si·cert

VARNI NA INTERNETU

INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER

ABC VARNOSTI IN ZASEBNOSTI NA MOBILNIH NAPRAVAH

V primeru težav se lahko obrnete na:
Informacijskega pooblaščenca - *www.ip-rs.si*
Varni na internetu - *www.varninainternetu.si*

si·cert

VARNI NA INTERNETU

INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER

VSEBINA

MOJI PODATKI
Vse, kar je treba vedeti o pametnih napravah in varovanju podatkov pri njihovih uporabi.

4

MOBILNE APLIKACIJE IN ZASEBNOST
Priporočila za varno rabo mobilnih aplikacij.

14

MOJA PISARNA
Navodila za uporabo mobilnih naprav za poslovne potrebe.

18

KLJUČNA TVEGANJA
Tegobe in težave, ki se vam lahko pripetijo v mobilnem svetu.

20

KLJUČNI NASVETI
Pregled nasvetov za varno rabo mobilnih naprav.

24

S PAMETJO V ROKAH V MOBILNI SVET

Še nimate pametnega telefona ali tablice? Statistični podatki namigujejo na to, da boste kaj kmalu postali lastnik katere od tovrstnih naprav iz široke ponudbe na trgu. Uporaba pametnih mobilnih naprav namreč strmo narašča iz leta v leto. Pametni telefoni in tablice so postali čisto prava konkurenca računalnikom in prenosnikom. Z njimi sicer v prvi vrsti še vedno kličemo in pošiljamo SMS-sporočila, vendar jih lahko precej bolj razširjeno uporabljamo; z njimi lahko brskamo po internetu, uporabljamo družbena omrežja, igramo igre, nakupujemo, opravljamo bančne storitve in tako dalje.

Mobilna naprava ima torej vse, kar ima računalnik: **lasten operacijski sistem** (npr. Android, iOS, Windows Phone) **in brskalnik**, s katerim brskamo po spletu. **Na internet se lahko povežemo** s prenosom podatkov našega mobilnega operaterja ali pa prek brezžične povezave, kjer je ta na voljo. Namesto programov na mobilnih napravah uporabljamo **aplikacije**: za prebiranje pošte, brskanje, družbeno mreženje, branje novičarskih portalov, igrice, budilko itd. Nekatere so prednaložene že ob nakupu, druge lahko kupimo ali jih brezplačno naložimo prek **aplikacijskih trgovin** (npr. Google Play, App Store, Marketplace).

Mobilne naprave tako vključujejo vse funkcionalnosti domačih računalnikov, le videz naprave in uporabniškega vmesnika je drugačen. Zelo podobne pa so nevarnosti in nevšečnosti, saj smo tudi na mobilnih napravah

izpostavljeni virusom in drugim škodljivim programom, zlonamernim kodam ter spletnim goljufijam.

Zato si pri uporabi pametnih naprav velja zapomniti osnovno vodilo, in sicer da so pametne toliko, kolikor je pameten njihov uporabnik.

Nataša Pirc Musar,
IP RS - pooblaščenka

Gorazd Božič,
vodja SI-CERT

MOJI PODATKI

Tudi pametni telefoni in tablice imajo **pomnilnik**, kamor shranjujemo podatke, pri tem pa so kapacitete pomnilnika zaradi velikosti naprave navadno manjše. Zato sodobne naprave omogočajo tudi hrambo podatkov v oblaku. Ponudnik hrambe v oblaku (Google, Apple, Microsoft, DropBox itd.) je odvisen od proizvajalca naprave ali od aplikacije, ki jo uporabimo. Elektronska pošta, imeniki, koledarji, fotografije, dostopi do družbenih omrežij – vsi ti podatki so lahko shranjeni neposredno na napravi ali pa v *oblaku*.

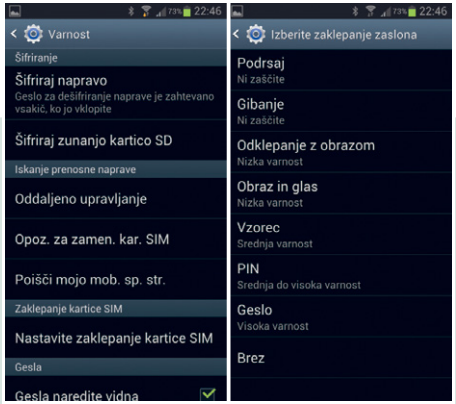
Kako torej poskrbimo za varno shranjevanje in prenos podatkov na mobilnih napravah?

PODATKI NA NAPRAVI

Ker je fizični dostop do mobilne naprave veliko lažji, so tudi vsi shranjeni podatki bolj izpostavljeni. Zato so prvi koraki do boljše zaščite uporaba PIN-kode za zaklep SIM-kartice, kot jo

NAMIG

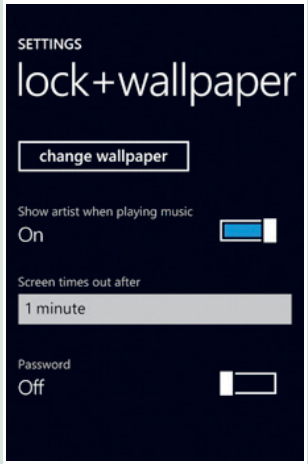
Pri zaščiti mobilnih naprav tako velja dejstvo, da bolj kot je koda za zaklep zahtevna, bolj so naši podatki zaščiteni!



Android:
za nastavitev zaklepanja odprite Nastavite, menija Varnost in Zakleni zaslon oz. Nastavitve, Položaj in varnost.

iOS:
Aplikacija Settings, izbira General, nato pa Passcode Lock.

Windows Phone:
Izberemo Settings, nato lock+wallpaper in aktiviramo Password On



poznamo še iz časov »navadnih« mobilnikov, kode za zaklep zaslona (vzorec, PIN-koda ali geslo), na novejših napravah pa tudi gesla za šifriranje shranjenih podatkov. Vedeti moramo, da koda za odklep naprave predstavlja tudi ključ za dostop do podatkov, shranjenih na njej.

OPOZORILO: ker je mogoče tudi takšne zaklepe zaobiti, na samo napravo vseeno **ne shranjujmo posebej pomembnih podatkov** v čisti obliki. Za shranjevanje le-teh uporabimo aplikacijo, ki nam omogoča močno šifriranje podatkov. Taki podatki so med drugim:

- gesla za dostop do storitev na spletu (družbena omrežja, e-bančništvo),
- PIN-kode bančnih kartic,
- številka potnega lista in drugi osebni podatki.

1Password
agilebits.com/onepassword

LastPass
lastpass.com

Roboform
www.roboform.com

KeePass
keepass.info

PODATKI V OBLAKU

Sinhronizacija podatkov z različnih naprav in računalnikov v *oblak* (»cloud«) ima veliko prednosti. Podatki so dostopni na vseh napravah (npr. koledarji in imeniki), ob okvari naprave jih lahko zelo enostavno povrnemo. S tem pa svoje podatke izvozimo v oblak ponudnika, ki se največkrat nahaja v drugi državi, kar lahko pomeni težave z vidika varovanja osebnih podatkov. Ponudnika ne moremo prosto izbirati – z nakupom

naprave se odločimo tudi zanj. Android naprave sinhroniziramo na Google, Windows Phone, telefone in tablice na račun live.com pri Microsoftu, na iPhonu in iPadu pa uporabljamo Applov iCloud (določene podatke lahko sinhroniziramo tudi z Googlom).

Ker vsa zaščita dostopa temelji zgolj na našem geslu, je zopet pomembno, da uporabljamo *močno* geslo. Kdor bo izvedel naše geslo za dostop do *oblaka*, bo lahko do naših podatkov prišel tudi prek spleta, torej tudi, ko bomo telefon imeli varno spravljen v svojem žepu.

Kadar ponudnik to omogoča, vklopimo dodatne zaščitne mehanizme, kot so npr. **dvofaktorska avtentikacija** in **unikatna gesla za aplikacije**. Pri spremembah ključnih podatkov ali prijavi z nove naprave ponudnik na naš mobilni telefon pošlje SMS s potrditveno kodo. Od večjih ponudnikov tako zaščito omogočajo Facebook, Google in Dropbox.

NAMIG:

KAKO SI IZMISLIM MOČNO GESLO? Z gesli je križ. Po navadi slišimo, da moramo mešati male in velike črke, številke in ločila, geslo mora biti dovolj dolgo in za vsako storitev moramo imeti svojega. Kako doseči vse to in si jih še zapomniti? Izmislimo si lahko svoj »sistem«: morda si izberemo dve ali tri besede, med seboj pomensko nepovezane, in jih združimo z ločili ter kje dodamo še številko. Si bomo npr. zapomnili »petka:janez=8«?Za shranjevanje gesel pa uporabimo namensko aplikacijo.

Več informacij:

Dodatna zaščita za Gmail:
https://vni.si/googlemail

Dodatna zaščita za Facebook:
https://vni.si/facebook

Dodatna zaščita za DropBox:
https://vni.si/dropbox

VARNOSTNO KOPIRANJE (»BACKUP«)

Varnostne kopije podatkov, hranjenih na napravi, so ključnega pomena pri odpravljanju posledic kraje, izgube ali okvare. Varnostno kopijo lahko shranite na domači računalnik ali v »oblak«.

iOS: varnostno kopiranje vključite v programu iTunes. Sinhronizacijo v iCloud vklopite v »Settings«.

Android: sinhronizacijo vključite v meniju Nastavitve, Računi (oz. Računi in sinhronizacija).

NAMIG:

Če je le mogoče, storite kar oboje. Na napravi vključite sinhronizacijo v oblak, vsak teden pa telefon ali tablico ob prihodu domov priključite na računalnik in poleg polnjenja baterije izdelajte še varnostno kopijo (»backup«).

Windows Phone: varnostno kopiranje izvedete prek aplikacije Zune, slike lahko samodejno prenašate na SkyDrive.

VARNO POVEZOVANJE

Nepogrešljiva lastnost mobilnih naprav je povezljivost. Na internet se lahko povežemo s prenosom podatkov mobilnega operaterja ali pa prek brezžične (WiFi) povezave doma, v službi, hotelu, baru ali v šoli. Nekatera od teh omrežij so bolj varna, druga manj.

Javna brezžična omrežja

V turističnih krajih, na letališčih, v kavarnah so pogosto na voljo javna brezžična omrežja, ki so brezplačna ali pa so dostopna po zmerni ceni. Če brezžična dostopna točka ni dovolj zavarovana, lahko pride do **prestrezanja omrežnega prometa**, kar pomeni, da lahko neznanec spremlja ves naš omrežni promet. Prav posebno previdnost pa zahteva t. i. **Ad-hoc brezžično omrežje**, ki ga **ustvari nekdo kar na svojem računalniku**. V tem primeru se povežete neposredno na prenosnik neznanca. Taka omrežja so po navadi prikazana z malce drugačno ikono. Pozanimajte se, katero je pravo omrežje hotela, kampa ali cybercafeja. Če lahko izbirate med nešifriranim in šifriranim omrežjem, izberite šifriranega.

NAMIG:

Tudi posamezne mobilne aplikacije s šifriranjem ščitijo podatke med prenosom. **Ali v brskalniku uporabljate šifrirano oz. varno povezavo, preverite tako, da v naslovni vrstici poiščete znak zaklenjene ključavnice.**

ANDROID

iOS

5 NASVETOV:

- Če je le mogoče, vzpostavite povezavo z brezžičnim omrežjem, ki zahteva omrežni varnostni ključ (protokol WPA ali WPA2).
- Povežite se na brezžično omrežje, le ko ga potrebujete, v nasprotnem primeru izklopite samodejno povezovanje na dostopne točke. Tudi baterija se bo počasneje praznila, če ne boste nenehno povezani.
- Pametno je, da sinhronizacije naprave na daljavo (npr. s svojim računalnikom ali v oblak) ne opravljate prek nezaščitenih brezžičnih omrežij, npr. na konferencah in v hotelih.
- Če želite v nezaščitenih javnih brezžičnih omrežjih uporabiti storitve, kjer morate posredovati uporabniško ime in geslo (prijava v elektronsko pošto, družbena omrežja), to storite le, če veste, da bo prenos podatkov varen, npr. z uporabo uradne aplikacije za storitev. Če pa uporabljate brskalnik, bodite pozorni na zaklenjeno ključavnico.
- **Nikoli ne izvajajte finančnih transakcij v nezaščitenih javnih omrežjih** (denimo vpis številke kreditne kartice v spletni trgovini ali opravljanje bančnih storitev).

Mobilni internet

Najvarnejša je uporaba mobilnega interneta za prenos podatkov (GPRS, EDGE, UMTS, poenostavljeno tudi kar 3G). Slaba stran tovrstne rabe so morebitni visoki stroški, ki pri tem nastanejo, še posebej v tujini (roaming). Stroške lahko povzročijo tudi določene aplikacije, ki se v ozadju brez vaše vednosti povezujejo na internet.

NAMIG:
V tujini izklopite gostovanje (roaming) ali pa podatkovno povezavo vklopite le po potrebi. Če je le mogoče, v tujini za dostop do interneta uporabljajte SIM-kartico lokalnega operaterja.

Bluetooth

Tehnologija Bluetooth omogoča brezžično povezljivost na razdalji nekaj metrov, običajno pa se jo uporablja za prenos

NAMIG:
Vidnost Bluetooth vmesnika nastavite zgolj, ko se povezujete z novo napravo, drugače pa naj bo Bluetooth vmesnik skrit.

zvoka do brezžičnih slušalk, uporabo zunanje tipkovnice ali za prenos manjših datotek med napravami.

Oddajanje podatka o geolokaciji

Sodobne storitve lahko uporabijo podatke o naši lokaciji za izboljšanje storitve (ko npr. iščemo najbližjo odprto trgovino). Podatek o lokaciji lahko na koncu prejme proizvajalec naprave, operacijskega sistema, upravljavec aplikacije pa tudi kaka tretja stranka, npr. oglaševalec, ki vas z oglasom želi ujeti takrat, ko boste v bližini njegove trgovine. Sliši se kočljivo. Zadeva ima vsekakor dve plati: pri uporabi nekaterih funkcionalnosti je oddajanje podatka o lokaciji nujno, npr. pri zemljevidih ali drugih storitvah, ki so vezane na vašo lokacijo. Po drugi strani pa je iz podatkov o vaših lokacijah mogoče zelo natančno izrisati vaše vsakdanje poti.

NAMIG:
Če ne želite, da vsaka aplikacija pozna vaše gibanje, potem izklopite privzeto oddajanje geolokacije in jo vklopite takrat, ko to dejansko potrebujete. Pri namestitvi in uporabi aplikacije razmislite, ali aplikacija res potrebuje podatek o vaši lokaciji.

MOBILNE APLIKACIJE IN ZASEBNOST

Aplikacije so posebna dodana vrednost mobilnih naprav. Saj poznate zdaj že pregovorni izraz: »Za to gotovo obstaja aplikacija« (»There is an app for that« v angleščini). Aplikacij je torej več vrst, težava pa je, da običajno zahtevajo veliko dovoljenj (»permissions«). Čeprav gre zgolj za aplikacijo za merjenje kilometrov, ki jih pretečete, in vam hkrati ponuja še statistiko vašega napredovanja, ali samo za najnovejšo zabavno igro, je čisto mogoče, da se boste morali strinjati, da aplikacija dostopa do vaših klicev, da lahko spreminja podatke na vaši pomnilniški kartici ali celo deli te podatke z drugimi, npr. oglaševalci.

STE VEDELI? Da aplikacije pogosto želijo vaše dovoljenje za dostop do praktično VSEH informacij, ki so na vašem telefonu? Da lahko snemajo zvok in slike brez vašega dovoljenja? Da lahko zapisujejo na spominsko kartico, ali pa, ups, izbrišejo kakšno fotografijo ali pomemben dokument? Lahko se zgodi celo, da aplikacija samovoljno aktivira kako plačljivo storitev. In vse to brez posebnega obvestila.

Kako torej poskrbimo za varno rabo mobilnih aplikacij?

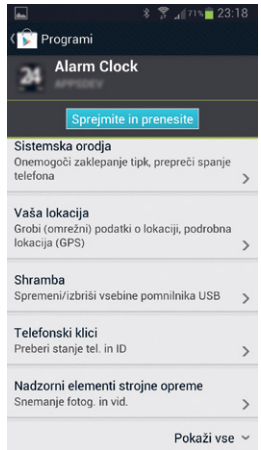
Aplikacije pogosto zahtevajo veliko več podatkov, kot jih dejansko potrebujejo za svoje delovanje. Ti podatki so za ponudnike aplikacij lahko veliko vredni – lahko ugotavljajo, kaj vam je všeč, in vam nato posredujejo oglase. Plačljive aplikacije običajno od vas zahtevajo manj dovoljenj.

NAMIG 1:

Pri brezplačnih aplikacijah velja stara spletna modrost – **če niste ničesar plačali, potem je cena morda skrita drugje**. *Morda boste morali čez nekaj časa plačati za nadaljevanje uporabe, morda bodo vaši podatki posredovani oglaševalcem, mogoče je vmes trik in se boste včlanili v kak SMS-klub. Zato vedno preverite, katera dovoljenja želi aplikacija in če je kje skrit strošek.*

NAMIG 2:

Dobro je vedeti, da lahko od slovenskega ali evropskega ponudnika aplikacije, ki ste jo namestili, vedno zahtevate, da vam pojasni, do katerih vaših podatkov dostopa in natančno opredeli, komu jih naprej posreduje. Če vam teh informacij ne sporoči, se lahko obrnete na Informacijskega pooblaščenca. Več informacij na spletni strani: https://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/#c313.



Aplikacija za budilko, ki zahteva dostop do natančne lokacije (GPS) in fotografiranje in snemanje videa brez vednosti uporabnika.

6 NASVETOV ZA VARNO RABO MOBILNIH APLIKACIJ

Ne naložite prav vsake aplikacije – če je le mogoče, nalagajte aplikacije zgolj iz uradne trgovine in vedno preverite ocene uporabnikov. Možnost, da ujamete virus, je pri nalaganju aplikacij iz neuradnih virov precej večja. Preverite spletno stran ponudnika aplikacije.

1. Vprašajte se, ali aplikacijo res potrebujete. Ko aplikacijo prenehate uporabljati, jo odstranite.
2. Vedno preverite, katera dovoljenja zahteva aplikacija. Če aplikacija zahteva preveč, je ne naložite. Raje izberite drugo. Prav tako bodite sumničavi pri aplikacijah, pri katerih ni informacij niti o tem, kaj zahtevajo.
3. Pazite na stroške: nekatere aplikacije se nenehno povezujejo z internetom. Če imate vklopljeno podatkovno povezavo, vam to lahko povzroči stroške, posebej v tujini.
4. Če obstaja posodobitev aplikacije, jo namestite. Posodobitve prinašajo nove funkcionalnosti ter odpravljajo napake in varnostne luknje v aplikaciji. Na nekaterih sistemih lahko vklopite samodejno posodabljanje aplikacij. Če posodobitev zahteva nova dovoljenja, jih preučite.
5. Preverite skrite stroške – morda po določenem času aplikacija za nadaljnjo rabo zahteva plačilo!

NAMIG:

Slovenski ponudniki aplikacij, ki uporabljajo osebne podatke, morajo spoštovati Zakon o varstvu osebnih podatkov, katerega nadzira Informacijski pooblaščenec. Če sumite, da aplikacija zlorablja vaše podatke, lahko podate prijavo. Če gre za ponudnika iz druge evropske države, bo Pooblaščenec prijavo posredoval nadzornemu organu te države.

Kontaktne podatke za prijavo najdete tukaj: *https://www.ip-rs.si/kazalo-kontakt-iskalnik/kontakt/*.

INFORMACIJSKI POOBLAŠČENEC

REPUBLIKA SLOVENIJA

MOJA PISARNA

Tablice v poslovni rabi že izpodrivajo klasične prenosnike, saj lahko osnovno poslovno komunikacijo opravimo kar s telefonom. Hitro odzivanje je pomembno, zato pride še kako prav, da lahko pošto spremljamo na poti in hitro priredimo ter pošljemo tudi kakšen dokument. Vsa tveganja, ki smo jih našteli do sedaj, veljajo seveda tudi za poslovne uporabnike, le da ima lahko kraja podatkov v poslovnem okolju zelo jasne motive in hude posledice.

Kako torej varno uporabljati mobilne naprave v poslovni komunikaciji?

Spodaj je nekaj temeljnih razmislekov, ki jih morate upoštevati pred samim začetkom uporabe nove mobilne naprave in kasneje vsaj še enkrat na leto. Zakaj? Na začetku morda še ne boste vedeli, katere naloge boste z napravo opravljali. V velikih podjetjih naj IT-oddelek na podlagi teh predlogov poišče ustrezne rešitve, majhna podjetja in samostojni podjetniki pa naj rešitve poiščejo samostojno ali v sodelovanju s svojim izbranim ponudnikom.

Navodila, povezana z namenom naprave: razmislite, do katerih podatkov potrebujete dostop tudi z mobilne naprave. Je to res nujno ali pa pravzaprav prenosnik nikoli ne bo daleč in funkcij poslovanja dejansko ni treba prenašati tudi na mobilno napravo? Odločite se tudi, koliko boste mešali poslovno in zasebno uporabo, npr. boste z naprave sem in tja le pogledali kakšen film in odigrali priložnostno igrico ali pa boste napravo za dlje časa brez nadzora prepustili tudi svojim otrokom. Nekatere novejše naprave že omogočajo več uporabniških profilov – za resno delo uporabite zaklenjen uporabniški račun, otrokom pa igrice nameščajte v okviru drugega.

Navodila za povezljivost: uredite VPN-dostop s šifriranjem. S tem vso komunikacijo spravite v šifriran tunel in tako poskrbite za zaščito pred prestrezanjem. Razmislite, ali boste za VPN-avtentikacijo uporabili generatorje gesel za enkratno uporabo.

Navodila za elektronsko pošto: potrebujete res dostop do vse pošte ali samo do določenih predalov? Morda lahko podatke podjetja razdelite v bolj in manj občutljive kategorije, jih razvrstite v različne predale in temu primerno prilagodite tudi dostop do njih.

Navodila ob izgubi naprave: dobro razmislite, kaj se bo zgodilo ob okvari, izgubi ali kraji naprave. Do katerih podatkov bo dostopal lopov ali najditelj vaše naprave in kaj to pomeni za vaše poslovanje? Kaj pa če napravo dobi v roke konkurenca? Kako hitro boste lahko podatke povrnili na novo napravo in nadaljevali z delom? Ali imate urejene ustrezne varnostne kopije, da ne bo izguba naprave predstavljala motnje v vašem poslovanju?

Navodila za izbris podatkov z naprave: če vaša naprava omogoča brisanje na daljavo, ga omogočite in se naučite, kako se sproži. Prav tako preverite, ali obstaja nastavitev ali aplikacija, prek katere lahko napravo s pomočjo vgrajenega GPS-sprejemnika locirate.

Navodila za aplikacije: če naprava to omogoča, dovolite nameščanje novih aplikacij le z vpisom ustreznega gesla. Ko aplikaciji dovolite dostop do podatkov na napravi, pomislite, kaj lahko to pomeni s poslovnega vidika.

KLJUČNA TVEGANJA

IZGUBA ALI KRAJA MOBILNE NAPRAVE

Kaj storiti v primeru izgube ali kraje mobilne naprave?

- Takoj pokličite svojega operaterja in prekličite SIM-kartico. Nekdo lahko uporablja vaš telefon in vam povzroči stroške.
- Če je omogočen neposreden dostop do drugih uporabniških računov (elektronska pošta, družbena omrežja), nemudoma spremenite vsa gesla! Nekdo lahko z vaše naprave dostopa do vaših uporabniških profilov.
- Namestite aplikacijo za brisanje podatkov na daljavo. V tem primeru lahko izbrišete vse občutljive vsebine.
- Če krajo prijavite policiji, jim posredujte tudi IMEI-številko naprave. Zapisana je na embalaži, na garancijskem listu in na nalepki pod baterijo mobitela. IMEI se izpiše tudi na zaslonu mobitela po vnosu ukaza *#06#. Zapišite si jo in shranite na varno mesto!

ŠKODLJIVA ALI ZLONAMERNA KODA

Pri telefonih z operacijskim sistemom Android moramo za zaščito poskrbeti sami s protivirusnim programom, ki ga lahko dobimo tudi brezplačno v Google Play, na napravah iOS in Windows Phone pa za zdaj to ni potrebno zaradi drugačnega modela delovanja in nameščanja aplikacij.

Kako pride do okužbe?

Vaš sistem se lahko okuži tudi preko SMS- oziroma MMS-sporočila ali Bluetooth povezave. **Gotovo pa je največja verjetnost za okužbo, ko naložite »privlačno« (a nepreverjeno) aplikacijo, ki vsebuje škodljivo kodo.**

KAKO VEM, DA JE MOJ TELEFON OKUŽEN?

Virusi lahko povzročijo zelo hitro praznjenje baterije ali pa upočasnijo delovanje telefona. Lahko tudi prevzamejo nadzor nad katero od funkcij telefona in kličejo ali pošiljajo SMS-sporočila. Zato redno preverjajte izpiske svojega operaterja.

Kakšne so lahko posledice?

Škodljiva koda lahko krade podatke, ki jih hranite. Lahko si zapomni vaša gesla, jih prek omrežja sporoči storilcu, ta pa nato dostopa do vaših profilov na družbenih omrežjih ali še huje, v vašo spletno banko. Aplikacija lahko prestreza vaše pogovore in SMS-sporočila. Lahko izbriše kontakte iz imenika

NAMIG:

Aplikacije nameščajte samo iz uradnih trgovin za naprave. Pri tem preverite ocene drugih uporabnikov, prav tako preverite spletno stran ponudnika in njegov »sloves«. Nikoli ne slepo zaupajte povezavam do aplikacij, ki vam jih neznanci ponujajo prek elektronske pošte ali družbenih omrežij.

in slike iz galerije. Lahko se pri prenosu podatkov prenese tudi na druge naprave. Veliko zlonamernih aplikacij povzroča velike stroške uporabniku s pošiljanjem skritih SMS-sporočil na komercialne in »premium« številke.

APLIKACIJE IN ZAHTEVANA DOVOLJENJA

Veliko aplikacij na trgu zahteva od vas preveč dovoljenj, lahko bi dejali, da imajo prevelike apetite, dostopajo lahko do vseh podatkov na vaši napravi ali celo prevzamejo nadzor nad funkcijami naprave.

NAMIG:
Če nočete, da razvijalci aplikacije za budilko berejo vašo poslovno pošto in poslušajo vaše pogovore, potem vedno preverite, katera dovoljenja aplikacija želi od vas. Če hoče preveč, raje izberite drugo. Na trgu jih je veliko.

PREVZEMANJE NADZORA NAD NAPRAVO

Posebno tveganje predstavlja lomljenje naprave z namenom pridobitve popolnega nadzora t. i. »jailbreak« ali »rooting«. Na kratek rok dobimo več nadzora in fleksibilnosti, dolgoročno pa zaobidemo privzete varnostne omejitve naprave, ki nas ščitijo pred namestitvijo škodljive kode. Na napravo lahko na ta način nevede namestimo programsko opremo s škodljivo kodo in na široko odpremo vrata različnim zlorabam. Prav tako se lahko

pojavijo težave pri posodabljanju operacijskega sistema in uveljavljanju garancije pri morebitni okvari. Če se že odločite za ta poseg, obvezno namestite aplikacijo, ki ob vsakem posegu v sistem vpraša za dovoljenje (npr. SuperSU ali superuser za sisteme Android).

NAMIG:
STARŠI, POZOR! Obdržite nadzor nad aplikacijami, ki jih nalagajo otroci – na napravi lahko v nastavitvah blokirate nalaganje aplikacij. Prav tako to omogočajo nekateri operacijski sistemi. Tako morate vi dovoliti vsako aplikacijo, ki jo želi otrok. Previdno tudi pri aplikacijah, ki omogočajo nakupe znotraj aplikacije same. Zaklenite nakupe s PIN kodo (npr. Trgovina Play – Nastavitve – Za nakupe uporabi PIN).

KLJUČNI NASVETI

Vodila za varno in preudarno rabo mobilnih naprav naj nikakor ne segajo v polje groženj in prepovedi. Pametne naprave nam omogočajo priročno in nadgrajeno komuniciranje, sami pa lahko poskrbimo za to, da nam ga ne zagrenijo.

1. Aktivirajte PIN-kodo za zaklep SIM-kartice in kodo za zaklepanje zaslona. Če je mogoče, naj bo koda daljša od štirih znakov. Nekatere naprave omogočajo odklep s »skrivno« potezo (ki pa jo običajno vidijo skoraj vsi v naši bližini).

2. Uporabite napredne mehanizme za avtentikacijo, kadar so na voljo.

3. Naložite ustrezen protivirusni program, če je na voljo. Ta program bi moral biti ena prvih stvari, ki se znajde na vašem pametnem telefonu ali tablici. Večina uveljavljenih ponudnikov protivirusnih programov že tudi ponuja zaščito, specializirano za mobilne naprave, in tako plačljive kot tudi brezplačne različice. Poiščite informacije na njihovih uradnih straneh ali na spletni strani http://www.av-test.org/en/home/.

4. Redno ustvarjajte varnostne kopije podatkov, shranjenih na mobilni napravi. Kopije lahko hranite v oblak, občasno opravite varnostno kopiranje tudi na osebni računalnik.

5. Pregledujte račune svojega operaterja. Redno preverjajte račune, saj je lahko visok znesek za klice na neznane številke ali nenavadno velika količina prenesenih podatkov znak okužbe z virusom. Posebno pozorni bodite na morebitne klice na »premium« plačljive številke ali prejemanje komercialnih SMS-sporočil oz. včlanitev v SMS-klube.

6. Redno posodabljajte operacijski sistem in aplikacije. Posodobitve namreč odpravljajo na novo odkrite varnostne luknje.

7. Aplikacije vedno nameščajte le iz uradnih trgovin in preverjenih virov. Bodite sumničavi pri tistih, ki želijo dostopati do prevelikega števila vaših podatkov.

8. Izklopite privzeto oddajanje svoje geolokacije – vklopite funkcijo le takrat, ko to potrebujete.

ABC VARNOSTI IN ZASEBNOSTI NA MOBILNIH NAPRAVAH

si·cert
VARNI NA INTERNETU
INFORMACIJSKI POOBLAŠČENEC
INFORMATION COMMISSIONER