsoft računom.

RAČUNALNIK

Vsaj dvakrat letno še poveži napravo z računalnikom in kopiraj fotografije in video posnetke.



OBLAK

Nastavi shranjevanje fotografij in video posnetkov na OneDrive.

MojeZnanje.si

BACKUP V 3 KORAKIH I Hitra finta #2

Varni na internetu

ZAŠČITA

Okužbe z izsiljevalskimi virusi se zgodijo na različne načine:

- preko nevarnih in lažnih spletnih strani
- prenosa programske opreme in
- škodljivih priponk.

Nasveti za zaščito:

- Redno izvajate varnostno kopiranje podatkov na svojem računalniku in preprečite, da bi okužba z izsiljevalsko programsko opremo za vedno uničila vaše osebne podatke.
- Ne klikajte spletnih povezav v vsiljeni, neznani ali sumljivi elektronski pošti.
- Izogibajte se deljenju osebnih podatkov.
- Bodite previdni z občutljivimi podatki.
- Razmislite o uporabi večfaktorske avtentikacije pri pomembnih spletnih računih.
- Bodite previdni pri brskanju po internetu in ne klikajte sumljivih povezav, pop-up ali pogovornih oken.
- Iščite in prenašajte zgolj uradne verzije programske opreme s preverjenih spletnih strani.
- Za zaščito sistema pred izsiljevalsko programsko opremo uporabite zanesljivo protivirusno programsko opremo.
- Na svoje sisteme nikoli ne priklaplajte neznanih USB naprav.
- Zagotovite, da sta vaša varnostna programska oprema in operacijski sistem posodobljena.

NAPADI ONEMOGOČANJA

Napade, ki neposredno ali posredno povzročajo onemogočanje storitev, imenujemo napadi **DoS (ang. Denial of Service) in DDoS (ang. Distributed Denial of Service)**.
Napadalec omrežja nenehno obsipava z lažnimi zahtevami in ukazi, ki jih le-te ne zmorejo obdelati v realnem času. S tem onemogoči drugim uporabnikom dostop do omrežja in njegovih storitev, v določenih primerih pa celo njegovo sesutje. Napad se izvaja praviloma iz računalnika ali množice računalnikov, ki niso v napadenem omrežju.

MojeZnanje.si

ZNAKI OKUŽBE

- Povečana zakasnitev pri dostopanju do spletnih strani ali aplikacij
- Nedosegljive spletne storitve
- Nenavadno visok promet
- Nenavadno vedenje strežnika
- Povečana uporaba omrežnih virov
- Prekinitve povezave z omrežjem
- Pojav neobičajnih vzorcev prometa

MojeZnanje.si

SOCIALNI INŽENIRING

Socialni inženiring je izraz, ki se uporablja za široko paleto zlonamernih dejavnosti, ki se izvajajo s človeškim sodelovanjem. Osnovni princip takšnih napadov je preslepiti človeka, da stori nekaj, kar mu škodi. V mnogih primerih gre za pridobivanje informacij od ljudi. S temi informacijami nato izvedejo kaznivo dejanje, s katerimi oškodujejo žrtev neposredno ali posredno.

Socialni inženiring izkorišča človeška čustva in lastnosti, npr. zaupanje, pohlep, strah, radovednost, naivnost, osamljenost. Najbolj pogoste oblike socialnega inženiringa so:

- zvabljanje podatkov (ang. phishing),
- lažno predstavljanje (ang. impersonation),
- goljufije in prevare (ang. scam, fraud).

https://www.varninainternetu.si/nocnamora/#

MojeZnanje.si

LAŽNE SPLETNE TRGOVINE

Kot pri večini prevar, je ponudba izjemno privlačna. Problem nastopi, ko naročenega izdelka ne dobimo. Razen tega goljufom razkrijemo osebne podatke, ki jih lahko uporabijo za prodajo kriminalnih združbam in/ali za pošiljanje novih prevarantskih predlogov. Nekatere spletne trgovine ponujajo izdelke znanih blagovnih znamk po izjemno ugodnih cenah. V večini primerov gre za trgovine s ponaredki. Naročeno blago pošljejo, a ga na carini zasežejo. Kupec ostane brez denarja ter brez blaga in je lahko vesel, če ne plača še kazni.

www.varninainternetu.si

TEŽAVE PRI SPLETNEM NAKUPU. KAM PO POMOČ?

PRODAJALEC IZ SLOVENIJE IN EU Uveljaviš lahko reklamacijo (menjava blaga, vračilo kupnine). Za pomoč pri tem se lahko obrneš na potrošniške institucije.

ČE JE PODJETJE IZ SLOVENIJE

Tržni inšpektorat RS

gp.tirs@gov.si

01 280 87 00

ČE JE PODJETJE IZ EU, NORVEŠKE ALI ISLANDIJE

Evropski potrošniški center

epc.mgrt@gov.si

01 400 3729

PODJETJE IZVEN EU (ZDA, Kitajska, Srbija ...). Trgovci niso zavezani k slovenski oz. evropski zakonodaji, ki varuje potrošnika, zato niso dolžni upoštevati tvoje reklamacije.

'Kar dobiš, to imaš!'

LAŽNA SPLETNA TRGOVINA je samo kulisa z lepimi fotografijami, za spletno stranjo ne stoji podjetje.

1. Trgovec ne obstaja.
2. Plačanega izdelka ne dobiš.
3. Pogoste so zlorabe kreditnih kartic.

Če so lepe slike, slovenščina in domena .si, še ne pomeni, da je trgovec iz Slovenije!

VEDNO PREVERI PRODAJALCA!

- Kdo stoji za spletno trgovino (sedež podjetja)?
- Kje in kdaj je domena registrirana (https://whois.domaintools.com/)?
- Kakšna so mnenja drugih kupcev?

LAŽNA SPLETNA TRGOVINA?

1. **Neverjetno ugodna ponudba in vedno na zalogi** - kadar neka ponudba po ceni ter dostopnosti močno odstopa od ostalih, potem je to razlog za previdnost. Zelo pomembno je tudi, kako ste do te trgovine prišli. Kje ste zanjo izvedeli? Ste kliknili na oglas na spletni strani ali na družbenih medijih?

2. **Dobre novice se hitro širijo, slabe še hitreje -** poiščite ocene drugih kupcev ali uporabnikov spletne trgovine, spoznajte njihove izkušnje, kritike in mnenja.

3. **Preverite, kdo stoji za spletno trgovino** - preverite, ali so sploh navedeni kontaktni podatki podjetja, ki stoji za spletno trgovino. Se elektronski naslov ujema z naslovom spletne trgovine? Je na voljo zgolj kontaktni obrazec, brez kakršnihkoli drugih podatkov?

4. **Kaj pravijo podatki o domeni -** pogosto so podatki o registrantu oz. nosilcu domene veliko bolj zgovorni kot opisi, navedeni v sami spletni trgovini. Poiščite več informacij o domeni; predvsem bodite pozorni, kje in kdaj je bila domena registrirana in kateri kontaktni podatki so navedeni.

5. **Način plačila** - lažni spletni trgovci praviloma zahtevajo plačilo zgolj z uporabo kreditne kartice. Nekatere lažne trgovine omogočajo tudi plačilo po povzetju, ki pa žal ni garancija za varen nakup, saj se v paketih praviloma nahajajo ponaredki ali prazni paketi; vračilo tovrstnih produktov pa je praktično nemogoče.

LAŽNA SPLETNA TRGOVINA

Kontakt

https://www.converseslovenijaonline.com/contact_us.html

Brezplačna Dostava Za Nakupe Nad €80

CONVERSE

Women Men Boys Girls

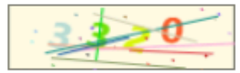
Domov

Kontakt

Full Name:

E-mail Naslov:

Preverjanje Računa



Opiši Svojo Skrb Tukaj:

Pošlji

POŠTA SLOVENIJE

Dragi kupec,

Obveščamo vas, da je bil paket, ki ga pričakujete, zaradi (nepopolnega/nepravilnega) naslova vrnjen v naše skladišče. Čim prej posodobite svoj domači naslov, da odpravite to težavo.

- Dostava: DPD
- ime dostave:
- teža: 1,9 KG
- številka za sledenje: YT22212114500355
- stari dobavni rok: 08.11.2022
- predviden rok dostave: 09.11.2022

Da bi zagotovili hitro dostavo vašega paketa, morate čim prej popraviti svoj domači naslov.

Če želite izvedeti več podrobnosti o vašem paketu in popraviti svoj naslov, skenirajte to kodo QR.

Upoštevajte, da vam bomo od jutri dalje zaračunavali strošek hrambe v višini 1 € na dan v vašem paketu.

S Spoštovanjem, Posta Slovenije

Pošta Slovenije

https://postaslovenije-redelivery.web.app/Confirm_Delivery?packet_id=8524568879

Pošta Slovenije

Moji paketi - 1 paket

Paket YT2227221276000355

Utež: 0,71 kg

Znesek: 1

€ 2,84

Predviden datum dostave

15/11/2022 - 17/11/2022

Izberite način plačila

VISA AMERICAN EXPRESS mastercard PayPal

Povzetek

Izpolnite svoje podatke

email@address.com

Polno ime

Naslov ceste

Mes

Poštna števill

Država	**Slovenija**
Prevoz	Brezplačno
Stroški pošiljanja (vključno z DDV-jem)	**€ 2,84**

Nadaljujte s plačilom

Privacy - Terms

DEEP FAKE

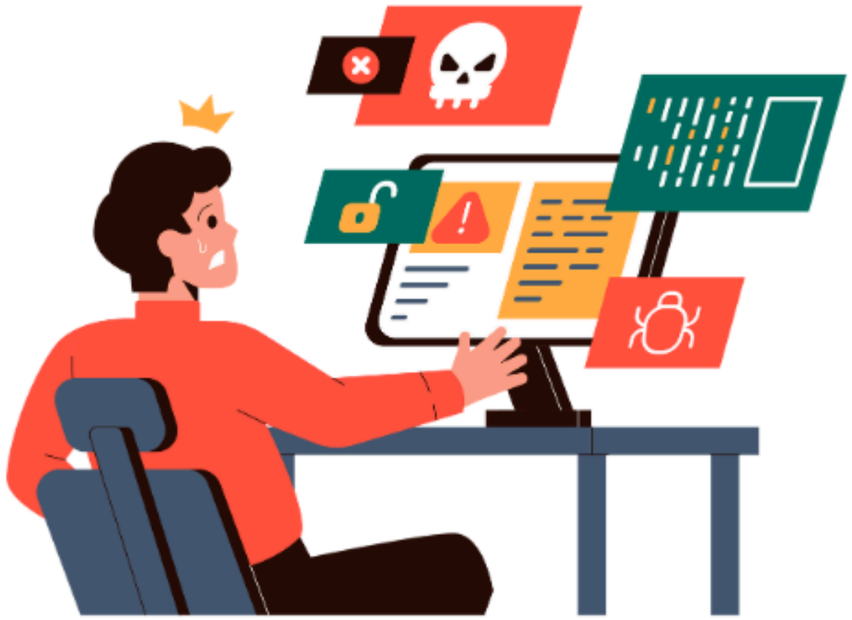
Tehnološko napredni kriminalci ustvarjajo sintetične vsebine ali globoke ponaredke (ang. deepfake). To so lažna in goljufiva besedilna, slikovna, zvočna ali video sporočila, ki so ustvarjena z umetno inteligenco ali strojnim učenjem. Izraz deepfake je nastal iz sestavljanke deep learning (globoko učenje) in fake (ponaredek). Gre za umetno narejeno vsebino.

ZAŠČITA

- Izobraževanje in ozaveščanje
- Osebna pazljivost
- Dvofaktorska avtentikacija (2FA)
- Preverjanje istovetnosti
- Filtriranje e-pošte in blokiranje sumljivih povezav
- Antivirusna in antiphishing orodja
- Previdnost pri nenavadnih zahtevah po denarju ali dostopu
- Vzpostavite politiko močnih gesel
- Uvajanje politike najmanjših pravic
- Omejitev deljenja informacij na spletu
- Redno spremljanje in pregled varnostnih politik

TOP 10 ČLOVEŠKIH RANLJIVOSTI NA SPLETU

#1 RADOVEDNOST
#2 ŽELJA PO ZASLUŽKU
#3 ŽELJA PO LJUBEZNI
#4 STRAST
#5 NAIVNOST
#6 STRAH
#7 NEPOZORNOST
#8 SOČUTJE
#9 NAVELIČANOST
#10 IGNORANCA



www.varninainternetu.si

MojeZnanje.si

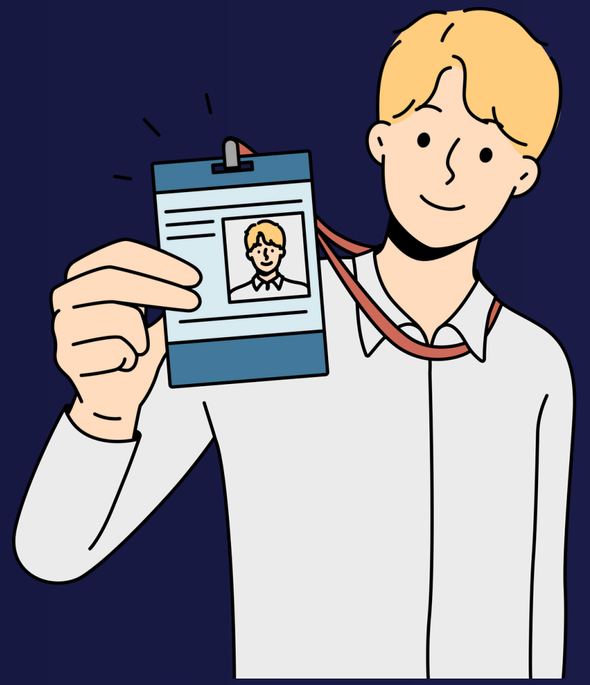
HEKERJI

Črni hekerji je izraz za najslabše hekerje v smislu škodoželjnosti in sicer beseda izvira iz ameriških filmov, kjer so slabi fantje nosili črne kape dobri pa bele. Črni heker je posameznik kateri poskuša ilegalno oziroma nepooblaščeno vstopiti v nek sistem ali omrežje iz zlonamernih razlogov in ga poskuša uničiti.

Sivi hekerji izkoriščajo računalniška omrežja na podoben način kot črni hekerji, vendar brez zlonamernih namenov. Običajno sivi hekerji vdirajo v računalniške sisteme, da obvestijo skrbnike da njihov sistem oziroma omrežje vsebuje vsaj ranljivosti. Sivi hekerji običajno zahtevajo denar za odpravljanje napak.

Beli hekerj so etnični hekerji, kateri sodelujejo z organizacijami, da izboljšajo njihov varnostni sistem. Beli klobuki imajo dovoljenje za napadanje tarč ampak v skladu z pravili o napadu katera so predpisana v naprej. Ko beli hekerji odkrijejo pomanjkljivost v varnostnem sistemu jo vedno razkrijejo in poskušajo odpraviti pred drugimi hekerji. Veliko podjetij najame bele hekerje, da predčasno odkrijejo pomankljivosti v varnostnem sistemu in to napako pravočasno odpravijo.

NOTRANJI AKTERJI



Grožnje od znotraj in z njimi povezane osebe znotraj organizacije so pomemben dejavnik na področju kibernetskih groženj. Tako kot kibernetski kriminalci tudi osebe znotraj zasledujejo predvsem finančno pridobitne cilje s tem, da neposredno ali posredno prodajajo svoje storitve na črnem trgu.

Gre za zaposlene ali partnerje organizacij, ki imajo dostop do notranjih informacij.
Pogosto so motivirani z zamero, pohlepom ali izsiljevanjem.

V primeru oseb znotraj, ki so nenamerni akterji, gre običajno za zlorabo njihovih dostopov ali okužbe njihovih računalnikov. Dejansko so pod nadzorom drugih akterjev groženj in se ne zavedajo, da so krivci za zlorabo sistema.

DRŽAVE

Države kibernetske vdore uporabljajo predvsem za vohunjenje in kot orožje. Kibernetsko vojskovanje (ang. cyber warfare) oz. bojevanje vključuje dejanja neke nacionalne države ali mednarodne organizacije, ki napade informacijska omrežja druge države ali organizacije (npr. teroristične) z računalniškimi virusi, napadi onemogočanja storitve in drugimi oblikami kibernetskih napadov.
Glede na napredne zmogljivosti te skupine, je njihove napade pogosto težko identificirati in se jim zoperstaviti. Zelo verjetno je, da je dejansko število njihovih napadov veliko večje kot kažejo statistike

HEKTIVISTI

Hektivisti spadajo med pet najpomembnejših akterjev kibernetskih groženj. Spodbujeni z nekaterimi političnimi dogodki, so odgovorni za spletne strani ter kraje in kršitve podatkov, prvenstveno usmerjenih proti vladam ter organizacijam in podjetjem v javnem sektorju.
Skupina je predvsem aktivna na področju razobličenja spletnih strani, širjenja propagande in medijsko odmevnih DDoS napadih.

Za svoje napade imajo običajno politične motive, ki lahko pritegnejo tudi druge akterje kibernetskih groženj, predvsem države, ki hektiviste pogosto uporabijo kot krinko za svoje kibernetske napade.

Hektivisti pa nimajo samo političnih ciljev. Hektivist je vsak aktivist, ki uporablja hekerska dejanja za promocijo stališč ali doseganje političnih ciljev. Stališča so lahko verska, zdravstvena (npr. anticepilci), okoljska ...

VARNOSTNE STORITVE IN UKREPI

Zaščito informacijske tehnologije lahko opredelimo da v primeru neljubih dogodkov kot so kibernetski napadi minimiziramo škodo. Zaščita informacijske tehnologije obsega naslednje elemente varovanja:

- fizično varovanje elektronskih naprav,
- arhiviranja podatkov,
- zaščita pred električnimi udari (strele),
- zaščita podatkov,
- ukrepanje v primeru napak opreme ali uporabnikov,
- zaščita IT sistemov pred zlonamernimi programi in s tem povezanimi nepooblaščenimi vdori v informacijske sisteme.

Misel “meni se to ne more zgoditi” je pogosta posebej med naprednejšimi uporabniki. To pa je izjemno nevarno v poslovnem okolju, kjer lahko pretirano zaupanje v lastno nepremagljivost privede do katastrofe in resnega oškodovanja.

VARNOSTNE STORITVE

Varnostne storitve so namenjene zaščiti omrežij, računalniških naprav, uporabnikov in podatkov pred različnimi grožnjami. Zagotavljajo jih računalniške in omrežne naprave ter programi s pomočjo različnih varnostnih algoritmov, protokolov in tehnologij.

Najpomembnejše varnostne storitve so:

- overjanje - avtentikacija,
- kontrola dostopa,
- razpoložljivost,
- zaupnost,
- celovitost,
- preprečevanje zanikanja,
- zagotavljanje zasebnosti.

MojeZnanje.si

AVTENTIKACIJA

Overjanje ali avtentikacija je storitev, ki omogoča preverjanje in dokazovanje identitete. Kdo je uporabnik ali oseba s katero komuniciramo? Identiteto dokazujejo uporabniki in naprave, kar je pomembno tako v lokalnem omrežju podjetja kot na internetu. Overjanje se izvaja na samem začetku komunikacije, pred dejansko izmenjavo podatkov.

Zelo pogost način overjanja uporabnikov je s pomočjo uporabniškega imena in gesla. Ta pristop je sicer enostaven in pogosto uporabljen, vendar ne omogoča zanesljivega overjanja uporabnika.

MojeZnanje.si

GESLA

- Ali so vaša geslo kratka (krajša od 8 znakov)?
- Ali vaše geslo vsebuje zgolj črke?
- Ali za določitev gesel uporabljate kombinacijo imen, letnic rojstva, zaporednih števil ali logične besede oz. besede iz slovarja?
- Ali uporabljate identično geslo za različne uporabniške račune?
- Ali imate vseskozi isto geslo za posamezen račun?
- Ali si gesla zapišete na papir?

MojeZnanje.si

GESLA

Uporaba gesel je zelo razširjena, a tudi zelo problematična, saj si večina uporabnikov izbere preveč preprosta gesla. Preprosta gesla je mogoče enostavno in hitro odkriti. Metoda, s katero napadalci odkrivajo enostavna gesla, se imenuje napad z grobo silo (ang. brute-force attack).

Najboljša gesla so unikatni, dolgi nizi naključnih znakov (16+).

Primer dobrega gesla:
MmAg”P”vdo7uz.
"MojaBabiPavlaima#8Krav!"

MojeZnanje.si

PRAKTIČNA VAJA

Preverite za nekaj vaših gesel, koliko časa je potrebnega, da ga zlorabijo.

https://www.security.org/how-secure-is-my-password/

Igrajte igro na spodnji povezavi in poskušajte priti čim dlje.

https://neal.fun/password-game/

Preverite ali je morda bilo vaše geslo zlorabljeno?

https://haveibeenpwned.com/

MojeZnanje.si

GESLA

Primeri slabih gesel, ki močno prevladujejo, so:

- privzeta gesla
- besede iz slovarja,
- besede (iz slovarja) ali imena z dodanim številom, npr. password1, zajec2000, jana1234
- besede s preprostim zakrivanjem npr. p@ssw0rd, b@l0n …
- podvojene besede, npr. konjkonj, stopstop …
- enostavne kombinacije s tipkovnice, npr. qwerty, 12345, asdfgh, fred,
- dobro znana števila, npr. 314159 (iz π), 9112001 (ameriški zapis za 11. 9. 2001, rojstni datumi kot števila …
- registrska številka avtomobila,
- osebne številke, npr. EMŠO, davčna, telefonska, rojstni dan,
- športna ekipa,
- imena hišnih ljubljencev, sorodnikov, prijateljev, znancev …

MojeZnanje.si

GESLA

Pri izbiri gesel je potrebno čimbolj slediti naslednjim priporočilom, ki neposredno izhajajo iz pogostih primerov slabih gesel.

1. Geslo naj bo dovolj dolgo, po možnosti vsaj 10 znakov, raje pa še več. Vsebuje naj male in velike črke, ločila ali posebne znake.
V pomoč pri pomnjenju gesel so vam lahko posebne povedi. Npr: Po kaj gre mali Petja 2x tedensko na Slomškovo 7? Vaše geslo je tako: **PkgmP2xtnS7?**

2. Primer dobrih gesel, ki se jih je lažje zapomniti, so tudi besede, ki med sabo nimajo nobenega vsebinskega pomena. Npr: FotosintezaSrečaSonce. Še bolj varno geslo pa je, če se povezanim besedam doda posebne znake (+,*,-, #,...) in številke. Npr: **Fotosinteza-Sreča+Sonce4.**

3. Uporabljajte različne stopnje kompleksnosti gesel.
Za kakšne nepomembne spletne račune, lahko uporabite tudi kakšno manj kompliciranо geslo, ki ga lahko uporabljate tudi za več podobnih storitev. Za pomembne storitve, kot so npr. elektronska pošta ali spletna banka, pa morajo biti gesla kompleksna in predvsem unikatna.

MojeZnanje.si

GESLA

Pri izbiri gesel je potrebno čimbolj slediti naslednjim priporočilom, ki neposredno izhajajo iz pogostih primerov slabih gesel.

4

Uporabljajte upravljalnik gesel (password manager).
Vseh različnih gesel si seveda ni enostavno zapomniti. Zato lahko uporabite poseben program, ki je namenjen zgolj varni hrambi gesel. Vendar pa mora biti vstopno geslo za eno od omenjenih aplikacij res dovolj dolgo in kompleksno. Gesel nikoli ne shranjujte v beležnici.

5

Kjerkoli je mogoče vklopite dvofaktorsko avtentikacijo (2FA oz. preverjanje v več korakih).
V nastavitvah uporabniških računov preverite, ali je možen vklop dvofaktorske avtentikacije. To pomeni, da boste morali ob prijavi v novi napravi vnesti tudi kodo. To boste prejeli v SMS sporočilu, ali pa to kodo zgenerirate s posebno aplikacijo. Napadalec se brez kode ne bo mogel prijaviti v vaš račun, tudi če vam ukrade geslo.

6

Gesel nikoli ne razkrivajte drugim osebam, sploh pa ne, če to od vas zahtevajo ali pa vas zaprosijo zanje.

MojeZnanje.si

GESLA

„Pa tudi če mi ukradejo geslo, saj nič ne skrivam!“
„Z mojimi podatki si ne morejo pomagati…“

To enostavno ne drži!

Spletnih goljufov ne zanima vsebina vaše komunikacije, ampak možnosti, kako lahko vaš elektronski predal uporabijo za nadaljnje prevare.

"Geslo je kot zobna ščetka – ne deli ga z drugimi in ga redno menjaj!"

MojeZnanje.si

TRIKI ZA KREIRANJE VARNEGA GESLA

1. **Izberite si stavek:**
   “al’ lepše od Urške bilo ni nobene”.
   Če uporabimo prve črke vsake besede dobimo:
   aloUbnn

2. **Dodajte posebne znake:**
   “a’loUbnn”

3. **Dodajte številke ali števila:**
   “a’loUbnn”7

4. **Povežite geslo s spletnim imenom:**
   gMa“a’loUbnn”7 - za gmail
   Fba’loUbnn”7 - za facebook

MojeZnanje.si

KAKO PRIDOBIJO GESLO

1. Phishing (Ribolov)

Napadalci posredujejo lažna sporočila (e-pošta, SMS, spletne strani), ki se pretvarjajo, da so legitimne (npr. banka, Facebook, Netflix). Uporabnika prevarajo, da vnese geslo v lažno prijavno stran.

Primer:

- E-pošta, ki se pretvarja, da je od Googla in zahteva ponovno prijavo.

2. Malware (Zlonamerna programska oprema)

Virus, trojanec ali keylogger se namesti na napravo in beleži pritiske tipk (vključno z gesli) ali krade shranjene podatke iz brskalnika.

Primer:

- Prenesena okužena datoteka (npr. "free_game.exe"), ki v ozadju krade podatke.

3. Bruteforce napad

Napadalec uporablja program, ki avtomatsko poskuša milijone kombinacij gesel, dokler ne najde pravega. Učinkovito proti šibkim geslom (npr. "123456").

Primer:

- Avtomatski poskusi prijave na spletno stran z uporabo pogostih gesel.

MojeZnanje.si


What is Your Password?
Share
Watch on YouTube

DVOFAKTORSKA AVTENTIKACIJA

Dvofaktorska avtentikacija (2FA) je način varnega dostopa do računalniških sistemov, aplikacij in storitev, ki zahteva uporabo dveh neodvisnih načinov preverjanja identitete uporabnika. Gre za dodaten sloj varnosti, ki preprečuje nepooblaščen dostop, tudi če je geslo ukradeno ali uganjeno.

Dvofaktorska avtentikacija (2FA) pomeni dvojno preverjanje pristnosti uporabnika.

2FA je bistvenega pomena za spletno varnost, saj zmanjša tveganja, ki so povezana z gesli. Napadalcem ne zadošča ukradeno geslo, saj je brez uporabe drugega dejavnika geslo neuporabno.

MojeZnanje.si

DVOFAKTORSKA AVTENTIKACIJA

Dvofaktorska avtentikacija temelji na treh kategorijah preverjanja:

1. **Nekaj, kar veš:**
   - Geslo, PIN koda ali odgovor na varnostno vprašanje.
2. **Nekaj, kar imaš:**
   - Fizična naprava, kot je telefon, pametna kartica ali generirana koda iz aplikacije.
3. **Nekaj, kar si:**
   - Biometrične lastnosti, kot so prstni odtis, prepoznavanje obraza..

Za uspešno avtentikacijo mora uporabnik dokazati identiteto z vsaj dvema od teh treh kategorij.

MojeZnanje.si

DVOFAKTORSKA AVTENTIKACIJA

PRIMERI UPORABE:

- E-pošta: Po vnosu gesla morate vnesti še kodo, ki jo prejmete prek SMS-a ali aplikacije (npr. Google Authenticator).
- Družabna omrežja: Facebook, Instagram... omogočajo prijavo z dodatno potrditvijo prek aplikacije ali varnostnega ključa.
- Spletno bančništvo: Običajno uporabljajo kombinacijo gesla in kode, poslane prek SMS-a ali generirane z namensko aplikacijo.
- Prijava na delovna mesta: Uporaba varnostnih ključev ali biometrije za dostop do sistemov podjetja.

PRAKTIČNA UPORABA

MojeZnanje.si

AVTORIZACIJA

Avtorizacija je postopek preverjanja in dodeljevanja pravic uporabniku, napravi ali aplikaciji za dostop do določenih virov, podatkov ali funkcionalnosti v sistemu. Gre za korak, ki običajno sledi avtentikaciji in zagotavlja, da ima uporabnik dovoljenje za izvedbo določenega dejanja.

Avtorizacija je pomembna, saj je potrebno zagotoviti, da ima uporabnik ali računalnik potrebne pravice za dostop do vira ali storitve in da jih nima, če jih ne potrebuje ali ne sme imeti.

Med avtorizacijo sistem preveri pravila dostopa overjenega uporabnika in odobri ali zavrne dostop do virov. Pravice uporabnikov so običajno navedene v seznamu za kontrolo dostopa

AVTORIZACIJA

Avtentikacija	Avtorizacija
Preverja identiteto uporabnika.	Preverja pravice uporabnika.
Odgovarja na vprašanje "Kdo si?".	Odgovarja na vprašanje "Kaj smeš narediti?".
Izvaja se najprej.	Sledi po uspešni avtentikaciji.
Primer: Geslo za prijavo.	Primer: Dovoljenje za ogled dokumenta.

VARNOSTNO KOPIRANJE

Varnostno kopiranje (ang. backup) pomeni ustvarjanje kopije pomembnih datotek, da jih lahko obnovimo, če:

- računalnik odpove (npr. okvara diska),
- po nesreči izbrišemo datoteke,
- naprava postane žrtev virusa, izsiljevalske kode (ransomware),
- izgubimo ali nam ukradejo napravo.

Dejstvo: 30 % ljudi nikoli ne naredi varnostne kopije. A podatke izgubi vsak 10. uporabnik vsako leto!

MojeZnanje.si

31. MAREC

SVETOVNI DAN VARNOSTNEGA KOPIRANJA

PESEM O BACKUPU

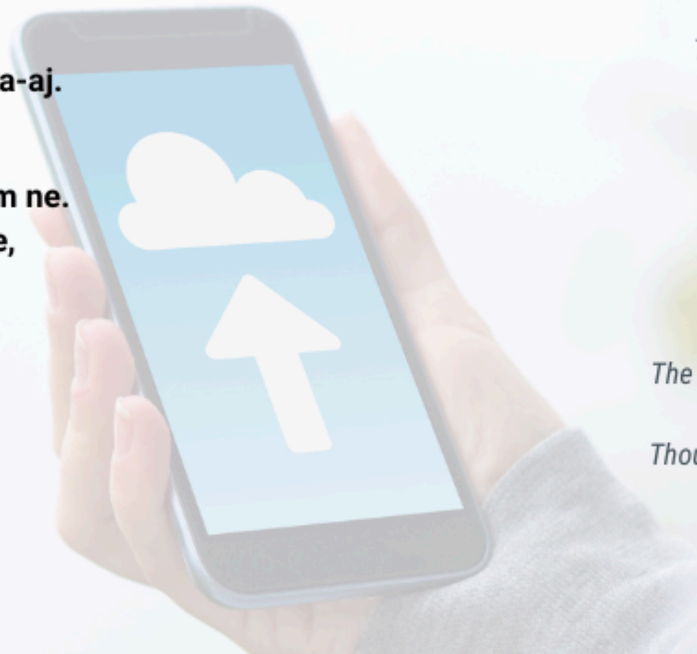
Včeraj še
datoteke varne so bile.
Kopije brezvezne zdele se,
oh, imel sem vse včeraj še.

Naenkrat pa
polovica vseh datotek je šla.
Vso trdo delo vzela megla
po napadu hekerskega virusa.

Oh, joj, kliknil sem,
kaj, težko je reči zdaj.
Datotek pa kar ni naza-a-a-aj.

Včeraj še
v backup kopije verjel sem ne.
Zdaj vse to me resno tepe,
oh, ko bilo bi včeraj še.

Kopije
varnostne naredil bi vse,
a zdaj žal prepozno je.
Včeraj še imel sem vse.



Prirejeno po:

Yesterday,
All those backups seemed a waste of
pay.
Now my database has gone away.
Oh I believe in yesterday.

Suddenly,
There's not half the files there used to be,
And there's a deadline
hanging over me.
The system crashed so suddenly.

I pushed something wrong
What it was I could not say.
Now my data's gone
and I long for yesterday-ay-ay-ay.

Yesterday,
The need for back-ups seemed so far
away.
Thought all my data was here to stay,
Now I believe in yesterday.
(Steve Roberts)

VARNI NA INTERNETU
Od mene je odvisno vse.

MojeZnanje.si

NAMEN VARNOSTNEGA KOPIRANJA

- **Zaščita pred izgubo podatkov:** Zaradi tehničnih okvar, človeških napak, kibernetskih napadov, naravnih nesreč ali druge nepredvidene situacije.
- **Obnovitev delovanja:** Hitrejša ponovna vzpostavitev sistemov in dostopa do podatkov po nesreči.
- **Zakonodajna skladnost:** V nekaterih panogah je varnostno kopiranje obvezno zaradi zakonodajnih zahtev (npr. GDPR, HIPAA).
- **Poslovna kontinuiteta:** Omogočanje nemotenega poslovanja tudi v primeru katastrofe.

KAJ JE POTREBNO KOPIRATI?

- Fotografije, videoposnetke
- Osebne dokumente (npr. Word datoteke, PDF, šolske naloge)
- Elektronsko pošto in kontakte
- Gesla in varnostne ključe (npr. 2FA kode)
- Certifikate
- Spletne strani
- Nastavitve računalnika in pomembne programe

MojeZnanje.si

PRAVILO 3-2-1

- 3 kopije podatkov: Original + 2 kopiji.
- 2 različni napravi: Npr. računalnik in USB ključek.
- 1 kopija zunaj: Npr. v oblaku ali na drugem mestu.

Primer: Projekt je na računalniku, kopija na USB ključku in kopija na Google Drive.

MojeZnanje.si

Način	Prednosti	Slabosti
Zunanji disk / USB	Hiter, pod nadzorom	Lahko odpove, se izgubi
Cloud storitve	Avtomatsko, dostop od kjerkoli	Omejen prostor brezplačno, zahteva internet
NAS strežnik	Za napredne uporabnike, domače omrežje	Drago, zahteva več znanja
DVD/CD	Trajno shranjevanje	Star način, majhna kapaciteta

SPLETNI BONTON

Spletni bonton pomeni pravila vljudnega, spoštljivega in varnega vedenja na internetu. Tako kot v resničnem svetu tudi na spletu veljajo določena pravila, ki ohranjajo spoštljivo komunikacijo, varnost in dobro počutje vseh udeležencev.

Kar ne bi rekel v obraz, ne napiši na internet.

MojeZnanje.si

OSNOVNA PRAVILA

1. **Bodi spoštljiv:** Piši vljudno, tudi če se z nekom ne strinjaš.
2. **Varuj zasebnost:** Ne deli osebnih podatkov (npr. naslova, gesel) ali slik brez dovoljenja.
3. **Preveri, preden deliš:** Prepričaj se, da so informacije točne, preden jih posreduješ.
4. **Uporabljaj primeren jezik:** Izogibaj se kletvicam ali žaljivkam.
5. **Spoštuj pravila platforme:** Vsaka platforma (npr. Kahoot, Discord) ima svoja pravila.
6. **Odgovarjaj premišljeno:** Ne pošiljaj sporočil v jezi ali naglici.
7. **Priznaj avtorstvo:** Če uporabiš sliko ali besedilo nekoga drugega, navedi vir.

Etični vidiki:

- Ne širi lažnih informacij: Preverjaj dejstva, tudi če jih ustvari AI (npr. ChatGPT).
- Ne sodeluj v spletnem nasilju: Če vidiš žaljive komentarje, jih prijavi ali ignoriraj.
- Spoštuj raznolikost: Na spletu so ljudje iz različnih kultur – bodi odprt in strpen.

ZAŠČITA IDENTITETE NA SPLETU

Tvoja digitalna identiteta je vse, kar o tebi obstaja na internetu – od uporabniških imen, fotografij, e-pošte, IP-naslova, do objav, komentarjev in celo kako pišeš.

Na internetu imaš obraz – tudi če ga ne vidiš v kameri.

Kraja identitete pomeni, da nekdo uporabi tvoje osebne podatke, da se izdaja za tebe – za krajo, goljufijo ali nadlegovanje.

Primer:
Nekdo ustvari profil z vašim imenom in sliko ter piše drugim, da zbira denar za “nujno pomoč”.

MojeZnanje.si

ZAKAJ ZAŠČITA

1. Preprečuje krajo identitete (nekdo se izdaja za tebe)
2. Ščiti pred zlorabami (npr. neprimerna raba tvoje slike)
3. Otežuje spletno nadlegovanje ali vdore
4. Ohranja tvoj ugled – kar objaviš, ostane!
5. Povečuje tvojo digitalno varnost in zaupanje v splet

MojeZnanje.si

🔐 Nasvet	💡 Zakaj je pomemben	✅ Primer
1. **Uporabi močna gesla**	Lažje se zaščitiš pred vdorom	Namesto "janez123" ➜ "T4!rLj2024%"
2. **Ne objavljaj osebnih podatkov javno**	Podatki lahko končajo v napačnih rokah	Ne deli naslova, telefona, …
3. **Imej različna gesla za različne račune**	Če ti kdo ukrade eno, ne dobi dostopa do vsega	Ločeno geslo za e-pošto, Instagram, …
4. **Uporabi dvofaktorsko avtentikacijo (2FA)**	Tudi če nekdo pozna geslo, rabi še kodo iz tvojega telefona	Google Authenticator, SMS koda
5. **Pazi, kaj deliš na slikah**	Slike razkrivajo lokacijo ali navade	Na selfiju pred hišo ➜ vidi se naslov
6. **Bodi pozoren na lažne profile in prevare**	Nekdo se lahko izdaja za prijatelja	“Hej, lahko mi daš tvojo številko za nagradno igro?” = Ne!
7. **Redno preverjaj nastavitve zasebnosti**	Določaj, kdo vidi tvoje objave	Instagram: samo prijatelji, ne “javno”
8. **Ne klikaj sumljivih povezav**	Lahko ukradejo tvoje podatke (phishing)	Mail: “Prijavi se tu za nagrado” = PREVARA
9. **Bodi previden z javnimi WiFi-ji**	Lahko ti prestrežejo podatke	Na javnem WiFi ne preverjaj bančnega računa
10. **Redno posodabljaj naprave**	Popravki zaprejo varnostne luknje	Posodobitev sistema in aplikacij = bolj varno!

PREVERIMO ZNANJE

https://forms.office.com/e/x7quPCbcRV?origin=lprLink

MojeZnanje.si

HVALA ZA POZORNOST

MojeZnanje.si