

VARNOSTNA PRIPOROČILA BYOD



Kaj je BYOD (Bring Your Own Device)?

Večina zaposlenih danes na delovnem mestu uporablja pametni telefon ali tablični računalnik, ali pa oboje. Mobilne naprave uporabljamo za različne vidike svojega osebnega in poslovnega življenja, npr. ko prek mobilnega telefona dostopamo do službene e-pošte ali ko med sestankom delamo zapiske na tabličnem računalniku.



Mobilna naprava lahko hrani veliko zaupnih podatkov, na primer osebne koledarje, sezname stikov, poslovne e-naslove, osebne identifikacijske številke (številke PIN), prijavnne podatke, lastniške podatke podjetja ali evidence strank.

Pri konceptu BYOD oz. 'prinesi svojo napravo' gre torej za mobilne naprave, ki ste jih kupili za lastno uporabo, a preko njih dostopate tudi do službenih podatkov.

Tveganja, ki jih prinaša

Poleg tehničnih izzivov sta varnost in zasebnost dve osnovni tveganji BYOD-a. Med tehnične izzive sodijo povezava do brezžičnega omrežja, dostop do omrežnih virov, kot so skupne datoteke ali tiskalniki, in reševanje težav z združljivostjo naprav.

Izguba podatkov

Fizična izguba ali kraja naprave (in s tem izguba ali ogrožanje občutljivih podatkov). Več kot eno od treh mobilnih naprav prvotni lastnik izgubi ali mu jo ukradejo.



Mešanje zasebnih in poslovnih podatkov

Eno od številnih tveganj shranjevanja osebnih in poslovnih podatkov na isti napravi je, da se lahko poslovni podatki nenamerno izbrišejo.

Zlonamerne aplikacije

Zlonamerna programska oprema na prvi pogled lahko deluje povsem pristno, vendar običajno vsebuje zlonamerne funkcije. Ko jo enkrat naložite, se izpostavite hudemu tveganju, včasih pa se celo zgodi, da napadalec popolnoma prevzame nadzor nad vašo napravo.

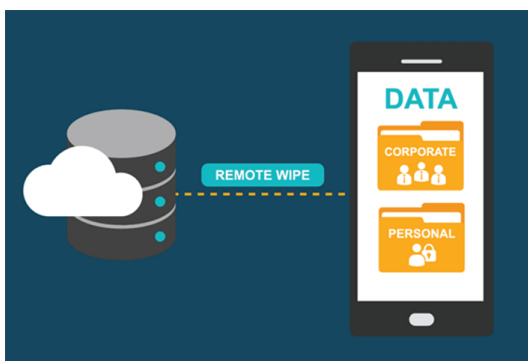


Posebne varnostne prilagoditve

»Jailbreak«, »root« in »unlock« so trije priljubljeni postopki, ki jih lahko izvajate na osebnih napravah, da odstranite omejitve konfiguracije proizvajalcev. Zato so naprave bolj ranljive za nevarne aplikacije. Ti postopki lahko omogočijo nemoten dostop do senzorjev naprave (npr. mikrofona, kamere) ali občutljivih podatkov, ki so shranjeni v napravi.

Neposodobljena programska oprema

Nobena programska oprema ni popolna in tudi aplikacije na vaši napravi niso izjema. Težava je v tem, da ranljivosti pogosto predstavljajo priložnost za napadalce, ki jih lahko izkoristijo in tako prevzamejo vašo napravo.



Vprašanja glede varnosti

Ker BYOD dostopa do strežnikov in omrežij podjetja, lahko tudi vaša organizacija zakonito dostopa do njih. Varnost BYOD se lahko nanaša na programsko opremo, ki ne razlikuje med osebnimi in poslovnimi podatki. Če je torej zaznana kršitev varnosti, se lahko vsi podatki v napravi – osebni in poslovni – samodejno izbrišejo (kar se imenuje oddaljeno brisanje podatkov).

Pomanjkanje podpore vaše organizacije

Podpora mobilnim tehnologijam IT-ekipe je zaradi velike raznolikosti naprav, operacijskih sistemov, platform itd. mobilne tehnologije lahko pomanjkljiva.





Uhajanje podatkov

Morebitno uhajanje ali razkritje podatkov podjetja iz nezavarovane naprave. Dovzetnost za napade in prisluškovanje na javno dostopnih točkah Wi-Fi, ki jih oddaljeni zaposleni pogosto uporabljajo.

Povezovanje v osebno omrežje (PAN), npr. z uporabo tehnologije Bluetooth, predstavlja podobna varnostna tveganja.

15 nasvetov za zaščito

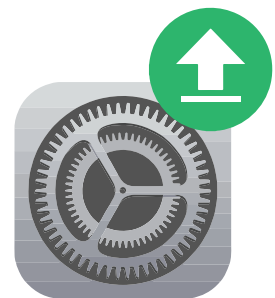
Vaša mobilna naprava vsebuje pomembne informacije o vas, vašem podjetju ter vaših prijateljih in družini – kontaktne številke, fotografije, lokacijo in druge podatke. Zato morajo biti vaše mobilne naprave zaščitene.

Pri uporabi mobilnih naprav upoštevajte naslednje varnostne ukrepe.

1

Nameščajte posodobitve

Ključnega pomena je, da programsko opremo na svojem telefonu posodobite, takoj ko so nove različice na voljo. To lahko preverite tako, da na svoji napravi odprete meni Nastavitve, kjer vidite, ali so posodobitve na voljo. Ta preprost korak je najboljši način, da se izognete tveganjem povezanih z mobilnimi napravami.



Zavarujte napravo

2



Morda se zdi očitno, toda nastavitev gesla/kode PIN je ključni prvi korak v varnosti BYOD, ki ga mnogi uporabniki ne upoštevajo. Gesla morajo biti edinstvena za vsako napravo/račun in ne smejo biti splošna ali tako enostavna, da se jih lahko ugane. Ustvarite močna gesla, ki vsebujejo črke in številke ter simbole, če je to mogoče. Uporabljajte različna gesla za osebno in poslovno uporabo. V najboljšem primeru uporabite edinstveno geslo za vsako spletno mesto, ki zahteva podatke za prijavo.

3

Ko končate, izbrišite

Pogosto nalagamo aplikacije za posebne namene, denimo za načrtovanje počitnic, ko jih po tem ne potrebujemo več ali pa smo v preteklosti prenesli aplikacije, ki niso več koristne ali zanimive. Brisanje vseh aplikacij, ki jih ne uporabljate več, je dobra varnostna praksa.





Poišči svojo napravo

4

Omogočite funkcijo »Poišči svojo napravo«, ki je na voljo v večini glavnih operacijskih sistemov, kot je aplikacija »Find My iPhone« proizvajalca Apple. Če svojo napravo izgubite, se lahko prijavite v Applov oblak iCloud in vidite, kje natančno se nahaja vaša naprava. Napravo lahko na daljavo tudi očistite, če je na lokaciji, ki je ne prepoznate ali ji ne zaupate, in tako vaši zaupni podatki niso ogroženi.

5

Varujte svojo zasebnost

Uporabite nastavitve varnosti in zasebnosti na spletnih mestih in v aplikacijah in s tem nadzirajte, kateri podatki so v skupni rabi in kdo jih vidi.



6

Aplikacije nalagajte iz zaupanja vrednih trgovin



Aplikacije prenašajte samo iz zaupanja vrednih trgovin, kot sta Applov iTunes in Androidov Google Play. Postopki kvalifikacije in filtracije aplikacij, preden so vključene v te uradne spletne trgovine, znatno zmanjšajo vse možnosti, da se bo vaša naprava okužila z zlonamerno programsko opremo.

7

Bodite pozorni na brezplačne aplikacije

Obstaja veliko brezplačnih aplikacij, ki sledijo uporabnikom in njihove informacije delijo z oglaševalci ali tretjimi osebami.



8

Bodite pozorni na Wi-Fi



Connect

Bodite previdni pri dostopanju do odprtega omrežja Wi-Fi s svojim mobilnim telefonom. Obstajata dve vrsti javnih omrežij Wi-Fi, in sicer zavarovana in nezavarovana omrežja. Z nezavarovanim omrežjem se je mogoče povezati v neposredni bližini brez gesla ali podatkov za prijavo.

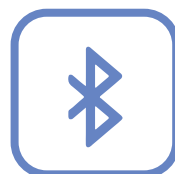
Zavarovano omrežje običajno zahteva, da se strinjate s pravnimi pogoji in si z geslom zagotovite dostop do omrežja. Kadar je le mogoče, se povežite z zaščitenim omrežjem Wi-Fi, če pa se morate povezati z nezaščitenim omrežjem, se prepričajte, da zahteva poverilnice za prijavo.

Bodite pozorni, da poiščete TOČNO ime omrežja Wi-Fi na lokaciji, kjer se nahajate, in da se s svojim telefonom povežete na TOČNO to omrežje.

9

Ne pustite si slediti

Nekatere trgovine in druge lokacije iščejo naprave z vklopljeno funkcijo Wi-Fi ali Bluetooth in spremljajo vaše premike, ko ste v dosegu. Povezave Wi-Fi in Bluetooth je treba izključiti, ko jih ne uporabljate.



Backup

Vsi uporabniki bi morali periodično narediti varnostno kopijo podatkov na svojih napravah. Varnostno kopiranje podatkov skupaj z uvedbo varnostnih in obnovitvenih postopkov vam bo močno olajšalo delo v primeru izgube ali kraje naprave.

11

Omogočite storitev oddaljenga brisanja

Omogočite možnost oddaljenega brisanja naprave, kar je ključni ukrep za zagotavljanje varnosti BYOD v primeru izgubljene ali ukradene naprave.



Unlock Phone

Omogočite samodejno zaklepanje naprave

12

Napravo nastavite tako, da se po določenem časovnem obdobju samodejno zaklene. Tako jo lahko odklenejo le tisti, ki poznajo geslo.

13

V napravo nikoli ne shranjujte osebnih finančnih podatkov

Izogibajte se shranjevanju finančnih ali drugače občutljivih podatkov na svojih napravah. Ta previdnostni ukrep zagotavlja varnost zaupnih podatkov, tudi če je naprava ogrožena.

Notepad

Visa Pin

5987

15/04/2020

Mastercard Pin

4668

15/04/2020



Zaženite mobilno protivirusno programsko opremo ali diagnostična orodja

14

Na trgu obstaja veliko protivirusnih in varnostnih aplikacij, ki diagnosticirajo in ščitijo naprave pred običajnimi grožnjami.

15

Ne dovolite, da se vaši otroci igrajo s telefonom, ki ga uporabljate v službene namene

Ne dovolite, da mobilne naprave uporabljajo otroci, ki pogosto prenašajo neznane brezplačne aplikacije, ki so videti zabavne, a imajo lahko zlonamerne vsebine.

