A1 Digitalni vodič za bezbednost na netu

Ako čitaš ove redove, znači da već poznaješ stranicu A1 Kutak za bezbedan net i da tvoje uzbudljivo putovanje kroz svet sajber bezbednosti može da počne. Za odgovorno i bezbedno istraživanje neograničenih mogućnosti koje ti online svet pruža savetujemo ti da se prvo dobro informišeš o potencijalnim opasnostima koje mogu da ti naprave mnogo problema ukoliko ne vodiš računa.

Pred tobom su neki od osnovnih pojmova i zanimljivih podataka koji će ti pomoći da se lakše snađeš u digitalnom svetu.

Spremi se, polećemo!

Fišing (Phishing)

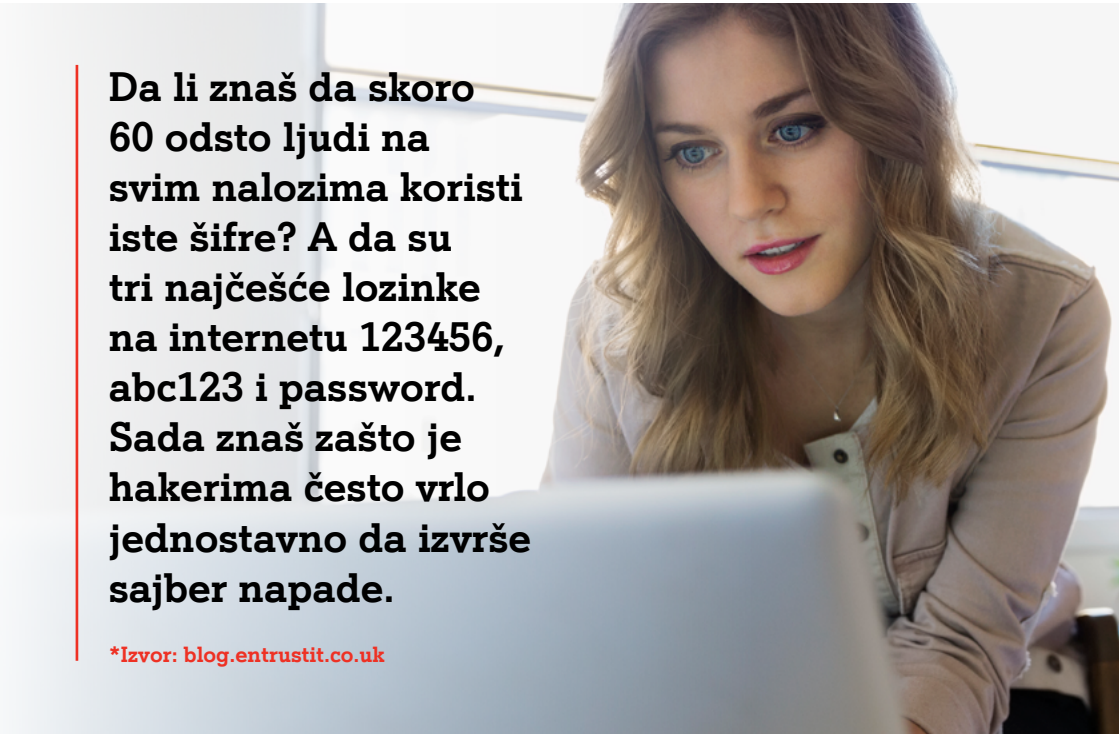
Fišing (Phishing) – Jedan od najstarijih i najučestalijih sajber napada koji se najčešće pojavljuje u obliku imejla u kojem se od tebe traži da na nešto klikneš. Ime vodi poreklo od engleske reči za pecanje (fishing), samo što se umesto riba love lični podaci, brojevi kreditnih kartica, važni kontakti i poverljive informacije, a umesto mamaca se koriste izgovori o dobijenoj uplati, nasledstvu ili nagradi. Ukoliko ti bilo ko, bilo kada, traži da klikneš na neki link u imejlu, NE PECAJ SE!

Da li si znaš da se svakog dana širom sveta dogodi više od 135 miliona napada ove vrste?
To znači da se dogodi skoro 100.000 pokušaja fišinga u jednom minutu.

***izvor phishingbox.com**

Šifra ili password

Šifra ili password (popularno pass) – Niz slova i brojeva koji će testirati tvoju kreativnost i memoriju. Kada praviš šifre za imejl ili korisničke naloge na različitim sajtovima, trudi se da uvek budu kombinacija slova, brojeva i specijalnih znakova, sa najmanje 8 karaktera. Ako se pitaš zašto je najmanje 8 karaktera neophodno, odgovor je jednostavan: to je minimalan broj karaktera za bezbednu šifru, što su procenili i popularni servisi (Gmail) i društvene mreže (Facebook, Instagram). Zato, kada smišljaš lozinku, slobodno pusti mašti na volju! Osloni se na sopstvenu kreativnost i napiši kompleksnu reč ili više reči. Ne štedi na broju slova, kombinuj velika i mala. Možda se nađe mesta i za neki simbol ili broj – što kreativnije, to sigurnije.



Da li znaš da skoro 60 odsto ljudi na svim nalozima koristi iste šifre? A da su tri najčešće lozinke na internetu 123456, abc123 i password. Sada znaš zašto je hakerima često vrlo jednostavno da izvrše sajber napade.

***Izvor: blog.entrustit.co.uk**

Javna mreža (Public Wi-Fi)

Javna mreža (Public Wi-Fi) – Slično kao i s javnim toaletima, u javnu mrežu ulazi samo ako nemaš drugu mogućnost, jer ne znaš ko je sve tu bio pre tebe i šta sve možeš da „zakačiš" dok tamo boraviš. Koristi samo u krajnjoj nuždi!

Da li znaš da izraz Wi-Fi zapravo ne znači ništa? Nastao je kao kovanica jedne brending kampanje 1999. godine za neprofitnu organizaciju WiFi Allience.

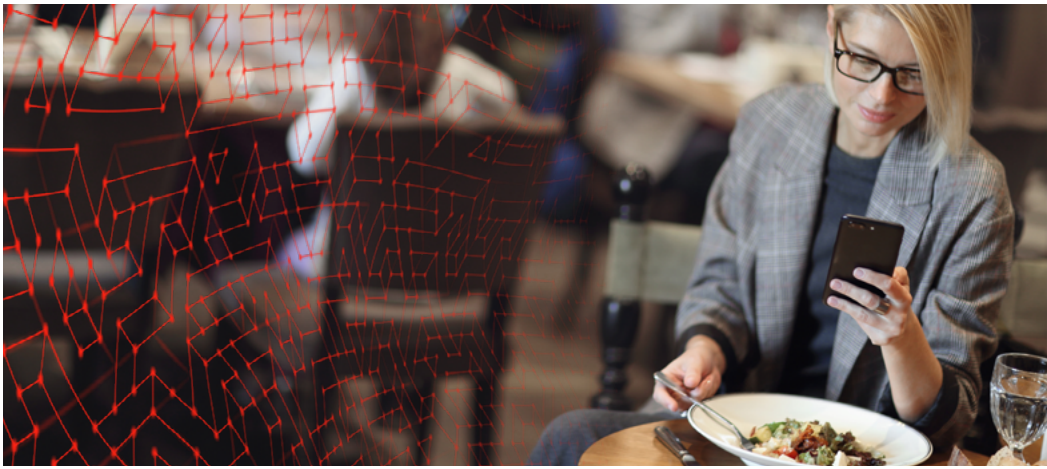
***Izvor: airtime.com**

Mobile data

Mobile data – Drugo ime za mobilni internet i ikonica koja bi morala da ti bude uključena na mobilnom telefonu za pristup internetu. Koliko će biti brz tvoj mobilni internet, zavisi od mreže koju koristiš i broja Mbps.

Da li znaš da je od januara 2021. godine bilo 4,66 milijardi aktivnih korisnika interneta širom sveta – 59,5 odsto svetske populacije? Od ovog ukupnog broja 92,6 odsto (4,32 milijarde) pristupilo je internetu putem mobilnih uređaja. Procenjuje se da će u 2022. godini mesečni saobraćaj mobilnog interneta na svetu dostići rekordnih 77,5 milijardi gigabajta.

***izvor statista.com**



Etički hakeri

Etički hakeri – Za razliku od onih loših, etički hakeri koriste svoje veštine kako bi otkrili slabosti nekog sistema i onda aktivno rade na tome da preduprede eventualne sajber napade. Takođe, uvek se ljubazno jave komšijama i prevode starije sugrađane preko prometnih ulica.

Da li znaš da najveći broj etičkih hakera dolazi iz Indije i SAD? U ove dve zemlje živi skoro polovina ukupnog broja etičkih hakera na planeti i mogu da zarade milionske sume godišnje.

Upoznajte neke od njih.

Antivirus

Antivirus – Rešenje za većinu digitalnih problema! Radi se o softveru koji aktivno čuva jedan ili više uređaja od virusa ili „zlonamernih programa“ (Malware). Obrati pažnju kada koristiš neki antivirus program, jer će se neretko dešavati da su to u stvari virusi koji se lažno predstavljaju.

Da li znaš da se prvi virus namenjen pametnim telefonima pojavio 2005. godine i zvao se Commwarrior?

USB drive

USB drive – Prenosivi uređaj na koji možeš da prebaciš onoliko podataka (slike, muziku, filmove, knjige) koliko USB ima memorije. Osim podataka, moguće je preneti i virus, pa zato ne koristi nepoznate USB uređaje na svom računaru i ne kači svoje USB uređaje na nepoznate računare.

Da li znaš da broj koji stoji pored USB (1.0, 2.0, 3.0) određuje brzinu kojom skidaš ili unosiš različite fajlove? Što je broj veći, to je i brzina veća.

SPAM

SPAM – Neželjena elektronska pošta su svi imejlovi koji ti stignu, a koje ne želiš. To mogu biti informacije, reklame, pitanja, raznorazne ponude itd. Neretko mogu biti i zlonamerni pokušaji dobijanja pristupa uređaju i krađe podataka. Ukoliko sadrže maliciozni link, pogađaš, u pitanju je jedan od oblika **fišinga**. Nikada nemoj da klikneš na neprovereni link i ne otvaraj prilog u imejlu koji je sumnjivog porekla.

Da li znaš da je u periodu između 2020. i 2021. godine čak 85 odsto ukupnog broja svih imejlova na svetu bilo spam? Zvuči neverovatno, zar ne?

***Izvor - dataprot.net**

Bot

Bot – (skraćeno od robot) – kompjuterski program dizajniran da imitira ljudsko ponašanje ili upravlja nekim drugim programom. Na primer, na društvenim mrežama možeš da naletiš na lažne profile – botove – koji pokušavaju da te dodaju za prijatelja ne bi li došli do tvojih informacija. Slično je i sa popularnim sajtovima na kojima ti se otvori prozor za čet s nekom osobom na različite teme. Pogađaš, ta osoba nije stvarna nego je bot.

Da li znaš da je 2016. godine kompanija Twitter zajedno s kompanijom Microsoft predstavila Tai, prvi bot namenjen tome da piše tvitove na osnovu interakcija s korisnicima širom sveta? Bilo je potrebno samo 16 sati da bude ukinut zato što je za to vreme od ljubaznog bota evoluirao u propagandno sredstvo hakerskih organizacija za širenje fašističke ideologije, ksenofobije i rasizma.

Malware

Malware – Krovni naziv za zlonameran/štetan softver koji ne želiš da ti se nađe u računaru ili telefonu – virusi, trojanci, kompjuterski crvi (Worms), Spyware, Adware ili Ransomware, sve su to mnogobrojni oblici Malware-a koji za cilj imaju da ti ukradu privatne podatke, uspore rad računara ili plasiraju reklame koje ne želiš da gledaš.

Da li znaš da je Malware skoro pa nemoguće izbeći? To se pre svega odnosi na reklame, jer na velikom broju sajtova dobijaš softver za plasiranje reklama automatski.

Ransomware

Ransomware – Jedan od oblika **Malware-a** koji poslednjih godina postaje sve masovniji. Ime je nastalo kao kovanica engleske reči ransom (otkup) i označava maliciozni softver koji, nakon što „inficira" računar, limitira ili potpuno blokira korisnika da pristupi podacima uz poruku da će podaci biti ponovno dostupni ukoliko se uplati naznačena suma novca (obično neka anonimna kriptovaluta). Ransomware je digitalni oblik ucene ili iznude. Korisnici računara ovaj maliciozni softver najčešće dobijaju kroz imejl, tj. kroz spam i fišing imejlove, ali može doći i usled skidanja sumnjivih fajlova sa interneta, posećivanjem sumnjivih sajtova ili povezivanjem zaraženih USB uređaja na računar.

Da li znaš da je samo u 2021. godini potrošeno oko 20 milijardi dolara na otkup podataka pogođenih Ransomware-om, a procenjuje se da će do 2031. godine ta cifra iznositi neverovatnih 265 milijardi dolara?

***Izvor: cloudwards.net**

Cryptoware ili Cryptominer

Cryptoware ili Cryptominer – Specifičan oblik **Ransomware-a** dizajniran da napada računare koji rudare, odnosno stvaraju kriptovalute poput bitcoina ili eterijuma. Umesto da se traži otkup, Cryptoware radi u tajnosti i preusmerava resurse sve dok ne bude otkriven. Ovaj oblik malicioznog softvera je postao popularan s porastom interesovanja javnosti za kriptovalute. Napad se svodi na pokretanje malicioznog programa koji često iskorišćava resurse računara (mreža, grafička karta, procesor, memorija, disk), zavisno od kriptovalute, i tako otežava rad na računaru. Često sajtovi imaju Cryptominer-e umesto reklama i otvoreno informišu korisnike o tome kao načinu da zarade za održavanje sajta ili web servisa, pa korisnik može da bira da li hoće da pusti reklame ili Cryptominer kako bi dobio pristup sadržaju sajta (obično su to nelegalni video striming i torent sajtovi).

Da li znaš da je ovaj oblik napada veoma teško otkriti jer će hakeri najčešće uzimati veoma male količine resursa kako ne bi bili otkriveni?

Backdoor

Backdoor – Što u prevodu znači sporedan ulaz (vrata) jeste metod koji hakeri koriste prilikom napada, ali se odnosi na mogućnost pristupa sistemu zaobilazeći sigurnosne mere. Može biti u softveru za šifrovanje ili čak hardveru, kao što su procesori. Svesni da će, pre ili kasnije, kompjuter biti očišćen od virusa, hakeri naprave Backdoor, diskretan softver koji je nevidljiv za većinu antivirusa, kako bi i nakon što je kompjuter „izlečen" imali pristup poverljivim podacima. Što je haker bolji, to će i Backdoor biti teže detektovati. Backdoor je teško otkriti jer je najčešće dizajniran da bude sakriven, ali da u isto vreme lako i neopaženo omogućava nekome pristup sistemu.

Da li znaš da se Backdoor najčešće koristi u industrijskoj špijunaži? To je jedan od glavnih razloga zbog čega velike kompanije svake godine povećavaju budžete za sajber zaštitu.

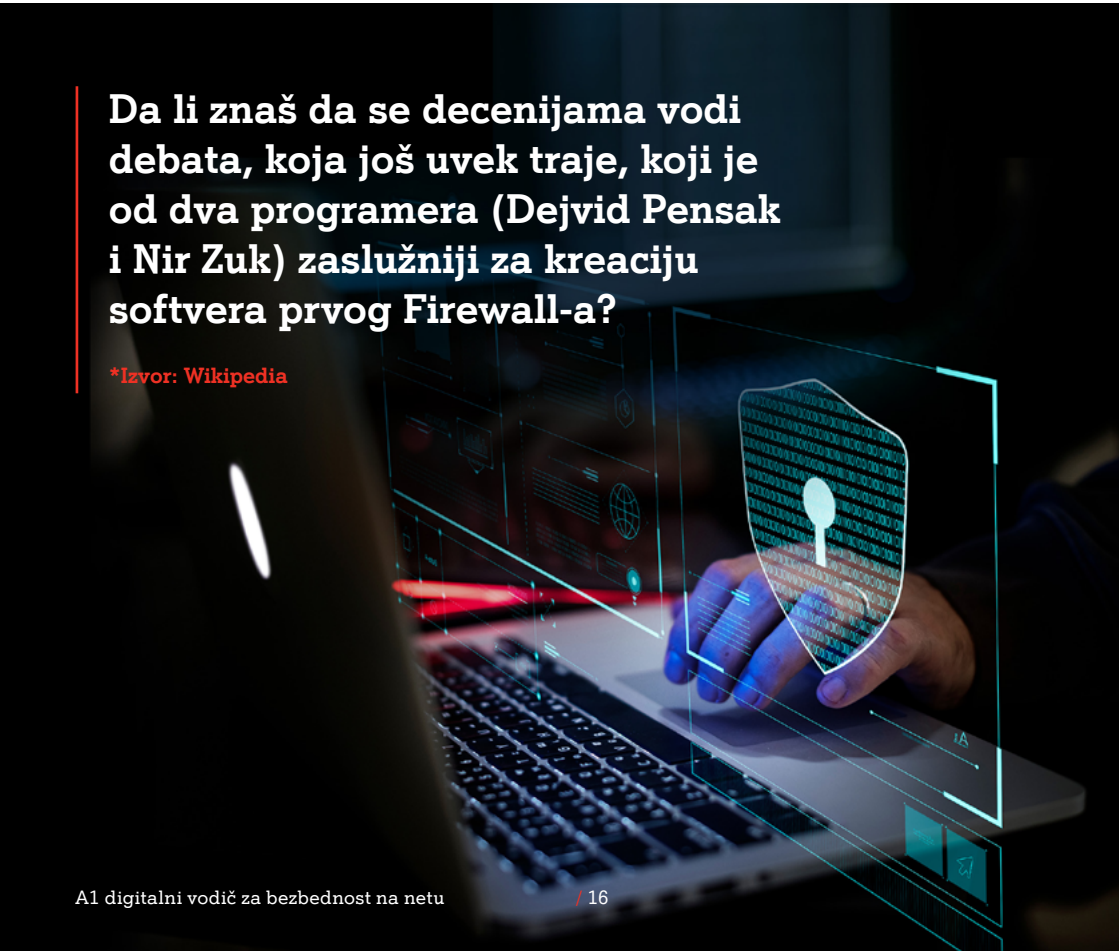
***Izvor: Wikipedia**

Firewall

Firewall (vatreni zid) – sredstvo zaštite, bilo softversko bilo hardversko, čija je namena da filtrira informacije i zaštiti uređaj i/ili mrežu. Ako je hardverski, onda štiti mrežu od neželjenih Malware-a i drugih napada. Firewall može imati i neke druge funkcionalnosti, osim što izigrava saobraćajca na mreži. Firewall može i da identifikuje vrstu saobraćaja (da vidi pakete i da ih analizira) i da na osnovu toga određeni saobraćaj propusti ili blokira.

Da li znaš da se decenijama vodi debata, koja još uvek traje, koji je od dva programera (Dejvid Pensak i Nir Zuk) zaslužniji za kreaciju softvera prvog Firewall-a?

*Izvor: Wikipedia



Virtual Private Network (VPN)

Virtual Private Network (VPN)
Koristi se da bi se sigurnom vezom pristupilo nekoj internoj mreži firme. Kada su zaposleni van kancelarije, ali ipak moraju da pristupe mrežnom disku koji je u firmi, štampaču ili bazi podataka, onda se koristi VPN kako bi zaposleni od kuće poslao ili preuzeo poslovne podatke i pristupao resursima na mreži kao da se nalazi u kancelariji. Poslodavac obično postavi Firewall kako bi zabranio pristup internoj mreži s javnog interneta, ali Firewall može da propusti VPN saobraćaj. Pošto može da sakrije identitet korisnika, VPN može da se koristi prilikom upotrebe javnih mreža kako bi se izbegli bezbednosni rizici.

Da li znaš da je VPN omiljeni alat svih onih koji ilegalno skidaju video i audio sadržaje poput filmova, serija ili muzičkih albuma?

Proxy

Proxy – u prevodu znači posrednik. To je server koji omogućuje posredan pristup određenom tipu sadržaja i maskira identitet (IP adresu) uređaja. Ako koristiš sajt Pirate bay (iako znamo da to sigurno ne radiš i da nikada nećeš), verovatno znaš da postoje i Proxy sajtovi zato što se originalan server često obara.

Da li znaš da, uprkos informacijama koje možeš pročitati na internetu, Proxy NIJE jedan od najboljih načina da zaštitiš svoje lične podatke od hakera? Proxy je lakše i jeftinije namestiti od VPN-a, pa ga često hakeri koriste kako bi besplatno pružili Proxy uslugu, da bi zapravo namamili žrtve na njihov server, gde im jednostavno mogu ukrasti podatke.

Digitalni otisak

Digitalni otisak – Sve što radiš i što ćeš ikada raditi u online svetu, a može da se pronađe, čini tvoj digitalni otisak. Digitalni otisak čine sve online aktivnosti – pretraživanja, komunikacija, omiljeni sajtovi, vreme zadržavanja na određenom sadržaju itd.

Prijateljski savet, pazi šta pretražuješ jer skoro je nemoguće potpuno zamaskirati digitalni otisak.

IP
(Internet protokol) adresa

IP (Internet protokol) adresa
Svaki uređaj, bilo da se radi o računaru, mobilnom telefonu bilo o tabletu, ima jedinstven broj koji označava njegovo prisustvo svaki put kada se „nakači" na internet. To je praktično oznaka tvog uređaja u online svetu i ne mogu postojati dve iste.

Da li znaš da trenutno na svetu postoji nešto manje od 4,3 milijarde IP adresa?

***Izvor: worldpopulationreview.com**

Mračni veb (Dark web)

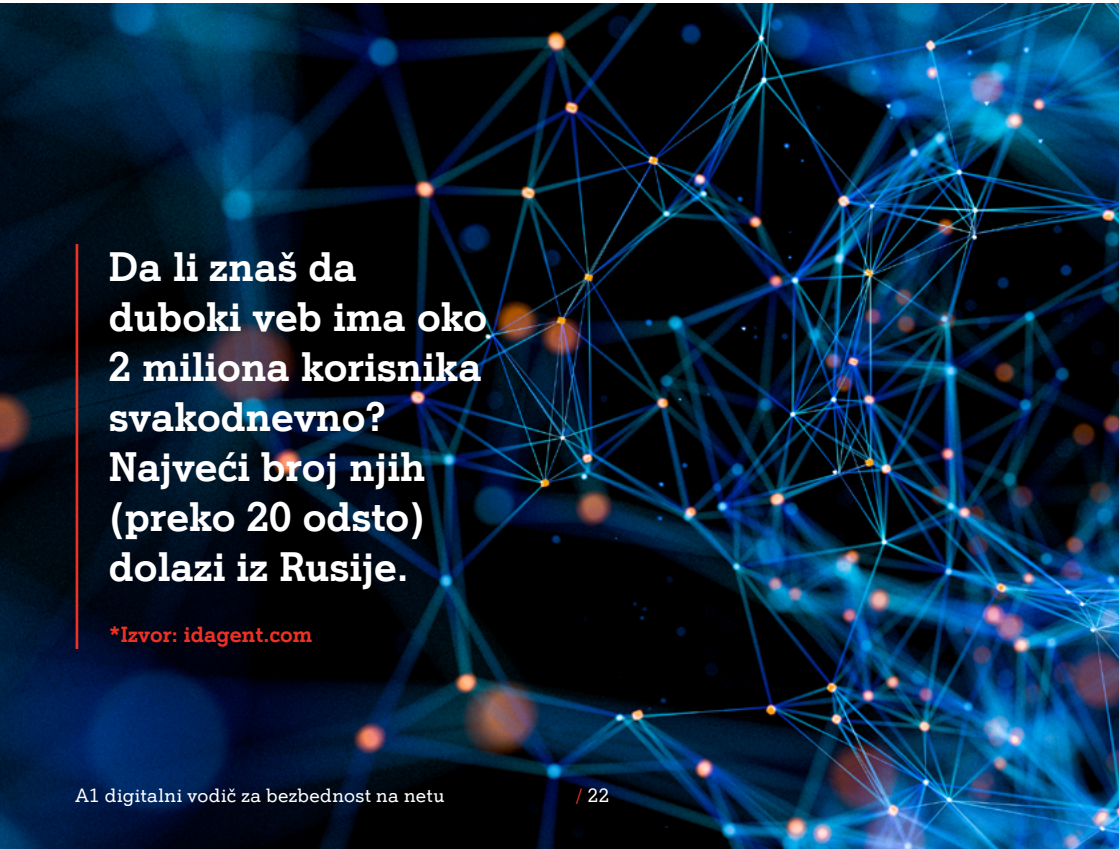
Mračni veb (Dark web) – To je skriveni skup internet sajtova kojima može pristupiti samo specijalizovani veb pretraživač. Koristi se za čuvanje anonimnosti internet aktivnosti. Korisnici mogu da sakriju lokaciju, IP adresu i druge informacije koje bi mogle da dovedu do uređaja. Dark webu može da se pristupi s bilo kog uređaja ukoliko se veb pretraživač podesi na odgovarajući način.

Da li znaš da se Dark web ne može koristiti ukoliko ne poseduješ određeni alat za enkripciju koji ti skriva identitet?

***Izvor: pcpress.rs**

Duboki veb (Deep web)

Duboki veb (Deep web) – Ovo je deo interneta kojem ne možeš (i ne želiš) da pristupiš. To su stranice koje postoje negde na mreži, ali ih internet pretraživači jednostavno ne registruju. Duboki veb se često koristi kao sinonim za Dark web, ali je zapravo mnogo širi pojam, jer uključuje korisničke baze podataka, vebmejl stranice, veb forume koji zahtevaju registraciju i stranice koje zahtevaju od korisnika da se pretplate na sajt. Postoji ogroman broj takvih stranica i one nisu nužno nebezbedne.



Da li znaš da duboki veb ima oko 2 miliona korisnika svakodnevno? Najveći broj njih (preko 20 odsto) dolazi iz Rusije.

***Izvor: idagent.com**

Exploit

Exploit – Termin koji se koristi za hakerski napad koji koristi vrlo specifičnu slabost sistema i onda je eksploatiše (otuda i termin) kako bi uspešno izvršio napad. Kompanije često koriste etičke hakere kako bi otkrili slabosti sistema.

Da li znaš da velike kompanije koje se bave izdavanjem softvera redovno objavljuju sigurnosne zakrpe (patches) kako bi dodatno zaštitile softver i povećale nivo sigurnosti? Na primer, kompanija Microsoft svakog drugog utorka u mesecu objavljuje paket sa zakrpama za svoje operativne sisteme i druge programe koje nude.

*Izvor: microsoft.com

Ovde se završava naše kratko zajedničko putovanje kroz najčešće pojmove sajber bezbednosti. Nadamo se da će ti ovaj **A1 Digitalni vodič za bezbednost na netu** pomoći da ih bolje savladaš. Uvek možeš da se podsetiš koje su najčešće sajber pretnje i kako da ih izbegneš kroz kurseve na stranici **A1 Kutak za bezbedan net**.

Vidimo se u digitalnom svetu!