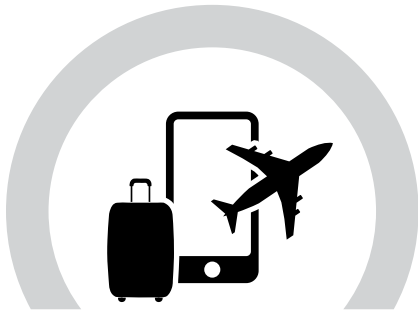




VARNI NA INTERNETU,
TUDI NA POČITNICAH



VARNI
NA INTERNETU



VARNI NA INTERNETU,
TUDI NA POČITNICAH

V primeru težav se lahko obrnete na:

Varni na internetu - www.varninainternetu.si

SI-CERT - www.cert.si



**VARNI
NA INTERNETU**

Od mene je odvisno vse.

VARNI NA INTERNETU, TUDI NA POČITNICAH

Počitnice se začnejo za domačim računalnikom. Treba je načrtovati pot, poiskati in rezervirati hotel ali kamp, kupiti letalske vozovnice ali vstopnice za glasbeni festival. Zaslona, takrat tisti na pametnem telefonu ali tablici, postane nepogrešljiv tudi med dopustovanjem. Da bi le-to bilo čim bolj brezskrbno, smo pripravili nekaj koristnih nasvetov.

NAJPOGOSTEJŠA TVEGANJA - NAJ SE DOPUST NE KONČA, ŠE PREDEN SE ZAČNE

FANTOMSKI APARTMAJI

Če se odločite za najem apartmaja prek zasebne ponudbe, je največje tveganje, da rezervirate in plačate neobstoječi apartma. Če je le mogoče, **iščite ponudbe na uveljavljenih posredniških portalih oz. spletnih oglasnikih, kjer so na voljo ocene in izkušnje drugih uporabnikov**. Izogibajte se nakazilu denarja neposredno na bančni račun ponudnika, še posebej če od vas zahteva **plačilo apartmaja prek sistema Western Union - potem je to velik znak STOP**. Vsekakor pokličite ponudnika po telefonu in še enkrat preverite vse pogoje najema. Zahtevajte tudi natančen naslov oz. lokacijo in jo preverite prek [Google Maps](#).

LAŽNE AGENCIJE

V poplavi turističnih ponudb na spletu svoje žrtve iščejo tudi lažne turistične agencije, lažni portali za prodajo letalskih vozovnic, celo lažni rent-a-car ponudniki. Tudi na SI-CERT smo že obravnavali prijavo uporabnika, ki je pri tuji agenciji na internetu naročil letalske karte in namestitvev za potovanje na Tajsko, kart in ostalih materialov pa ni nikoli prejel. **Takšne lažne ponudbe hitro prepoznate po neverjetno ugodnih cenah.**

Prav tako bodite pozorni na kontakte, navedene na strani. Če "agencija" uporablja brezplačni elektronski predal, npr. Gmail, je to gotovo znak za previdnost. Še bolj zaskrbljujoče je, če na strani ni nobenih podatkov o ponudniku oz. registriranem podjetju. **Vpišite ime agencije v brskalnik in poiščite čim več informacij, mogoče se na različnih forumih oglašajo ogoljufani kupci.**

NAKUP VSTOPNIC ZA FESTIVALE ALI ŠPORTNE PRIREDITVE

Če načrtujete obisk koncerta, glasbenega festivala ali tekme, vedno preverite na **uradni spletni strani organizatorja, katere agencije so pooblašene za prodajo vstopnic**. Ne zaupajte drugim super ponudbam neveljavljenih posrednikov, obrnite se na pooblašene prodajalce. Vstopnice lahko prodajajo tudi posamezniki prek različnih spletnih oglasnikov (npr. eBay) in v takšnih primerih vztrajajte pri plačilu prek posrednika PayPal, ne nakazujte denarja neposredno na bančni račun.

REZERVACIJE IN PLAČEVANJE S KREDITNO KARTICO

Še preden na kateremkoli spletnem mestu vpišete številko kreditne kartice, poiščite znake, ki kažejo na varno povezavo:

- URL-naslov spletnega mesta se začne s **HTTPS**, kar pomeni, da je prenos podatkov varen in šifriran.
- V URL-naslovnih vrstici je tudi **ikona s ključavnico**, kar je signal za varno oddajanje podatkov o kreditni kartici.
- **Zeleno obarvana vrstica** z varnostnim stanjem pove, da je digitalno potrjeno dodatno preverjeno.



VARNA UPORABA INTERNETA

Če na potovanjih in počitnicah potrebujemo dostop do interneta, je običajno na voljo več možnosti, ki pa niso vse enako varne. Zato pretehtajmo in izberimo najustreznejšo.

1. Javni računalniki

Ko uporabljamo javni računalnik, se moramo zavedati, da je lahko tudi okužen s škodljivo kodo (virusi, trojanci, črvi). Uporaba okuženega računalnika pomeni, da ima lahko nekdo dostop do vseh podatkov, ki jih vpisujemo, do vseh spletnih strani, ki jih obiščemo, lahko beleži vsako pritisnjeno tipko in gib miške.

Pri uporabi javnih računalnikov močno odsvetujemo, da kamorkoli vpisujete svoje osebne podatke in gesla, se prijavljate v vašo elektronsko pošto, družbena omrežja, dostopate do službenega omrežja ipd. Če bi radi zgolj prebrali novice in spremljali vremensko napoved, pa so tudi javno dostopni računalniki povsem primerna izbira.

2. Brezžično omrežje (Wi-Fi)

Na letališčih, v kavarnah in hotelih so pogosto na voljo javna brezžična omrežja (Wi-Fi), ki so brezplačna ali pa so dostopna po zmerni ceni. Ta možnost dostopa je dosti varnejša od javnih računalnikov, saj uporabljamo svoje naprave. Če brezžična dostopna točka ni dovolj zavarovana, lahko pride do **prestrežanja omrežnega**



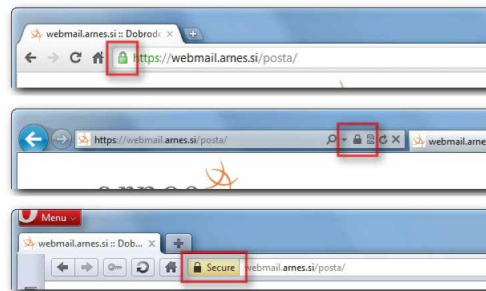
Pozor, ne gre za Wi-Fi letališča ampak ad-hoc brezžično omrežje, ki ga je neznanec postavil na svojem prenosniku.

prometa, kar pomeni, da lahko neznanec spremlja ves naš omrežni promet.


Prav posebno previdnost pa zahteva t. i. **ad-hoc brezžično omrežje**, ki ga **ustvari nekdo kar na svojem računalniku**. V tem primeru se povežete neposredno na prenosnik neznanca! Taka omrežja so po navadi prikazana z malce drugačno ikono. Zato se vedno pozanimajte, katero je pravo omrežje hotela ali cybercafeja. Če lahko izbirate med nešifriranim in šifriranim omrežjem, izberite šifriranega (vprašajte natakara ali receptorja za geslo).

PA ŠE NEKAJ NASVETOV ZA VARNO POVEZOVANJE:

- Če je le mogoče, vzpostavite povezavo z Wi-Fi omrežjem, ki je zaščiteno z geslom.
- V nezaščitene javnih Wi-Fi omrežjih posredujte uporabniško ime in geslo (prijava v elektronsko pošto, družbena omrežja) le, če veste, da bo prenos podatkov varen. Torej na pametnem telefonu **uporabite uradno aplikacijo**, če pa uporabljate brskalnik, bodite **pozorni na zaklenjeno ključavnico, ki kaže na šifrirano oz. varno povezavo**.



- **Nikoli ne izvajajte finančnih transakcij v nezaščitenih javnih omrežjih** (vpis številke kreditne kartice v spletni trgovini ali opravljanje bančnih storitev).

 Izklopite samodejno povezovanje in se povežite na Wi-Fi, le, ko ga potrebujete. Tudi baterija vaše pametne naprave se bo počasneje praznila, če ne boste nenehno povezani.

3. Mobilni internet

Najvarnejša je uporaba mobilnega interneta za prenos podatkov (GPRS, EDGE, UMTS, poenostavljeno tudi kar 3G). Slaba stran so morebitni visoki stroški, ki pri tem nastanejo, še posebej v tujini (roaming). Stroške lahko povzročijo tudi določene aplikacije, ki se v ozadju brez vaše vednosti povezujejo na internet.

V tujini izklopite gostovanje (roaming) ali pa podatkovno povezavo vklopite le po potrebi. Če je le mogoče, v tujini uporabljajte SIM-kartico domačega operaterja z možnostjo zakupa prenosa podatkov.



Več informacij o spletnih tveganjih:
www.varninainternetu.si




Bodite obveščeni o aktualnih spletnih goljufijah
facebook.com/varninainternetu

POMEMBNE ŠTEVILKE

V primeru izgube ali kraje mobilne naprave takoj pokličite svojega operaterja in prekličite SIM-kartico. Nekdo lahko uporablja vaš telefon in vam povzroči stroške.

Klicni center operaterja:

 Če je omogočen neposreden dostop do drugih uporabniških računov (elektronska pošta, družbena omrežja), nemudoma spremenite vsa gesla! Nekdo lahko z vaše naprave dostopa do vaših profilov.

Če krajo prijavite policiji, jim posredujte tudi **IMEI-številko naprave**. Najdete jo na embalaži, na garancijskem listu in na nalepki pod baterijo mobitela. IMEI se izpiše tudi na zaslonu mobitela po vnosu ukaza *#06#.

IMEI številka naprave:

Izgubljeno ali ukradeno kartico (debetno ali kreditno) takoj prijavite izdajatelju! Zapišite si telefonsko številko klicnega centra, najdete jo na hrbtne strani kartice. Sum kraje kartice obvezno prijavite najbližji policijski postaji, čeprav ste v tujini.

Preklic kartice:

 Še več nasvetov o **varni rabi kartic** je pripravilo Združenje bank Slovenije.



VARNI NA INTERNETU,
TUDI NA POČITNICAH

si·cert 



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE,
ZNANOST IN ŠPORT

Program ozaveščanja Varni na internetu
v celoti financira Ministrstvo za izobraževanje,
znanost in šport.