1. Bezbednost prilikom upotrebe računara i internet

Onog momenta kada je internet postao široko dostupan svi smo dobili beskonačne mogućnosti za komunikaciju, informisanje, učenje, zabavu... U poslednje vreme za sve više stvari se oslanjamo na internet. Plaćamo račune, kupujemo, planiramo, ostvarujemo poslovne i privatne kontakte sa ljudima na drugom kraju sveta. Imati pristup internetu znači imati pristup svetu. Sedeći za svojim stolom možete posmatrati egzotične lepote skoro svih krajeva sveta, možete obići piramide, Ajfelov toranj i to sve za nekoliko minuta. Iako je to teško zamisliti dok sedimo za radnim stolom, „lutanje" internetom je poput lutanja ulicama nepoznatog mesta, gde se nikada ne zna šta vam se sve može dogoditi, podjednako i dobro, ali i loše. U tom smislu, biti odgovoran korisnik Interneta znači sprečiti niz negativnih situacija u kojima se možemo naći.

* 1. Kako se zaštititi

 Jako je važno da naučite po nešto o osnovama rada na internetu, saznajte koje su to akcije koje mogu da vas dovedu u neželjenu situaciju, a koje su bezbedne. Jednostavno morate znati koje su potencijalne posledice vaših akcija.

* + 1. Zaštitite se.

Svaki računar koji koristite za surfovanje i slične aktivnosti mora da poseduje program za prepoznavanje i uništavanje virusa koji bi mogli biti destruktivni za vaš računar i podatke koje na njemu čuvate. Sada postoje razni programi koji vam to omogućavaju i koji su veoma pristupačni (veliki broj je i besplatan).

Tipovi programa koji mogu da zaštite vaš kompjuter od „upada" drugih računara su „firewall-ovi" i oni će sprečiti da neko drugi (sa svog računara) pristupi vašem računaru i potencijalno napravi neku štetu.

Antivirus programi će zaštititi vaš računar od opasnih (zaraženih virusom) programa koji mogu da budu na vašem računaru. Pri izboru antivirus programa, treba biti pažljiv. Postoje paketi antivirus programa koji se mogu kupiti (Nod32, Kaspersky) i onih koje možete besplatno da skinete sa interneta (AVG, avast), pri čemu treba biti pažljiv jer nije sve antivirus pa čak iako se tako zove. Trebalo bi prvo da istražite kredibilitet tog programa, da vidite koliko je pouzdan i bezbedan i tek tada da ga skinete.

Jako je važno da naučite po nešto o osnovama rada na internetu, saznajte koje su to akcije koje mogu da vas dovedu u neželjenu situaciju, a koje su bezbedne. Jednostavno morate znati koje su potencijalne posledice vaših akcija.

* + 1. Birajte mesta na Internetu na koje ćete odlaziti.

Postoje sadržaji i sajtovi koji su u startu opasniji i gde možete lakše da zarazite kompjuter nekim virusom ali i vi da naletite na neke neprijatne situacije. To su uglavnom porno sajtovi i sajtovi koji su koncipirani oko ilegalnih tema, kao što su hakerski sajtovi, piraterija i slično.

* + 1. Kontrolišite elektronsku poštu.

 Putem mejla mogu da vam stignu razni virusi i sadržaji koji mogu da naštete vašem kompjuteru. Ukoliko ne znate od koga je mejl ili nije jasno naglašeno koja je tema ili vam deluje kao spam (neželjena reklama), nemojte ga otvarati jer možda sadrži u sebi virus koji bi mogao da zarazi vaš računar. Isto važi i za mejlove koji sadrže neki dodatak (attachment), ukoliko ne znate šta je u njemu i/ili ne znate od koga je, najbolje bi bilo da taj mail obrišete. Jedina akcija koja može da spreči neželjene posledice je momentalno brisanje takvih mejlova. Bilo koji način odgovaranja na takav mejl će samo pogoršati situaciju.

* 1. Pažljivo postavljanje ličnih podataka na internet
		1. Internet ne zaboravlja.

Podaci koji se jednom nađu na internetu će tamo verovatno i ostati jer ćete se poštenosličica namučiti da ih uklonite. Informacije koje ste postavili nekada davno su verovatno još uvek tu negde i ovo treba da imate u vidu jer ne razmišljamo isto sa 12, 22 i 32 godine. Ono što vam je nekada bilo super zanimljivo sada ćete možda hteti da sakrijete. Savet je da pažljivo birate šta ćete postavljeti na internet, bez obzira jesu li to lični podaci ili vaše slike.

* + 1. Zaštitite podatke o sebi.

Funkcija interneta je da nam olakša život u koliko god aspekata je moguće. Sve više poslova možemo da završimo preko interneta (plaćanje računa preko interneta, slanje izveštaja, konkurisanje na neko radno mesto, kontaktiranje klijenata i prijatelja), on nam štedi vremem i resurse, što nije zanemarljivo. Ali isto kao što prilikom podizanja novca na bankomatu nećete dozvoliti da svako vidi vašu šifru, tako ne bitrebalo da objavljujete svoje lične podatke (broj lične karte, računa u banci ili slično) svugde već samo na sajtovima za koje znate da su pouzdani.

Ukoliko privatne podatke koristite na računaru koji nije vaš, nemojte koristiti opciju "zapamti". Pokušajte da lozinke za pristup nikome ne govorite i prilikom odlaska sa nekog sajta koristite opciju za odjavljivanje (log off), kako niko ne bi mogao da koristi vaš nalog. Ukoliko se nalazite u nekom internet kafeu, ne dozvolite da neko vidi vašu lozinku ili podatak koji može da se zloupotrebi.

* + 1. Pazite kome i šta pričate.

Sve je učestalija pojava internet zajednica, soba za ćaskanje i sl. koje za mnoge predstavljaju najvećeg „potrošača vremena". Kada se nađemo na nekom od takvih mesta upoznajemo ljude sa kojima pričamo i neposredno delimo informacije za koje ne smatramo da mogu da nam štete. Ukoliko ste aktivni na bilo kojoj sličnoj mreži, treba da znate da najobičnijim ćaskanjem odajete lične informacije o sebi koje drugi mogu da iskoriste, pa u tom smislu obratite pažnju na to šta pričate.

* 1. Plaćanje putem interneta
		1. Birajte pouzdan sajt.

Jedna od novina koja je pratila razvoj tehnologije je plaćanje putem interneta. Ovakav način plaćanja još uvek nije postao u svim zemljama potpuno uobičajen i ljudi, koji nisu upoznati sa načinom na koji sve to funkcioniše, ga se klone. Važno je znati da prilikom plaćanja putem interneta, treba da koristite samo proverene i dobro poznate sajtove. Dakle, ukoliko sajt ne poznajete, niti ste za njega čuli, izbegavajte da plaćate preko njega. PIN broj je podatak koji i u "online" plaćanju treba dobro da razmislite gde ćete koristiti. Ali ako vam to može olakšati posao, a uverili ste se da je sajt bezbedan - ne treba da bežite od ove opcije jer može da vam uštedi čekanje po redovima a samim tim i mnogo vremena.

* + 1. Obratite pažnju na sigurnost samog sajta.

Unošenje podataka potrebnih za plaćanje zahteva mrežu tj. internet sajt koji je siguran. Oznaku da je sajt zaštićen ćete prepoznati prikazom ključa ili zaključanog katanca. Ovo naravno nije apsolutno pravilo, ali je nešto na šta vredi obratiti pažnju kada unosite broj kartice. Takođe, kada se koristi zaštićena mreža početak internet adrese prodavca treba da se promeni, umesto skraćenice "http" treba da stoji skraćenica "http". Ovako označena adresa ne može da bude praćena ili prisluškivana na bilo koji način.

* + 1. Obratite pažnju na način i uslove plaćanja.

Kao i prilikom uobičajene trgovine, treba da se raspitate o uslovima plaćanja tj. da ukoliko želite nešto da kupite, aktivirate opciju jednokratnog plaćanja a ne mesečnu pretplatu, plaćanje na rate ili nešto tome slično. Prilikom elektronskog plaćanja u nekom momentu od vas može biti tražen CVC (Card Verification Code). Reč je o trocifrenom broju koji se nalazi na poleđini kartice, gde se nalazi Vaš potpis i koristi se kao još jedna mera predostrožnosti i zaštite vaših podataka. Međutim, opasnosti koje mogu da vas vrebaju su skrivene i maskirane, na primer kada od vas traže da pošaljete broj kartice kako biste potvrdili dobitak neke nagrade ili u bilo kom slučaju kada plaćanje nije išlo na vašu inicijativu. Ovo su uglavnom pokušaji da se saznaju podaci o vama , koji su posle podložni zloupotrebi.

* 1. Deca i internet

Ukoliko imate decu posvetite pažnju i njima, informišite ih koje sve opasnosti vrebaju i koje benificije mogu imati koristeći internet i računar. Iako smatrate da je dete dok sedi u svojoj sobi bezbedno, ako ne vidite koje sadržaje posećuje to može da bude izuzetno opasno. Najbolje poređenje koje možete napraviti sa svim opasnostima koje vrebaju na internetu jeste da zamislite da putujete negde u nepoznato mesto.. Gotovo ista pravila kojih se držimo prilikom posete mestu koje ne poznajemo, važe i kada je internet u pitanju. Mnogo lepih mesta, pametnih stvari i zanimljivih podataka možemo videti i naučiti, važno je samo da budemo svesni i obavešteni o ćorsokacima, mračnim ulicama i opasnim "krajevima grada" koje ne treba da posećujemo.

* + 1. Ograničavanje dostupnih sadržaja.

Ne postoji apsolutno sigurna zaštita deteta na internetu ali postoje programi (velika većina je besplatna i mogu se naći jednostavnom google pretragom) koji mogu da prate aktivnost vašeg deteta i da mu zabrane pristup ka neželjenim sadržajima. Sa sve većim širenjem interneta pojavio se i veliki broj provajdera koji sada već i sami u sklopu svojih paketa nude određenu mogućnost blokade nedozvoljenog materijala na kompjuteru koje vaše dete koristi. Oni se baziraju na biranju liste sa neželjenim sadržajem, na osnovu čega softver dalje zabranjuje pristup određenom sajtu i ograničava slanje ličnih podataka sa računara na mrežu. Još jedan od korisnih načina da zaštitite svoje dete je da tačno znate šta ono radi na internetu. Za tu svrhu postoje softeveri koji rade u pozadini (korisnik računara ne zna da se prate njegove aktivnosti) i beleže aktivnosti na mreži. Međutim, najbolje je ipak da razgovarate sa detetom i da vidite koja su njegova interesovanja i kakav utisak internet ostavlja na njega. Internet ne bi trebao da za meni prijatelje i igru, pa se zato potrudite da dete internet koristi u edukativne i praktične svrhe a ne samo za zabavu. Pratite sadržaje koje koristi i blokirajte one neželjene.

* + 1. Saveti za što veću bezbednost dece na internetu.

Ukoliko računar budete držali na sigurnom mestu (tako da nije lako dostupan detetu), bićete upućeni u to na koji način i koliko dete koristi internet. Redovno pregledajte posećivane sajtove, pa možda čak i mejlove ako imate razloga za brigu u pogledu toga šta vaša deca rade na Internetu. Iako ovo deluje kao narušavanje privatnosti, deca nisu uvek u mogućnosti da spoznaju namere loših ljudi ili da uvek savesno izbegavaju spam. Elekrtonska pošta je posle četa uživo najopasnija stvar za decu jer se u tim momentima njima može svašta sugerisati a njihova naivnost ih sprečava da budu oprezni. Iz istog razloga treba obratiti pažnju na korišćenje društvenih zajednica od strane dece. Sa druge strane, ukoliko detetu u programu za pretragu Interneta snimite omiljene sajtove (bookmark, favourites) i time mu olakšate pristup njima, manje su šanse da će "lutati" od sajta do sajta , tražeći ono što ga zanima. Mada, ovo se ne može u potpunosti izbeći tako da je najbolje da uz sve mere predostrožnosti ipak redovno pričate sa decom na ovu temu i razvijete kod njih osećaj odgovornosti kako bi oni razumeli vašu brigu, odnosno kako vaše mere zaštite ne bi tumačili samo kao kaznu ili bezrazložna ograničenja., pomoći će vam da upoznate njegov svet i interesovanja.