SURFANJE U DIGITALNOM SVIJETU
KAKO SE ZAŠTITITI NA INTERNETU

ŽIVJETI ZAJEDNO

3 Osvrt na globalni cyber kriminal
4 Uvod
5 Sigurnost i osnovna zaštita osobnog računala
8 Odabir sigurne lozinke
11 Internetska kupovina
13 Sigurno korištenje pametnih telefona
16 Sigurno korištenje aplikacija
18 Bez ostavljanja tragova na internetu
22 Phishing
25 Socijalni inženjering
27 Pametno korištenje društvenih mreža
31 Računalstvo u oblaku
33 Rječnik pojmova vezanih uz privatnost

OSVRT NA GLOBALNI CYBER KRIMINAL

113 mlrd $ - iznos štete prouzročene cyber kriminalom u 2013. godini (dovoljno za organizaciju 10 olimpijskih igara u Londonu).
Tih 113 mlrd $ sastoji se od:

- Prevare 38%
- Krađa ili gubitak 21%
- Popravci nastale štete 24%
- Ostalo 17%

Prosječan gubitak po žrtvi cyber kriminala: 298 $

Najnovije upozoravajuće brojke:

- 378 mil žrtava cyber kriminala godišnje (više od 1 mil dnevno, 12 svake sekunde!)
- 50% online punoljetnih osoba bile su žrtve cyber kriminala ili su imale negativna iskustva u protekloj godini (npr. primili su obnažene fotografije od nepoznatih osoba, bili praćeni ili zlostavljani)

Izvor: Norton Cybercrime Report 2013.

UVOD

Teško je danas zamisliti život bez interneta: kupujemo putem interneta, komuniciramo s prijateljima koji žive na drugim kontinentima, gledamo filmove na internetu putem streaminga – mogućnosti su neograničene. Ne postoji potpuno efikasan način zaštite od prevaranata, ali primjenom nekoliko jednostavnih mjera možete poboljšati svoju sigurnost u online svijetu.

Na sljedećim stranicama nalaze se dodatni savjeti i alati: **http://www.t.ht.hr/odgovornost/privatnost.asp**. Na njima ćete također naći informacije o zaštiti privatnosti podataka i pitanjima IT sigurnosti, kao i o aktualnim prijetnjama na internetu u pogledu sigurnosti. Ukoliko imate pitanja o privatnosti ili IT sigurnosti, molimo da nam se u bilo koje vrijeme obratite na našim internet stranicama ili putem e-pošte info@t.ht.hr (s napomenom "Za povjerenika za zaštitu osobnih podataka").

SIGURNOST I OSNOVNA ZAŠTITA OSOBNOG RAČUNALA

Zaštita privatnosti i sigurnosti privatnih podataka na vašem osobnom računalu.

UVIJEK IMAJTE NA UMU U KOJOJ MJERI SU PODACI OSJETLJIVI

Nikada ne unosite povjerljive informacije na javno računalo jer ne možete biti sigurni da li je ono odgovarajuće zaštićeno od **→ VIRUSA, → CRVA, → TROJANACA** i drugih vrsta napada. Zaštitite svoje osobno računalo od znatiželjnika. Prije unosa osjetljivih podataka kao što su korisničko ime ili lozinka obratite pozornost na to tko može vidjeti vaš ekran.

UVIJEK AŽURIRAJTE SVOJ SUSTAV

Pružatelji softvera stalno ažuriraju svoj softver zbog novootkrivenih sigurnosnih propusta. Ažurirajte svoj softver, a naročito antivirusni softver, kako biste se zaštitili od napada. Postoje i besplatni antivirusni programi, kao npr. Avast, Avira, AVG.

PRAVILNO KONFIGURIRAJTE SVOJ SIGURNOSNI SOFTVER

Provjerite jeste li instalirali antivirusne i **→ ANTISPYWARE** programe za zaštitu podataka. Također je važno da postavite osobni **→ VATROZID (FIREWALL).** Odgovarajuće postavke štite vas od napada s interneta. Za osobna računala s Windows operativnim sustavom preporuka je aktivirati barem **→ VATROZID** operativnog sustava i odabrati odgovarajuću vrstu mreže (kućna mreža ili javna mreža). Također koristite **→ SKENER ZA VIRUSE** davatelja e-maila kako biste postigli veću razinu sigurnosti. Ne obavljajte svakodnevne zadatke na osobnom računalu koristeći svoj administratorski račun; umjesto toga kreirajte standardni račun.

PROVJERITE PREUZIMANJA I PRIVITKE E-POŠTE

→ VIRUSI se obično šire putem datoteka u privitku e-pošte. Otvarajte samo privitke osoba koje zaista poznajete. Slična pravila vrijede i za preuzimanje softvera: ukoliko se pružatelj usluge ili internet stranica ne čine pouzdanima, odustanite od preuzimanja.

OSIGURAJTE SVOJE OSOBNO RAČUNALO LOZINKOM

Za zaštitu osobnog računala (a time i vaših podataka) od neovlaštenog pristupa trećih osoba uvijek biste trebali koristiti lozinku. Osigurajte visoku razinu sigurnosti svoje lozinke, primjenjujući savjete iz poglavlja Odabir sigurne lozinke. Preporuka je da se postavi automatsko zaključavanje zaslona i tipkovnice nakon pet minuta neaktivnosti. Za otključavanje zaslona i nastavak rada treba unijeti ispravnu lozinku. U slučaju kućnih računala, vrijeme aktivacije naravno ovisi o vama. Također postoji mogućnost da se zaključavanje postavi odmah, ukoliko je to potrebno. Kod operativnog sustava Windows ono se pokreće pritiskom na kombinaciju tipki Ctrl + Alt + Del i odabirom opcije „zaključavanje računala".

ISKLJUČITE BEŽIČNA SUČELJA

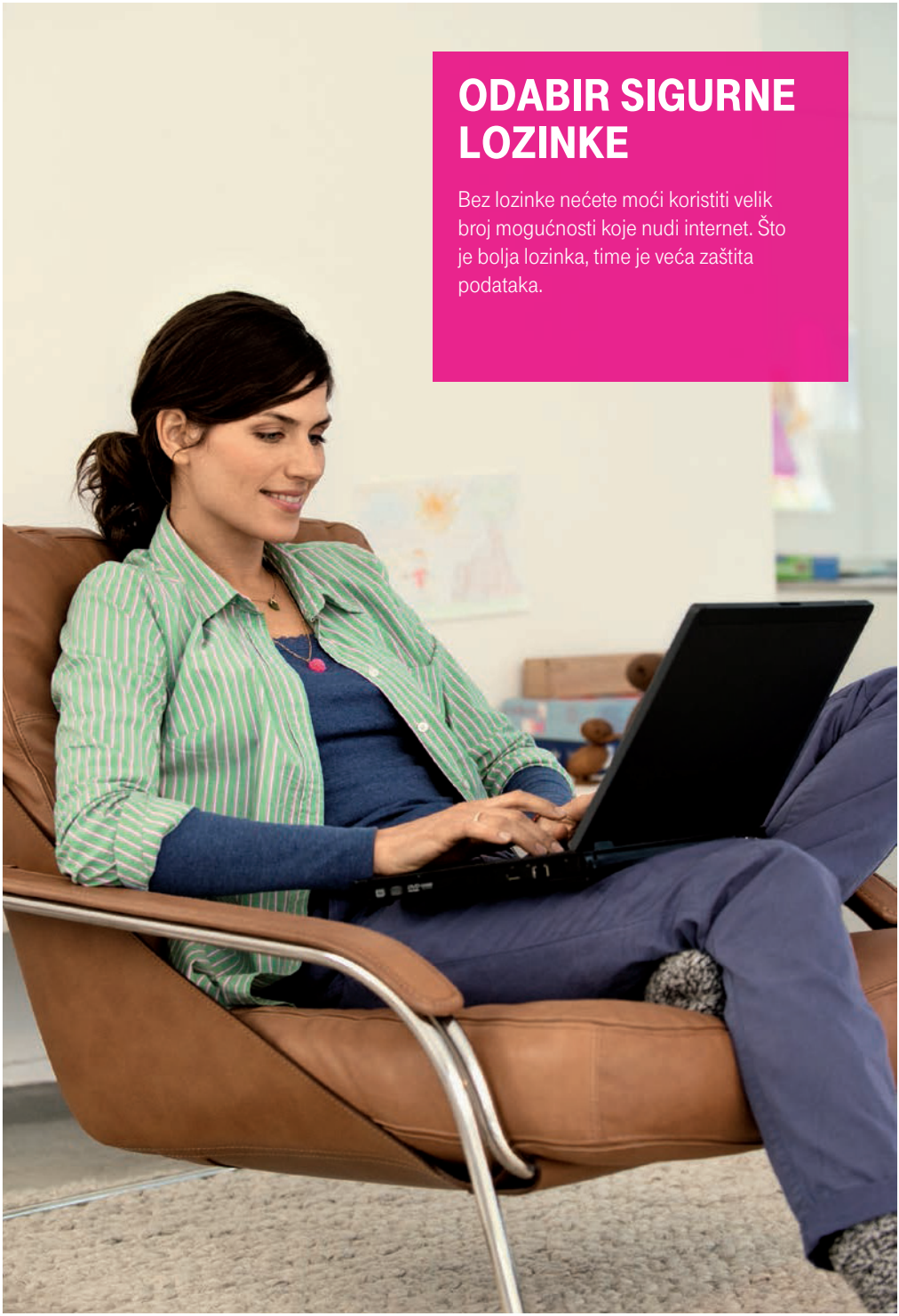
Za zaštitu osobnog računala od vanjskih napada isključite sva nepotrebna bežična sučelja – kada napuštate prostoriju, također ugasite svjetla! Bilo bi dobro isključiti i odašiljač signala → **WLAN-A** iz routera (usmjerivača) kada ne surfate internetom. Danas većina modela ima prekidač na stražnjoj strani. Ukoliko je isti router potreban drugim korisnicima, možete isključiti WLAN prijemnik na svojem krajnjem uređaju. Jednostavno je, a isto tako štedi energiju. Isto vrijedi i za vaš mobitel – na primjer s → **BLUETOOTH** pristupnom točkom, a u cilju zaštite od → **VIRUSA,** → **CRVA** i → **TROJANACA** i sprječavanja pristupa neovlaštenih korisnika vašim osobnim podacima, uključujući adresar, kalendar i fotografije. Pobrinite se da lozinka za → **WLAN** na vašem routeru uvijek bude tajna (vidi „Odabir sigurne lozinke").

SIGURNOSNE KOPIJE PODATAKA

Najsigurnije je redovito raditi sigurnosne (backup) kopije važnih podataka, na primjer na CD-ROM-u / DVD-u ili vanjskom tvrdom disku. Imamo mogućnosti koristiti i Spremalicu kao dio Multimedia paketa te pohraniti datoteke u sigurnom HT oblaku (vidi „Računalstvo u oblaku").

ODABIR SIGURNE LOZINKE

Bez lozinke nećete moći koristiti velik broj mogućnosti koje nudi internet. Što je bolja lozinka, time je veća zaštita podataka.



Svatko tko koristi internet treba korisnička imena i lozinke kako bi pristupio raznim forumima i zajednicama, kao i za kupovinu putem interneta. Nakon pete lozinke teško je pamtiti sve lozinke. Osim toga, sigurne lozinke se uglavnom ne pamte lako. No, postoji rješenje.

KAKO KREIRATI SIGURNU LOZINKU?

Zlatno pravilo za sigurnu lozinku: Sigurna lozinka ne bi smjela biti nešto što bi vanjski svijet mogao prepoznati kao nešto sadržajno! Evo jednostavnog trika: jednostavno odaberite rečenicu koju ćete lako zapamtiti, zatim koristite prvo slovo svake riječi u rečenici kako biste formirali novu riječ. Kako biste učinili lozinku što neprobojnijom, dodajte rečenici brojeve i posebne znakove, na primjer: **„My mother buys 16 eggs every Saturday at the Farmer's Market" postaje „Mmb16eeSatFM!"**

Stručnjaci preporučuju da koristite minimalno osam – što više nasumično odabranih – znakova (npr. kombinacija brojeva, velikih i malih slova i posebnih znakova), no lozinka može biti i duža. Zlatno pravilo glasi: što duža i **složenija** lozinka, to bolje.

ONEMOGUĆAVANJE HAKIRANJA

Evo zašto: Hakeri koriste posebne programe koji sistematski isprobavaju sve mogućnosti vezano uz način sastavljanja lozinke. Svaki znak dodan lozinki povećava broj mogućih lozinki, a time i broj lozinki koje ovi računalni programi moraju izvoditi kako bi pokušali i „probili" vašu lozinku.

KREIRAJTE RAZLIČITE LOZINKE ZA RAZLIČITA PODRUČJA PRIMJENE

Druga važna preventivna mjera: koristite različite lozinke za različite prijave, ukoliko je to moguće. Kradljivac podataka ponekad dođe do kompletnih korisničkih podataka na način da uključi sve pristupne podatke. Lozinka koja dođe u ruke kradljivaca nije više sigurna jer će je kradljivac iskoristiti kako bi ušao i u druge račune. Zbog toga je sigurnija lozinka ona koja se koristi za samo jedan korisnički račun, npr.jedna lozinka za pristup MojTelekom portalu, druga za pristup elektroničkoj pošti i slično. U svakom slučaju, navedeno se svakako odnosi na vašu lozinku za internetsko bankarstvo.

POHRANITE LOZINKU NA SIGURNO MJESTO

Lozinku pohranjujte uvijek na sigurno mjesto kojem samo vi imate pristup. Najsigurnija lozinka je onu koju ste zapamtili. Najgore mjesto je vjerojatno vaš preglednik. Bolja je ideja koristiti program s kojim možete sigurno pohraniti lozinke kao što je Passwordsafe, Keypass, lastpass ili 1Password. Ovi programi također mogu generirati za vas sigurne lozinke.

REDOVNO MIJENJAJTE VAŽNE LOZINKE

Važne lozinke trebate mijenjati u redovnim intervalima kako biste povećali zaštitu od krađe podataka. Preporuka je da lozinke mijenjate otprilike svaka tri mjeseca.

KADA VAM JE POTREBNA SIGURNA LOZINKA?

Možda vam neće uvijek trebati lozinka koja ispunjava najstrože sigurnosne standarde. Vjerojatno ne morate biti tako oprezni s klubom ribolovaca mušičara kao što je to slučaj s internetskim bankarstvom.

Prije odabira lozinke pažljivo razmotrite sljedeće:

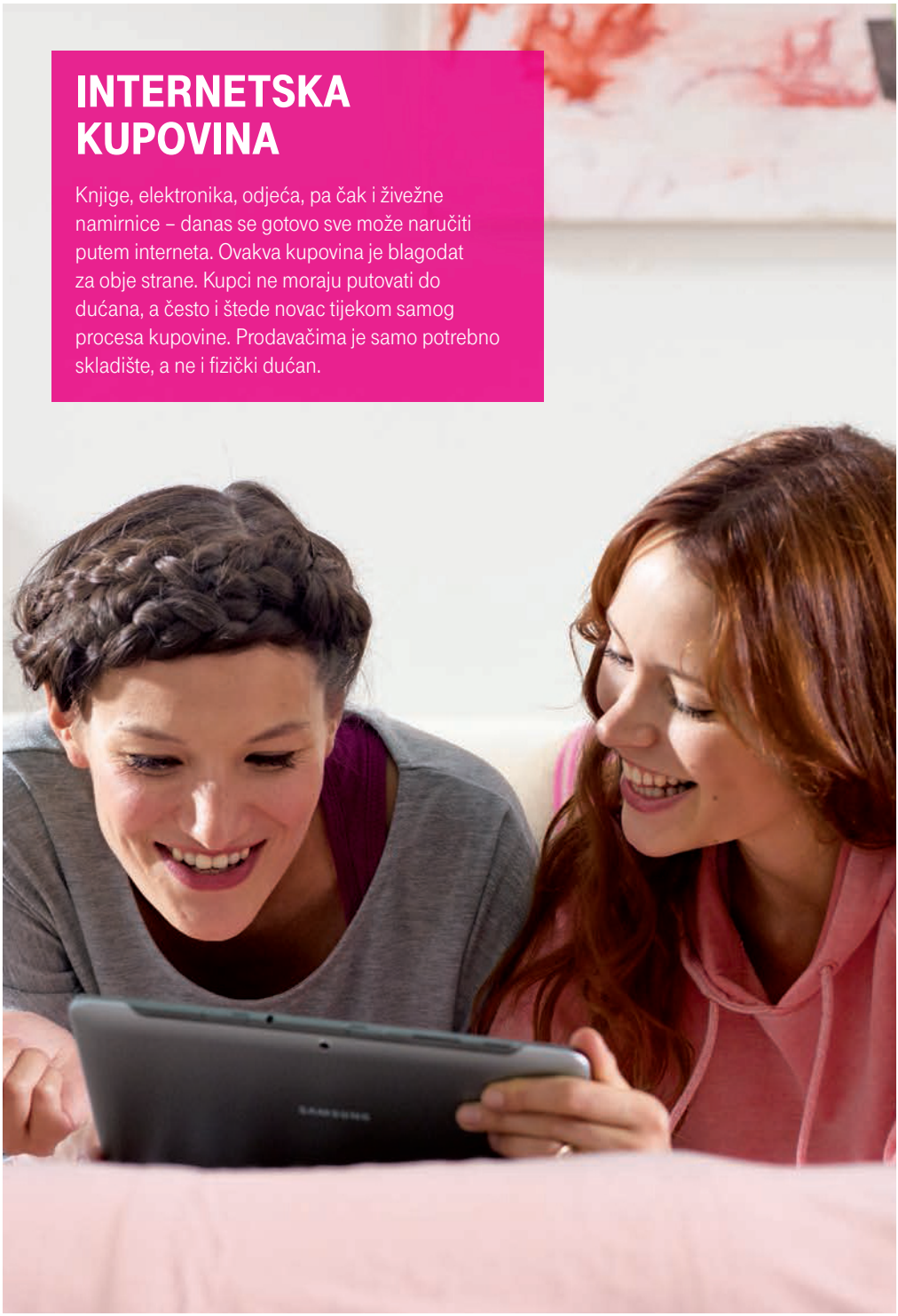
- Hoće li lozinka štititi osobne ili poslovne informacije (kao što su e-adrese i kontakti)?
- Bi li osoba koja pristupi predmetnom računu mogla izvršiti financijske transakcije (na primjer putem internetskog bankarstva ili internetskih aukcijskih kuća)?
- Omogućuje li pristup predmetnom računu također i pristup drugim važnim podacima kao što su brojevi kreditnih kartica ili bankovni brojevi?

Ukoliko ste na bilo koje od navedenih pitanja odgovorili pozitivno, svakako morate odabrati najsigurniju moguću lozinku. Također imajte na umu da velik broj internet aplikacija šalje početne lozinke ili „resetiranje zaboravljene lozinke“ putem e-pošte. Haker koji može preuzeti kontrolu nad računom vaše e-pošte također će automatski imati pristup ovakvim lozinkama. Stoga zaštitite svoju e-mail lozinku s posebnom pažnjom i promijenite lozinke čim ih dobijete e-poštom.

Ukratko: Uvijek imajte na umu najgori mogući scenarij u slučaju da vaša lozinka dospije u pogrešne ruke – i na temelju toga donesite odluku o jačini lozinke.

INTERNETSKA KUPOVINA

Knjige, elektronika, odjeća, pa čak i živežne namirnice – danas se gotovo sve može naručiti putem interneta. Ovakva kupovina je blagodat za obje strane. Kupci ne moraju putovati do dućana, a često i štede novac tijekom samog procesa kupovine. Prodavačima je samo potrebno skladište, a ne i fizički dućan.



ŠTO TREBATE IMATI NA UMU KADA KUPUJETE PUTEM INTERNETA?

Vjerujte samo onim kompanijama koje su vam poznate. Kada kupujete putem interneta raspitajte se o dućanu u kojem želite kupovati. Ocjene korisnika i ocjene na forumima mogu vam pomoći da izbjegnete pogreške i da budete upoznati s mogućim štetama.

Kada kupujete na internetu provjerite, prilikom postupka prijave ili najkasnije tijekom unošenja osobnih podataka, da se u adresnoj traci nakon „http“ pojavilo „s“, npr. **https://www.hrvatskitelekom.hr**, što znači da je uspostavljena sigurna veza. Sigurnu vezu možete prepoznati po znaku za zaključavanje u adresnoj traci vašeg preglednika.

Uvijek unosite adresu dućana ručno u preglednik, ili učitajte prethodno spremljenu stranicu (bookmark). Ne slijedite linkove koje ste dobili e-poštom jer bi vas oni mogli dovesti do internet stranica koje nisu sigurne. Na taj način prevaranti neće imati priliku ukrasti vaše podatke i lozinku.

U svakom slučaju, odaberite sigurnu lozinku za svoj račun vezan za dućan. Više informacija o načinu odabira možete naći u poglavlju „Odabir sigurne lozinke“.

Ne otkrivajte nikome svoju lozinku! Trebalo bi je koristiti samo za prijavu u dućan. Potrebna je određena doza skeptičnosti. Ugledan dućan nikada neće od vas tražiti podatke za prijavu putem e-pošte ili telefona. Ukoliko ipak dobijete e-poruku u kojoj se od vas traže ovakvi podaci, gotovo sigurno se radi o → **PHISHING** napadu (lažnoj e-poruci u svrhu krađe identiteta). Više savjeta o zaštiti od → **PHISHINGA** možete naći u poglavlju „Phishing“.

Odaberite siguran način plaćanja kao što je virman, faktura ili COD ili koristite online uslugu plaćanja kao što je HT Payway.

SIGURNO KORIŠTENJE PAMETNIH TELEFONA

Zaštita privatnosti i sigurnosti vaših privatnih podataka na pametnom telefonu

Pametni telefoni su bez ikakve dvojbe telefoni budućnosti. No, paralelno s rastućom prodajom postali su i glavna meta za razne maliciozne programe.

KAKO PRIJEĆI NA MOBILNE UREĐAJE, A PRI TOME ZADRŽATI SIGURNOST?

Ni najbolji softver ne može vam pomoći ukoliko je zastario. Uvijek pravovremeno instalirajte ažuriranja. Postupak je lakši ako instalirate samo aplikacije koje su vam zaista potrebne. Aplikacije koje vam više nisu potrebne možete jednostavno deinstalirati.

Također ažurirajte operativni sustav uređaja. Kod uređaja s iOS-om dobivat ćete obavijesti o dostupnim ažuriranjima u obliku broja koji se pojavi na ikoni „Postavke". Kod uređaja s Android operativnim sustavom korisnici se obično kod prvog pokretanja telefona moraju registrirati kod proizvođača uređaja, nakon čega će dobiti obavijest o ažuriranjima. Važno je da se registrirate na ovaj način jer se stalno pronalaze nove ranjivosti mobilnih operativnih sustava, kao što je to slučaj i s operativnim sustavima osobnih računala, koje se uklanjaju sigurnosnim ažuriranjima.

Ne instalirajte aplikacije iz nepoznatih izvora. Čuvajte se skrivenih troškova aplikacije kao što su pretplate ili „in-app" kupovine. Više informacija o tome možete naći u poglavlju „ Sigurno korištenje aplikacija".

ZA OSNOVNU ZAŠTITU NIJE POTREBNA NIKAKVA ČAROLIJA

Zaštitite svoje podatke od neovlaštenog pristupa, a svoj uređaj zaštitite od gubitka i krađe.
Uvijek zaštitite svoj pametni telefon lozinkom i uključite funkciju automatskog zaključavanja (auto-lock) za vrijeme neaktivnosti, što će onemogućiti pristup vašim podacima od strane drugih osoba u slučaju da podignete pogled s telefona ili da izgubite telefon. U slučaju gubitka ili krađe vašeg pametnog telefona, nekoliko proizvođača nudi opciju praćenja/pronalaženja i udaljeno brisanje sadržaja telefona.
U tom slučaju sigurnosne kopije vaših podataka (backups) postaju još važnije. Neki pametni telefoni nude opciju izrade sigurnosne kopije na osobnom računalu ili u oblaku (npr. iTunes oblak za uređaje s iOS-om).

U ovakvim situacijama važno je blokirati SIM karticu uređaja kako bi se spriječili svi dodatni troškovi. Raspitajte se koje opcije (blokiranje, udaljeno brisanje, praćenje) određeni telefon ima prije same kupnje.

Od neovlaštenih upada također će vas zaštititi isključivanje raznih opcija povezivanja kao što su **→ BLUETOOTH**, **→ WLAN** i **→ NFC** (komunikacija kratkog dometa) ili čak mobilne podatkovne veze ukoliko je ne koristite aktivno. Na taj način ćete također uštedjeti energiju baterije.

Ako ne želite da vaš pametni telefon šalje podatke o vašoj lokaciji, možete isključiti funkciju usluga lokacije (kao što je GPS).

SIGURNOST À LA CARTE

Pametni telefoni rade s raznim operativnim sustavima (Windows Phone, iOS, Android, BlackBerry OS ili novi Firefox OS). Što je sustav raširenији, time je i privlačniji napadačima.

Postavite svoj račun e-pošte tako da koristi → **SSL** ili → **TLS** kada šalje ili prima e-poštu. Koristite funkcije na pametnom telefonu koje kriptiraju vaše podatke i memorijsku karticu u uređaju. Aktualni uređaji s iOS-om uvijek kriptiraju podatke. Pristup uređaju svakako bi trebao biti zaštićen lozinkom. Aktualni Android uređaji također nude opcionalno kriptiranje interne pohrane uređaja. Raspitajte se o opcijama koje nudi vaš uređaj.

Ne pohranjujte lozinke, brojeve računa → **PIN-OVE** i slično na pametnom telefonu. Za pametne telefone je dostupan i sigurnosni softver za zaštitu od postojećih internetskih prijetnji.

BRISANJE PODATAKA NA STARIM UREĐAJIMA

Kod kupovine novog telefona često puta se postavlja pitanje: što učiniti sa starim uređajem? Većina ih završi u nekoj ladici ili kod članova obitelji ili prijatelja. No, što se događa s osobnim podacima na starom mobitelu? Je li ih dovoljno samo izbrisati? Kako bismo bili sigurni da strane osobe ne mogu obnoviti izbrisane podatke, treba ih u potpunosti ukloniti na način da se preko njih pišu novi podaci. Navedeno se izvodi na nekoliko različitih načina koji se primjenjuju kod raznih operativnih sustava. Više informacija o načinu trajnog brisanja privatnih informacija s vašeg uređaja možete naći na: **http://www.telekom.com/ratgeber** (samo na njemačkom jeziku). Također izvadite karticu za pohranu iz pametnog telefona. Obrišite sve pohranjene lozinke. Uklonite linkove na online dućane i s aplikacija (e-adrese, chatovi, FaceTime).

Ukoliko želite kupovati na internetu s pametnog telefona, svakako pročitajte savjete u poglavljima „Internetska kupovina“ i „Phishing“.

SIGURNO KORIŠTENJE APLIKACIJA

Aplikacije, ili skraćeno apps, mogu puno toga: dati vam brzu informaciju kada dolazi sljedeći vlak podzemne željeznice, aktualnu vremensku prognozu ili igricu dok čekate vlak. Nekoliko jednostavnih savjeta koji će vam pomoći u sigurnijem korištenju aplikacija.

ŠTO TREBATE IMATI NA UMU KADA KORISTITE APLIKACIJE?

Kada instalirate neku aplikaciju na Android uređaj, dobit ćete prikaz podataka kojima aplikacija može pristupiti. Budući da aplikacije često puta moraju slati i primati podatke, pravo na internetsku vezu obično se nalazi u samom vrhu prioriteta. Neki programi zahtijevaju znatno veći pristup, na primjer vašem telefonskom imeniku, popisu poziva ili lokaciji. Pametni telefoni s operativnim sustavom iOS imaju posebnu stavku izbornika („Postavke / Privatnost“) koja pruža opciju onemogućavanja određenih postupanja s podacima, kao što je eksport podataka o lokaciji. Međutim, u velikom broju slučajeva operativni sustavi ne nude ovakve opcije. Tada su jedine opcije dopustiti prosljeđivanje podataka ili deinstalirati softver.

Problematično: Aplikacije koje dobivaju puni pristup adresaru (kontaktima). Većina korisnika ima osim telefonskih brojeva upisane i e-adrese, rođendane i slike svojih prijatelja i poslovnih partnera. Najgori mogući scenarij bio bi da se ovi podaci neopaženo proslijede proizvođaču aplikacije.

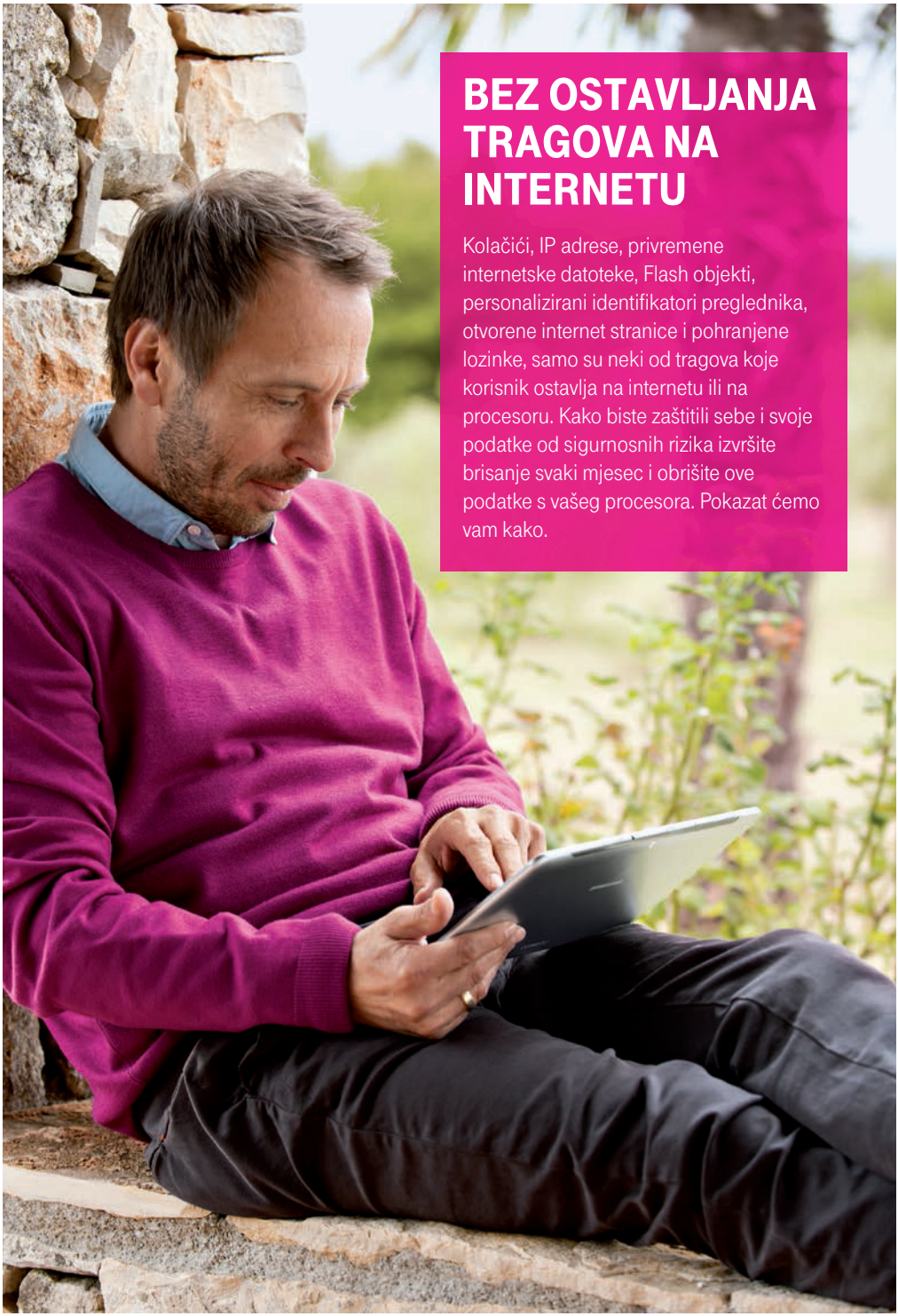
U cilju maksimalne sigurnosti proučite sve podatke o aplikaciji prije nego što je instalirate, naročite one u pogledu politike privatnosti. Trebale bi postojati jasne informacije o načinu na koji aplikacija postupa s vašim podacima. Nakon što ih proučite, moći ćete donijeti odluku o tome jeste li spremni prihvatiti uvjete proizvođača aplikacije.

Ukoliko otkrijete da se vaši podaci obrađuju na načine koji nisu navedeni u informacijama za korisnike ili samom sustavu, prijavite to direktno dežurnoj službi pružatelja usluge trgovine aplikacija. Tako npr. aplikacija koja koristi vaš pametni telefon kao svjetiljku ne treba imati pristup vašem adresaru ili vašoj trenutnoj lokaciji. Većina trgovina aplikacija ima pravila protiv obrade privatnih podataka.

Instalirajte samo one aplikacije koje dolaze iz pouzdanog izvora (npr. Apple App Store ili Google Play Store).

Čuvajte se skrivenih troškova kao što su pretplate i tzv. „in-app“ kupovine.

Istražite na koji način možete spriječiti in-app kupovine prije nego što dopustite nekoj osobi da koristi vaš uređaj. Kod nekih uređaja autentikacija ostaje tijekom određenog razdoblja nakon kupovine aplikacije, što bi moglo omogućiti drugim osobama da obave kupovine na vaš trošak, a da pri tome ne moraju ponovno unositi lozinku.



BEZ OSTAVLJANJA TRAGOVA NA INTERNETU

Kolačići, IP adrese, privremene internetske datoteke, Flash objekti, personalizirani identifikatori preglednika, otvorene internet stranice i pohranjene lozinke, samo su neki od tragova koje korisnik ostavlja na internetu ili na procesoru. Kako biste zaštitili sebe i svoje podatke od sigurnosnih rizika izvršite brisanje svaki mjesec i obrišite ove podatke s vašeg procesora. Pokazat ćemo vam kako.

OBRIŠITE KOLAČIĆE

→ **KOLAČIĆI** se nalaze svugdje – na njima su izgrađene cijele internetske stranice te bez njih ne mogu pravilno funkcionirati. → **KOLAČIĆI** su male datoteke koje na vaše računalo postavlja neka internetska stranica, a sadrže informacije kao što su osobne postavke stranice, podatke o prijavi ili prepoznavanje jedinstvenog korisnika. Kolačići mogu poboljšati iskustvo surfanja. Ukoliko koristite funkciju potrošačke košarice nekog internetskog dućana ili mijenjate postavke jezika internet stranica koriste se → **KOLAČIĆI**. Međutim, → **KOLAČIĆI** se također mogu koristiti i za kreiranje potpunog, personaliziranog korisničkog profila. Osim HTML kolačića, postoje i Flash kolačići te Super kolačići pomoću kojih operatori internet stranice ili oglašivači pohranjuju internet stranice i kasnije ih dohvaćaju. Za sve koji to žele onemogućiti popularni preglednici kao što su Internet Explorer, Firefox ili Opera omogućuju korisnicima da odrede koji će → **KOLAČIĆI** biti odnosno neće biti prihvaćeni. Neki preglednici već nude opciju za korisnike da navedu operatore internet stranica i oglašivače za koje ne žele da ih prate. Navedena funkcija temelji se na inicijativi vezanoj za standardizaciju opcije Do-Not-Track (Ne prati me) koju podržava i HT te svi postojeći davatelji usluge preglednika. Više informacija o blokiranju → **KOLAČIĆA** u vašem pregledniku možete naći na npr.
http://www.allaboutcookies.org/

Koristite različite preglednike.
Instalirajte preglednike raznih proizvođača softvera i mijenjajte ih kada posjećujete internetske stranice. Na taj ćete način davateljima usluge dati različite „otiske“ i onemogućiti im kreiranje vašeg osobnog profila.

Mijenjajte tražilice.
Na tražilicama također ostavljate tragove koje možete svesti na najmanju moguću mjeru tako da koristite različite tražilice.

MALI POMAGAČI

Nije jednostavno naći i obrisati informacije kao i podatke o prometu i korištenju. Međutim, postoje programi koji će gotovo sav taj posao obaviti za vas. Spomenut ćemo dva najpoznatija:

Spybot Search&Destroy
Program zaštite od → **ŠTETNIH PROGRAMA** otkriva razne oblike → **SPYWAREA** (špijunskog softvera) koji pokušava ući u procesor i pratiti navike korisnika vezane za surfanje. Program briše sve podatke o korištenju, uključujući povijest surfanja i preuzimanja. Također uklanja ranjivosti u pregledniku i blokira moguće točke ulaska za napade od strane štetnih programa i malicioznih internet stranica.

Ccleaner
Program za brisanje pokušava ukloniti nepotrebno i moguće curenje podataka iz računala. Ispituje, između ostalog, središnji Windows registar i direktorije gdje se obično pohranjuju podaci kao što su → **KOLAČIĆI**.

ŠTO MOŽETE UČINITI UKOLIKO NA INTERNETU POSTOJE INFORMACIJE O VAMA, A VI IH NE ŽELITE?

Fotografije iz vaših školskih dana, s ludih tuluma, sa zadnjeg godišnjeg odmora ili vikenda: velik broj ljudi voli dijeliti uspomene s prijateljima na društvenim mrežama. No, što učiniti ako se nalazite na fotografijama, a ne želite da one budu dostupne svima?

I kako možete saznati što postoji o vama na internetu? Svake 1,5 do 2 sekunde negdje u svijetu se registrira nova internetska adresa. Uz milijune postojećih internet stranica praktički je nemoguće imati uvid u sve objavljene informacije.

http://www.secure.me je servis osmišljen u suradnji s Deutsche Telekomom AG u svrhu pronalaženja, procjene i brisanja neželjenih informacija s Facebooka. Program za ispitivanje internetske privatnosti i ugleda na internetu namijenjen je privatnim osobama, kompanijama i obiteljima.

ANONIMNO SURFANJE S IPV6

Uvođenje novog internetskog standarda IPv6 omogućit će do 340 sekstiliona novih IP adresa – što je dovoljno da svaki uređaj u svijetu s internetskom vezom ima svoju vlastitu stalnu IP adresu koja ga jasno može povezati s jednim korisnikom. Deutsche Telekom je razvio rješenje koje će omogućiti anonimno surfanje s novim internetskom standardom IPv6, a Hrvatski Telekom, kao član DT Grupe ažurno prati sve novosti vezane uz IPv6. Kao korisnik možete odabrati željenu razinu anonimnosti prilikom pretraživanja interneta.

Nove IPv6 128-bitne adrese imaju dvije komponente: takozvani mrežni ID dodijeljen od strane davatelja usluge mreže i dio koji se odnosi na uređaj (router), a novorazvijeno rješenje za anonimno surfanje u biti je mogućnost krajnjeg korisnika da sam, na jednostavan način modificira svoju IP adresu s vremena na vrijeme i da na taj način omete pokušaje praćenja po IP adresi.

SAVJET

Prilikom prve navigacije na nekim internet stranicama pregledajte politiku zaštite privatnosti i opće uvjete u kojima je opisano na koji način davatelj usluge postupa s podacima. Ukoliko niste suglasni s politikama, napustite dotične internetske stranice.

PHISHING

Koristeći lažnu e-poštu i internet stranice cyber kriminalci mogu pristupiti osjetljivim podacima: „pecaju“ lozinke, PIN-ove i TAN-ove (Transaction Authentication Number).

Riječ → PHISHING nastala je spajanjem riječi password (lozinka) i fishing (pecanje) kako bi se opisala vrsta prijevare kod koje se lažnim predstavljanjem dolazi do lozinki, PIN brojeva i brojeva transakcije (TAN). Cyber kriminalci dobivaju pristup osjetljivim podacima tako što korisnike navode, lažnim e-porukama i internet stranicama, da unesu podatke o svojem računu, uključujući lozinke. Najčešća verzija phishinga je korištenje linka kako bi se korisnik preusmjerio na lažne internet stranice za određenu banku ili kompaniju koje izgledaju vrlo realistično. Kako biste se zaštitili od ovakvih napada, slijedite sljedeće korake:

ZAŠTITITE SE OD PHISHING NAPADA

Obratite pozornost na kompanije s kojima poslujete. Ukoliko pošiljatelj poruke nije jedna od ovih kompanija, e-poruka bi vrlo lako mogla biti lažnog porijekla ili vrlo vjerojatno neželjena promotivna poruka (spam).

Obratite pozornost na predmet poruke: ugledne banke i davatelji usluga e-pošte nikad vam neće poslati e-poruku u kojoj predmet glasi „HITNO je potrebno izvršiti provjeru vašeg računa“ ili slično.

Od kompanije koja pruža usluge možete očekivati da će znati vaše ime i prezime. Većina → PHISHING e-poruka je impersonalna, a primatelj se u najboljem slučaju oslovljava s „Poštovani člane“ ili „Poštovani korisniče XY banke”.

Uslužne kompanije slijede određena pravila komunikacije. Vaša banka nikad neće od vas tražiti povjerljive podatke kao što je → PIN ili → TAN putem e-maila ili telefonskog poziva. Iznimka: Potpisali ste s bankom ugovor o telefonskom bankarstvu i morate dati svoj → PIN radi autentikacije. U slučaju dvojbe nazovite javno objavljen broj banke i zatražite informaciju.

Pravopisne i gramatičke pogreške moguće su i u e-porukama uglednih kompanija. Međutim, ako e-poruka obiluje ovakvim pogreškama, tada treba posumnjati u njenu vjerodostojnost.

Znak upozorenja često puta je pogrešno upotrijebljen padež.

Isto su tako sumnjivi zahtjevi za deaktivacijom mehanizama zaštite kao što su blokatori skočnih prozora (pop-up blocker) i → SKENERI VIRUSA.

Uvijek prijeđite kursorom miša preko ponuđenih linkova i provjerite adresu destinacije koja je prikazana u statusnoj traci na dnu stranice, što će vam omogućiti da provjerite vodi li link do željenih internetskih stranica.

Aktivirajte → **ANTIPHISHING** funkcije preglednika. Razni preglednici imaju unaprijed instalirane ovakve funkcije - Firefox 3 i više, Opera 9.5 i više i Internet Explorer 7 i više.

Uvijek kada trebate unijeti osobne podatke na internetu, otvorite novi prozor preglednika. Nakon što je transakcija završena, najbolje je da se, ako je to moguće, odmah odjavite i zatvorite prozor.

ČUVAJTE SE PHISHING INTERNET STRANICA

Uvijek potražite certifikat za sigurnost pomoću znaka za zaključavanje na adresnoj traci vašeg preglednika. Ukoliko nema ovog znaka, vjerojatno se nalazite na internet stranicama koje nisu sigurne.

Ako postoji sigurna veza, u adresnoj traci vašeg preglednika pojavit će se skraćenica https://. Postupak kriptiranja onemogućava čitanje podataka ili manipulaciju podacima dok radite.

Budite sumnjičavi kada su u pitanju nepoznati certifikati za sigurnost! Certifikati za banke i renomirane internetske dućane poznati su standardnim preglednicima. Kontaktirajte svoju banku ili internetski dućan prije nego što prihvatite nove certifikate.

Ne slijedite linkove do internet stranica banke. Umjesto toga unesite adresu ručno ili koristite spremljenu stranicu (bookmark). Linkovi iz e-poruka često puta vode do lažnih internet stranica koje izgledaju kao prave i koje vas navode da otkrijete svoje podatke.

Stranica vaše banke za prijavu nikada neće od vas tražiti TAN kodove. Ako se to dogodi, molimo da odmah kontaktirate banku.

Također možete koristiti adresnu traku kako biste odredili originalni naziv domene. Dijelovi na početku nisu važni. Na primjer: www.firstnationalbankofplainville.financedepartment.randomISP.com. Ono što gledate nije First National Bank domene Plainville, već je ista hostirana na randomISP.com.

Najbolja zaštita od phishing e-poruka:
obrišite ih bez čitanja!

SOCIJALNI INŽENJERING

Prevaranti ciljano manipuliraju ljudskom osjetljivošću i slabostima kako bi došli do povjerljivih podataka.

ŠTO JE SOCIJALNI INŽENJERING?

Cilj socijalnog inženjeringa je ostvariti neovlašteni pristup privatnim i osjetljivim podacima putem međuljudske interakcije. Kriminalci ispituju osobnu situaciju svoje žrtve i imaju lažni identitet.

KAKO IZBJEĆI OVAKAV NAPAD?

Teško se obraniti od napada socijalnog inženjeringa budući da napadač u pravilu iskorištava pozitivne ljudske osobine: najvažniji faktor u obrani od napada socijalnog inženjeringa je uporno inzistiranje potencijalne žrtve na jasnom utvrđivanju identiteta i ovlaštenja pozivatelja odnodno pošiljatelja e-poruke prije davanja informacija.

Jednostavno traženje imena i prezimena i telefonskog broja pozivatelja ili molba da pozdravi nepostojećeg kolegu mogu otkriti slabo informiranog napadača. Nepoznatim osobama ne treba davati čak niti naizgled nevažne ili nekorisne informacije; iste bi se mogle koristiti zajedno s drugim informacijama u cilju manipulacije. Važno je pravovremeno upozoriti sve potencijalne žrtve. Vaša prva točka kontakta trebao bi biti odjel kompanije nadležan za sigurnost, kontakt adresa davatelja usluge elektroničke pošte i osoba čiji su podaci korišteni u lažnom identitetu.

Imajte na umu sljedeće:

- Uvijek budite sumnjičavi prema svim e-porukama s nejasnim identitetom pošiljatelja.
- U slučaju telefonskog poziva nemojte davati stranim osobama osobne informacije koje se naizgled čine nevažnima jer se one mogu povezati u korisne informacije i upotrijebiti za daljnje napade.
- Nikad ne otkrivajte osobne ili financijske podatke u ispitivanjima putem e-pošte bez obzira na jasan identitet pošiljatelja poruke.
- Nemojte davati osobne podatke na internetskim stranicama do kojih ste došli preko linkova iz e-poruka. Sami unesite URL u preglednik.
- Ukoliko niste sigurni u identitet pošiljatelja e-poruke, kontaktirajte ga telefonom kako biste potvrdili njegovu autentičnost.

PAMETNO KORIŠTENJE DRUŠTVENIH MREŽA

Društvene mreže su postale važan dio naše svakodnevice. Evo što treba imati na umu kada ih koristite.

Facebook, Google+, LinkedIn, Twitter i niz drugih mreža: u namjeri da ostanu u kontaktu s prijateljima, poznanicima i kolegama, velik broj ljudi otkriva privatne podatke o sebi, a da pri tome ne razmišlja o opasnostima koje vrebaju na društvenim mrežama.

Internet nije mjesto na kojem vlada bezakonje. Važeća pravila ne slijede sve osobe, niti sve zemlje imaju ista pravila: propisi vezani uz zaštitu podataka kojima se želi zaštititi vaše pravo na upravljanje vlastitim imidžom ili autorska prava često se ne shvaćaju ozbiljno. Upravo zbog toga je važno da pažljivo pročitate opće uvjete i politiku zaštite privatnosti na stranicama društvene mreže koju koristite.

IZRADA VLASTITOG PROFILA

Kao prvo, trebali biste objaviti što manje osobnih podataka – kao što su e-adrese, telefonski brojevi, IM poruke, fotografije itd. Konačno, svatko tko otkriva previše podataka o sebi više će biti izložen → **PHISHING** napadima i spam porukama.

Na raspolaganju su i postavke kojima se može ograničiti tko može vidjeti vaš profil. Najsigurnija je opcija omogućiti pristup samo prijateljima.

PRIVATNOST NA DRUŠTVENIM MREŽAMA

Saznajte više o postavkama svake društvene mreže u pogledu zaštite vaše privatnosti. Uz politike privatnosti i uvjete za svaku društvenu mrežu, više informacija o najboljim načinima zaštite vaše privatnosti na raznim društvenim mrežama kao i o društvenim mrežama općenito možete naći na: **http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2009-08-273.pdf** .

Osobnim podacima trebali bi, uz vas, imati pristup samo pravi prijatelji i o tome trebate voditi računa kada odlučujete tko će sve imati pristup podacima u vašem profilu u sklopu neke društvene mreže. Neke mreže nude mogućnost podjele prijatelja u različite grupe s time da su svakoj grupi dodijeljena različita prava pristupa, što omogućuje jednostavnu kontrolu tko može vidjeti određene informacije.

FOTOGRAFIJE PROFILA I FOTO ALBUMI

Iako je osobno prezentiranje na internetu putem fotografija postala uobičajena praksa, neke fotografije predstavljaju stvarnu prijetnju za vašu privatnost. Prije nego što postavite fotografije pažljivo razmislite želite li da se one pojave na internetu.
Kada kreirate foto album, uvjerite se da samo

prijatelji imaju direktan pristup albumu, što se lako može definirati u postavkama albuma.
Uvijek učitavajte samo one fotografije za koje imate autorska prava.

Fotografije koje ste učitali na internet često puta ostanu dugo spremljene u → **CACHE** memoriji, čak i ako obrišete fotografije ili pak cijeli foto album.

Kao što ni vi ne želite biti negativno prikazani na slikama, isto tako biste trebali poštivati i privatnost prijatelja i poznanika te staviti njihove slike na internet tek nakon što ste dobili njihovu privolu, odnosno izbrisati slike na njihov zahtjev.

DODAVANJE PRIJATELJA

Prije prihvaćanja zahtjeva za prijateljstvo ili slanja zahtjeva drugim osobama provjerite tko se nalazi na drugoj strani.

DOGOVARANJE SASTANAKA PUTEM INTERNETA

Društvene mreže često se puta koriste za dogovaranje sastanka s prijateljima ili slične dogovore. Nikad ne otkrivajte privatne informacije, uključujući i onu „Danas sam sama doma“ na mjestima dostupnima širokoj publici. Ovakve informacije trebalo bi razmjenjivati samo u privatnim porukama, putem e-pošte ili IM poruka!

FUNKCIJA PRIJAVE I IGNORIRANJA

Osobe, sadržaji ili grupe koje krše etičke standarde mreže odmah treba prijaviti. Na vašem profilu obično postoji programska tipka za prijavu.

Funkciju ignoriranja (ignore) možete koristiti za postupanje s korisnicima koji vas uznemiravaju te im onemogućiti pristup vašem profilu. Navedena funkcija također će im onemogućiti slanje direktnih poruka. Ovakve osobe treba prijaviti njihovom davatelju internetskih usluga.

SINKRONIZACIJA ADRESARA

Mnoge mreže nude opciju povezivanja vanjskih adresara e-pošte sa zajednicom. Ove stranice koriste navedene podatke za usporedbu, naime tko je već član zajednice odnosno tko (još) nije. Nejasno je što se pri tome događa s podacima – i koriste li se ti podaci u druge svrhe.

NIJE VAŽNO ŠTO KAŽETE, NEGO KAKO TO KAŽETE

Prije pojave interneta svaka je priznata edukacija uključivala čitanje i primjenu pravila lijepog ponašanja iz Bontona i sličnih knjiga. Ovakva pravila vrijede i u današnjem svijetu digitalne komunikacije.

RAČUNALSTVO U OBLAKU

Podaci su dostupni svugdje, 24 sata na dan, 7 dana u tjednu, a sve to omogućuje računalstvo u oblaku. Datotekama koje pohranjujete u internetske repozitorije, uključujući HT-ovu Spremalicu, može se pristupiti na internetu, bez obzira na vrstu uređaja.

PRESELJENJE U OBLAK – ALI SIGURNO

→ RAČUNALSTVO U OBLAKU znači da datoteke i programi više nisu pohranjeni lokalno. Umjesto toga, fizički su smješteni na serverima u računalnim centrima koji se nalaze u prostorijama pružatelja usluga u oblaku. Velika prednost sastoji se u tome da su sadržaj i aplikacije dostupni u svakom trenutku, kako u kući, tako i izvan nje, na svim uređajima s pristupom internetu. Međutim, **→ RAČUNALSTVO U OBLAKU** također donosi i probleme u pogledu sigurnosti.

Odaberite sigurnog davatelja usluga u oblaku.
Ne povjeravajte svoje podatke svakome. Detaljno ispitajte svakog davatelja usluga i njegove usluge. HT pohranjuje osobne korisničke datoteke u Spremalicu isključivo na serverima koji se nalaze u Hrvatskoj i koji podliježu strogim propisima o zaštiti podataka. Podaci se prenose na servere, koji su zaštićeni **→ VATROZIDIMA**, uz korištenje najnovije tehnologije zaštitnog kriptiranja.

Držite se osnovnih pravila korištenja informacijskih tehnologija.
Naročito ovih: koristite samo sigurne lozinke i pohranite ih na način da su dobro zaštićene od pristupa trećih strana. Također je važno mijenjati lozinke u redovnim intervalima (vidi „Odabir sigurne lozinke“).

RJEČNIK POJMOVA VEZANIH UZ PRIVATNOST

→ **ANTI-SPYWARE** (protušpijunski program) odnosi se na programe koji onemogućuju špijuniranje korisničkih podataka korištenjem malicioznih → **SPYWARE** programa.

→ **BLUETOOTH** je način umrežavanja dvaju uređaja na maloj udaljenosti putem radio signala za razmjenu podataka.

→ **CACHE** je često korišten pojam za prostor privremene pohrane u računalnoj memoriji koji automatski sprema sadržaj koji se gleda na računalu kako bi se korisnik drugi puta brže vratio ovome materijalu. Svi internet preglednici koriste cache kako bi ubrzali proces prikaza internet stranica. Najpoznatije tražilice također koriste cache za obradu internetskog sadržaja.

→ **CRVI** su štetni programi koji se šire na računalne mreže. Šire se putem mrežnih usluga ili korisničkih sučelja. Primjer komunikacijskog kanala za računalne crve je e-pošta ili preuzimanje softvera s interneta.

→ **IM (INSTANT MESSAGING)** je razmjena tekstualnih poruka kroz softversku aplikaciju u realnomvremenu

→ **KOLAČIĆI (COOKIES)** su datoteke koje su pohranjene na osobnom računalu kako bi se olakšao postupak naknadnog ili ponovljenog pristupa istom internet serveru.

→ **PHISHING** je pokušaj korištenja lažnih internetskih adresa kako bi se dobio pristup podacima korisnika interneta. Pojam je nastao spajanjem riječi password (lozinka) i fishing (pecanje).

→ **PIN** je skraćenica od Personal Identification Number. To je tajni broj ili kod koji se sastoji od slova i brojki, a potreban je za prijavu na sigurnije funkcije kao što je internetsko bankarstvo ili otključavanje SIM kartice.

→ **RAČUNALSTVO U OBLAKU** je model pohrane podataka ne (samo) na osobnom računalu, već i na udaljenim serverima davatelja usluge. Podaci mogu biti dostupni ovlaštenim korisnicima u svakom trenutku i s bilo kojeg mjesta. Jedan od primjera je Mediacenter Deutsche Telekoma.

→ **SKENERI VIRUSA** su programi koji otkrivaju i blokiraju poznate računalne viruse → **TROJANCE** i → **CRVE** u procesoru, nakon čega ih uklanjaju.

→ **SPYWARE** programi (špijunski programi) pokušavaju nadgledati korisničke informacije i podatke bez znanja korisnika, nakon čega se podaci tajno vraćaju kreatoru programa. Kako bi se spriječilo ovo špijuniranje instaliraju se programi poznati pod nazivom → **ANTI-SPYWARE**.

→ **SSL** ili Secure Sockets Layer je prethodnik → **TLS-A** (Transport Layer Security), kriptografskog protokola za siguran prijenos podataka.

→ **ŠTETNI ILI MALICIOZNI PROGRAMI (MALWARE)** predstavljaju krovni pojam za računalne programe koji su razvijeni kako bi vršili neželjene radnje, uključujući i one koji mogu izazvati štete. Riječ malware nastala je spajanjem riječi malicious (maliciozni, štetni) i software.

→ **TAN** je skraćenica od Transaction Authentication Number. Radi se o jednokratnoj lozinki koja se prvenstveno koristi u internetskom bankarstvu, a najčešće se sastoji od šest brojeva ili kombinacije brojeva i slova. Ako se TAN šalje na mobilnom uređaju, na primjer putem poruke, tada se koristi pojam mobilni TAN ili mTAN.

→ **TLS** ili Transport Layer Security, ili stariji naziv → **SSL** (Secure Sockets Layer), je kriptografski protokol za siguran prijenos podataka.

→ **TROJANAC** je računalni program koji se predstavlja kao neki drugi program s korisnim ili poželjnim funkcijama. Međutim, obično izvodi štetne aktivnosti bez znanja korisnika.

→ **VIRUS**I su računalni programi koji se skrivaju u drugim računalnim programima i ondje se repliciraju. Nakon što korisnik pokrene ovakav program, neće ga moći kontrolirati, a program će preuzeti kontrolu nad hardverom, operativnim sustavom ili softverom. Pojam „virus“ odnosi se način širenja programa – poput zaraze.

→ **VATROZID (FIREWALL)** prati tok podataka na mreži i osigurava dolazni i odlazni mrežni promet od neovlaštenog pristupa. Vatrozid koristi unaprijed definirana pravila kako bi se provjerilo treba li slati podatkovne pakete, na primjer između računala i interneta.

→ **WLAN** – Wireless Local Area Network. WLAN bežično povezuje jedan ili više uređaja s baznom stanicom, što stvara lokalnu mrežu s prijenosom podataka putem radio valova. WLAN bazna stanica obično sadrži ruter koji uspostavlja vezu s internetom.

Hrvatski Telekom d.d.
www.hrvatskitelekom.hr

ŽIVJETI ZAJEDNO