

Otvaranjem profila na nekoj od brojnih društvenih mreža (poput Facebooka ili Twittera) tinejdžeri zadovoljavaju svoju potrebu da budu viđeni onakvima kakvima se žele prikazati. Tako na svoje profile stavljači isključivo fotografije koje žele, koje ih prikazuju privlačnima i slično.

No, za razliku od odraslih, tinejdžerima Facebook služi i za kontrolu imidža svojih vršnjaka u javnosti te tu često nastaju problemi. Naime, osim što sebe žele prikazati društveno poželjnima, istovremeno koriste Facebook da vršnjake koji im se iz različitih razloga ne sviđaju prikažu u negativnom svjetlu.

Društvene mreže su im za to idealan medij iz više razloga:

- one su njihovo prirodno okruženje;
- vrlo brzo mogu iznijeti negativne stvari o svojoj kolegici ili kolegi iz razreda;
- kreatori ostaju anonimni;
- u vrlo kratkom vremenu velik broj osoba ima mogućnost doći do takvih informacija;
- ne gledaju žrtvu u lice što im omogućuje da budu bezobzirniji nego inače jer je prisutno potpuno odsustvo empatije: žrtvu ne vide pa ni ne znaju što žrtva proživljava.

Česti smo svjedoci različitih oblika zlostavljanja putem društvenih mreža među vršnjacima od npr. kreiranja "grupa" koje u svom nazivu, pokraj imena i prezimena žrtve imaju i riječ "mrzitelji", objavljuvanja video uredaka koji prikazuju zlostavljanje, otvaranje lažnih profila u žrtvino ime i slično.

Naravno i na društvenim mrežama prijete sve one opasnosti koje su uobičajene za internet te za njihovo sigurno korištenje vrijede svi oni savjeti koji su već dani u poglavljima "Savjeti mladim korisnicima" i "Savjeti roditeljima".

No, pokraj već navedenih uobičajenih savjeta roditeljima i mladim korisnicima, možemo savjetovati...

Savjeti roditeljima:

ukoliko vaše dijete ima otvoren profil na nekoj društvenoj mreži i vi otvorite profil na istoj mreži i budite prijatelj svom djetetu;

ako se ne znate koristiti društvenom mrežom neka vas vaše dijete pouči tome;

objasnite djeci da su osim njihovih prijatelja korisnici društvenih mreža i osobe koje mogu imati loše namjere te da stoga ne objavljaju osobne podatke koji se lako mogu zloupotabiti;

budite sigurni da vaše dijete razumije osnove sigurnosti i privatnosti na internetu;

savjetujte svom djetetu da mu prijatelji budu osobe koje poznaje u stvarnom životu, odnosno, da oprezno prihvata zahtjeve za novim prijateljstvima;

povremeno zajedno s djecom prokomentirajte aktivnosti na društvenoj mreži, neka vaša djeca znaju da ste zainteresirani i za njihov virtualni život;

djeca nerijetko putem društvenih mreža igraju igrice od kojih neke mogu stvarati nerealnu sliku o stvarnim životnim situacijama (primjerice: učestalo dobivanje čipova na poker igrici može dijete potaknuti na razne igre sreću i klađenja u stvarnom životu); prekomjerno provođenje vremena u igranju igrica i komunikaciji putem društvenih mreža može izazvati stvarnu ovisnost i bitno utjecati na kvalitetu djetetova života;

na svim društvenim mrežama postoje sigurnosni mehanizmi koji služe zaštiti svih korisnika - naučite se koristiti njima; obično se pokraj svake poruke, posta, objavljene fotografije nalazi link klikom na koji možete prijaviti neprimjereni sadržaj; moderatori ili administratori mreže će razmotriti vašu primjedbu i ukloniti s mreže neprimjereni sadržaj; autor, odnosno osoba koja je objavila sporni sadržaj, neće znati tko je prijavio sporni sadržaj;

ukoliko želite prijaviti policiji neki neprimjereni sadržaj, prije no što to učinite moderatoru/administratoru društvene mreže, spremite ga na svoje računalo ili prijavite to policiji; to lako možete učiniti na taj način da u svom internet pregledniku potražite opciju "Save as ..." ili "Spremi kao .." te na taj način spremite spornu internet stranicu (sadržaj) i pohranite eventualne dokaze;

također, na većini društvenih mreža postoji sigurnosna opcija blokiranja određenih korisnika; potaknite i podržite svoje dijete u prijavi neprimjerениh sadržaja.

Savjeti mladim korisnicima:

budi siguran/na da razumiješ osnove sigurnosti i privatnosti na internetu;

ne daj nikome svoje korisničke podatke (lozinke) - ni najboljim prijateljima ili dečku/djevojci;

slušaj savjete svojih roditelja, oni ti žele dobro, nemoj se bojati potražiti pomoći ili savjet od njih;

neka ti prijatelji budu samo osobe koje uistinu i poznaješ u stvarnom životu;

pažljivo prihvaćaj nove prijatelje;

nemoj se bojati prijaviti neprimjerene sadržaje - to je lako napraviti, a prijava je anonimna;

ako neprimjerene sadržaje želiš prijaviti policiji, učini to prije nego što ih prijavиш administratoru/moderatoru društvene mreže ili neprimjerene sadržaje pohrani na svoje računalo, kako bi eventualno kasnije mogao/la pokazati policiji, odnosno, kako bi mogli poslužiti kao dokaz;

blokiraj korisnike s kojima ne želiš komunicirati;

ne čini ništa u virtualnom svijetu što ne bi učinio u stvarnom svijetu!

## Krađa identiteta

Kazneni zakon RH ne propisuje kazneno djelo "krađe identiteta" kao posebno kazneno djelo. Pojam "krađe identiteta" koristi se u Republici Hrvatskoj u neformalnoj komunikaciji te se može odnositi na više kaznenih djela kojima je, u pravilu, krajnji cilj pribavljanje protupravne imovinske koristi ili prouzročenje kakve štete drugome.

Korištenjem aplikacija i web stranica koje su nezavisne od društvene mreže, korisnik pristaje dijeliti svoje podatke izvan društvene mreže. Međutim, Facebook i ostali društvene mreže moraju poštivati dogovor o pravima i odgovornostima. Ti dogovori daju niz ograničenja na korištenje prikupljenih podataka od korisnika. Međutim, nitko ne može garantirati da te društvene mreže neće prekršiti neko od pravila ili ga pokušati pogrešno interpretirati.

Jedno od važnijih obilježja "krađe identiteta" su načini počinjenja koji se neprestano mijenjaju, a za kradu u virtualnom svijetu značajno je:

korištenje raznih zlonamjernih programa za prikupljanje podataka, lozinki i slično (spyware, adware, keylogeri, crvi...);

lažne internet stranice (pharming);

korištenje lažnih poruka e-pošte (phishing);

obavijesti o lažnim lutrijskim dohicima;

tzv. nigerijska pisma;

neautorizirani pristupi podacima, tzv. hakerske provale u računalne sustave (financijske institucije, osiguravajuća društva, banke...).

Kako spriječiti krađu identiteta?

koristite složene lozinke;

ne pohranjujte lozinke u web preglednik;

ne slijedite sumnjive poveznice u e-mail porukama;

pratite sigurnosna upozorenja;

ne postavljajte povjerljive podatke;

postavite odgovarajuće sigurnosne i postavke za ograničavanje dostupnosti podataka;

upoznejte se s politikom privatnosti određenih web stranica, odnosno, društvenih mreža.