Na ovom linku možete naći definicije (opis) svih pojmova koji vam trebaju za internetske usluge, a posebno će vam pomoći u zaštiti.

**http://www.sigurnostnainternetu.hr/index.php/rjecnik-pojmova.html**

**VRSTE PRIJEVARA I KAKO IH IZBJEĆI**

Bilo da plaćate račune, koristite usluge *online* kupovine ili razmjenjujete poruke s prijateljima, iznimno je važno da ste sigurni i zaštićeni dok ste na internetu. Elektroničke i tekstualne poruke, telefonski pozivi i pisma koje vam upućuju prevaranti često su uvjerljivi i izgledaju posve vjerodostojno, stoga je nužno biti na oprezu u slučaju da naiđete na nešto sumnjivo.

Izlažemo pregled uobičajenih sigurnosnih prijetnji i prijevara te jednostavne savjete i preporuke o tome kako sigurno koristiti internet:

**PHISHING („pecanje podataka“ putem e-pošte)**

***Phishing* je proces putem kojega prevaranti dobivaju pristup osjetljivim podacima** poput korisničkih imena, lozinki ili podataka s kreditnih kartica, slanjem lažnih elektroničkih ili tekstualnih poruka koje izgledaju kao da su ih poslale legitimne organizacije. Poruke najčešće izgledaju kao da dolaze od banaka, popularnih društvenih mreža ili internetskih stranica za prodaju i kupnju.

*Phishing* se uglavnom izvodi putem e-poruka ili tekstualnih poruka u realnom vremenu (*instant messaging*), u kojima se od korisnika često traži da na lažnim internetskim stranicama (koje su gotovo identične stvarnim stranicama) ostave svoje podatke. Čak i dok koristite legitimne stranice banke, ponekad se na njima mogu pojaviti lažni skočni prozori (*pop-ups*). Čim kliknete na takav prozor ili unesete svoje osobne podatke ili podatke za identifikaciju, vaši podaci odlaze nekom drugom pružatelju usluga ili trećoj strani koja nije vaša banka. To znači da od toga trenutka nadalje netko drugi može pristupiti vašim računima. Postoje e-poruke koje sadrže linkove i žele vas navesti da posjetite web stranice na kojima ćete preuzeti štetne ili maliciozne programe (*[malware](http://www.sigurnostnainternetu.hr/index.php/vrste-prijevara/malware.html)*) uz čiju pomoć prevaranti mogu doći do vaših podataka i vašeg novca.

**Iz privitka se može instalirati i tzv. *ransomware*, a ne samo *malware***. Takvi programi šifriraju vaše datoteke, uključujući glazbu i fotografije, a prevaranti od vas traže „otkupninu“ kako biste ih dobili natrag.

Zaštitite vaša računala i druge uređaje najnovijim sigurnosnim rješenjima i programima najnovijim sigurnosnim rješenjima te budite na oprezu prilikom otvaranja privitaka ili poveznica (linkova) u neočekivanim e-porukama ili porukama za koje niste sigurni da su vjerodostojne. Svakako napravite sigurnosne kopije svih važnih datoteka u neumreženim mapama te nikada ne plaćajte otkupninu kriminalcima.

**E-poruke od vaše banke**

Vaša vam banka povremeno može poslati e-poruku s korisnim savjetima ili informacijama o proizvodima ili uslugama, ali vam:

* **nikada neće poslati e-poruku koja sadrži poveznicu (link) koja vas izravno vodi na stranicu Internet bankarstva,**
* **nikada neće poslati e-poruku u kojoj od vas traži da potvrdite podatke o svom bankovnom računu,**
* **nikada neće poslati e-poruku (ili vas nazvati) kako bi vas pitala za podatke o kreditnim karticama, PIN-ove, kôdove za prijavu (*one time passworde* - OTPove) i kôdove za autorizaciju transakcija (MACove) koje generira token, kao i lozinke,**
* **nikada neće poslati e-poruku u kojoj od vas traži da potvrdite nedavno obavljenu transakciju.**

Ako ste dobili sumnjivu e-poruku koju je navodno poslala vaša banka, proslijedite je vašoj banci, a zatim čim prije obrišite poruku koju ste dobili.

**Kako ga prepoznati?**

**Nestandardna e-adresa :** Krivotvorene e-poruke mogu biti poslane s adresa koje su naizgled slične službenim adresama vaše banke, ali ako ih pažljivije pogledate uočit ćete razliku u odnosu na pravu adresu.

**Neformalni pozdravi i osjetljiva pitanja:** Lažna e-poruka može ali i ne mora biti naslovljena na vas osobno. Može počinjati vašim osobnim imenom ali i sa „Cijenjeni korisniče“ i slično. **Obično prevarant od vas traži osobne informacije poput lozinke, podataka o korištenju Internetskoga bankarstva, kontakata ili brojeva kreditnih kartica**.

**Neodloživi zahtjevi:** U lažnim e-porukama često možete naići i na izraze poput ovoga: **„Moramo potvrditi informacije o vašem računu“.** Na taj vas način žele natjerati da im odgovorite smjesta i bez razmišljanja.

**Loš pravopis i oblikovanje teksta:** E-poruka može sadržavati gramatičke i pravopisne greške. Nadalje, lažna internetska stranica može imati nešto drugačiji izgled te sadržavati pogrešno napisane riječi. E-poruka može biti napisana na lošem hrvatskom odnosno zvučati kao loš automatizirani prijevod (npr. s Google prevoditelja).

**E-poruka bez teksta:** Ako **primite e-poruku bez teksta, samo s privitkom u prilogu, svakako postupite oprezno**. Banka vam nikada neće poslati e-poruku bez ikakva sadržaja.

**Neobične poveznice (linkovi):** Iako se poveznica (link) može činiti ispravnom, prije klika svakako provjerite pravu destinaciju na koju vas šalje. Prije nego kliknete, prijeđite mišem preko poveznice (linka) i provjerite kako glasi adresa stranice na koju vas usmjerava. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.

**Što poduzeti?**

* Ograničite količinu osobnih podataka koji su javno dostupni na internetu, uključujući društvene mreže.
* Oprezno postupajte sa svim e-porukama. Povratne adrese ili adrese pošiljatelja mogu se lažirati. Potpunu e-adresu pošiljatelja možete provjeriti tako što ćete mišem prijeći preko naziva pošiljatelja. Zaglavlje e-poruke i poveznica na internetsku stranicu također se mogu lažirati. Prijeđete li mišem iznad poveznice, možete vidjeti potpuno drugačiju stranicu.
* Ne otvarajte poveznice iz neočekivanih ili sumnjivih e-poruka. Upišite adresu u internetski preglednik. Banka vam nikada u e-poruci neće poslati poveznicu na stranicu na kojoj se logirate u svoj bankovni račun ili na stranicu koja od vas traži sigurnosne ili osobne podatke. Budući banka nikad neće slati direktni link na stranicu Internet bankarstva, stranici Internet bankarstva uvijek pristupajte direktno (upisom adrese u internet preglednik), a ne putem linka u e-poruci.
* **Nikada ne otvarajte privitke iz neočekivanih e-poruka (pogotovo one s nastavcima .exe, .pif ili .vbf)**

**Prijavi *phishing***

Dobijete li lažnu e-poruku, ostanite pribrani jer opasnost ne leži u primanju takve poruke. No nemojte otvarati poveznice (linkove)ili privitke iz takve poruke ili otkrivati podatke o internetskom ili mobilnom bankarstvu. Jednostavno ne odgovarajte na nju i izbrišite je. Ako vas neki od skočnih prozora traži vaše sigurnosne podatke, nemojte ih odavati. Prijavite lažnu e-poruku vašoj banci i pomozite u sprječavanju takvih prijevara.

**VISHING („pecanje podataka” putem telefonskih poziva)**

***Vishing* j**e sličan *phishingu*, ali **se odnosi na lažne telefonske pozive u kojima se prevaranti predstavljaju kao zaposlenici banke ili druge poznate organizacije te od vas traže da novac s vlastitoga računa prebacite na neki nepoznati račun.** Kako bi vas nagovorili da otkrijete vaše podatke, prevaranti će vam pokušati „prodati“ uvjerljivu priču.

Primjerice, prevarant će se predstaviti kao djelatnik pružatelja usluga satelitske televizije, telekoma ili komunalnoga poduzeća i ponuditi vam povrat novca. U tu svrhu će od vas tražiti da vašu debitnu karticu umetnete u token i date im kôd za autorizaciju transakcija (MAC).Kôd će zatim iskoristiti kako bi izvršili transakcije s vašeg računa. Nikada ne otkrivajte svoje PIN-ove, lozinke, kôdove za prijavu (one time passworde - OTPove) i kôdove za autorizaciju transakcija (MACove) koje generira token.osobama koje vas na bilo koji način kontaktiraju.

**Kako ga prepoznati?**

**Prevaranti se obično služe sljedećim metodama:**

* + kažu vam da postoje određeni problemi s vašim računom,
  + kako bi zadobili vaše povjerenje, kažu vam da nazovete broj telefona ispisan na pozadini vaše debitne ili kreditne kartice, a onda vašu liniju drže otvorenom jer ne žele spustiti slušalicu i traže od vas da novac s vlastitoga računa iz sigurnosnih razloga prebacite na neki drugi račun.

**Što poduzeti?**

Ako zaprimite poziv osobe koja se predstavi kao djelatnik banke ili odjela za sigurnost neke od kartičnih kuća, budite oprezni kako ne biste postali žrtvom prijevare.

**Kako se možete zaštititi?**

* + Banka nikada od vas neće tražiti da novac prebacite na nepoznati račun. Ako netko zatraži takvo što od vas, smjesta prekinite vezu.
  + Ako vas netko nazove i kaže vam da nazovete broj ispisan na stražnjoj strani kartice ili bilo koji drugi broj, učinite sljedeće:
    - * poslužite se nekim drugim telefonom,
      * ako nemate drugi telefon, najprije nazovite nekoga od vaših prijatelja ili članova obitelji kako biste se uvjerili da je linija slobodna.

**Prijavite vishing**

Ako mislite da vas je nazvao prevarant ili da ste nekome nenamjerno dali pristup financijskim podacima, što prije nazovite svoju banku. Obavite poziv s nekoga drugog telefona, a ne s onoga na koji vas je prevarant nazvao. Naime, prevaranti često ostavljaju liniju otvorenom kako bi vas spriječili u zvanju te čak proizvode zvukove biranja brojeva kako biste mislili da je vaša linija slobodna.



**PRIJEVARA S KURIRIMA (courier fraud)**

Prevaranti se često pokušavaju predstaviti kao djelatnici banke ili policijski službenici te vas obavijestiti da postoje određeni problemi s vašom debitnom ili kreditnom karticom, na primjer kažu da je zloupotrijebljena (podignut određeni iznos s računa).Obično kažu da će doći po karticu i PIN zbog istrage, sprječavanja daljnje zloupotrebe ili povrata novca. Može se dogoditi i da vas traže da unesete vaš PIN putem telefona te reći da će poslati dostavljača po vašu karticu. Osim toga, mogu vas zamoliti da podignete određeni iznos novca s računa ili kupite neki skupi proizvod te ih predate dostavljaču i na taj način pomognete u tekućoj istrazi. Isto tako vas mogu pokušati nagovoriti da prebacite sredstva na novi, „sigurniji“ račun.

 Što poduzeti?

Banke i policija od vas nikada neće tražiti PIN-ove, kartice ili gotovinu, niti će vas nagovarati da kupujete skupe proizvode ili prebacujete novac na druge račune. Ako vas netko nazove i zamoli da učinite nešto od navedenoga, prekinite poziv. Uvijek provjerite je li poziv zaista prekinut prije negoli nazovete banku ili policiju i prijavite cijeli slučaj – pričekajte pet minuta ili uzmite drugi telefon.

 Prijavite prijevaru s kuririma

Ako mislite da vas je kontaktirao ili se na vašim vratima pojavio opisani prevarant, odnosno da vas je već uspio prevariti, što prije nazovite svoju banku i policiju. Obavite poziv s nekoga drugog telefona, a ne s onoga na koji vas je prevarant nazvao. Naime, prevaranti često ostavljaju liniju otvorenom kako bi vas spriječili u zvanju te čak proizvode zvukove biranja brojeva kako biste mislili da je vaša linija slobodna.

**MALWARE**

***Malware* je zajednički naziv za štetne ili maliciozne programe koje prevaranti koriste kako bi pristupili vašim računalima. Takvi su programi obično skriveni u privicima ili besplatnom sadržaju**. Koriste se za niz nezakonitih radnji kao što su krađa osobnih podataka, brisanje ili oštećivanje podataka, stvaranje *botnet* mreža (mreža zaraženih računala) i zaobilaženje sigurnosnih programa.

**Postoji cijeli niz različitih štetnih programa, uključujući viruse, trojance, špijunske programe (*spyware*)/reklamne programe (*adware*) i programe za zastrašivanje (*scareware*).**

**Virusi**

Virus je program koji se može reproducirati i koji često sa sobom donosi štetne programe koji mogu naštetiti datotekama i programima na vašim računalima. Nadalje, virusi se koriste za praćenje svega što radite na računalima te omogućavaju nedozvoljen i potencijalno štetan pristup vašim osobnim računalima.

Većina korisnika interneta svjesna je opasnosti koju donose virusi, a zaštita je moguća zahvaljujući raznim antivirusnim programima i vatrozidima. Međutim, osobe koje stvaraju viruse neprekidno pronalaze nove načine širenja virusa na vaša računala.

**Kako prepoznati virus/trojanca?**

Ako je vaše računalo zaraženo virusom, primijetit ćete sljedeće:

* + vaše se računalo ponaša neobično ili neuobičajeno,
  + glazba se uključuje sama od sebe,
  + na zaslonu računala vidite poruke i skočne prozore ,
  + datoteke su promijenjene ili izbrisane,
  + vaš tvrdi disk je oštećen ili izbrisan i / ili
  + vaše računalo je sporo ili ne reagira.

**Kako izbjeći viruse/trojance?**

* + Na računalo instalirajte antivirusni program/program protiv *malwarea*.
  + Provjerite jesu li antivirusni program/program protiv *malwarea* ažurirani.
  + Svaki tjedan pregledajte cjelokupno računalo.
  + S interneta preuzimajte isključivo sadržaj koji dolazi iz vjerodostojnih izvora. Zapitajte se možete li vjerovati izvoru i izgleda li stranica pouzdano.
  + Prije nego što kliknete na 'OK' i date svoju suglasnost, provjerite o čemu je riječ.
  + Ne preuzimajte piratske sadržaje (uključujući filmove, glazbu i računalne programe). Iako su besplatni, takvi sadržaji mogu sadržavati štetne programe.
  + Pazite da su vaše uobičajene aplikacije i programski dodaci (*plug-ins*) kao što su *Microsoft Office*, *Adobe Acrobat* i *Adobe Flash* uvijek ažurirani i imaju sve sigurnosne zakrpe. Brojne aplikacije mogu se automatski ažurirati.
  + **Budite oprezni prilikom plaćanja putem interneta; uvijek provjerite je li stranica na kojoj se nalazite zaštićena. Kako biste bili sigurni da idete na vjerodostojnu stranicu, upišite adresu u preglednik umjesto da kliknete na poveznicu (link).**

**Trojanci**

Na internetu vas često zatrpavaju zahtjevima za preuzimanjem različitih **sadržaja, uključujući pozadine za radnu površinu (*wallpapers*), *screensavere* i *widgete***. Odlučite li se na preuzimanje takvih sadržaja, morate znati da u tom slučaju možda preuzimate **trojanca.**

Kao što mu i saminaziv govori, trojanac je štetni program koji se pretvara da je nešto što nije i koji u sebi sadrži skriveni program čija je svrha činjenje štete. Trojanac na vašem računalu može napraviti raznu štetu:

* + izbrisati ili presnimiti podatke na vašem računalu,
  + snimiti udarce po tastaturi kako bi pristupili vašim osobnim podacima,
  + deaktivirati vatrozid i antivirusni program i / ili instalirati druge viruse.

Budući da trojanci dolaze u različitim oblicima, nema sigurnog načina na koji ih se možete riješiti. Osim toga, neke od njih iznimno je teško ukloniti s računala. Najbolja obrana protiv trojanaca je **korištenje ažuriranih antivirusnih programa**.

**Kako prepoznati virus/trojanca?** Ako je računalo zaraženo virusom:

* + **vaše se računalo ponaša neobično ili neuobičajeno,**
  + **glazba se uključuje sama od sebe,**
  + **na zaslonu računala vidite poruke i skočne prozore ,**
  + **datoteke su promijenjene ili izbrisane,**
  + **vaš tvrdi disk je oštećen ili izbrisan i / ili**
  + **vaše računalo reagira sporo ili ne reagira.**

**Kako izbjeći viruse/trojance?**

* + Na računalo instalirajte antivirusni program/program protiv *malwarea*.
  + Provjerite jesu li antivirusni program/program protiv *malwarea* ažurirani.
  + Svaki tjedan pregledajte cjelokupno računalo.
  + S interneta preuzimajte samo onaj sadržaj koji dolazi iz vjerodostojnih izvora. Zapitajte se možete li vjerovati izvoru i izgleda li stranica pouzdano.
  + Prije nego što kliknete na \\\'OK\\\' i date svoju suglasnost, provjerite o čemu je riječ.
  + Ne preuzimajte piratske sadržaje (uključujući filmove, glazbu i računalne programe). Iako su besplatni, takvi sadržaji mogu sadržavati štetne programe.
  + Pazite da su vaše uobičajene aplikacije i programski dodaci (*plug-ins*) kao što su *Microsoft Office*, *Adobe Acrobat* i *Adobe Flash* uvijek ažurirani i imaju sve sigurnosne zakrpe. Brojne aplikacije mogu se automatski ažurirati.
  + Budite oprezni prilikom plaćanja putem interneta: uvijek provjerite je li stranica na kojoj se nalazite zaštićena. Kako biste bili sigurni da idete na vjerodostojnu stranicu, upišite adresu u preglednik umjesto da kliknete na poveznicu (link).

**Spyware / Adware**

***Spyware* je program koji „špijunira“ vaše aktivnosti na internetu, dok je *adware* program koji na vaša računala instalira skočne prozore i oglase**. Mnogi od ovih virusa rade i jedno i drugo.

*Spyware* u najboljem slučaju može biti prilično bezopasan – može prikupiti informacije o vašim navikama surfanja i prikazivati oglase koji odgovaraju onome što vas zanima (*adware*). Pa čak i tada je riječ o svojevrsnom napadu na vašu privatnost i može značajno usporiti rad računala.

U najgorem slučaju *spyware* može biti maliciozan i skenirati vaš tvrdi disk u potrazi za osobnim podacima, poput bankovnih podataka i lozinki, te ih otkriti kriminalcima. Osim toga, može pokušati srušiti vaše antivirusne i *anti-spyware* programe.

**Kako prepoznati da je računalo zaraženo spywareom/adwareom?**

* + Na zaslonu računala pojavljuju se skočni prozori s oglasima (*adware*) čak i kada niste spojeni na internet i ne surfate.
  + Početna stranica u vašem pregledniku ili postavke pretraživanja mijenjaju se bez prethodnog upozorenja.
  + U vašem se pregledniku pojavila nova, neočekivana i neželjena alatna traka.
  + Vaše računalo sve je sporije, a sustav se sve češće ruši.

**Kako izbjeći spyware/adware?**

Budete li se držali sljedećih savjeta, bit ćete sigurni od *spywarea/adwarea,* ali i brojnih drugih sigurnosnih prijetnji na internetu.

* + S interneta preuzmite i instalirajte *anti-spyware* program.  
    Korisnicima OS-a *Windows* Microsoft nudi besplatni *anti-spyware* program *Windows Security Essentials*. Drugi proizvođači programskih rješenja nude slične proizvode – bilo koji renomirani isporučitelj računalnih programa može vam preporučiti najprikladnije rješenje za vaš sustav.
  + Ažurirajte programe.  
    Pazite da su programi na vašem računalu, posebice operativni sustav, ažurirani. Koristite li *Windows*, dopune za svoje programe možete preuzeti s Microsoftove stranice. Na istoj toj stranici možete omogućiti svom računalu da se automatski ažurira, zbog čega nećete morati sami brinuti o preuzimanju najnovijih programskih dopuna i verzija.
  + Oprezno surfajte internetom i preuzimajte sadržaj.  
    Programe preuzimajte samo sa stranica kojima vjerujete. Ako sumnjate u sigurnost pojedinoga programa, možete upisati njegov naziv u preglednik i provjeriti je li netko prijavio da spomenuti program sadrži i *spyware*.
  + Čitajte sva sigurnosna upozorenja, ugovore o licenci i izjave o zaštiti privatnosti prije nego preuzmete bilo koji program.
  + Nikada nemojte kliknuti na 'OK' ili 'I agree' u skočnom prozoru, osim ako niste sigurni da znate na što pristajete.
  + Budite oprezni s programima za razmjenu besplatne glazbe ili filmova i svakako proučite rješenja koja dolaze u paketu s takvim programima.

**Scareware**

***Scareware* ili program za zastrašivanje** je vrsta malicioznoga programa koji generira skočne prozore slične porukama operativnoga sustava *Windows* i koji se zatim pretvara da je antivirusni ili *anti-spyware* program, vatrozidna aplikacija ili čistač baze podataka.

Cilj takvih poruka je uvjeriti korisnika da se na njegovom računalu nalazi niz zaraženih datoteka. **Korisniku se onda savjetuje kupnja određenoga softverskog rješenja koje će riješiti njegov problem. Problem zapravo uopće ne postoji, a preporučeni program je vrlo vjerojatno pravi *malware*.** Ako korisnik povjeruje porukama, ne samo da će izgubiti novac potrošen na beskorisni program, već će se njegovi bankovni podaci vrlo vjerojatno naći u rukama pravih prevaranata. Osim toga, gotovo je nemoguće raditi na zaraženom računalu.

**Kako izbjeći scareware?**

* Pazite da na računalima uvijek imate instalirane valjane i legitimne antivirusne te *anti-malware* programe. Kontaktirajte svoje pružatelje internetskih usluga i provjerite nude li neka besplatna sigurnosna rješenja ili rješenja koja korisnicima daju pod posebnim uvjetima.
* Nikada nemojte kliknuti na skočne prozore koji tvrde da je računalo zaraženo ili nude skeniranje računala u potrazi za greškama. Gotovo je uvijek riječ o prijevarama.

**Prijavite maliciozne programe**

Ako na zaslonu vašega računala skočni prozor ili nešto nije onako kako bi trebalo biti, snimite zaslon i pošaljite ga vašoj banci. Ta će nam informacija pomoći u prepoznavanju virusa i drugih vrsta malicioznih programa.

**DRUŠTVENE MREŽE I KRAĐA IDENTITETA**

Ponekad vam se čini da za gotovo svaku aktivnost na internetu morate smisliti lozinke i korisnička imena te dati određene osobne podatke. **To je postalo nužno jer internetske stranice žele zaštititi vas i vaš identitet, a pojedine također nude usluge društvenog umrežavanja.**

**Sve popularnije društvene mreže otvorile su vrata i prevarantima**! Naime, takve nas stranice potiču na otkrivanje sve više osobnih podataka te razmjenu informacija i fotografija putem interneta. No, budite na oprezu jer što više informacija otkrijete o sebi, to ste podložniji napadima prevaranata.

Nažalost, danas postoje kriminalci koji traže upravo one osobe koje su otkrile previše osobnih informacija. Često koriste tzv. **društveni inženjering** (*social engineering*) ili manipuliranje kako bi naveli osobe da otkriju previše podataka o sebi. Ti se podaci zatim nezakonito koriste u svrhu pribavljanja proizvoda i usluga bez njihova znanja. Problemi koji time nastaju uključuju uhođenje u virtualnom svijetu *(****cyber stalking****)*, nasilje (***bullying***), krađu identiteta i iznude.

Budite iznimno oprezni prilikom otkrivanja osobnih podataka. Razmislite o tome tko te informacije može vidjeti i na koji se način mogu upotrijebiti protiv vas.

 Zaštitite se Slijedi nekoliko jednostavnih koraka koje biste trebali poduzeti kako biste zaštitili svoj identitet od prevaranata u sljedećim situacijama:

**Ispis osobnih dokumenata**

* + Zaštitite svoje poruke i poštu, te ostale sadržaje koje ispisujete izravno s interneta, baš kao što biste zaštitili sadržaj svog novčanika ili torbe.
  + Pregledajte bankovni izvod čim ga dobijete i prijavite sve transakcije koje su vam nepoznate.
  + Spremite bankovne izvode, račune i povjerljivu korespondenciju na sigurno mjesto, baš kao što biste uradili i s drugim vrijednim predmetima.
  + Uništite sve osobne dokumente koje više ne trebate.

**Na javnim mjestima**

* + **Pripazite na osobe koje vam „vire preko ramena“ – ljude koji stoje iza vas u redu za blagajnu ili bankomat i pokušavaju vidjeti vaš PIN. Osim toga, jednom kada svoju karticu predate djelatniku trgovine kako biste platili kupljeno, ne ispuštajte je iz vida.**
  + **Ne koristite bankomat ako mislite da ga je netko neovlašteno dirao ili otvarao, te prijavite svoje sumnje banci.**
  + **Novčanik, torbu, mobilni telefon, organizer, ključeve od kuće i sve ostale osobne stvari čuvajte izvan dosega drugih ljudi.**

**Na internetu i putem telefona**

* + **Za svaki račun i aplikaciju koristite drugi PIN i lozinku. Koristite li istu lozinku za sve, a prevarant dođe u posjed iste, imat će pristup svemu.**
  + **Ne koristite korisnička imena koja su očita i lako se pamte.**
  + **Nikome ne otkrivajte lozinke, čak niti putem telefona. Vaša vas banka nikada neće tražiti PIN ili lozinku.**
  + **Budite oprezni kada koristite internet u kafićima ili ste aktivni na forumima, virtualnim sobama za chat ili društvenim mrežama – prevaranti ih često koriste kako bi otkrili vaše osobne podatke.**
  + **Nikada na internetu ne ostavljajte osobne podatke poput telefonskih brojeva, datuma rođenja ili informacija o zaposlenju.**
  + **Naučite se služiti sigurnosnim opcijama na internetu i postavite ih onako kako vam najviše odgovaraju. Pazite s kime ste „prijatelji“ na društvenim mrežama i kome dozvoljavate da se pridruži vašoj mreži.**
  + **Izbjegavajte korištenje opcije automatskoga dopunjavanja i ispunjavanja obrazaca na internetu. Prevaranti vrlo jednostavno mogu pristupiti takvom programu.**
  + **Pripazite na lažne e-poruke ([phishing](http://www.sigurnostnainternetu.hr/index.php/vrste-prijevara/phishing.html)) financijskih institucija u kojima se od vas traži da potvrdite podatke o računu. Takve e-poruke prijavite institucijama od kojih navodno dolaze kako biste pomogli u razotkrivanju prevaranata. Banke nikada od svojih korisnika ne traže potvrdu putem e-poruka.**
  + **Redovno ažurirajte antivirusni program i postavke vatrozida na računalu.**

[](http://www.sigurnostnainternetu.hr/index.php/component/content/2-uncategorised/46-galerija.html?Itemid=239) **Prijavite krađu**

Mislite li da vam je netko ukrao identitet, da prevarant posjeduje podatke o vašem bankovnom računu ili da je vašem računu na internetu netko nezakonito pristupao odmah kontaktirajte svoju banku i policiju.

Opreznim postupanjem s vašim osobnim podacima zaista možete pomoći u smanjivanju rizika od krađe identiteta.

**POSREDNICI ZA PRIJENOS NOVCA (money mules)**

Nemate novaca, ali ste vidjeli oglas za brzu zaradu? Sve što trebate učiniti zauzvrat jest prenijeti neki novčani iznos s vašega bankovnog računa na račun nepoznate osobe. Što ćete učiniti?

***Money mule* ili posrednik za prijenos novca naziv je za osobu koju prevaranti nagovore na pranje nezakonito stečenoga novca. Posrednik na svoj račun primi određeni iznos novca, a zatim ga prenosi dalje, uglavnom u inozemstvo, uz određenu proviziju. Riječ je o novcu kojeg su prevaranti ukrali od drugih ljudi. Kriminalci tako putem e-poruka, stranica za traženje posla ili oglasa regrutiraju nevine osobe za prijenos novca uz određenu naknadu. Prevaranti se drže dosta povučeno pa će gotovo uvijek od vas tražiti da banci ili policiji ne otkrivate razlog uplata i isplata.**

Morate znati da je rukovanje s nezakonito stečenim novcem kriminalno djelo, čak i ako ne znate njegovo porijeklo. Nemojte dozvoliti da se vaš bankovni račun koristi za prebacivanje tuđega novca.

**Posljedice pranja novca**

* + Iako je riječ o brzoj zaradi, ulozi su visoki, a posljedice razorne.
  + Dozvolite li da se vaš bankovni račun koristi za prijenos nezakonito stečenog novca, kršite zakon, čak i ako toga niste svjesni.
  + Kada vas uhvate, vaš će račun biti zamrznut. Sav novac na računu bit će podignut, uključujući i novac poslan u inozemstvo, a račun će biti zatvoren. Riječ je o kriminalnom djelu koje će biti prijavljeno policiji.
  + Nakon što dobijete etiketu prevaranta, teško ćete ikada više moći otvoriti bilo kakav bankovni račun ili dobiti zajam.

**Kako izbjeći prijevare s prijenosom novca**

* + Budite oprezni kada je riječ o bilo kakvim iznenadnim ponudama ili prilikama za brzu zaradu.
  + Nikada ne odgovarajte na sumnjive e-poruke i ne otkrivajte osobne ili financijske podatke.
  + Bankovne podatke nikome ne otkrivajte osim ako ne poznajete osobu.
  + Budite oprezni kada je riječ o ponudama koje dolaze od pojedinaca ili kompanija iz inozemstva jer je moguće da se isti lažno predstavljaju.
  + Provjerite jesu li kompanija koja vam nudi takvo što i njezini kontakti (adresa, broj telefona, e-adresa i internetsku stranica) autentični.

**Prijavite pranje novca**

Ako mislite da ste žrtva prijevare koja uključuje pranje novca ili bilo kakve druge internetske prijevare, odmah prijavite Vašoj banci i policiji.

**SPAM (NEŽELJENE PORUKE)**

Svi koji imaju e-adresu dobivaju *spam* – neželjene promotivne e-poruke koje se automatski šalju tisućama ljudi, a oglašavaju ili promoviraju različite proizvode i usluge. **I prevaranti šalju milijune takvih e-poruka u kojima tvrde da predstavljaju financijske institucije.** Njihove e-poruke sadrže privitke u kojima se navodno nalaze podaci o, primjerice, sumnjivoj transakciji, račun, faks ili glasovna poruka.

**Niz je načina na koje možete završiti na popisu za distribuciju neželjene pošte:**

* + prijava za *newsletter* na nekoj od beskrupuloznih internetskih stranica koja e-adrese svojih pretplatnika onda prodaje drugima,
  + otkrivanje vlastite e-adrese na nekoj *newsgroupi*, forumu ili na vlastitoj stranici i / ili
  + odabir adrese koju zatim softver lako može „pogoditi“ (automatski generirati).

**Cilj nekih neželjenih e-poruka je prevariti vas ili oštetiti vaše računalo:**

* + Mogu zaraziti vaše računalo nekim virusom. U tom je slučaju riječ o programu koji će uzrokovati štetu, primjerice, poslati nasumično odabrane datoteke (ili vlastitu kopiju) s vašega računala na sve adrese iz vašeg imenika.
  + Mogu sadržavati trojanca, maliciozni program koji izgleda sasvim bezopasno (ili je nevidljiv), ali će učiniti nešto neočekivano, primjerice, poslati vaše povjerljive podatke na udaljeno računalo.
  + Mogu biti lažne e-poruke (*phishing*) u kojima se od vas traži da otkrijete svoje osobne podatke.

**Što možete učiniti u vezi spama?** Kako biste zaštitili svoj korisnički račun te smanjili broj neželjenih e-poruka, morate poduzeti sljedeće korake:

* + **Maknite kvačicu u polju za potvrdu.** Ako vas neka kompanija traži vašu e-adresu, pročitajte i tekst napisan sitnim slovima te jasno dajte do znanja da ne želite da se vaši podaci otkrivaju drugima.
  + **Uključite filtar za neželjenu poštu.** Vaš će vam pružatelj e-pošte ponuditi opciju filtriranja dolazećih e-poruka i preusmjeravanja *spama* u mapu s neželjenom poštom. Ta će se mapa povremeno prazniti pa ubuduće nećete primati toliko neželjenih e-poruka. Kontaktirajte vašega pružatelja e-pošte ako niste sigurni kako aktivirati spomenutu opciju.
  + Dio neželjenih e-poruka ipak će završiti u mapi dolazne pošte i morat ćete ih izbrisati. Svakoga se dana šalje na tisuće neželjenih e-poruka, većina kojih je bezopasna. Označite takve poruke, ignorirajte ih i izbrišite.
  + Dobijete li e-poruku s neočekivanim privitkom ili linkom, nemojte ga otvarati. Ako e-poruka izgleda kao da je poslana iz vaše banke, prijavite to vašoj banci.