SPARKASSE
Pay

PRIPOROČILA GLEDE VARNEGA SPLETNEGA DOSTOPA IN UPORABE APLIKACIJE D-MOBILE SPARKASSE PAYA TER VARNIH SPLETNIH NAKUPOV

Priporočila glede varnosti vašega osebnega računalnika ali telefona

1. Za ogledovanje in uporabo spletne strani SP ni potrebno nameščati dodatne programske opreme
Sparkasse Pay ne zahteva namestitve nobene dodatne programske opreme. Nikoli ne nameščajte programa, za katerega se zatrjuje, da je kakorkoli povezan z Sparkasse Pay!

2. Uporaba varnega računalnika in javnih omrežij
Ne uporabljajte računalnika za vnos osebnih podatkov, do katerega ima dostop veliko ljudi. Poskusite onemogočiti dostop do svojega osebnega računalnika osebam, ki jim ne zaupate. Izogibajte se uporabi javnih Wi-Fi omrežij, ki niso zaščitena s geslom ali pa so brez VPN povezave za dostop do občutljivih podatkov.

3. Uporaba programov za zaščito pred virusi
Da bo na računalniku vedno posodobljena različica programske zaščite proti virusom, je nujno omogočiti samodejno nadgradnjo in posodabljanje protivirusnega programa. Zaželeno je tudi, da se v operacijskem sistemu vključi požarni zid, s čimer se prepreči neželena in nedovoljena komunikacija.

4. Ustrezno in redno vzdrževanje računalnika ali telefona, varnostno kopiranje podatkov
Če sumite, da je vaš računalnik okužen z virusom ali škodljivo programsko opremo, oziroma ste ugotovili, da je okužen, sledite priporočilom na spletni strani https://www.varninainternetu.si. Uporabljajte le računalnik, ki je redno posodobljen z najnovejšo licenčno različico operacijskega sistema. Spletni brskalnik mora biti redno posodobljen in opremljen z najnovejšimi popravki proizvajalca. V spletnem brskalniku vključite še filtriranje lažnega predstavljanja. V izogib izgubi pomembnih podatkov, skrbite za shranjevanje varnostno kopije pomembnih podatkov za zunanji disk ali v oblak.

5. Uporaba najnaprednejših in najpogosteje uporabljenih spletnih brskalnikov
Spletne brskalnike je potrebno redno posodabljati. Izogibajte se uporabi nepotrebnih dodatkov v brskalniku. Poleg tega ni priporočljivo nalaganje dodatkov s sumljivih in nepreverjenih spletnih mest. Obvezno je treba vključiti samodejno nadgradnjo dodatkov, kot so PDF-pregledovalnik (Adobe Reader, FoxIT. Vedno morajo biti vključeni spletni filtri proti škodljivim spletnim stranem (Block reported web forgeries, SmartScreen Filter ...).

6. USB ključi, spominske kartice in CD- ali DVD-pogoni
Ob uporabi ali priključitvi zunanjih enot je potrebna posebna pozornost. Zunanji nosilci podatkov (USB ključki, CD ali DVD-pogoni, SD-kartice, XD-kartice in zunanji trdi diski) so lahko potencialni vir škodljive programske opreme. Poskrbite, da boste vključili dodatno zaščito pred tako strojno in programsko opremo, in/ali na svojem računalniku pred priključitvijo teh naprav namestite protivirusno zaščito.

7. **E-sporočila, ki jih pošljejo neznani pošiljatelji in sumljiva vsebina**
   Eden najpogostejših načinov za povzročitev škode računalniku so e-sporočila s sumljivo vsebino, ki jih pošlje neznani pošiljatelj. Ne odpirajte prilog v takih e-sporočilih niti ne klikajte na povezave v telesu e-sporočila. E-sporočila so lahko ponarejena, zato pred odprtjem sumljivega e-sporočila preverite identiteto pošiljatelja.

8. **Uporaba močnih gesel in dvofaktorska avtentikacija(2FA)**
   Uporabljajte dolga in zapletena gesla, ki vsebujejo velike in male črke, številke in posebne znake. Če je le mogoče, si za dodatno zaščito namestite tudi dvofaktorsko avtentikacijo.

Priporočila v zvezi z varno uporabo spletnih mest in aplikacije D-Mobile Sparkasse Pay

1. **Izogibajte se spletnim mestom z nezakonito programsko opremo in vsebino ter sumljivim spletnim stranem**
   Zaradi možnosti nenamernega prenosa raznih škodljivih vsebin z nepreverjenih spletnih mest je najbolje, da do teh spletnih mest ne dostopate z istim računalnikom ali telefonom, prek katerega opravljate spletne nakupe, ampak raje uporabljajte drug računalnik ali telefon. Izogibajte se poganjanju zagonskih datotek na vašem računalniku ali telefonu, prenesenih s sumljivih in nepreverjenih spletnih mest. Če bi se take datoteke kljub temu zagnale na osebnem računalniku ali telefonu, je priporočljivo preveriti ime podpisanega izdajatelja, če pa aplikacija ni podpisana, je njena namestitev odsvetovana.

2. **Ob vsakem spletnem nakupovanju obvezno preverite naslov spletnega mesta**
   Najverjetnejša možnost za napad je, da se v pristni spletni naslov Sparkasse Pay oziroma spletne trgovine podtakne en znak, zaradi katerega se spletni naslov sicer razlikuje od izvirnega, a uporabnik te razlike ne opazi. Ta znak je lahko pika, pomišljaj ali neka črka, ki je vpisana tako, da je spletni naslov na prvi pogled zelo podoben izvirnemu. Pred vnosom občutljivih podatkov preverite ali spletna stran uporablja varno povezavo (HTTPS) in ima veljaven SSL certifikat (znak ključavnice v naslovu).

3. **Preverjeni trgovci, pogoji poslovanja, vračila in reklamacije**
   Nakupujte pri preverjenih trgovcih z dobrimi ocenami in varnostnimi certifikati. Izogibajte se sumljivo nizkim cenam in preverite morebitne ocene drugih uporabnikov. Spletni trgovec mora imeti jasno navedene kontaktne podatke in pogoje poslovanja. Pred nakupom skrbno preverite pogoje vračil in reklamacij. Po opravljenem nakupu pa si shranite potrditvena e-sporočila in račune za morebitne reklamacije.

4. **Aplikacija za potrjevanje spletnih plačil**
   Za potrjevanje spletnih plačil uporabljajte le uradno aplikacijo D-Mobile Sparkase Pay, ki ste jo prenesli iz uradnih trgovin (Google Play, Apple App Store in Huawei AppGallery)

5. **Nastavitve obveščanja in redno preverjanje izpiskov**
   Vklopite si varnostni sms za vsako izvedeno transakcijo. Redno preverjajte svoje transakcije in prijavite morebitne sumljive aktivnosti.

6. **Varnost uporabniškega imena in gesla**
   Nikoli ne razkrijte ali javno objavite osebnih podatkov potrebnih za registracijo v D-Mobile Sparkasse Paya in nastavitev mPIN-a, številke vaše kartice ali drugih

podatkov z vaše kartice (npr. PIN, datum veljavnosti, CVV2 številka, itd.). S tem bi bil napadalcu omogočen neposredni dostop do vaših osebnih podatkov in nastavitev storitve.

7. **Shranjevanje zaupnih informacij na računalniku ali telefonu**
   Izogibajte se zapisovanju in shranjevanju osebnih podatkov, potrebnih za registracijo v aplikacijo D-Mobile Sparkasse Pay in nastavitev mPIN-a ali katerih koli podatkov o vaši osebni kartici, na svojem računalniku ali telefonu, saj jih je mogoče iz zunanjega sveta (svetovnega spleta) zelo preprosto najti. Priporočljivo je, da se podatki o vaši osebni kartici, ki jo uporabljate za spletne nakupe, ne shranjujejo niti v sklopu spletnega brskalnika.

8. **Obvestilo o spremembi uporabniškega imena ali gesla v zvezi z vašimi elektronskimi dostopi do storitev Sparkasse Pay**
   Sparkasse Pay vas nikoli ne bo pozival k podajanju osebnih podatkov potrebnih za registracijo v aplikacijo D-Mobile in podatkov o vaši osebni kartici. Omenjenih podatkov ne pošiljajte po e-pošti, niti jih ne razkrivajte po telefonu. Če vendarle opazite tako aktivnost ali ste dobili zahtevek za navedbo uporabniških podatkov za dostop do aplikacije D-Mobile, takoj pokličite na telefonsko številko 01 5617 800 kontaktnega centra Sparkasse Pay ali pišite na info@sparkassepay.si ter prijavite tak dogodek.

Kako Sparkasse Pay skrbi za vašo varnost

1. **Varstvo podatkov**
   Vsi podatki, ki se izmenjujejo v sklopu aplikacije D-Mobile Sparkasse Pay, so varovani s šifriranjem SSL. Povezava med vašim računalnikom in On-line storitvami Sparkasse Pay se vzpostavlja z uporabo SSL (Secure Sockets Layer). Vsak podatek v komunikaciji v aplikaciji D-Mobile Sparkasse Pay se šifrira, šele nato se prenese spletnemu strežniku Sparkasse Pay, kjer se dešifrira s ključem, ki ga ima le Sparkasse Pay. Podobno so zaščiteni tudi podatki, ki jih Sparkasse Pay pošilja vam.

2. **Samodejna odjava**
   Če po prijavi v sistem ne uporabljate aplikacije D-Mobile Sparkasse Pay (na primer, če morate nekaj nujnega opraviti na nekem drugem mestu), boste samodejno odjavljeni iz aplikacije D-Mobile Sparkasse Pay. Za nadaljevanje dela v aplikaciji D-Mobile Sparkasse Pay se morate znova prijaviti. S tem se preprečuje neželeni dostop do pregleda vaših kartic in transakcij v času, ko niste pri telefonu.

3. **Varni spletni nakupi**
   Sparkasse Pay za izvajanje spletnih nakupov z vašo osebno kartico zagotavlja močno avtentikacijo preko mobilne aplikacije D-Mobile. Več informacij o opravljanju varnih spletnih nakupov z vašo osebno kartico prek mobilne aplikacije D-Mobile najdete na www.sparkassepay.si.