ABC VARNOSTI NA SPLETU

www.varninainternetu.si

si·cert

Nacionalni odzivni center za kibernetsko varnost

VARNI NA INTERNETU

Od mene je odvisno vse.

www.varninainternetu.si

Aktivnosti SI-CERT v celoti financira Urad Vlade Republike Slovenije za informacijsko varnost, pristojni nacionalni organ za informacijsko varnost.

Na Nacionalnem odzivnem centru za kibernetsko varnost SI-CERT smo si zadali izziv: **kratko in enostavno pojasniti, kako prepoznamo spletne nevarnosti.**

Ker je nemogoče opisati prav vse prevare, na katere lahko naletite, smo nasvete oklestili podrobnih pojasnil in opisov različnih prevar ter številnih nastavitev aplikacij. Osredotočili smo se na eno skupno lastnost spletnih prevar: goljufi želijo vplivati na čustva – predvsem vzbujajo strah ali željo po hitrem zaslužku.

Vodnik, ki je pred vami, pojasnjuje temeljne pristope in način komunikacije spletnih goljufov. Ti principi so enaki, če komunicirate prek elektronske pošte, nakupujete v spletni trgovini ali uporabljate družbena omrežja.

Ta vodila varnosti bodo dobrodošla predvsem za uporabnike, ki splet in njegove zakonitosti šele spoznavajo, pa tudi izkušenejši uporabniki bodo našli precej uporabnih nasvetov. Če je v vašem družinskem ali prijateljskem krogu oseba, ki potrebuje več pojasnil, bo ta vodnik lahko v veliko pomoč.

A

Kako prepoznam nevarnost na spletu?

V kibernetskem svetu obstaja veliko varnostnih sistemov, ki občutno pripomorejo k vaši zaščiti. Medtem ko vi obiskujete različne spletne strani in uporabljate elektronsko pošto, neopazno delujejo v ozadju in tudi pravočasno ustavijo marsikateri napad. Vendar vas ti sistemi žal ne bodo zaščitili pred vsemi nevarnostmi na spletu.

Le vaša presoja in poznavanje temeljnih principov, kako delujejo spletne prevare, vam bodo pomagali, da na spletu ostanete varni.

Zapomnite si: **spletni goljufi želijo vzpostaviti komunikacijo z vami, želijo vzbuditi vašo pozornost!**

Nato vas v nadaljevanju postopoma prepričujejo, da storite nekaj, kar jim prinaša koristi. To bodo poskušali na najrazličnejše načine. Domišljija spletnih goljufov nima meja.

Strnili smo tri ključne pristope, s katerimi spletni goljufi gradijo lažne zgodbe in podobe. Takoj ko prepoznate enega od teh izgovorov ali pritiskov, se ustavite in prekinite nadaljnjo komunikacijo.

NEVARNOST ŠT. 1

OBLJUBE

ČE NEKAJ ZVENI PREVEČ DOBRO, DA BI BILO RES, ŽAL TUDI NI RES

Ljudje se težko upremo dobrim ponudbam. Velike obljube o zaslužkih, bogatih nagradah in ugodnih ponudbah so se izkazale za preverjeno formulo spletnih prevar.

Predstavljamo vam nekaj najbolj tipičnih primerov lažnih obljub, ki lahko vodijo v izgubo vašega denarja, zlorabo osebnih podatkov ali okužbo računalnika.

DENAR, DENAR, DENAR

Prejmete elektronsko sporočilo, da je v tujini umrl vaš daljni sorodnik, ki vam je zapustil veliko vsoto denarja ali sporočilo z ugodno ponudbo kreditov brez kreditnega preverjanja. Med novicami boste naleteli na oglas, kako je nek zvezdnik s pomočjo investicij v kriptovalute zaslužil celo premoženje. Na družbenem omrežju naletite na nagradno igro z bogatimi nagradami, za sodelovanje pa je treba zgolj všečkati in deliti objavo.

POCENI PONUDBE

Zelo ugodne ponudbe, ki odstopajo od konkurence, lahko kažejo na prevaro. Znaki, da gre za lažno trgovino, so lahko izjemno nizke cene, brezplačna dostava po vsem svetu, vsi artikli so vedno na zalogi. Nikjer pa ni najti podatka, katero podjetje upravlja trgovino.

VELIKO ZASLUŽKA ZA NIČ DELA

Star pregovor pravi, da se brez muje še čevelj ne obuje. Če vam nekdo obljublja velik zaslužek za nič dela, se morda že lepo sliši, vendar pa so te obljube vedno lažne.

Vseeno je, kje jih zasledite:

- na družbenih omrežjih,
- kot spletni oglas,
- objavo na forumu,
- sporočilo, ki ga prejmete po telefonu ali elektronski pošti ipd.

ČUDEŽNI UČINKI

Če naletite na oglase za razne čudežne pripomočke, ki vam bodo povrnili sluh, izboljšali vid ali ozdravili revmo, dobro premislite, ali ste res na sebi pripravljeni uporabiti zdravilo, ki ni bilo izdelano in preizkušeno v skladu s strogimi predpisi. Z nepreverjenimi izdelki lahko resno ogrozite svoje zdravje. Slika zdravnika, ki to zdravilo toplo priporoča vsem svojim pacientom, je lahko tudi ponarejena. Glede zdravil, medicinskih pripomočkov in prehranskih dopolnil se vedno obrnite na svojega zdravnika.

NEVARNOST ŠT. 2

GROŽNJE

PRAVIJO, DA JE STRAH VELIK GOSPOD

Ko smo prestrašeni, zmedeni in v paniki, lahko storimo marsikaj nespametnega. In prav na to računajo tudi goljufi, ki z ustrahovanjem dosežejo, da jim pošljemo denar ali omogočimo dostop do računalnika.

Prepoznajte nekaj tipičnih groženj:

VAŠ NABIRALNIK JE POLN

Prejeli boste elektronsko sporočilo, da je vaš poštni nabiralnik poln ali da morate posodobiti varnostne nastavitve. Če takoj ne kliknete na povezavo, bo vaš račun blokiran. Ko to storite in vnesete geslo za prijavo, bo geslo dobil goljuf in prevzel nadzor nad vašo elektronsko pošto.

ČAKA VAS PAKET

Prejeli boste elektronsko sporočilo, ki naj bi ga poslala dostavna služba, ker vas čaka paket, za dostavo pa morate s kreditno kartico plačati nekaj drobiža. Če to naredite, vam bodo popolnoma izpraznili račun.

SMS BANKE

Prejeli boste sporočilo SMS, da je prišlo do zlorabe vaše spletne banke. Za ponovno aktivacijo morate klikniti na povezavo in vpisati podatke za dostop. Ne nasedajte, verjetno gre za prevaro! Če niste prepričani, pokličite banko po telefonu.

POSNELI SMO VAS

Prejeli boste elektronsko sporočilo, da so vam vdrli v računalnik in vas posneli s kamero, od vas pa bodo zahtevali denar. Gre za prazne grožnje, sporočilo lahko brez skrbi izbrišete.

NUJNO ODPRI PRIPONKO

Prejeli boste elektronsko sporočilo z zadevo »nujno preberi« ali »nujno odpri priponko«. Priponka je lahko okužena z virusom, ki napadalcem omogoči popoln nadzor nad vašim računalnikom.

TEHNIČNA POMOČ

Poklicali vas bodo lahko tudi prek telefona in se predstavili kot tehnična pomoč. Rekli bodo, da je računalnik okužen z virusom in vam ponudili pomoč. Vodili vas bodo po korakih, vi boste klikali, na koncu pa bodo popolnoma prevzeli nadzor nad vašim računalnikom in vam prek spletne banke izpraznili bančni račun.

POLICIJA

Lahko boste prejeli elektronsko sporočilo v imenu slovenske policije, kjer vam bodo očitali huda kazniva dejanja. Spet gre zgolj za strašenje, naj vas ne zavedejo logotipi policije in podpis direktorja, vse to je lahko ponarediti.

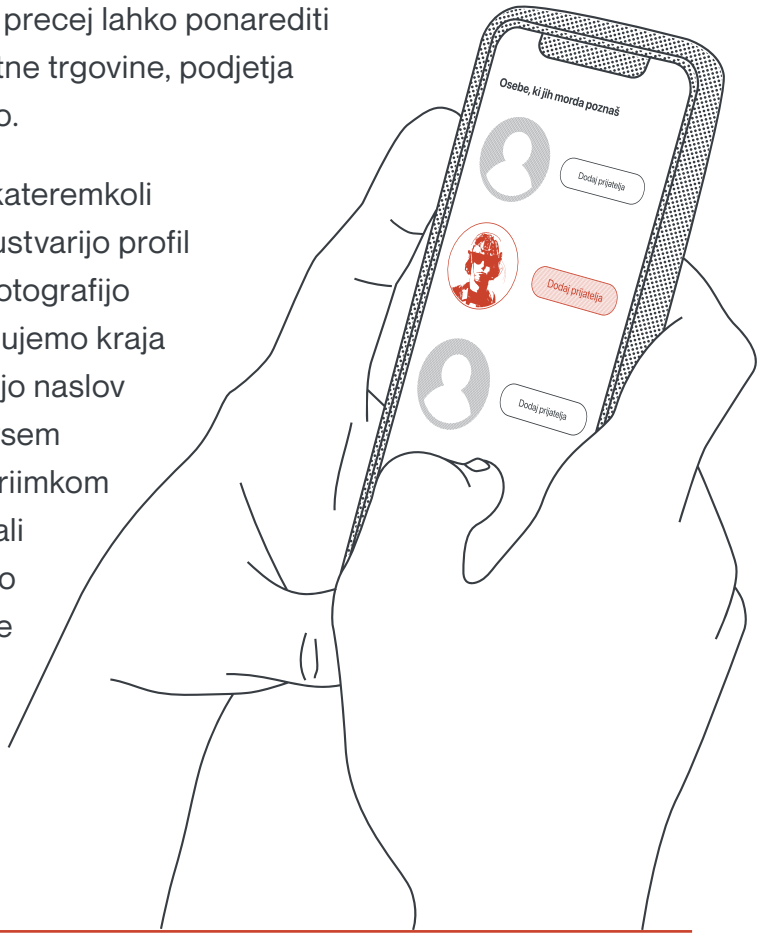
NEVARNOST ŠT. 3

PRETVARJANJE

NA SPLETU NI VSE, KAR VIDITE, TUDI RESNIČNO

V svetu računalništva je precej lahko ponarediti slike, imena, izjave, spletne trgovine, podjetja in tudi elektronsko pošto.

Spletni goljufi lahko na kateremkoli družbenem omrežju poustvarijo profil z imenom, priimkom in fotografijo »prave« osebe, kar imenujemo kraja identitete. Lahko ustvarijo naslov elektronske pošte s povsem izmišljenim imenom in priimkom (janez.novak@email.si) ali celo pošljejo elektronsko sporočilo, kjer piše, da je pošiljatelj vaša banka.



VOJAK NA MIROVNI MISIJI

Tipičen primer takšnega pretvarjanja je **ljubezenska prevara**. Goljufi ustvarijo lažni profil, največkrat zdravnika ali vojaka na mirovni misiji, in poskušajo navezati stik prek družbenih omrežij. So osamljeni, iščejo sorodno dušo in v dolgih večernih pogovorih z žrtvijo vzpostavijo zaupen odnos. Kmalu sledijo pretresljivi dogodki, želijo vam poslati kovček z velikim bogastvom ali pa potrebujejo denar za nujno operacijo otroka. Le kdo ne bi pomagal človeku v stiski. Žal se prošnje za denar končajo šele takrat, ko se žrtev zave, da je bilo vse skupaj zgolj in samo laž.

MLADA ZAPELJIVA DEKLETA

Tudi moški so pogosto tarča prevarantov, ki se pretvarjajo, da so mlada, zapeljiva dekleta. Na družbenem omrežju odprejo profil z zapeljivimi fotografijami. Ko vzpostavijo stik, kmalu pošljejo razgaljene fotografije ali videoposnetke – seveda ne svojih, pač pa jih ukradejo na spletu. Nato še žrtev povabijo, da se sleče. Ko dobijo njene fotografije ali posnetke, začnejo z izsiljevanjem za denar in grozijo z javno objavo. Posamezniki, ki se ujamejo v takšno prevaro, lahko doživljajo zelo hude psihične pritiske in stisko. Kaj storiti, če se ujamete v njihovo past: ohranite mirno kri in takoj prekinite vso komunikacijo z izsiljevalci!

B

Kako ostati na varni strani?

Na spletu lahko uporabniki sami storimo največ za našo varnost. Ne polagajmo vseh upov v tehnologijo, saj ne obstaja čudežni program, ki nas bo zaščitil pred vsemi nevarnostmi. Največ bomo storili, če bomo kritično brali informacije.

Nekdanja evropska komisarka za digitalno agendo Neelie Kroes je strnila najenostavnejši recept, kako ostati varni na spletu: ***»Imejte odprte oči in uporabljajte zdravo pamet.«***

Zapomnite si: **na spletu vedno sledite pravilu - preberem, preverim, poiščem pomoč.**

PRAVILO ŠT. 1

PREBEREM

ZAPOMNITE SI – NA SPLETU SO NAJVREDNEJŠI VAŠI PODATKI!

Vaš elektronski naslov, telefonska številka, kopija osebnega dokumenta, številka bančne ali kreditne kartice odpirajo vrata nadaljnjim prevaram.

PREBEREM, KOMU POSREDUJEM PODATKE

Bodite pozorni vsakič, ko morate vpisati svoje podatke in natančno preverite, komu bodo posredovani. Preberite, katero podjetje je navedeno, kako bodo vaše podatke obdelovali, komu jih bodo posredovali.

PREBEREM POGOJE UPORABE

Včasih je meja med prevaro in zavajanjem spletnih uporabnikov tanka, saj lahko podjetje na drobno spiše pogoje uporabe, vi pa v dobri veri posredujete svoje podatke in se naročite na neko plačljivo storitev. Ko se pritožite, je odgovor kratek: *»Sami ste krivi, saj je vse pisalo.«*

PREVERIM, KOMU ZAUPAM TELEFONSKO ŠTEVILKO

Tipičen primer so komercialni SMS-klubi. Na njih največkrat naletite, ko se vam na telefonu izpiše obvestilo: *»Vaš IP-naslov je bil izžreban«*, ali pa se na neki spletni strani izpiše: *»Sodelujte v anketi, nagradni igri, rešite križanko, kviz, IQ-test ...«*. V naslednjem koraku vpišete svojo telefonsko številko, pošljete potrditveni SMS in že ste včlanjeni v SMS-klub, ki ga boste vsak mesec dodatno plačevali.

PRAVILO ŠT. 2

PREVERIM

KDO JE NA DRUGI STRANI?

Preden opravimo nakup na spletu, stopimo v kontakt z neznancem ali podjetjem, se vedno pozanimamo, kdo je na drugi strani.

PREVERIM POŠILJATELJA

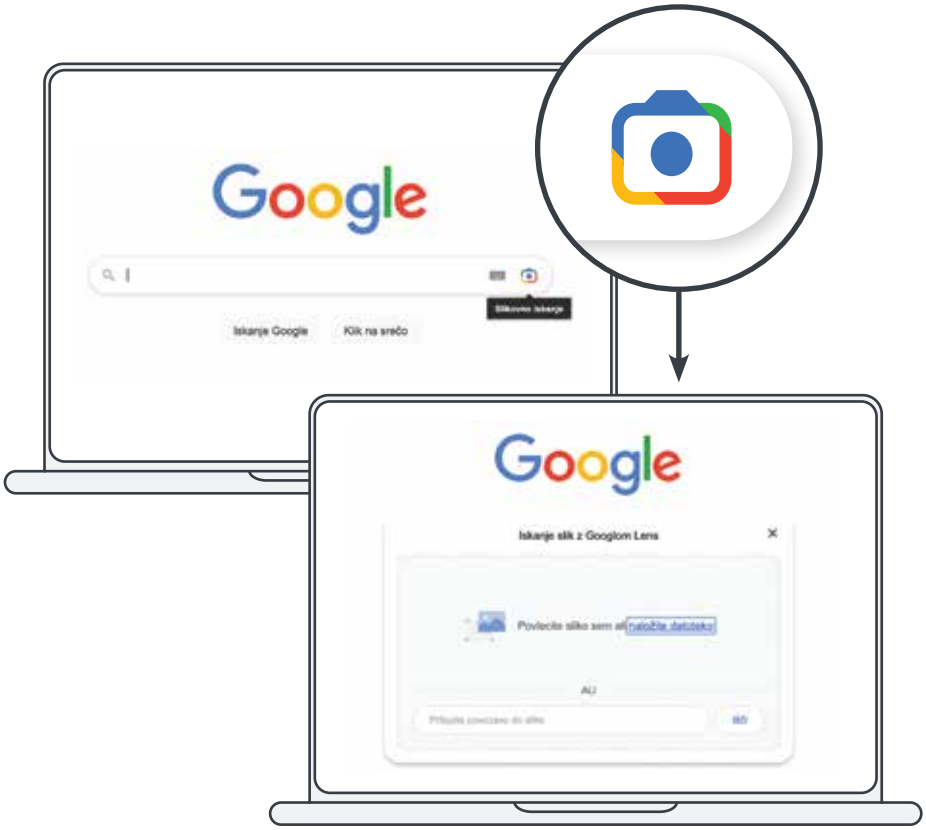
Raziščite vir: prejeli ste obvestilo o dobitku, prošnjo za pomoč ali zahtevo za plačilo. Uporabite spletni iskalnik, poiščite podjetje ali organizacijo, obiščite njihovo uradno stran, kontaktirajte ali pokličite jih in povprašajte, ali je to res.

PREVERIM DOMENO

Podučite se, kako preveriti lastnosti domene (domena je edinstveni naslov spletne strani), saj je starost domene odličen kazalnik, da gre za prevaro. Natančna in enostavna navodila, kako preverite domeno, so vam na voljo na tej spletni strani: **https://www.varninainternetu.si/domena**.

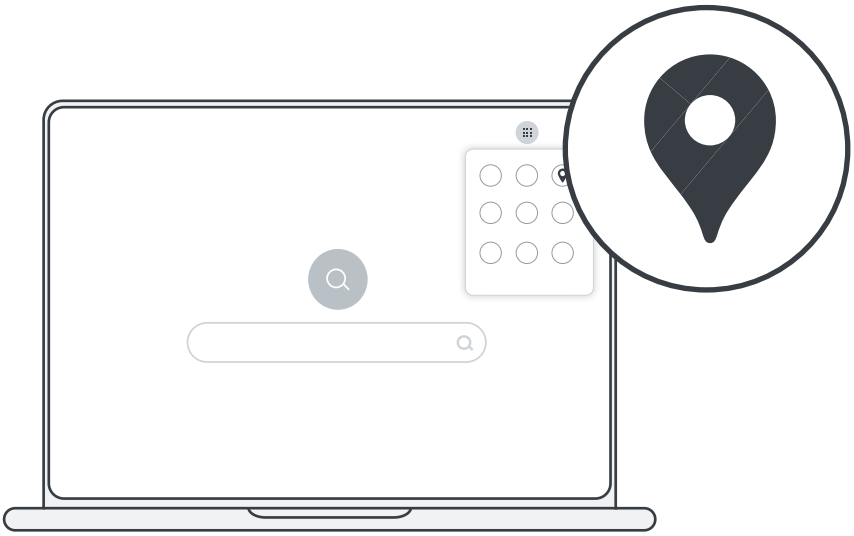
PREVERIM SLIKO

Ste pravkar sprejeli prijateljstvo od neznane osebe in si izmenjujete fotografije? **Uporabite iskalnik slik** (npr. Googlov iskalnik slik) in preverite, ali gre res za osebo, za katero se izdaja, ali pa so slike zgolj prekopirane z neke spletne strani. Tako lahko preverite tudi sliko artikla, ki ga nekdo prodaja prek spletnega oglasnika.



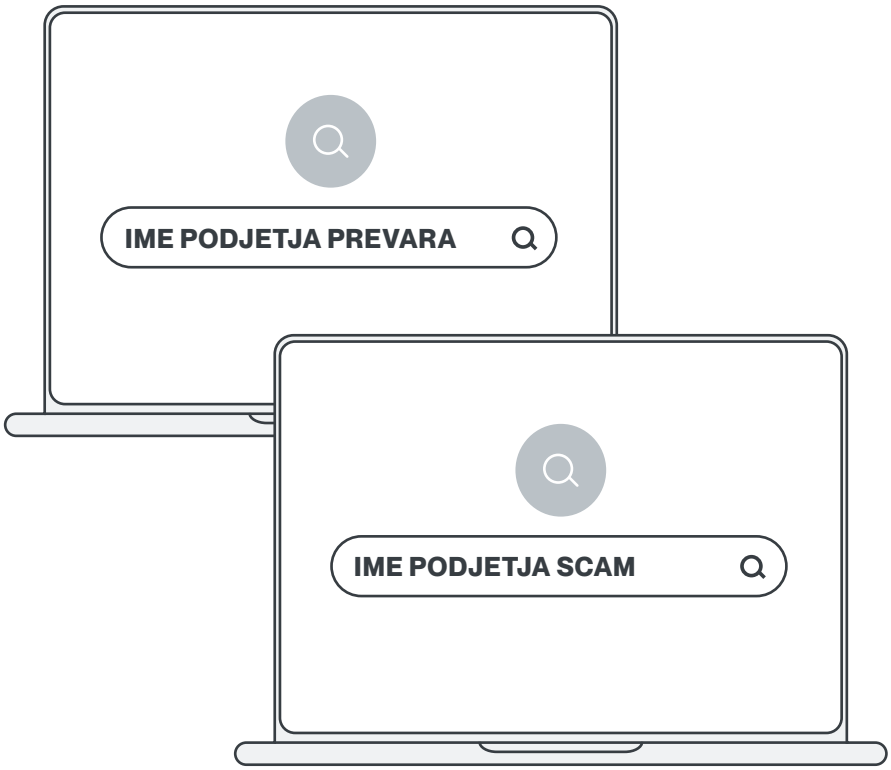
PREVERIM NASLOV PODJETJA

Neverjetno poceni izdelki na spletni strani in čisto nova spletna trgovina? Poiščite na spletu podatke o podjetju, komentarje, forume. Preverite naslov podjetja na Google Zemljevidih, lahko tudi pokličete navedeno številko, ki je namenjena uporabnikom. Če ni navedenega niti enega podatka (naslov trgovca, matična številka podjetja, elektronski naslov, telefonska številka), potem je to znak za alarm!



PREVERIM V ISKALNIKU

Še vedno niste prepričani? Preprosto, uporabite Googlov iskalnik, vpišite ime podjetja ali spletne trgovine in besedo prevara (ali angleško besedo »scam«). Večina prevar poteka po podobnem vzorcu. Če gre za znano prevaro, boste hitro naleteli na opozorila drugih uporabnikov, da neka trgovina ali podjetje nista vredna zaupanja.



PRAVILO ŠT. 3

POMOČ

NAJ VAS NE BO SRAM ALI STRAH PROSITI ZA POMOČ

Ne hitite. Vzemite si čas in preverite nenavadno elektronsko sporočilo ali sumljivo ugodno spletno trgovino. Če niste prepričani, da imate dovolj znanja, se ustavite in obrnite po pomoč.

POIŠČEM POMOČ PRI DRUŽINSKEM ČLANU ALI PRIJATELJU

Kadarkoli dvomite, želite več pojasnil, niste prepričani, da povsem razumete, kaj se dogaja na zaslonu – prosite za pomoč družinskega člana ali prijatelja, ki je računalniško bolje podkovan. Kratek telefonski klic vas lahko reši velikih težav.

POIŠČEM POMOČ NA BANKI

Če prejmete nenavadno elektronsko sporočilo, ki naj bi ga poslala vaša banka (blokada računa, blokada kartice, posodobitev sistema ipd.), se brez zadržkov obrnite neposredno na banko oz. njihov kontaktni center. Podobno storite, če prejmete nenavadno sporočilo, ki naj bi ga poslala druga slovenska ustanova ali podjetje, npr. Finančni urad, Pošta, Policija, ponudnik telekomunikacijskih storitev ipd. Pokličite jih na številko, ki jo imajo navedeno na svojih spletnih straneh.

POIŠČEM POMOČ NA SPLETNI STRANI VARNI NA INTERNETU

Po nasvet se obrnite na spletno stran Varni na internetu – v naslovno vrstico brskalnika vpišite **www.varninainternetu.si**. Na začetni strani so opisi najpogostejših spletnih prevar, ki trenutno pestijo slovenske spletne uporabnike, na zavihku Prevare pa najdete opise preostalih spletnih goljufij.

C

Koristni nasveti o varnosti na spletu

Kako varno uporabljam **elektronsko pošto?**

Večina spletnih nevarnosti se začne s preprostim elektronskim sporočilom, ki ga boste prejeli v nabiralnik elektronske pošte. Na prvi pogled sporočilo ne bo vzbudilo sumov. Vendar podrobnejši pregled pokaže, da lahko skriva marsikatero nevarnost.

Vedno preverite ključne 3 P:

P1 = **POŠILJATELJ**

P2 = **PRIPONKA**

P3 = **POVEZAVA**

P1

POŠILJATELJ

Preverite, kdo vam pošilja sporočilo, ali naslovnika poznate in sporočilo pričakujete. Če je sporočilo prišlo iz popolnoma neznanega naslova, predstavlja pa se kot banka, pošta, ponudnik elektronske pošte ali neka druga organizacija, je lahko prevara. Ne pozabite: **spletni goljufi znajo tudi ponarediti pošiljatelja elektronskega sporočila**.

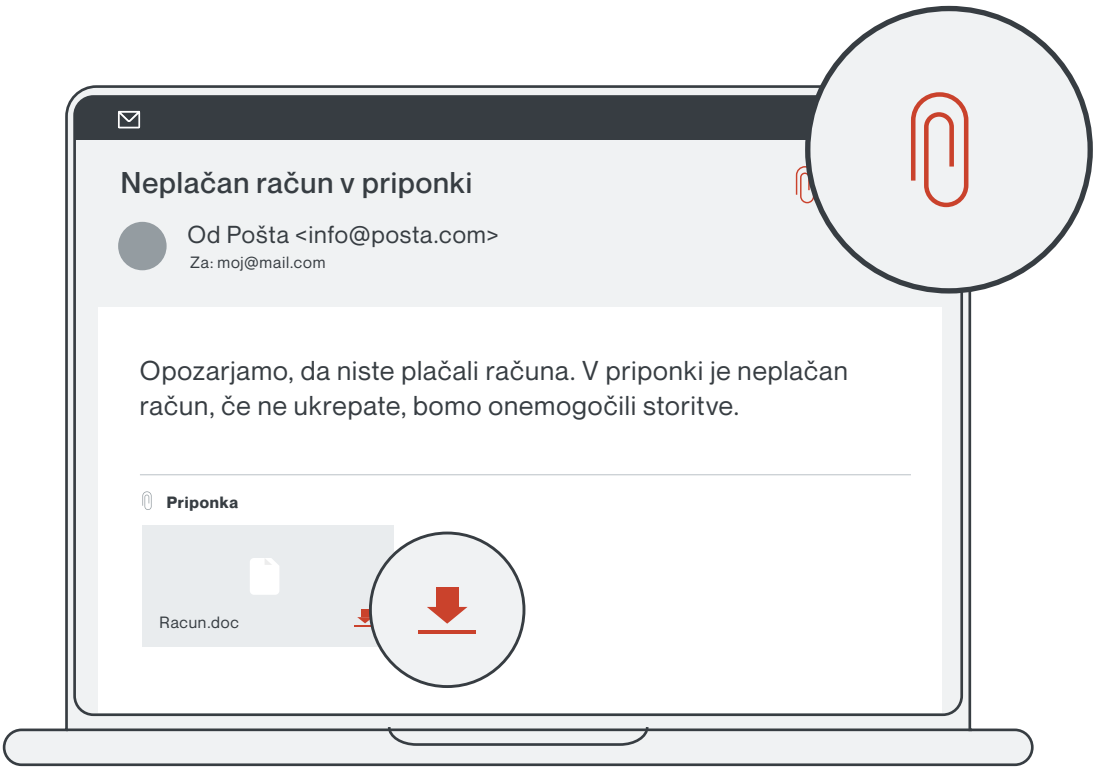
Primerjajte prikazano ime in dejanski e-naslov pošiljatelja. Prevaranti se pogosto izdajajo za nekoga drugega.

P2

PRIPONKA

Sumljivo je, če elektronsko sporočilo zahteva, da nujno odprete priponko, ker pošiljatelj zahteva takojšen odgovor. Sporočila, ki jih niste pričakovali, lahko v priponki vsebujejo škodljiv računalniški virus, ki ukrade vsa shranjena gesla na računalniku.

Ne odpirajte priponk sporočil, ki jih niste pričakovali. Priponka lahko vsebuje škodljiv računalniški virus.



P3

POVEZAVA

Tudi povezave v neobičajnih elektronskih sporočilih so lahko škodljive in tudi tu velja enako pravilo: če niste prepričani, ne klikajte! Povezava v sporočilu lahko tudi vodi drugam, kot je napisano. Kako to preverite? Če se z miško postavite na povezavo (ampak nanjo ne kliknete), se vam spodaj izpiše točen spletni naslov. Če ni povsem enak kot pravi, pojdite na spletno stran raje preko zaznamka ali spletnega iskalnika.

Vedno preverite verodostojnost povezave, tako da se z miško zgolj postavite nanjo, ne da nanjo kliknete.
Ne pozabite: če ste v dvomu, ne kliknite!

Kako varno uporabljam **družbena omrežja?**

Družbena omrežja nam omogočajo, da vzdržujemo stike z oddaljenimi sorodniki, ponovno oživimo stara prijateljstva in tudi izvemo marsikaj koristnega.

Ne pozabite: **na družbenih omrežjih tudi spletni napadalci iščejo nove žrtve.**

Slej ko prej boste naleteli na lažni profil zdravnika na misiji, ki išče sorodno dušo, poznavalca kriptovalut, ki obljublja velike zaslužke, znanega športnika, ki promovira nagradno igro ipd. Goljufi celo zakupijo oglase na družbenih omrežjih, da se ti prikažejo ravno najbolj ranljivi skupini uporabnikov.

Da se ne boste opekli, ne potrjujete prošenj za prijateljstvo osebam, ki jih ne poznate, in ne odgovarjajte na neobičajna zasebna sporočila. Na nekaterih omrežjih lahko tudi določite, ali bodo vaše objave vidne vsem, ali zgolj omejenemu krogu oseb, ki jim zaupate. Ko naletite na šokantne objave, imejte v mislih, da gre lahko tudi za napačne informacije. Neprimerne vsebine pa kar prijavite, saj s tem pripomorete k varnejšemu spletu.

Kako varno **nakupujem prek spleta?**

Med prebiranjem novic se vam prikaže oglas za spletno trgovino, kjer prodajajo ravno to, kar ste prejšnji dan iskali na spletu. Na voljo so vse velikosti, poštnina je brezplačna, cena pol nižja kot drugje, vendar pa morate takoj dokončati nakup, saj bo zaloga sicer pošla. Vse to so triki lažnih spletnih trgovin, ki so zgolj fasada, za njimi ne stoji nobeno podjetje, slike izdelkov pa so enostavno prekopirane iz drugih spletnih trgovin.

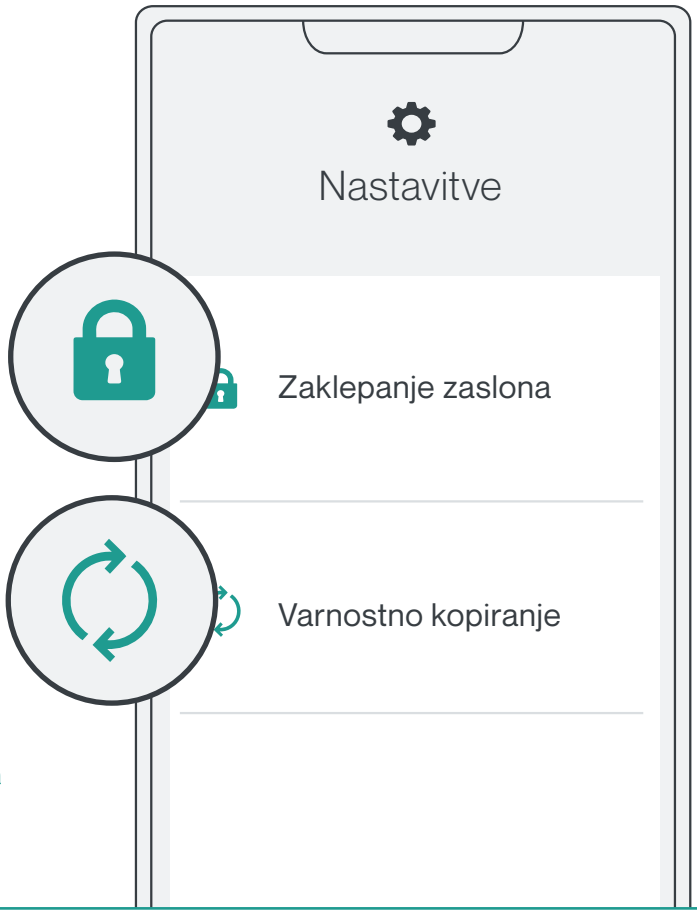
Tudi če prodajate prek spletnih malih oglasnikov, vas bodo verjetno kontaktirali potencialni kupci, ki se ne bodo pogajali za ceno, želeli pa bodo, da uporabite neko novo poštno storitev, za katero še niste slišali.

Ne pozabite: **brez slabe vesti lahko vztrajate pri tem, da uporabljate zgolj vam znane postopke, pa tudi če vas bodo prepričevali, da je nova storitev za vas povsem varna.**

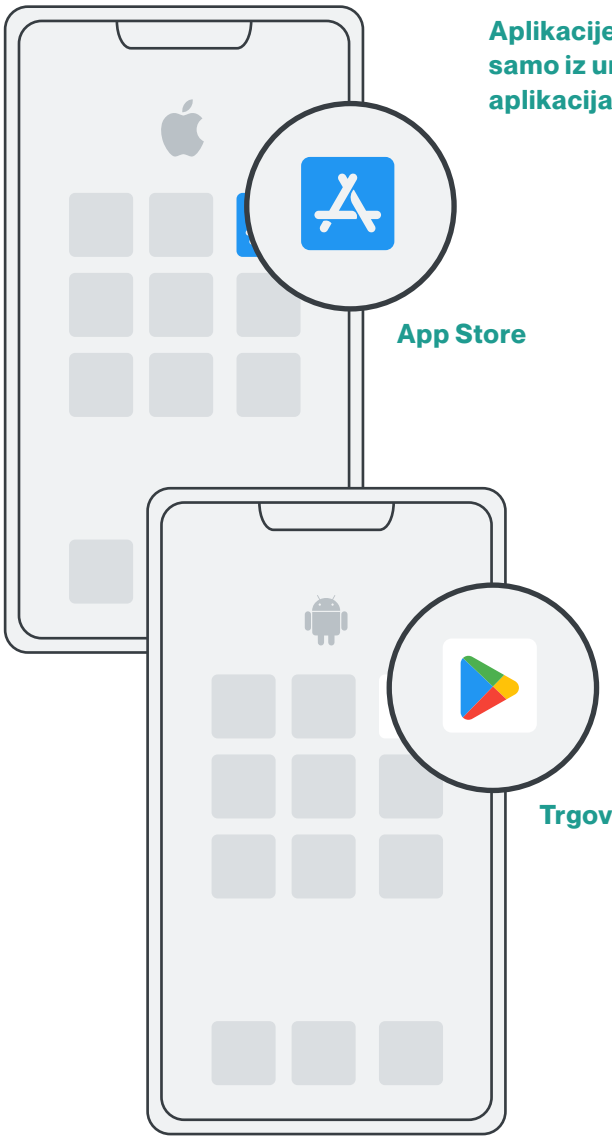
Kako varno uporabljam **pametni telefon?**

Pametni telefoni omogočajo veliko več kot zgolj klicanje in pošiljanje sporočil SMS. Z njimi brskamo po spletu, dostopamo do družbenih omrežij, elektronske pošte in mobilne banke, plačujemo, uporabljamo navigacijo ... **so torej pravi računalniki v malem in prav tako potrebujejo zaščito**.

Nastavite zaklepanje zaslona, npr. s PIN-kodo, vzorcem ali prstnim odtisom.



Vključite sinhronizacijo in naredite varnostno kopijo fotografij, npr. s kopiranjem na računalnik.



Aplikacije vedno nameščajte samo iz uradnih trgovin z aplikacijami.

App Store

Trgovina Play

ABC VARNOSTI NA SPLETU

Leto izida: 2022

Natis: 2000 izvodov

Založnik: Javni zavod Arnes

Oblikovanje in prelom: KOFEIN

Vsi priročniki, ki jih
izdajamo na SI-CERT,
so dostopni na naslovu
varninainternetu.si/gradiva/

si·cert
Nacionalni odzivni center za kibernetsko varnost

www.varninainternetu.si

---

si·cert

Nacionalni odzivni center za kibernetsko varnost