NAJSTRAŠNEJŠA ŽIVAL JE ... MIŠ!

VARNI NA INTERNETU
Od mene je odvisno vse.
www.varninainternetu.si

Kažipot za varnost na spletu

10 NASVETOV

ZA MALA PODJETJA

Vsebina

Podjetjem grozijo iznajdljivi spletni goljufi

Goljufi so že marsikateremu podjetju nakopali težave z domiselnimi poskusi kraje denarja:

Spletni goljuf, ki se je lažno predstavljal kot direktor podjetja, je napisal elektronsko sporočilo, da je v stiski in prosi za nakazilo večje vsote denarja.

V proces nakazila denarja za opravljeno storitev ali kupljeno blago se je vrinil spletni goljuf in kupcu sporočil svojo številko transakcijskega računa.

Lažni krediti, ki podjetjem pomagajo prebroditi finančno težke čase, in lažne spletne trgovine, ki za znane in uveljavljene blagovne znamke obljubljajo neverjetne popuste. Ko ponudba po ceni močno odstopa od drugih, je to zanesljiv razlog za previdnost.

Zaposlene temeljito poučite, naj bodo vselej zelo pozorni na elektronski naslov pošiljateljev tovrstnih sporočil. Naučite jih tudi prepoznavati med pravim in lažnim ponudnikom blaga oziroma storitev.

PREVIDNO RAVNAJTE Z ELEKTRONSKO POŠTO

Največ poskusov vdorov v informacijske sisteme se zgodi prek elektronske pošte. Če za tarčo – naključno ali ne – izberejo prav vas, bodo to storili s phishing napadom oziroma krajo vašega gesla ali poskusom namestitve izsiljevalskega virusa. Pri uporabi elektronske pošte je zato pomembno vedeti naslednje:

01

A. Nikoli ne odpirajte priponk neznanih pošiljateljev.

Če vam je pošiljatelj sporočila znan, preverite ime pripete datoteke. Če je ime priponke sumljivo, na primer 226KL2100.docx, po telefonu ali e-pošti stopite v stik s pošiljateljem in ga vprašajte, ali vam je priponko res poslal on.

Če prejmete datoteko formata .doc ali .xls in ob odprtju datoteke program od vas zahteva vklop makra, tega ne storite. Izjema so interne datoteke med sodelavci, vendar tudi takrat preverite, ali vam je datoteko res poslal sodelavec, preden vklopite makre.

NAMIG:
Za hitro in enostavno preverjanje vprašljive priponke uporabite spletno orodje VirusTotal. Priponko z desnim klikom shranite na računalnik (ne odpirajte!), pojdite na spletno stran VirusTotal (https://www.virustotal.com/#/home/upload) in kliknite gumb »Upload and scan file«. Izberite sumljivo priponko, ki ste jo shranili na računalnik. VirusTotal bo datoteko pregledal in vas opozoril, če bi lahko bila okužena.

B. Preverite stran, na kateri vpisujete svoje uporabniško ime in geslo.

Če prejmete elektronsko pošto, v kateri vas »nujno« pozivajo k vpisu vašega uporabniškega imena in gesla (za elektronsko pošto ali kako drugo storitev), tega nikoli ne storite.

NASTAVITE ZAPLETENA IN MOČNA GESLA

Če imajo spletni goljufi vaša gesla za dostop do različnih storitev, imajo prosto pot do zlorab različnih oblik in razsežnosti. Zato bodite še posebej pozorni na naslednje:

Vaša gesla za različne spletne storitve naj bodo raznolika. Nikoli ne uporabljajte enakih gesel za prijavo v računalnik, elektronsko pošto, spletno banko in druge spletne storitve.

Gesel ne pišite na listke, ki bi ji pustili v bližini računalnika, pod tipkovnico ali celo nalepljene na zaslon.

Vaša gesla naj bodo zapletena.

KAKO USTVARITE MOČNO GESLO?

1. Vaše geslo naj bo dolgo vsaj 8 znakov in naj vsebuje male in velike črke, številke in ločilo (ki ga spletno mesto dovoli uporabiti). V pomoč pri pomnjenju gesla so vam lahko posebni stavki: Po kaj gre mali Petja 2x tedensko na Slomškovo 7? Vaše geslo je tako: PkgmP2xtnS7? Če za geslo ni zgornje meje dolžine, lahko uporabite celotne stavke, najbolje izmišljene. Recimo: Petje naključno odstira ...

2. Če geslo po dolžini ni omejeno, si izberite daljšo frazo namesto ene besede; uporabite lahko tudi daljši stavek, ki si ga boste zlahka zapomnili, in ga nekoliko spremenite oz. iz njega vzemite dele po nekem ključu.

3. Ne uporabljajte zaporednih črk ali številk, prav tako ne sosednjih tipk na tipkovnici (npr. 12345678 ali asdfghj).

4. Ne uporabljajte gesel, ki jih je lahko uganiti (npr. ime in priimek, imena otrok, datum rojstva in kombinacije teh podatkov).

5. Ne uporabljajte samo enega gesla za vse uporabniške račune (oblikujte različna gesla za npr. elektronsko pošto, Facebook, forume, spletno bančništvo).

6. Nikomur ne zaupajte svojega gesla!
Ne shranjujte zapisanega gesla v bližini svojega računalnika (listek z vašim geslom, zalepljen na monitor ali na pisalni mizi).

02

VARNO UPORABLJAJTE SPLETNO BANKO

Spletno bančništvo je enostavna oblika finančnega poslovanja, a tudi zlata jama novodobnih spletnih kriminalcev. Za to, da jim preprečite dostop do spletne banke, lahko največ naredite sami:

Certifikat, ki vam omogoča dostop do spletne banke, imejte vedno shranjen na zunanji napravi, na primer pametnem USB-ključu ali pametni kartici.

Ko končate delo, pametni USB-ključ oziroma pametno kartico odstranite iz računalnika.

Če se vaš računalnik okuži z virusom, se lahko zgodi kraja podatkov in goljufi bodo imeli prost dostop do spletne banke. Zato redno posodabljajte vso programsko opremo (ne nameščajte nelicenčne), namestite zanesljiv antivirusni program in ga prav tako redno posodabljajte, službeni računalnik pa uporabljajte samo v službene namene.

Spletne banke nikoli ne uporabljajte na računalniku, ki je namenjen širšim množicam.

Če vaš poslovni partner sporoči, da je spremenil številko poslovnega transakcijskega računa, to osebno preverite pri njem in ne zaupajte zgolj elektronskemu sporočilu.

Ko nakupujete prek spleta, če le imate možnost, izberite plačilo prek zaupanja vrednih posrednikov (na primer PayPala).

03

POSKRBITE ZA VARNOST SPLETNIH STRANI

Spletna stran je zrcalo vašega podjetja v splet in običajno prvi stik kupca z vami. A pomembna nista le videz in vsebina, poskrbite tudi za njeno varnost:

Spletna stran naj bo dosegljiva prek varne povezave (prepoznamo jo po »https« v URL-naslovu spletne strani). Še posebej je to pomembno, ko ima spletna stran vnosne obrazce (ime in priimek, elektronski naslov) ali spletno trgovino in možnost spletnega plačevanja blaga oziroma storitev.

Spletno mesto redno vzdržujte in posodabljajte. Še posebej to velja, če vaša spletna stran temelji na odprtokodnih rešitvah za urejanje vsebine, na primer Joomli, Wordpressu, Magenti, Prestashopu, Drupalu, OpenCartu, Typo3 in podobnih.

Izdelavo in vzdrževanje spletne strani vedno zaupajte kredibilnemu in z referencami podprtemu ponudniku gostovanja in programerju. Spletno mesto nujno vzpostavite ob pomoči profesionalne in strokovno podkovane podpore.

NAMIG:
Prenesite si vodnik ABC varnosti za lastnike spletnih strani (https://vni.si/spletnastran), v katerem so zbrani nasveti za vzdrževanje spletne strani in pravilno skrb za domeno ter kontaktni naslovi, kamor se lahko obrnete, če bi imeli težave.

Ne dovolite, da se kot nosilec domene vpiše izdelovalec vaše spletne strani. Če že, naj svoje kontaktne podatke vpiše kot tehnični stik. Ob registraciji tudi navedite elektronski naslov, do katerega ne dostopajo vsi zaposleni.

Na spletno stran napišite samo splošen elektronski naslov podjetja (na primer info@imepodjetja.si). Kontaktnih podatkov zaposlenih ne objavljajte, saj jih goljufi lahko premeteno izkoristijo za različne vrste spletnih goljufij.

04

VARNOSTO KOPIRAJTE, KOPIRAJTE IN ŠE ENKRAT KOPIRAJTE

Karkoli se zgodi, vedno boste najbolj varni, če (najbolje vsakodnevno!) varnostno kopirate datoteke. Če vas spletni goljufi presenetijo na primer z vdorom v sistem ali okužbo z izsiljevalskim virusom, so varnostne kopije (t. i. backupi) edino zagotovilo, da boste še lahko dostopali do svojih podatkov. Nobenega jamstva ni, da bo ob kraji ali zaklenitvi podatkov tudi najbolj usposobljen IT-strokovnjak lahko pridobil šifrirane podatke. A pozor, tudi redno varnostno kopiranje se lahko izjalovi, pa za to morda sploh ne veste. Zato upoštevajte:

05

Podatke varnostno kopirajte na zunanji medij, do katerega nimajo dostopa vsi zaposleni. Najbolje je, da medij z varnostnimi kopijami fizično umaknete, ga denimo zaklenete v omaro.

Varnostne kopije ustvarjajte dosledno in na vsaj dve različni lokaciji (ena kopija naj bo v službi, druga na ločeni lokaciji, na primer doma, v bančnem trezorju, oblaku).

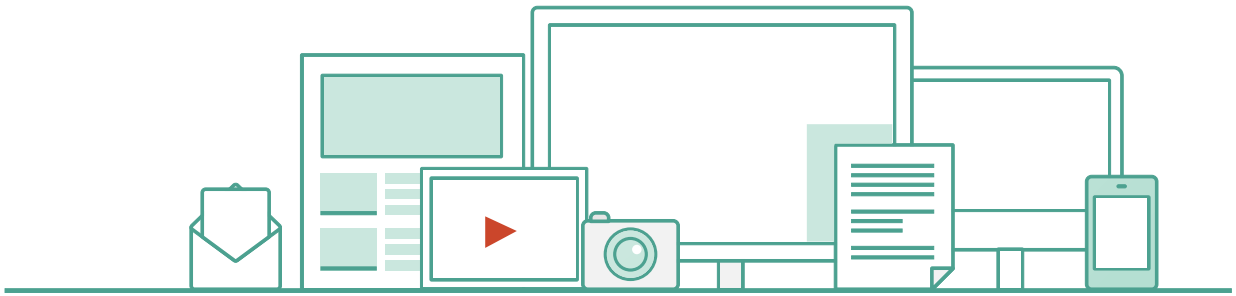
Če varnostne kopije shranjujete v oblaku, izberite zaupanja vrednega ponudnika. Za dostop nastavite avtentikacijo v dveh korakih. Preden podatke izvozite v oblak, jih šifrirajte s svojim šifrirnim ključem.

NAMIG:
Ko naredite varnostne kopije, vedno preverite, ali delujejo. Med kopiranjem dokumentov namreč lahko nastane napaka in dokumenti bodo v tem primeru neuporabni.

VODITE POPIS OSNOVNIH SREDSTEV

Naredite popis vseh sredstev in virov, s katerimi razpolaga podjetje. To vključuje:

- vso strojno opremo: računalnike, strežnike, tiskalnike, USB-ključe, zunanje diske, mobilne telefone;
- programsko opremo: poleg licenčnih tudi brezplačne programe;
- zaposlene: zaposlene in zunanje sodelavce ter »moč« njihovih dostopov;
- informacije: poleg elektronskih baz in datotek (v PDF-ju, Wordu, Excelu …) popišite tudi papirnato dokumentacijo;
- zunanje storitve: celoten nabor spletnih storitev, ki jih uporabljate, kot sta DropBox ali Gmail;
- infrastrukturo: pisarno, klimatske naprave in potek električne napeljave, ker lahko ta sredstva vplivajo na dosegljivost informacij.



06

PREVIDNO UPORABLJAJTE SLUŽBENE PRENOSNIKE IN TELEFONE

07

Če v podjetju uporabljate službene prenosnike in telefone, poskrbite za varnost teh naprav:

Z namensko programsko opremo (na primer BitLocker) omogočite šifriranje diska, kar vam lahko koristi, če službeni računalnik ukradejo.

Zaposleni naj imajo na službenih računalnikih le toliko pravic, kot jih zares potrebujejo. Administratorski dostop naj ima le tisti, ki skrbi za naprave, za običajno delo pa uporabljajte račune z omejenimi pravicami.

Na službene naprave ne nameščajte aplikacij, ki niso namenjene službeni uporabi.

Nameščajte zgolj aplikacije, ki ste jih našli na uradnih tržnicah, kot sta Google Play ali App Store.

NAMIG:
Bodite pazljivi pri klicih iz tujine. Če na telefon prejmete klic človeka, ki se v polomljeni angleščini predstavi kot Microsoftova tehnična pomoč, naj se vam vklopijo vsi alarmi. Tovrstni prevaranti sogovorniku pojasnijo, da je bila v njegovem računalniku zaznana težava, za pomoč pri reševanju pa želijo, da jim omogočite oddaljen dostop do svojega računalnika. Gre za tipično prevaro, o kateri si lahko več preberete tukaj (https://vni.si/klic).

Še en poskus zlorabe poteka v obliki klica s premijske ali satelitske številke. Goljufi pozvonijo le enkrat ali dvakrat, tako klicani nima časa odgovoriti. Ko pokliče nazaj, si povzroči visoke stroške, del denarja pa pristane v rokah kiberkriminalcev.

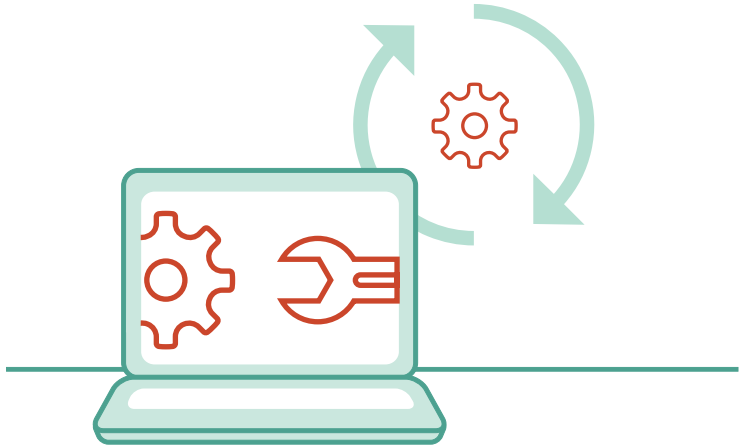
Če izgubite službeni pametni telefon ali vam ga ukradejo, nemudoma ukrepajte. Navodila za telefone z operacijskim sistemom Android najdete tukaj https://vni.si/android, navodila za mobilnike iPhone pa tukaj https://vni.si/iphone.

PROGRAMSKO OPREMO REDNO POSODABLJAJTE

Poskrbite za nekaj ključnih ukrepov:

POSODABLJAM ...

- Na vseh službenih računalnikih redno posodabljajte nameščene aplikacije in operacijski sistem.
- Na elektronske naprave namestite zanesljiv antivirusni program z najnovejšimi posodobitvami.
- Na računalnik ali telefon nikoli ne nameščajte nelicenčne (t. i. piratske) programske opreme.



08

POSKRBITE ZA VARNO DELO OD DOMA

Če zaposleni delajo od doma, poskrbite za varnost:

VPN Zaposleni naj za dostop do službenega omrežja uporabljajo varno VPN-povezavo.

Dostop od doma naj bo omogočen le tistim uporabnikom, ki to zares potrebujejo.

Oddaljen dostop do službenega omrežja naj bo dobro zaščiten, tudi s požarnim zidom. Zaposleni naj uporabljajo močno geslo in večstopenjsko avtentikacijo.

09

NE POZABITE NA VARNOST BREZŽIČNEGA OMREŽJA

Službeno brezžično omrežje, ob pomoči katerega zaposleni in obiskovalci dostopajo do spleta, ustrezno zaščitite:

Uporabite kompleksno geslo za dostop do omrežja.

Uporabite šifriranje (WPA2, AES).

Na brezžičnem usmerjevalniku (t. i. routerju) spremenite privzete oziroma tovarniške nastavitve.

1. 2.

Ločite omrežji Wi-Fi za zaposlene in obiskovalce. Obiskovalcem onemogočite dostop do službenega omrežja.

Skrijte ime brezžičnega omrežja, tako da se ne prikaže na seznamu razpoložljivih omrežij (skriti SSID).

10

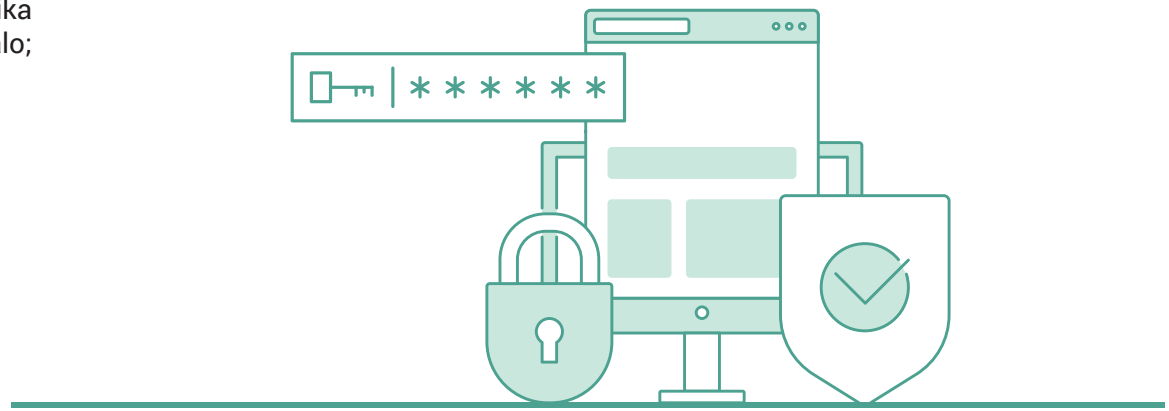
Je za varstvo podatkov v vašem podjetju dobro poskrbljeno?

Če v okviru svoje dejavnosti zbirate podatke fizičnih oseb ali vaša storitev temelji na uporabi osebnih podatkov, boste morali od konca maja 2018 upoštevati določbe Splošne uredbe o varstvu podatkov. Več o njej boste izvedeli na spletni strani Informacijskega pooblaščenca: https://www.ip-rs.si/.

Med osebne podatke poleg imena, priimka, naslova in EMŠA štejemo tudi IP-naslov, ID-piškotke, RFID-oznake in druge identifikatorje. Informacijski pooblaščenec svetuje:

- da že pri zasnovi poslovnega procesa poskrbite, da boste obdelovali le toliko osebnih podatkov, kot je nujno;
- da pridobite veljavno soglasje uporabnika, ki mora biti prostovoljno, izrecno, nedvoumno in dokazljivo, in uporabnika jasno obvestite o tem, kaj se bo z njegovimi podatki dogajalo;
- da se zavedate pravic posameznikov do seznanitve, izbrisa, popravka in prenosa podatkov;
- da s svojimi partnerji (na primer ponudniki storitev oblaka, hrambe podatkov) sklenete ustrezne pogodbe.

Če vaša dejavnost vključuje obsežno obdelavo osebnih podatkov (na primer računovodski servisi, ponudniki raznih IT-rešitev), si na spletni strani Informacijskega pooblaščenca preberite več o novih obveznostih po GDPR.



VARNI
NA INTERNETU
Od mene je odvisno vse.
www.varninainternetu.si

EVROPSKI
MESEC
KIBERNETSKE
VARNOSTI

si·cert

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

Več nasvetov o varni rabi interneta in prepoznavanju
spletnih prevar poiščite na portalu www.varninainternetu.si.