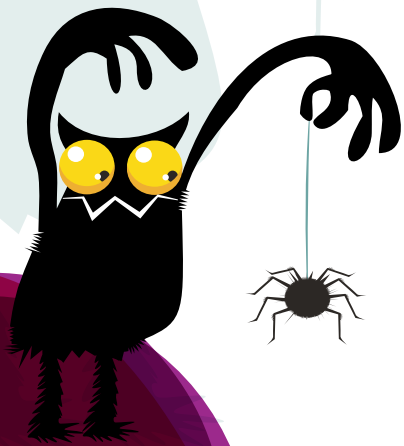
HAKOM

KAKO ZAŠTITITI DIJETE

u svijetu interneta, mrežnih tehnologija i mobilnih telefona

1. OPASNOSTI na internetu

Kad pristupimo internetu, kao da imamo svijet u svojim rukama. U najmanjem mogućem vremenu možemo saznati gotovo sve potrebne informacije i gotovo sve što se događa u svijetu. Možemo biti u stalnom kontaktu s prijateljima i u svakom trenutku znati što se događa u ekipi. **No, internetu ne pristupaju samo ljudi koji vole mačke, žele mir u svijetu ili traže recepte za kolače.** Nažalost, internetu pristupaju i ljudi koji nas žele iskoristiti!



Opasnosti na internetu

Opasnosti na internetu su velike. Ne biste vjerovali, ali postoji čitava vojska ljudi čiji je jedini cilj pronaći način da iskoriste naše podatke i računalo za ispunjenje svojih ciljeva. Da bi ostvarili pristup našim podacima i računalima, kriminalci se koriste raznim programima pomoću kojih zaobilaze „sigurnost“ naših računala.

Trenutno se dnevno otkrije 3000 novih malicioznih programa!

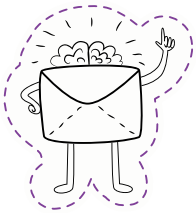
Računalne obrane jednostavno ne mogu držati korak s takvom bujicom i zbog toga je potrebno biti svjestan stvari koje nas vrebaju na internetu. **INFORMIRANOST JE NAJBOLJA OBRANA PROTIV NAPADAČA.**

Kako nas napadači na internetu mogu pokušati prevariti?

Putem elektroničke pošte, slanjem poruka za koje se na prvi pogled čini da dolaze od neke poznate tvrtke **(Facebook, Ebay, Paypal, Snapchat i sl.).**

Svrha takvih poruka je PREVARITI nas da **unesemo svoje pristupne podatke u aplikaciju čime računalnim kriminalcima dajemo pristup našim podacima.** A jednom kada imaju podatke o nama, u mogućnosti su uzeti kredit u naše ime, kupiti nešto našim karticama, predstavljati se kao mi i u naše ime raditi neželjene stvari.

Primjeri lažnih poruka:



From: **Skype Notify** <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: Deferred messages priming
To:

Skype

Deferred message.

View messages.

Yours truly
Skype support

From: **Secure FacebookService** <diaz@jasondoucette.com>
Date: 25 November 2015 at 23:36
Subject: Hi You have missed e-mails acculturate
To:

facebook

You have missed e-mail.

View e-mails.

Sincerely yours
Facebook support

U slučaju da primite sličnu poruku **NEMOJTE KLIKNUTI NA LINK**, već otipkajte u preglednik adresu servisa, npr. **www.facebook.com**, ulogirajte se i provjerite čekaju li vas zaista propuštene poruke .

Zlonamjerne poruke mogu doći i s nama poznatih adresa. Kada računalni kriminalci nekome provale u elektroničku poštu, često pošalju **lažne poruke svim ljudima koje nađu zapisane u imeniku.**

AKO PORUKA DOLAZI OD NEPOZNATE OSOBE NEMOJTE KLIKNUTI NA LINK ILI OTVORITI PRILOG (ATTACHMENT).
ČAK I AKO JE OD POZNATE OSOBE, BUDITE OPREZNI!

Kako prepoznati lažnu poruku?

Neki od znakova po kojima se može prepoznati da je poruka lažna:

NE OBRAĆA SE NAMA DIREKTNO već počinje nekim općenitim pozdravom npr. „Hi there“, ili „Hey you“ ili „Bok!”

IMA GRAMATIČKE POGREŠKE - posebno obratite pažnju ako se obraća u pogrešnom licu

IME SERVISA I ADRESA S KOJE PIŠE DA JE PORUKA DOŠLA NISU ISTI
- na primjeru Skypea izgleda kao da je poruka došla od Skypea, no Skype ima domenu **@skype.com**, a ova poruka je došla s **@pmw.de**

Od: petar <petar @gmail.com>
Datum: 2. prosinca 2015. u 16:16:51 GMT+9
Za: undisclosed-recipients:;
Predmet: **TREBAM TVOJU POMOĆ**
Odgovori: <petar @mail.com>

Oprosti što ti se javljam ovako. Otputovao sam u Turska, i moja torba, u kojoj je bila putovnica i kreditne kartice su mi ukrali. Kontaktirao sam banku, ali treba im još vremena da mi naprave novu karticu. Mislio sam te zamoliti da mi posudiš nešto novaca koje cu ti vratiti po povratku. Treba mi 1.400 eura da pokrijem troškove. Mogu ti proslijediti detalje o tome kako vi možeš slati novac. Molim te javi mi je li to moguce. Željno iščekujem tvoj odgovor!

S poštovanjem

Petar

From: **Skype Notify** <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: **Deferred messages priming**
To:

Kako zaštititi e-mail adresu, Facebook i sl.

Koristite različite lozinke za servise na internetu. Kako ne biste pamtili stotine lozinki poslužite se programom za upravljanje lozinkama – na ovoj stranici možete naći usporedbu najpopularnijih

http://www.pcmag.com/article2/0,2817,2407168,00.asp

Kada se ista lozinka koristi na više mjesta, računalni kriminalci se često koriste taktikom da provale na slabo zaštićene stranice i pokupe sve lozinke korisnika te ih isprobavaju na popularnijim internet stranicama!

Koristite lozinke od barem

8 znakova

koje sadrže velika i mala slova, brojeve i specijalne znakove.

NEMOJTE KORISTITI
imena svojih bližnjih, ljubimaca i datume rođenja ljudi oko vas!

Nemojte koristiti istu lozinku za elektroničku poštu, Facebook i druge stranice koje posjećujete!

Popularne stranice i servisi poput Facebooka, Googlea i Twittera nude mogućnost tzv. **POTVRDE U DVA KORAKA** koja štiti vaš profil ili e-mail adresu od neovlaštenog upada jer na vaš mobitel šalje kôd koji treba ukucati ako se prijavljujete s nepoznatog uređaja.

https://www.google.com/landing/2step/

https://support.twitter.com/articles/20170388

http://www.oxhow.com/setup-facebook-login-approvals-two-step-verification-method/

Budite oprezni kada vas putem socijalnih mreža **kontaktiraju nepoznate osobe.** Prije nego što ih prihvatite za prijatelje, provjerite jesu li stvarno osobe za koje se izdaju. Npr. uzmite profilnu sliku i potražite je na Googleu – prevaranti često koriste tuđe slike za profile.

Kada ste na Google pretraživaču, prijeđite na pretraživanje po slikama, kliknite na mali fotić u rubu tražilice, odaberite tab „Prenesite sliku“ i iskoristite sliku s profila za pretraživanje

Ako nađete sliku na više različitih mjesta, pod drugim imenom – sve vam je jasno! Netko se ne predstavlja svojim pravim imenom!

Prevare putem interneta

Internet je divno i krasno mjesto s puno interesantnih informacija, no s obzirom na to da su svi spojeni na internet i da svi komuniciramo putem poruka, puno nas ne razmišlja gdje sve ostavljamo svoju e - mail adresu te je velika šansa da ćemo prije ili poslije biti meta nekoga tko na neki način želi zaraditi na nama.

AKO DOBIJETE PONUDU ZA NEŠTO BESPLATNO, dobro razmislite je li to vrijedno ostavljanja svojih podataka. Naime, drevna mudrost kaže: **„Nema takve stvari kao besplatan ručak“**. Drugim riječima, ako nešto zvuči predobro da bi bilo istinito – vjerojatno je predobro da bi bilo istinito.

BUDITE OPREZNI KADA SE U SVIJETU DOGODI DOGAĐAJ KOJI ODJEKNE PO MEDIJIMA – bilo da se radi o slavnim osobama, terorističkom napadu ili humanitarnim akcijama – kriminalci često koriste takve situacije za slanje e - maila koji vas pokušavaju nagovoriti da otvorite određenu stranicu ili skinete neku datoteku.

Držite se internetskih stranica koje redovito posjećujete. Vijesti na njima bit će najvjerojatnije provjerene i sigurne. Ne nasjedajte na navlakuše!

Opreznost je potrebna i **KOD INSTALACIJE RAZNIH APLIKACIJA**, bilo na pametnom telefonu ili Facebooku. Provjerite koja sigurnosna prava aplikacija traži od vas tj. čemu sve traži pristup na vašem telefonu. Ako su zahtjevi nerazumni, npr. **kalkulator aplikacija** traži pristup vašim slikama i kontaktima, nemojte je preuzeti!

2. RODITELJSKA zaštita

Na internetu

OPERATORI NUDE uslugu **"Roditeljska zaštita"** koja omogućuje **FILTRIRANJE internetskog sadržaja** pomoću koje se djeca učinkovitije mogu zaštititi od neprimjerenih sadržaja dok surfaju internetom.
Navedena opcija omogućava **JASNO ODREĐIVANJE SADRŽAJA i VREMENA PRISTUPA INTERNETU ZA DJECU**, a istovremeno omogućava neograničeno surfanje za roditelje pomoću **sigurnosnog PIN**-a.

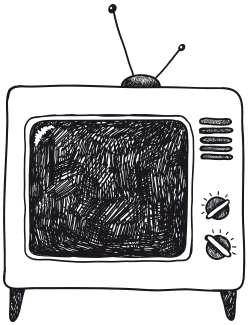
Pozivi i SMS ili MMS

Na isti način možete **ograničiti pozive ili slanje poruka prema nepoznatim brojevima.** U dogovoru s djetetom možete odrediti, kreirati listu brojeva, koje brojeve dijete može pozivati i s kim može razmjenjivati SMS ili MMS.

Ako dijete prima SMS ili MMS poruke sa sadržajem neprimjerenim djeci i maloljetnicima i namijenjene isključivo odraslima, obavijestite o tome operatora ili prijavite primitak takve poruke na adresu elektroničke pošte

nezeljeni.sms@hakom.hr, www.hakom.hr

Roditelji, zatražite od svog operatora postavljanje zabrane pristupa sadržajima koji su neprimjereni djeci!



IPTV

Postavljanjem roditeljske zaštite onemogućuje se pristup sadržajima neprimjerenim za djecu poput pornografskih ili nasilnih sadržaja. Postavljanjem roditeljske zaštite ujedno **sprečavate gledanje neprimjerenih TV programa ili filmova iz IPTV videoteke.**

Dodatne informacije o načinu postavljanja roditeljske zaštite možete pronaći na

www.hakom.hr

ili internetskim stranicama svog operatora.

3. KORISNI SAVJETI za roditelje

Zaštita djece pri korištenju mobilnih uređaja

Vezano uz aplikacije na mobilnim uređajima, **roditeljima** se savjetuje da djeci daju na korištenje **PRE-PAID KARTICE, odnosno SIM kartice s određenim iznosom novčanog bona.**

Također, **roditelji** imaju mogućnost postaviti **ZABRANE instaliranja i brisanja određenih aplikacija**.

Roditelji, možete onemogućiti djetetu da instalira neku iPad ili iPhone aplikaciju.

7 koraka kako postaviti ograničenja:

Uključite Vaš iPhone ili iPad uređaj. Na glavnom ekranu odaberite **Postavke** (Settings).

Unutar opcije **Postavke** (Settings) odaberite **Općenito** (General).

Pronađite dio koji se zove **Ograničenja** (Restrictions)**.** Kliknite na to.

Tapnite na **Aktiviraj ograničenja** (Enable Restrictions).

Kada aktivirate ograničenja (Enable Restrictions), trebat ćete **kreirati lozinku**. Svakako je negdje zapišite i nemojte je zaboraviti.

Tapnite na "prekidač" na kojem piše **In-App kupnja** (In-App Purchases) i isključite ga.

Kao što i sami vidite, možete definirati i neka druga ograničenja na iOS uređajima, kao što je **instaliranje ili brisanje aplikacija** (Installing Apps, Deleting Apps).

Android pruža mogućnost korisničkih ograničenja. Odaberite **Postavke** (Settings), dodajte korisnika ili novi profil i odaberite **Ograničen Profil** (Restricted Profile). Nakon toga može se odabrati koje **aplikacij**e će biti dostupne odgovarajućem računu.

4. USLUGE S POSEBNOM tarifom

Postoji čitav niz govornih i SMS usluga koje se naplaćuju po višim cijenama jer uz javnu komunikacijsku uslugu daju i neke dodatne sadržaje.

ZA SMS USLUGE – obavijest o cijeni naplate, uputa o načinu prekida korištenja usluge, prekid pružanja usluge nakon potrošenih **150,00kn ili 30 SMS/MMS.**

NA POČETKU SVAKOG POZIVA - najava cijene i mogućnost prekida poziva (2 sekunde) prije početka naplate.

ZA POZIVE KOJI SE NAPLAĆUJU PO MINUTI - najava i prekid poziva nakon isteka 30 minuta odnosno potrošnje novčanog iznosa od **150,00 kn.**

Roditelji, za promidžbu i pružanje ovih usluga postoje posebna pravila.

Radi zaštite djece uvedena je:

POSEBNA NUMERACIJA ZA USLUGE ZA ODRASLE (064 XXX XXX) koje su djeci zabranjene. Operator je u svim promidžbenim aktivnostima obvezan navesti da se radi o usluzi čiji sadržaj nije namijenjen djeci.

ZABRANA SLANJA I/ILI PRIMANJA SMS I MMS PORUKA U OKVIRU USLUGE S POSEBNOM TARIFOM (6xx xxx, 8xx xxx i sl.) koju **roditelji** mogu zatražiti od svog operatora.

POSEBNA NUMERACIJA ZA USLUGE ZA DJECU (069 XXX XXX).

NOVČANI LIMIT POTROŠNJE ZA USLUGE KOJE SU NAMIJENJENE DJECI (50,00 KN).

5. DRUŠTVENE MREŽE

facebook

Današnja djeca i mladi teško mogu zamisliti život bez društvenih mreža poput **Facebooka, Twittera** i njihova svakodnevnog korištenja. Pravila lijepog ponašanja na mrežama prilagođavaju se novim tehnologijama, ali ono staro pravilo koje vrijedi u stvarnom životu, vrijedi uvijek: **“Ponašaj se prema drugima onako kako želiš da se drugi ponašaju prema tebi.“**

Nažalost, to ponekad nije praksa jer pojedinci koriste društvene mreže za one radnje koje nikada ne bi napravili u stvarnom životu.

Kroz pravila lijepog ponašanja na mrežama djecu trebamo usmjeravati na ispravan način komunikacije.

Neka od pravila lijepog ponašanja na mrežama

PRIPAZI ŠTO ŠALJEŠ U SVIJET. Ne samo što stvaraš sliku o sebi već utječeš i na druge.

Facebook je ogledalo korisnika. **NAŠE PONAŠANJE UTJEČE NA UKUPNU KVALITETU DRUŠTVENE MREŽE.** Iskoristite blagodati Facebooka i nemojte se neprimjereno ponašati.

NAČIN KOMUNICIRANJA POTREBNO JE PRILAGODITI drugom korisniku ili grupi korisnika kako bi razmjenjivanje informacija uspjelo.

PROUČITE POSTAVKE FACEBOOKA I POSTAVITE PRIVATNOST vašeg profila na željenu granicu. **Za neželjeno širenje vaših informacija uglavnom ste sami krivi.**

POŠTUJTE PRIVATNOST - kako vlastitu, tako i ostalih korisnika.

Bez obzira na sva pisana i nepisana pravila, imajte na umu da je **SVE ŠTO JE ILEGALNO U STVARNOM ŽIVOTU, ILEGALNO I NA INTERNETU. Nemojte se zavaravati misleći da se možete sakriti iza izmišljenog nadimka.**

Nemojte brisati prijatelje dok ste ljuti.

Ne omalovažavajte i ne vrijeđajte ljude koje ne poznajete.

Prije otvaranja profila na Facebooku **cijepite se protiv ovisnosti** o virtualnim društvenim mrežama.

Ne povezujte svoj Twitter account s Facebookom. Tweetovi nisu namijenjeni tomu.

Na Twitteru ne postoje prijatelji.

Sigurnost na društvenim mrežama i kako zaštititi privatnost na Facebooku

Na istom mjestu se može podesiti **TKO IMA UVID U LISTU NAŠIH PRIJATELJA.** Inicijalno, Face čini listu naših prijatelja javno dostupnom **(Public).**

Kako biste to promijenili, potrebno je otići pod **„OBITELJ I ODNOSI“** (niže).

Tamo su navedeni naši prijatelji, a klikom na gumb s penkalom pa na **„UREDI PRIVATNOST“**, dolazimo do mjesta gdje definiramo tko vidi listu naših prijatelja.

Najbolje je odabrati opciju **„PRIJATELJI“.**

Ovdje je još važno napomenuti da Face, na isti način, NUDI KONTROLU NAD OBJAVOM SVAKE POJEDINE INFORMACIJE!!!

Preporučujemo ograničavanje objave sljedećih informacija samo na prijatelje (ili barem na prijatelje prijatelja):

- KONTAKT INFORMACIJA
- PREBIVALIŠTA
- MJESTA ROĐENJA
- INFORMACIJA O ZAPOSLENJU
- INFORMACIJA O ŠKOLOVANJU

Izvor: http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku

6. ZAŠTITA OSOBNIH podataka na internetu

Roditelji, imajte na umu da i vaša djeca imaju pravo na privatnost! Stoga ne objavljujte njihove fotografije bilo gdje.

Kako danas imamo pristup svemu preko interneta, tako možemo doći i do nekih osobnih podataka. Dobar primjer za ovo su društvene mreže na kojima ljudi ostavljaju fotografije koje se opet mogu iskoristiti ili zloupotrijebiti na način da iste posluže kao korisne informacije za pristup privatnim bazama podataka. **Stoga je važno koje se fotografije ostavljaju na webu te je ujedno važno što je tko rekao.**

PROBLEM SE JAVLJA U SLUČAJEVIMA KADA SE OSOBNI PODACI OSTAVLJAJU, MEĐUSOBNO RAZMJENJUJU, PRIKUPLJAJU ILI ŠIRE DALJE. Sve navedeno može ugroziti privatnost podataka. Zato je **važno koristiti pseudonim u društvenim mrežama i drugim online komunikacijama.** Kriminalni elementi u društvu, također koriste pravo na privatnost kao paravan za zloću. Poštujte privatnost - kako vlastitu, tako i ostalih korisnika.

Roditelji, imajte na umu da i vaša djeca imaju pravo na privatnost!

Kalkulator privatnosti

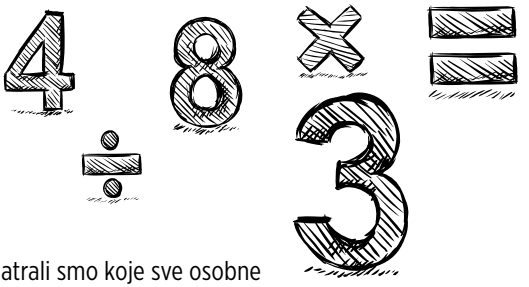
Mnoštvo usluga dostupnih putem interneta od korisnika traži **registraciju** tijekom koje korisnik mora predati svoje osobne podatke, **najčešće E-MAIL ADRESU, IME I PREZIME.**

Takav način registracije je očekivan i uobičajen i ne predstavlja prijetnju korisnicima. Međutim, do prevara može doći ako zlonamjerni pojedinci nekim načinom dođu do osobnih podataka korisnika.

Najčešći slučaj na internetu jest da napadači dobiju neovlašteni pristup usluzi na kojoj je korisnik pohranio vlastite podatke te na taj način očitaju osobne podatke koje koriste za daljnje napade i prevare.

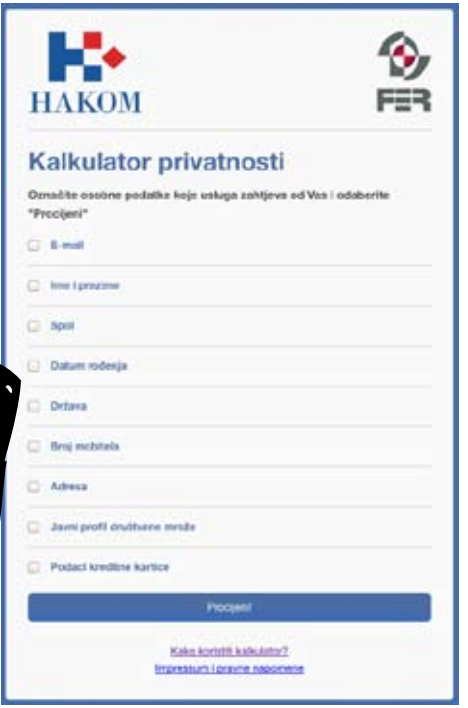
U tom smislu, nikako nam nije cilj zastrašiti korisnike interneta, nego ih educirati i potaknuti na razmišljanje o problemima sigurnosti i privatnosti na internetu.

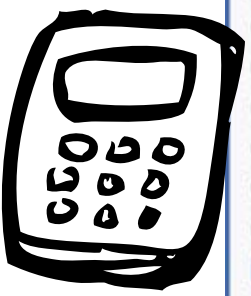
Kako koristiti kalkulator?



Prilikom osmišljavanja kalkulatora promatrali smo koje sve osobne podatke usluge zahtijevaju od korisnika tijekom registracije.
Tako smo izdvojili parametre koje možete vidjeti na naslovnici kalkulatora.

Odabirom parametara pokreće se sustav koji temeljem kombinacije odabranih osobnih podataka (parametara) **procjenjuje rizik za privatnost vlasnika tih podataka te nudi stvarne scenarije koji u najvećoj mjeri odgovaraju odabranim parametrima.**





Uz sam procijenjeni rizik, potičemo korisnike da pogledaju i scenarije **jer su upravo scenariji ključni za razumijevanje prevara** i problema koje internet može donijeti. Više na :

http://privatnost.hakom.hr/about.php

Pojmovnik:

IPTV - Usluga prijenosa televizijskog signala putem interneta.

SMS (Short Message Service) - Usluga slanja kratkih tekstualnih poruka unutar GSM standarda mobilne telefonije.

MMS (Multimedia Messaging Service) - Multimedijalni servis poruka koji omogućava slanje slika, zvučnih i videozapisa.

Maliciozni programi

– programi napravljeni da bi zaobišli zaštitu, otežali rad i omogućili kriminalcima pristup podacima na računalu.

CRVI – maliciozni programi koji imaju sposobnost dupliciranja i samostalnog širenja.

VIRUSI – maliciozni programi koji se šire posredstvom drugih programa, USB memorije ili CD/DVD diskova. Mogu usporiti računalo, otežati rad, obrisati podatke i sl.

TROJANCI – najopasnija vrsta malicioznih programa. Njihovo prisustvo se ne primjećuje, a omogućuju kriminalcima nesmetani pristup svim podacima na računalu.

SPECIJALNI ZNAKOVI – znakovi poput !, #, $ i sl. Dodavanjem takvih znakova u lozinku otežava računalnim kriminalcima pogađanje lozinke.