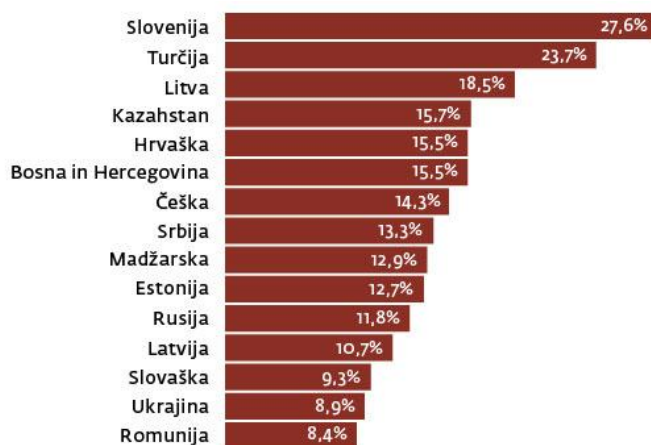


### Nevarnosti pametnih telefonov

Slovenci po številu pametnih telefonov v naši regiji izstopamo. Uporaba teh naprav nam lahko brez dvoma močno olajša delo in komuniciranje s prijatelji, po drugi strani pa nas lahko tudi drago stane. Se zavedamo nevarnosti?

Nedavna raziskava CEE Telco Industry Report, ki jo je objavila agencija za tržne raziskave GfK, je Slovenijo med petnajstimi državami srednje in vzhodne Evrope postavila na sam vrh. Pametne telefone pri nas uporablja že kar 27,6 odstotkov prebivalstva. Sledita nam Turčija s 23,7 odstotkov in Litva z 18,5 odstotkov.

Delež uporabnikov pametnih telefonov (vir: CEE Telco Industry Report, november 2011):



Pametni telefoni so postali pravi računalniki s sposobnostjo opravljanja klicev. Vse več ljudi te naprave uporablja za pošiljanje osebnih in drugih zaupnih podatkov bodisi pri uporabi spletnega bančništva, spletnega nakupovanja ali pri druženju v socialnih omrežjih. Trend naraščanja priljubljenosti pametnih telefonov ni ostal neopažen tudi med kiberkriminalci. Največ novih groženj za pametne telefone je spisanih za naprave, ki uporabljajo operacijski sistem Android. Priljubljenost slednjega je še vedno v vzponu, trenutno ga poganja že več kot polovica pametnih telefonov po celem svetu. Največjo nevarnost za te naprave predstavljajo okužene aplikacije, ki jih lahko občasno najdemo celo v uradni spletni trgovini Android Market. Možnosti za prenos okuženih aplikacij se močno povečajo, če aplikacije prenašamo iz neuradnih spletnih trgovin in s spletnih strani z nelegalno vsebino. Kiberkriminalci lahko namreč povsem legitimne aplikacije spreminjajo in vanje vpišejo svojo zlonamerno kodo. Takšne aplikacije so lahko sposobne pošiljanja SMS sporočil na plačljive telefonske številke, snemanja telefonskih pogovorov ali kraje podatkov na telefonu. Veliko novih groženj pa napadalcem omogoča celo oddaljen nadzor nad napravo. Pri nameščanju aplikacij na svojo napravo uporabljajte podobno previdnost kot pri nameščanju programske opreme na svoj računalnik. Aplikacije prenašajte le iz preverjenih spletnih trgovin, kot sta Android Market ali Apple App Store. Pred namestitvijo na spletu preverite tudi ugled izdajateljev aplikacije in izkušnje drugih uporabnikov. Posebno previdni bodite pri aplikacijah, ki za namestitev zahtevajo pravico pošiljanja sporočil SMS. Priporočljivo je tudi, da redno spremljate račune svojega mobilnega operaterja. Eden od znakov, da je vaša naprava že okužena, je lahko tudi hitro praznjenje baterije.



Časi brezskrbne rabe pametnih telefonov so žal minili, saj število novih groženj za te naprave narašča zelo hitro. Zaupajte zaščito svojega pametnega telefona avtorjem preizkušenega protivirusnika NOD32. Rešitev ESET Mobile Security lahko namestite na pametne telefone z operacijskimi sistemi Android, Windows Mobile ali Symbian. Zaščiteni boste z napredno tehnologijo preiskovanja tudi pred najnaprednejšimi grožnjami za mobilne naprave ne glede na to, kakšno povezavo na splet uporabljate. ESET Mobile Security je zelo uporaben tudi v primeru, da svoj telefon izgubite ali pa vam ga odtujijo. S preprostim SMS sporočilom lahko namreč svoj izgubljeni telefon zaklenete ali pa podatke na njem dokončno izbrišete in tako preprečite, da pridejo v neprave roke. ESET Mobile Security pa lahko s pomočjo funkcije GPS na napravah z Androidom izgubljeno ali ukradeno napravo celo izsledi. Več informacij o produktu si lahko ogledate na spletni strani [www.eset.si/android](http://www.eset.si/android)