POVODOM 15.OŽUJKA – SVJETSKOG DANA PRAVA POTROŠAČA

CONSUMERS INTERNATIONAL I HRVATSKA UDRUGA ZA ZAŠTITU POTROŠAČA (HUZP)

VAM PREPORUČUJU

10 NAJBOLJIH NAČINA KAKO SE ZAŠTITITI KAO ON LINE POTROŠAČ

Internet nam danas pruža velik raspon mogućnosti i izbora. Možemo se jednostavno spojiti i komunicirati sa prijateljima i članovima obitelji širom svijeta, obaviti našu tjednu kupovinu i obaviti plaćanje naših računa - sve na dodir gumba, čime štedimo i vrijeme i trud. Za sve ove aktivnosti koristimo naše osobne podatke – bankovne podatke za uplatu, fotografije i komentare i našu adresu za dostavu, te naše telefone za kontakte. Što je više podataka o nama online, rastu i rizici - poput krađe identiteta, hakiranja, ucjena i prijevara.

Slijedi niz jednostavnih savjeta koje svi mi možemo koristiti kako bi zaštitili naše osobne podatke online, te tako koristili internet sigurno:

1. **Koristiti različite i izvorne lozinke**

- To je najjednostavnija stvar za promjenu, ali i nešto što svi možemo učiniti. Važno je imati drugi pin ili lozinku za svaki vaš račun, tako da ako čak i neki račun bude hakiran , ostali će biti zaštićeni. Najvažnije je redovito mijenjati lozinku vašeg glavnog računa, jer se sa njega mogu ponovno postaviti(resetirati) zaporke za vaše druge račune. Ako vam se čini da ste hakirani,(a ljudi često ne znaju), odmah treba promijeniti lozinku.

- Izbjegavajte odabir očigledne lozinke, kao što su mjesto ili datum rođenja ili ime djeteta , jer je to lako otkriti. Umjesto toga koristite složene riječi ili fraze koje koriste velika slova, brojeve i interpunkcije za dodatnu sigurnost. Možete koristiti servis za lozinke koji osigurava sve vaše lozinke tako da trebate zapamtiti samo jednu.

2. **Koristite sigurnosne postavke**

- Većina tvrtki nudi potrošačima niz mogućnosti za osiguravanje uređaja, kao što su postavke privatnosti i lozinki. Uvijek treba postaviti zaporku na mobitel - iznenađujuće je koliko ljudi to ne čini, a bez toga su sve vaše aplikacije, karte, kalendari, kontakti, podaci o plaćanju i mnogo osobnih podataka lako dostupni. Uzmite vremena i proučite postavke privatnosti , postavite si kakve želite i nemojte se sramiti tražiti pomoć za to.

3. **Budite oprezni što razmjenjujete na društvenim mrežama**

- Ako se koristite društvenim mrežama ,trebate znati da sve što stavljate na društvene mreže može pogledati bilo tko i bilo gdje, pa zato razmislite prije nego bilo što

stavljate. Odvojite vrijeme i proučite postavke privatnosti, kako bi izbjegli dijeljenje osobnih podataka, a posebno onih koji bi mogli izgraditi potpunu sliku o vama, kao što su adresa, radno mjesto, planovi za godišnji odmor i imena članova bliske obitelj.

4. Oprezno sa Wi-Fi

- Besplatni bežični pristup internetu na javnim mjestima je jako zgodan, ali sigurnost može biti problem budući da dijelite mrežu sa puno ljudi. Koristite 'https' ako ste na Wi-Fi mreži za povezivanje s e-poštom, društvenim mrežama ili drugim osobnim računima. Ako ste kod kuće, uvijek postavite lozinku za pristup na mrežu.

5. Nemojte nasjedati na varljive poruke I tekstove

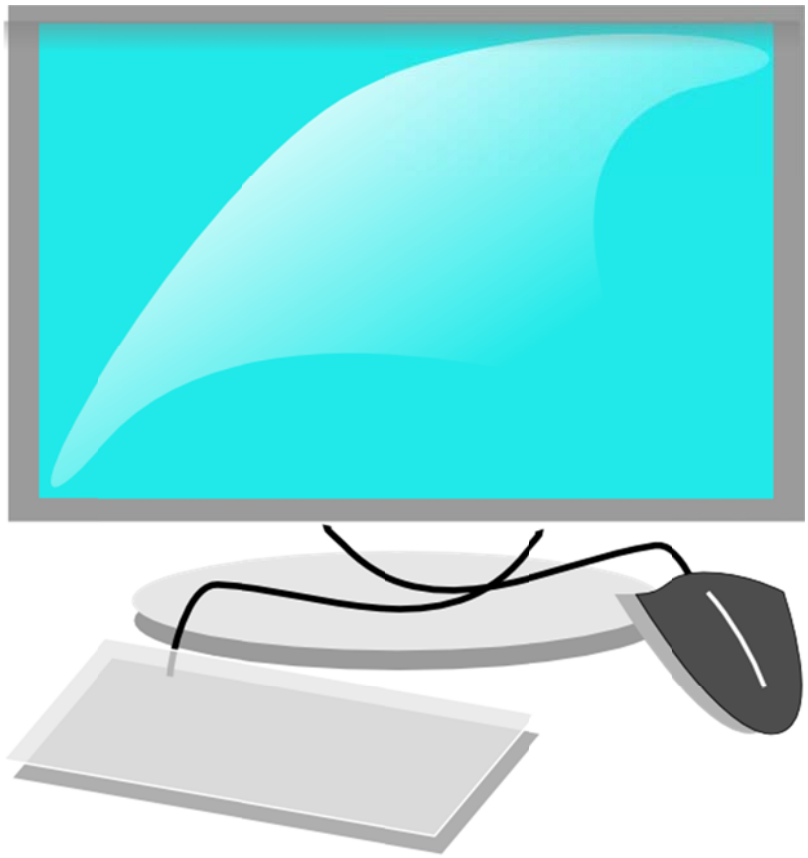
- Vrlo je lako namamiti ljude porukom da su dobili neku lutriju ili neku nagradu, ali budite oprezni. Ne vjerujte ponudama ili nagradama koje se čini predobre da bi bile istinite. Ako primite e-mail poruku koja navodi da ste primili veliku sumu novca i da trebate dati svoje bankovne podatke kako bi to primili- budite oprezni! To je jednostavan način da vam hakiraju bankovne podatke i da vas prevare.
- Ako primite poruku od vaše banke ili tvrtke koja traži vaše podatke, proslijedite to njihovoj službi za korisnike i provjerite je li poruka njihova i do tada ne šaljite nikakve podatke.

6. Izbjegavajte otvaranja privitaka e-pošte ili neobične linkove

- Virusi se često šalju putem e-mail privitaka ili linkova. Virus može ugroziti uređaj i pristup osobnim podacima. Ako ne prepoznajete pošiljatelja ili ne znate sadržaj privitka, nemojte poštu otvarati, isto vrijedi i za linkove od prijatelja. Ako ste poslali nešto prijateljima i ako vam je njihov račun pomalo čudan uvijek ih pitajte prije nego što poštu otvorite, jer je vjerojatno njihov račun hakiran.

7. Koristite privremene e-mail adrese

- Prilikom prijave na web stranice često vas traže adresu e-pošte i kontakt informacije, čak i ako samo jednom koristite uslugu. Ako želite izbjeći primanje elektroničkih poruka marketinga i prodaje, možete postaviti privremenu adresu elektroničke pošte. Korištenje privremene e-mail adrese pruža siguran način prijave na web stranice bez da morate dati svoju stvarnu e-mail adresu. Postoje mnoge web stranice koje nude ovu uslugu, jednostavno pretražite „adrese privremene elektroničke pošte“ i otkrijete mogućnosti.



8. Provjerite jesu li vaša plaćanja sigurna

- Prilikom plaćanja online, potražite web adrese koje počinju sa **'https://',**a ne samo **'http'**," s „ je znak za siguran. To znači da su ti podaci šifrirani dok putuju između web stranice i računala. Također treba biti **zeleni lokot** na lijevo ili desno od web adrese koji pokazuje da je web-mjesto sigurno.

- Korisno je također redovito provjeravanje računa nakon plaćanja kako bi se provjerilo jesu li ispravni plaćeni iznosi, te da nema lažnih transakcija.

9. Softver uvijek ažurirajte

- Uključivanje automatskog ažuriranja za vaš operativni sustav i softver je stvarno jednostavan način da si osigurate najbolje dostupnu zaštitu, budući da svako ažuriranje stvara dodatnu sigurnost automatski. Ako imate stari softver koji nema najnoviju zaštitu, jednostavno uključite automatsko ažuriranje za svoje uređaje.

10. Instalirajte i ažurirajte vatrozid, antivirus i protu-uhoda softver

- Ovo je važno imati na svim uređajima jer će vatrozid spriječiti neovlaštene osobe da vam hakiraju računalo, antivirusni softver štiti računalo od virusa, a protu-uhoda traži programe koji špijuniraju po računalu tražeći lozinke, račune i osobne podatke. Bez ove zaštite vaši su uređaji u velikom riziku od hakiranja.