telemach

ZAŠTITA POTROŠAČA: SAVJETI ZA ZAŠTITU OD ZLOUPORABE

Savjeti za zaštitu od zlouporabe

Savjeti za zaštitu pri korištenju SIM kartice u mobilnom telefonu:

- SIM kartica ima dodijeljeni PIN i PUK broj. PIN broj treba unijeti pri svakom uključivanju mobilnog telefona. Ako se PIN unese pogrešno tri puta zaredom, SIM kartica će se zaključati, a otključati se može unošenjem PUK broja.
  Čuvajte SIM karticu i pripadajuće PIN i PUK brojeve.
  Zapamtite PIN broj i nemojte ga nositi zapisanog uz mobilni telefon kako biste izbjegli mogućnost zlouporaba u slučaju gubitka mobilnog telefona. Na sigurno mjesto pospremite plastični držač SIM kartice na kojem se nalaze PIN i PUK brojevi.
- Kada se nalazite u područjima blizu hrvatske granice, provjerite je li mobilni telefon možda na signalu stranog operatora. U tom biste se slučaju uspostavom poziva koristili uslugu roaminga čija cijena korištenja može imati značajne razlike u odnosu na cijenu kada uslugu koristite unutar Hrvatske.
- Pri korištenju usluga s posebnom tarifom, poput igranja nagradnih igara, sudjelovanja u kvizovima ili kupnji sadržaja za mobilne telefone (npr. pozivi prema 060 brojevima, SMS poruke prema kratkim kodovima 61xxx67xxx, pretplatničke usluge na kratkim kodovima 8xxxx), obratite pozornost na uvjete korištenja i cijene usluga.
  Aktivnu SMS uslugu s posebnom tarifom možete deaktivirati slanjem ključne riječi STOP na kratki kod s kojeg primate poruke.
- Tijekom boravka u inozemstvu ne zaboravite da se i primanje poziva naplaćuje.
- Podsjećamo vas da pristup međunarodnim brojevima s posebnima tarifama može biti ograničen radi zaštite od zlouporabe i prijevarnog postupanja. Unatoč navedenom, ukoliko dobijete SMS poruku koja vas poziva na uspostavu poziva ili slanje SMS poruke prema nekom broju u inozemstvu ili prema broju s posebnom tarifom, nemojte uspostavljati poziv ili slati SMS poruku prema tom broju.

Savjeti za zaštitu za korisnike pametnih telefona (smartphones)

telemach

Pametni telefoni (smartphones) su napredni telefoni koje pokreće jedan od sljedećih operativnih sustava: Android, iOS, BlackBerry, Windows Mobile, Windows Phone, Symbian, MeeGo, Bada…
Prilikom svakodnevnog korištenja pametnih telefona veliku je pozornost potrebno posvetiti informacijskoj sigurnosti. Naime, pomoću pametnih telefona sve više obavljamo osjetljive financijske transakcije te se na njih pohranjuju povjerljivi osobni podaci.

Pridržavajte se sljedećih preporuka:

- Podesite postavke na pametnom telefonu koje će omogućiti zaključavanje telefona putem zaporke nakon određenog perioda neaktivnosti.
- Redovito instalirajte programske zakrpe operacijskog sustava i aplikacija. Većina proizvođača pametnih telefona omogućuje navedenu funkcionalnost.
- Koristite antivirusne programe u svrhu zaštite od malicioznog softvera dizajniranog za pametne telefone.
- Dobro provjerite pouzdanost aplikacija koje instalirate na pametni telefon. Nikada nemojte instalirati aplikacije s izvora koji nisu pouzdani. Primjeri pouzdanih izvora su: Google play, Windows Marketplace, Apple Store, BlackBerry App World.
- Pažljivo koristite javne Wi-Fi mreže. Izbjegavajte obavljati financijske transakcije, pristupati povjerljivim informacijama dok ste na javnoj Wi-Fi mreži.
- U slučaju da nemate namjeru više koristiti svoj pametni telefon, izbrišite sve povjerljive informacije s telefona. Primjeri takvih informacija su: povijest pregledavanja weba, pohranjene zaporke, adresar, povijest poziva, poslanih poruka, slike, razni dokumenti pohranjeni u memoriju uređaja.
- Redovito izrađujte pričuvnu kopiju podataka koji se nalaze na telefonu: adresar, multimedijalni materijali i sl.

Savjeti za zaštitu pri korištenje pametnih telefona u inozemstvu

Ako koristite pametni telefon izvan Europske unije, savjetujemo da isključite uslugu prijenosa podataka kako biste spriječili nastajanje velikih troškova zbog korištenja usluga u roamingu, koje su bitno skuplje od usluga prijenosa podataka u Hrvatskoj.

telemach

- Zabranu korištenja usluga prijenosa podataka izvan Europske unije (pristup internetu) možete zatražiti pozivom Službi za korisnike ili na ovlaštenom Telemach prodajnom mjestu.
- Poslovni korisnici uslugu zabrane mogu zatražiti na Telemach ovlaštenom prodajnom mjestu. Zaštitu možete aktivirati i sami na mobilnom telefonu, a postupak ovisi o operativnom sustavu (OS) mobilnog telefona. Aktivacija zabrane korištenja prijenosa podataka u inozemstvu za Android OS
    - U glavnom izborniku nađite i odaberite Postavke (Settings).
    - U podizborniku Postavke odaberite Bežične veze i mreže (Wireless & networks).
    - U podizborniku Bežično i mreža nađite i odaberite Mobilne mreže (Mobile networks).
    - U podizborniku Mobilne mreže potražite opciju Mobilni podaci (Cellular data) te ju isključite. Nakon toga mobilni se telefon više neće moći spojiti na internet (ostvarivati prijenos podataka) dok ponovno ne uključite opciju.
      Kada isključite opciju Mobilni podaci, onemogućeno je slanje i primanje MMS poruka.
    - Naziv opcije koju trebate isključiti može se razlikovati od uređaja do uređaja. Najčešći nazivi su: Mobilni podaci, MMS i podaci, Promet podataka itd. ili na engleskom jeziku Cellular data, Data traffic, MMS & data itd.

Aktivacija zabrane korištenja prijenosa podataka u inozemstvu za Symbian OS

Mobilni telefoni s operativnim sustavom Symbian mogu se samostalno spajati na internet u određenim vremenskim intervalima te tako omogućiti dodatne troškove. Najčešće se radi o postavkama e-mail pretinaca koji samostalno preuzimaju nove e-mail poruke u odabranom vremenskom intervalu, najčešće svakih sat vremena. Kako biste isključili automatsko spajanje e-mail pretinaca na internet, potrebno je za svaki e-mail pretinac namjestiti ručno preuzimanje na sljedeći način:

- Uđite u Glavni izbornik.
- Odaberite ikonu Poruke.

telemach

- Lijevom funkcijskom tipkom odaberite Opcije, a zatim u podizborniku odaberite opciju Postavke.
- Nađite i odaberite opciju E-pošta (e-mail).
- Odaberite opciju Spremnici.
- U podizborniku Spremnici ponuđeni su svi e-mail pretinci koji su trenutačno kreirani na mobilnom telefonu. Odaberite prvi e-mail pretinac na popisu.
- U sljedećem izborniku odaberite posljednju opciju, Automatsko preuzimanje, te opciju Preuzimanje e-pošte namjestite na Onemogućeno.
- Ako želite da se E-mail pretinac i dalje samostalno spaja na server i preuzima e-mail poruke, možete namjestiti vremenski interval za preuzimanje. Opciju Preuzimanje e-pošte namjestite na Omogućeno, a zatim uđite u opciju Interval preuzimanja i odaberite željeni interval koji, ovisno o mobilnom telefonu, može iznositi od pet minuta do šest sati.

Aktivacija zabrane korištenja prijenosa podataka u inozemstvu za BlackBerry OS

- Na početnom zaslonu uređaja pritisnite BlackBerry tipku (tipku s točkicama) kako biste ušli u Glavni izbornik.
- U Glavnom izborniku uđite u opciju Options.
- U podizborniku Options uđite u opciju Mobile Network.
- U podizborniku Mobile Network vidljiva je opcija While Roaming koja je početno namještena na Prompt. Pritiskom na opciju Prompt otvara se dodatni podizbornik u kojem je potrebno odabrati opciju Off. Aktivacija zabrane korištenja prijenosa podataka u inozemstvu za iOS (iPhone)
- Na početnom zaslonu nađite i odaberite ikonu Postavke (Settings).
- U sljedećem izborniku nađite i odaberite ikonu Općenito (General) te zatim opciju Mreža (Network).
- Ako je u izborniku Mreža klizač desno od opcije Data roaming namješten na O, spajanje u inozemstvu je onemogućeno, a ako nije, namjestite klizač na O (ako je izbornik na engleskom, klizač namjestite na OFF).

Aktivacija zabrane korištenja prijenosa podataka u inozemstvu za Windows mobile

telemach

- Prebacite se u glavni izbornik, s popisom svih aplikacija
- U glavnom izborniku nađite i odaberite opciju Settings/postavke.
- U podizborniku Settings nađite i odaberite opciju Cellular/mobilna mreža.
- U podizborniku Cellular nađite opciju Data roaming options/mogućnost podatkovnog roaminga ispod koje je potrebno odabrati opciju Don't roam/nemoj uključiti roaming.

Zaštita djece od neprimjerenih sadržaja

U svrhu zaštite djece od pristupa sadržajima koji nisu njima namijenjeni Telemach omogućava, na zahtjev korisnika, uključenje sljedećih zabrana:

- Uključenje zabrane prijenosa podatkovnog prometa
- Uključenje zabrane prijenosa podatkovnog prometa u roamingu
- Uključenje zabrane pozivanja brojeva sa dodatnom vrijednošću
- Uključenje zabrane slanja poruka na premium SMS brojeve

Jednom uključene zabrane ostaju na snazi sve dok korisnik ne zatraži njihovo ukidanje.

Savjeti za zaštitu pri korištenju SIM kartice za pristup internetu s računala

Redovito održavajte računalo zaštićenim, instalirajte antivirusne i antispam programe te ih uvijek obnavljajte novim inačicama i zakrpama. Obratite pozornost na programe koje instalirate na računalo. Neki programi zahtijevaju stalnu vezu s internetom (stalno skidanje i slanje podataka), čime se može stvoriti znatna količina podatkovnog prometa (npr. online videoigre).

Antivirus

Maliciozni program je program koji ima sposobnost kopiranja samog sebe i aktiviranja u računalu bez dopuštenja i znanja vlasnika. Pojam maliciozni program upotrebljava se kao zajednički naziv za sav štetan softver (računalni virusi, trojanski konji, crvi, spyware i dr.).
Najrašireniji način širenja malicioznih programa je elektroničkom poštom, stoga je nužan oprez pri otvaranju privitaka sumnjivih poruka. Pritom nije važno je li pošiljatelj netko koga poznajete ili nije (polje "from" u e-mail poruci) jer se noviji virusi (crvi) distribuiraju sa zaraženog računala bez znanja njegovog vlasnika te je moguće da dobijete zaraženu poruku i s adrese poznate osobe.

Ne otvarajte privitke u elektroničkoj pošti od nepoznatih pošiljatelja.

Za zaštitu od virusa koriste se specijalizirana programska rješenja.

telemach

Antispyware zaštita

Antispyware zaštita rješava većinu problema s neželjenim samopokretnim i skošnim prozorima (pop-up), reklamama i dodacima u pretraživaču interneta koji usporavaju ili onemogućavaju rad na internetu, a među ostalim nalaze i poništavaju dialer programe na računalu.

Ransomware

Ransomware napad jednostavan je za izvođenje. Sve što je potrebno za zaključavanje sadržaja računala (ili možda cijele mreže) je virus i neupućena osoba koja ga aktivira jednim klikom miša. Napadači često pružaju i Ransomware kao uslugu (eng. Ransomware-as-a-Service) te prodaju svoje usluge na dark webu (crnim internetskim tržištima) kako bi se maksimizirao prinos od troškova razvoja. Drugim riječima, svatko može naručiti napad na bilo koga. Ransomware napada ciljana računala, ali može pogoditi i Vaš mobilni telefon ili čak druge pametne uređaje kao što su pametni televizori i sl. Virus može doći iz različitih izvora preko privitka koji ste primili elektroničkom poštom, npr. .docx datoteka, kada posjetite mrežnu stranicu ili kliknite na elemente na njoj ili
iz datoteke koju preuzmete, itd. Napadom se sve datoteke kojima imate pristup zaključaju te im je onemogućen pristup bez zaporke. Od Vas se traži da platite otkupninu za lozinku. Budite oprezni oko datoteka koje otvorite kao i oko poveznica koje kliknete. Nikada ne otvarajte vrste datoteka koje ne prepoznajete.

Nadogradnje operativnog sustava i programa koje koristite

Proizvođači programa, operativnog sustava i paketa nadogradnje (service pack) uočavaju sigurnosne propuste te izdaju odgovarajuće sigurnosne zakrpe dostupne uobičajeno na stranicama proizvođača. Nadogradnju operativnih sustava Windows možete pokrenuti na stranici http://windowsupdate.microsoft.com/.

Nadogradnju MAC OS-a možete provjeriti putem App Store aplikacije, pod stavkom Update.

Savjeti za korištenje i zaštitu WLAN-a

Nezaštićena WLAN veza omogućava drugim računalima pristup vašoj mobilnoj pristupnoj točki (hot-spot) i zloporabu vašeg računa. Kako biste umanjili rizik narušavanja sigurnosti vašeg uređaja i podataka koji s nalaze na njemu:

telemach

- Dodajte enkripciju svojoj bežičnoj mreži kako biste spriječili neovlašteno korištenje vaše WLAN mreže.
- Preimenujte svoju WLAN mrežu i promijenite zadanu lozinku navedenu na uređaju.
- Isključivanje SSID prijenosa (naziv WLAN mreže) pruža dodatnu sigurnost jer druga računala moraju znati SSID kako bi se spojila.

Općenito

Sve informacije o Telemach proizvodima i uslugama potražite u pripadajućim uvjetima korištenja na www.telemach.hr

Firewall

Služi za zaštitu osobnog računala od napada preko mreže. Firewall prati cjelokupni mrežni promet te odlučuje koje će aktivnosti dopustiti, a koje neće. Na novijim Windows operativnim sustavima firewall je već instaliran na računalu te ga je potrebno postaviti na način koji osigurava sigurnost vašim podacima na uređaju.