Kako zaštititi svoje osobne podatke online?

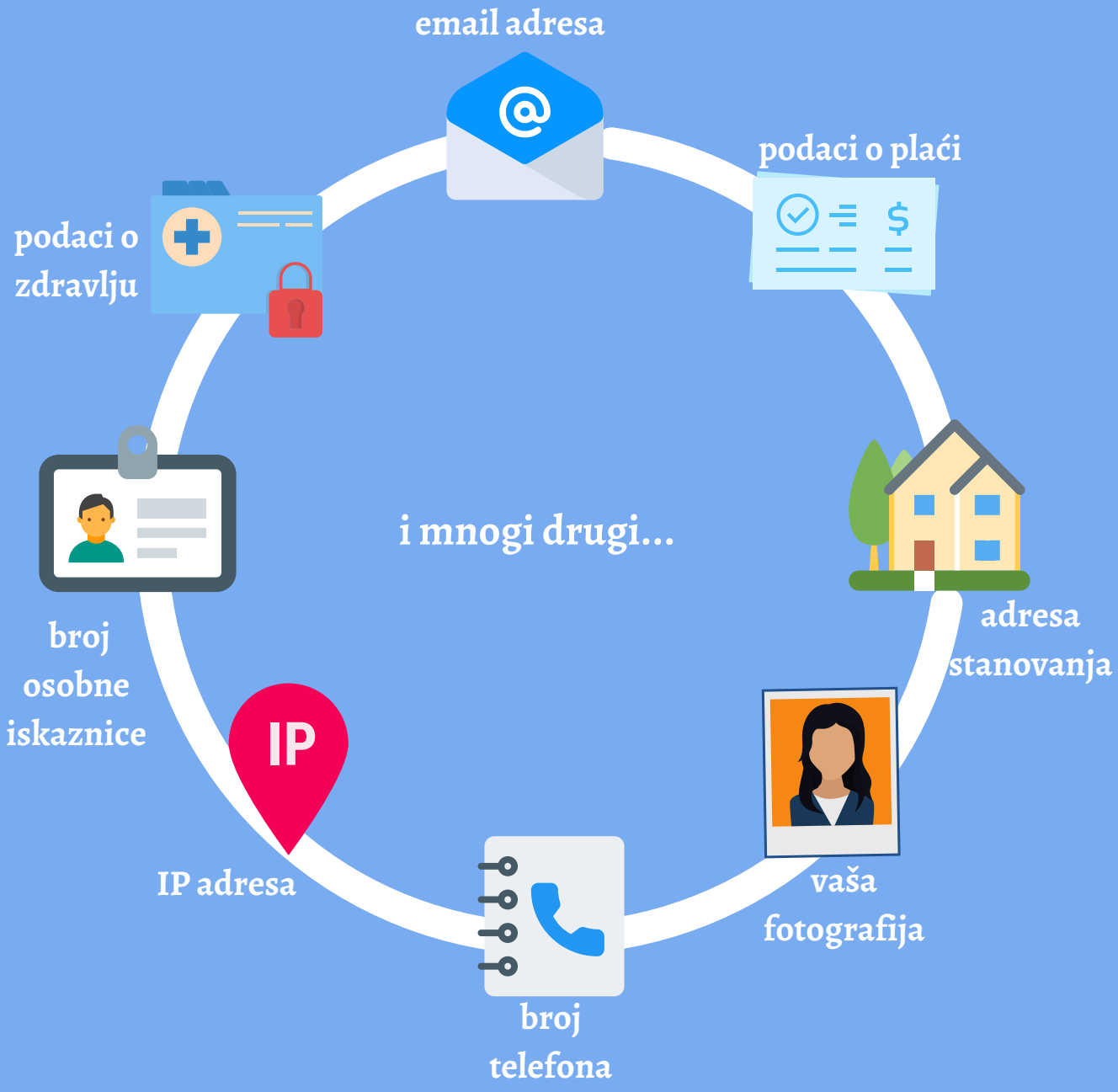
Saznajte kako se zaštititi na vrijeme

azop

www.azop.hr

Znate li što su sve osobni podaci?

osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi.



Zašto je zaštita osobnih podataka važna?

Znate li da ako vaši osobni podaci završe u rukama nepoznate i neprovjerene osobe postoji mogućnost nezakonite objave osobnih podataka, krađe identiteta i drugih zlouporaba osobnih podataka!

Moguće je da pretrpite materijalnu i/ili nematerijalnu štetu!

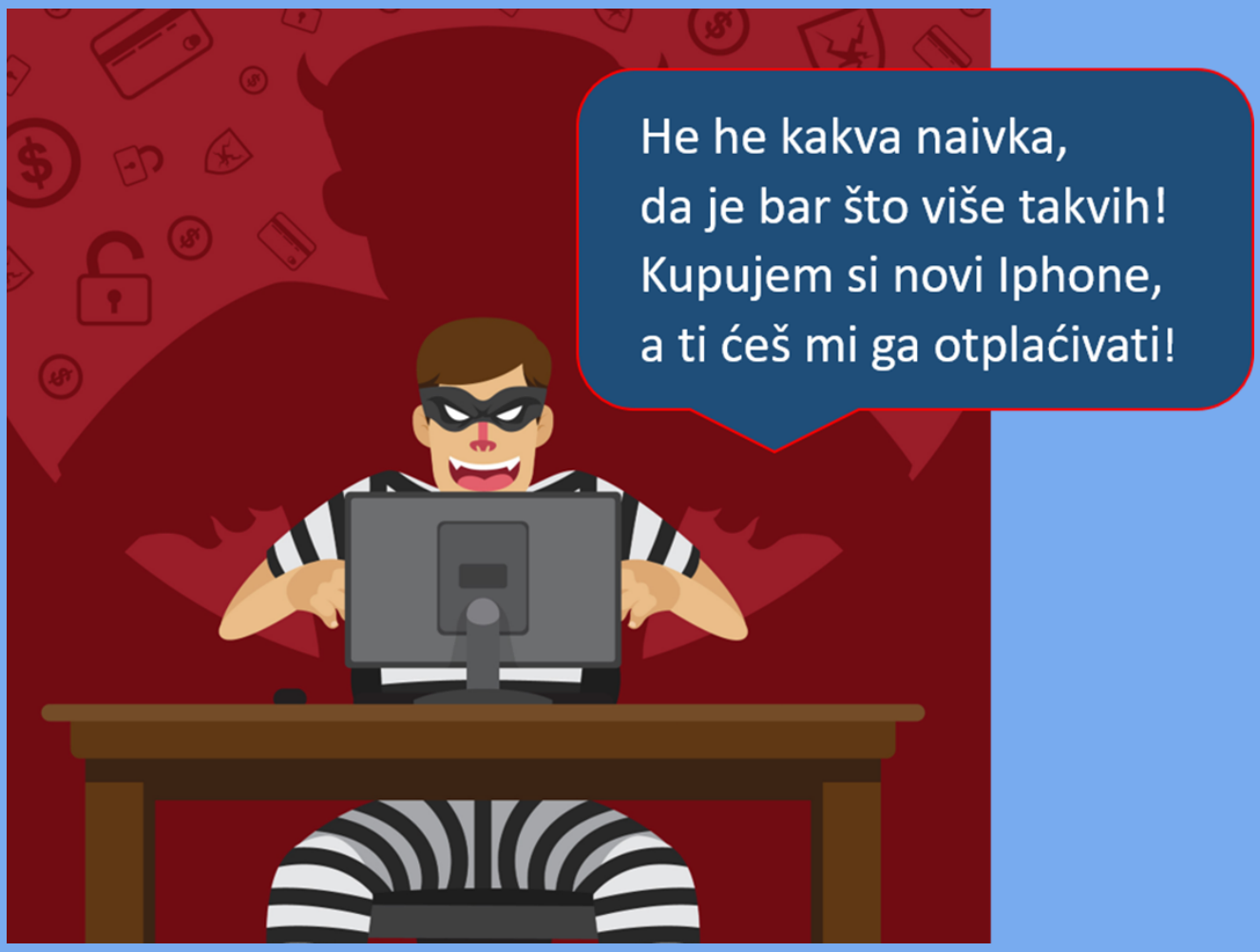
Vaši osobni podaci, vaša su najvrjednija imovina! Čuvajte ih!

Što je veći opseg osobnih podataka koje netko od vas traži putem interneta (primjerice potpuna preslika osobne iskaznice) to su veće mogućnosti zlouporabe!

BUDITE OPREZNI KOME ŠALJETE SVOJE OSOBNE PODATKE!

azop

Znate li da ukoliko pošaljete presliku osobne iskaznice (primjerice u uvjerenju da ste dobitnik u nagradnoj igri putem društvenih mreža), osoba s druge strane s tim podacima može ugovoriti uslugu na daljinu (primjerice kupiti novi mobitel) na vaše ime?



Ne šaljite preslike osobnih iskaznica, kreditnih kartica nepoznatim osobama putem društvenih mreža ili e-maila! Ukoliko ste osvojili nagradu na nagradnoj igri, nitko vas neće tražiti da putem inboxa dostavite presliku osobne iskaznice ili kreditne kartice!

Pazite što objavljujete na internetu!

Osim u ostvarivanju materijalne koristi, vaši osobni podaci mogu biti zlouporabljeni na način da osoba koja želi naštetiti vašem ugledu i časti te narušiti vašu privatnost, otvori lažni profil na društvenoj mreži u vaše ime te na tom profilu objavljuje sadržaj vulgarnog ili uvredljivog karaktera.

ZAPAMTITE: JEDNOM OBJAVLJEN SADRŽAJ ŠIRI SE BRZINOM MUNJE I NEMOGUĆE GA JE UKLONITI! Sadržaj koji ne biste htjeli da vide svi, ne objavljujte na internetu!

Ne objavljujte na društvenim mrežama slike i videozapise svoje maloljetne djece, datume rođenja, adrese, fotografije osobnih dokumenata, slike i videozapise unutrašnjosti kuće/stana, informacije da vas nema kod kuće, da ste otputovali i sl.

To je pozivnica provalnicima, zlostavljačima, pedofilima i osobama različitih zlih namjera!

azop

RAZMISLITE PRIJE SVAKE OBJAVE!

I još malo savjeta...

- dobro pročitajte pravila privatnosti na društvenim mrežama koje koristite, nemojte nekritički na sve „kliknuti AGREE“

- vaš profil neka bude vidljiv samo vašim prijateljima, a ne svim korisnicima te društvene mreže

- prilikom odabira prijatelja na društvenim mrežama, kao i u stvarnom životu, treba biti na oprezu i ne otkrivati osobne podatke i svoje privatne informacije osobama koje u stvari ne poznajemo

Neke od najčešćih internetskih prijevara

Ransomware

Zaprimili ste e-mail sadržaja:

Instalirali smo na Vaše računalo zlćudni računalni program (malware) putem kojeg smo ostvarili pristup vašim osobnim podacima. Uplatite 1500 EUR u bitcoinima ako želite spriječiti da javno objavimo vaše osobne podatke.

ILI

Nakon što otvorite privitak koji ste dobili u e-mailu, ucjenjivač preuzima kontrolu nad Vašim računalom i šifrira sve datoteke, a bez poznavanja posebnog ključa više ne možete pristupiti svojim osobnim podacima. **Ucjenjivač od Vas traži plaćanje otkupnine, a zauzvrat ćete dobiti ključ za dešifriranje svojih podataka.**

Ne odgovarajte na ovakve poruke, ne uplaćujte ucjenjivačima novce, ovakve poruke odmah obrišite! Ako ste otvorili privitak koji sadrži maliciozan kod, obavijestite o tome policiju! Ažurirajte lozinku za pristup elektroničkoj pošti! Svoje korisničke podatke, lozinke i ostale osobne podatke nemojte upisivati na sumnjivim internetskim stranicama!

azop

Phishing

internetske prijevare u vidu lažnih e-poruka koje izgledaju kao da su ih poslale legitimne organizacije (primjerice banka ili internet stranica za kupovinu), a koje primatelja navode na dijeljenje osobnih, financijskih ili sigurnosnih podataka.

Na ovaj način prevaranti dobivaju pristup korisničkim imenima, lozinkama ili podacima s kreditnih kartica.

Kako to spriječiti?

- **budite oprezni ako se od vas u e-poruci traže "osjetljivi podaci"** (primjerice podaci kartice, zaporka online računa i slično)
- **pažljivo pogledajte e-poštu:** usporedite adresu s prethodnim stvarnim porukama iz vaše banke. Provjerite pravopis i gramatiku
- **nemojte odgovarati na sumnjivu e-poruku:** proslijedite je svojoj banci tako da sami upišete pravilnu e-mail adresu
- **nemojte kliknuti na poveznicu niti preuzeti privitak**, već upišite adresu u preglednik
- **redovito ažurirajte softver**, uključujući vaš preglednik, antivirusni i operativni sustav!

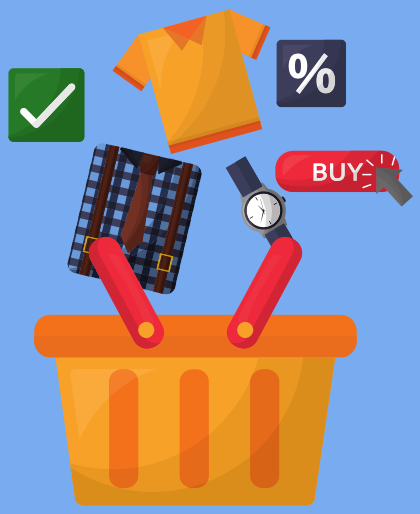
azop

Online kupovina

online ponude često su povoljne, međutim čuvajte se "predobrih ponuda" na neprovjerenim online shopovima. **KAD NEŠTO ZVUČI PREDOBRO DA JE ISTINITO, GOTOVO SIGURNO JE LAŽ!**

SAVJETI:

- ✓ koristite provjerene online trgovine
- ✓ istražite recenzije prije kupovine
- ✓ ako plaćate karticom, prilikom kupnje plaćajte samo preko sigurnog pružatelja usluge plaćanja - traže li uslugu prijenosa sredstava preko banke ili alternativno? Dobro razmislite!
- ✓ plaćajte samo kada ste spojeni na sigurnu vezu - izbjegavajte besplatni ili otvoreni WiFi
- ✓ plaćajte samo na sigurnom uređaju - redovito ažurirajte operativni sustav i sigurnosni softver



azop

Instaliranje aplikacija iz nepoznatih izvora

Prilikom instaliranja aplikacije za pametni telefon, često se od korisnika traži dopuštenje za pristup kameri, datotekama ili mikrofonu.

Sve navedeno može dovesti do zlouporabe osobnih podataka pohranjenih u uređaju. DOBRO promislite prije nego dozvolite takvim aplikacijama pristup svojim osobnim podacima!

NIKADA ne instalirajte aplikacije s nepoznatih i neprovjerenih izvora!

azop

Kako se zaštititi?

Voditelji obrade/izvršitelji obrade (organizacije, društva poput banke, teleoperatera, bolnica i slično) dužni su zaštiti vaše osobne podatke i raspolagati s njima sukladno propisima o zaštiti osobnih podataka, ali prvi i najvažniji korak u zaštiti vaših osobnih podataka trebate učiniti sami.

Savjeti:

- **Obavezno koristite antivirusne programe**

Redovito ažurirati i nadograđivati antivirusne i ostale sigurnosne alate kako bi mogli detektirati potencijalne prijetnje

- **Nadograđivati i ažurirati operacijske sustave i sve aplikacije na računalu**

uvijek imajte najnovije verzije

- **Ne otvarajte e-mailove i poruke koji stižu sa sumnjivih adresa/brojeva, neuobičajenih domena, pogotovo ne otvarajte sumnjive privitke**

ako Vam je identitet pošiljatelja sumnjiv, ne otvarajte e-mail! (npr. amagnus@india.com) Obratite pažnju i na ekstenziju datoteke u privitku, ne otvarajte privitke s neuobičajenim ekstenzijama kao što su .jar, .ace.

- **Ako e-pošta koju ste primili sadrži sumnjiv URL, prijeđite mišem preko URL adrese u mailu, ali ne klikajte!**

trebali biste vidjeti pravi URL do kojeg ćete bit preusmjereni. Ako izgleda sumnjivo ili završava kao .exe, .js or .zip, ne otvarajte link!

- **Kada prestanete koristiti društvenu mrežu, e-mail preglednik, ili neku drugu internetsku uslugu, odjavite se s računa**

ako ostanete prijavljeni i nastavite surfati, to je isto kao da ste ostavili otključanu kuću: hakerima i ucjenjivačima uvelike olakšavate posao.

- **Koristite snažne lozinke:**

- 16 ili više znakova (što više to bolje),
-velika slova (ABCDEFGH…),
-mala slova (abcdefgh…),
-brojke (123456…),
-simbole (@#$%{ } [ ] ( ) / \ ‘ ” , ; : . < >…).

SAMOZAŠTITNO PONAŠANJE NAJBOLJA JE PREVENCIJA!

azop

Na poveznici https://haveibeenpwned.com/ provjerite SVE svoje adrese elektroničke pošte koje koristite kao korisničko ime za prijavu u internet servise ili usluge, na ovaj način možete provjeriti jesu li kompromitirane, odnosno nalaze li se u hakerskim bazama.

Ukoliko utvrde da je određena adresa elektroničke pošte kompromitirana, savjetujemo sljedeće:

- iz predostrožnosti promijeniti lozinku za tu adresu elektroničke pošte u novu snažnu sigurnosnu lozinku
- u svim internet servisima i uslugama u kojima ste koristili tu adresu elektroničke pošte kao korisničko ime za prijavu (npr. društvene mreže, internetska trgovina, itd.) za svaki od tih servisa i usluga kreirajte novu zasebnu snažnu sigurnosnu lozinku. Ukoliko ta internetska usluga ili servis nude tu mogućnost, preporučljivo bi bilo uključiti **opciju dvostruke autentifikacije.**

azop

A što s kolačićima?

Kolačići (cookies) su male datoteke koje internetski preglednik (eng. web browser) pohranjuje na računalo, mobilni uređaj ili neki drugi uređaj kojim je korisnik posjetio internetsku stranicu.

Postavljanje kolačića na vaše uređaje je dozvoljeno samo uz vašu privolu te prethodnu jasnu informaciju koji će se podaci prikupljati i u koju svrhu, a u skladu sa propisima o zaštiti osobnih podataka. Od privole su izuzeti samo kolačići koji su tehnički neophodni za normalno funkcioniranje stranice ili pružanje usluge na zahtjev korisnika.

PRIJE NEGO ŠTO PRIHVATITE KOLAČIĆE, PROČITAJTE PAŽLJIVO OBAVIJESTI O TOME KOJE KOLAČIĆE STRANICE KORISTE, U KOJE SVRHE IH KORISTE! MNOGE INTERNETSKE STRANICE KORISTE MARKETINŠKE KOLAČIĆE, KAKO BI VAM PRIKAZIVALI CILJANE OGLASE I DIJELE VAŠE OSOBNE PODATKE S TREĆIM STRANAMA! ZAŠTITITE SVOJ VIRTUALNI IDENITET I SVOJE OSOBNE PODATKE!

Besplatno preuzmite aplikaciju GDPR Hrvatska i u svakom trenutku budite informirani o svojim pravima!

GDPR HRVATSKA

Download on the App Store

GET IT ON Google Play

Skenirajte za više informacija o vašim pravima

Čuvajmo svoje osobne podatke!

www.azop.hr

azop