1. **Toimingud internetis – internetipankja kaardimaksed veebis**
2. **Toimingud pangakaardiga – kaardimaksed ja sularaha**
3. **Nutitelefon ja turvalisus**
4. **Turvalised autentimisvahendid**
5. **Suhtlus pangaga**
6. **Seadmete turvalisus**

1. Toimingud internetis - internetipank ja kaardimaksed veebis

1.1 Internetipank

1. Jälgi, et panka sisenemisel küsitakse PIN1 koodi, mitte PIN2 koodi!
2. Võimalusel väldi pangatoimingute tegemist seadmetes, mis ei ole Sinu omad (avalik arvuti, internetikiosk, sõbra seade). Kui seda pole võimalik vältida, tuleb olla eriti hoolas ja mitte jätta arvutit järelevalveta, kui oled internetipanka sisse logitud. Kui asjad aetud, tuleb veenduda, et oled internetipangast välja loginud ja veebilehitseja on suletud.
3. Väldi internetipanga kasutamist kaitsmata avalikust *wifi* võrgust. Võimalusel tekita pigem traadita internetivõrk enda mobiiltelefoni abiga.
4. Pane paika mõistlikud limiidid raha väljavõtmiseks, ülekanneteks ja kaardiga tehtavateks tehinguteks.
5. Automaatsete maksete seadistamisel sea kõige madalam vajalik makselimiit, seda nii internetipangas kui kontoris lepingut sõlmides.
6. Jälgi jooksvalt oma krediitkaardi väljavõtet. Tähelepanelik tasub olla ka väikeste summade suhtes!
7. Ära kasuta internetipanka, kui veebilehitsejalt turvalisust, ühendust või sertifikaati puudutava veateate saad.
8. Kasutades internetipanka sisenemiseks e-kirjas või sõnumis olevaid linke veendu enne sisselogimist kindlasti, et sind on suunatud panga veebiaadressile. Panga veebiaadress on tavaliselt nimekujul https://www.panganimi.ee.
9. Kontrolli aeg-ajalt üle internetipanga kasutamiseks antud volitused, kui oled andnud kellelegi teisele voli kasutada enda nimel netipanga teenuseid.
10. Veendu, et arve, mida tasud, on õige. Vaata, et maksad saadud toote või teenuse eest õigesse kohta. Tähelepanu tasub pöörata IBAN-is olevale riigi tunnusele ning võimalusel võrrdle IBAN-it varem samale teenusepakkujale tehtud maksete IBAN-iga.

1.2 Kaardimaksed internetis

1. Internetis maksete sooritamisel eelista Eesti e-kaupluste ja teenusepakkujate puhul krediitkaardiandmete sisestamise asemel pangalinki. Mujalt maailmast ostes tasub eelistada mõne tuntud maksevahendaja (nt PayPal) abi – see annab täiendava turvagarantii tundmatutelt e-teenuste osutajatelt või e-poodnikelt ostes.
2. Eelista internetioste tehes tuntud teenuseosutajaid ja e-poode. Ülisoodsad pakkumised võõrastelt e-poodidelt jäta kasutamata – kui miski näib liiga hea, et tõsi olla, siis nii ka on.
3. Võimalusel väldi kaardiandmete sisestamist tundmatute veebipoodide lehtedele.
4. Võimalusel ära tee internetioste seadmetes, mis ei ole Sinu omad (avalik arvuti, internetikiosk, sõbra seade). Kui seda pole võimalik vältida, tuleb olla eriti hoolas ja mitte jätta võõrast arvutit panka järelevalveta, kui oled internetipanka sisse logitud. Kui asjad aetud, tuleb ka veenduda, et oled internetipangast välja loginud ja veebilehitseja on suletud.
5. Internetipood ei tohi mitte mingil juhul küsida Sinu kodupanka sisselogimiseks vajalikke koode. Ära kunagi sisestada panka logimise koode ühegi teise teenusepakkuja või poe netilehele!
6. Ole ettevaatlik "mustal reedel" ja "küberesmaspäeval" ostude tegemisel. Ülisoodsad pakkumised tundmatutelt müüjatelt võivad eriti neil ostelemisele suunatud päevadel tähelepanu hajutada ja tuua kaasa pettuse ohvriks langemise.
7. Ära kunagi postita pilte enda või kellegi teise maksekaardist internetti või sotsiaalmeediasse.

2. Toimingud pangakaardiga – kaardimaksed ja sularaha

2.1 Kaardimaksed poes ja teenuseosutajate juures

1. Ära lase kaarti silmist. Ka kaupluses tasudes jälgi, et müüja ei läheks kaardiga näiteks taharuumi või mujale, kus Sa kaarti ei näe.
2. Kaardimakset sooritades jälgi, et keegi ei näeks, kuidas PIN-koodi sisestad. Vajadusel varja PIN-koodi sisestamist käega.
3. Veendu enne viipemaksega tasumist, et tasutav summa on õige.
4. Ära kunagi hoia ühegi pangakaardi PIN-koodi rahakotis, veel vähem kaardi küljes.
5. Teavita kaotatud või varastatud kaardist kohe panka. Osade pankade mobiiliäpis on võimalik ka ise kaart ajutiselt sulgeda ja selle ülesleidmisel taas avada. Kui kohe kaardi sulged, väheneb oluliselt võimalus, et keegi saab omavolitseda sinu pangakontol oleva rahaga.
6. Reisile minnes veendu, et sul on lisaks igapäevasele kaardile maksmiseks olemas tagavara-variant.
7. Kui maksad kaardiga, uuri enne makseterminali. Ettevaatlik tasub olla, kui selle küljes on mingeid kummalisi seadmeid – nendega võidakse proovida kopeerida Sinu kaardi andmeid.
8. Kui oled viipekaardi omanik, sea viipemaksetele mõistlikud limiidid. Kui Sa viipemakseid teha ei soovi, sulge kaardil see võimalus.

2.2 Sularaha võtmine

1. PIN-kood on isiklik ja salajane! Ära jaga seda kellegi teisega ega hoia seda rahakotis kaardiga koos.
2. Sularaha välja võttes jälgi, et keegi ei näeks, kuidas PIN-koodi pangaautomaati sisestad. Vajadusel varja PIN-koodi sisestamist käega.
3. Hoia oma pangakontol toimuval silma peal! Jälgi regulaarselt internetipangas oma konto väljavõtet, veendumaks, et keegi teine ei ole sinu teadmata sealt raha välja võtnud.
4. Veendu, et pangakaart leiab pärast automaadis tehtud toiminguid tee tagasi rahakotti.
5. Kui märkad pangaautomaadi küljes midagi ebatavalist, näiteks liimijälgi kaardipilu juures või seda, et klaviatuur on ebatavalise kujuga, siis hoidu kaardi sisestamisest ning võta kohe ühendust pangaga.
6. Teavita kaotatud või varastatud kaardist kohe panka. Osade pankade mobiiliäpis on võimalik ka ise kaart ajutiselt sulgeda ja selle ülesleidmisel taas avada. Kui kohe kaardi sulged, väheneb oluliselt võimalus, et keegi saab omavolitseda sinu pangakontol oleva rahaga.

3. Nutitelefon ja turvalisus

1. Võimalusel seadista oma telefon nii, et selle kaotamisel oleks võimalik ka distantsilt telefoni sisu kustutada.
2. Tõmba oma telefoni äppe ainult telefonitootja poolt turvatud ametlikust äpi-poest.
3. Turva oma nutitelefon PIN-koodi või salasõnaga. Kasuta seadistust, mis ei kuva PIN-koodi sisestamisel ekraanile.
4. Ära vali telefoni PIN-koodiks iseenda või pereliikme sünnipäeva või muud lihtsalt ära arvatavat numbrit.
5. Kui kasutasid panka mobiiliäpiga ja nutitelefon kadus või varastati ära, teavita sellest ka panka.
6. Kui *wifit*, *bluetooth'i* ja *NFC'd* ei ole parajasti vaja, lülita need välja. Lisaks turvalisuse suurendamisele aitab see hoida ka telefoni akut.
7. Uuenda oma telefoni tarkvara regulaarselt ning paigalda alati kõige värskemad turvauuendused.
8. Kaalu telefoni välja vahetamist, kui telefoni tootja ei väljasta enam Sinu seadmele turvauuendusi. Aegunud tarkvara ja turvaseadistustega telefonidega ei pruugi
9. ühel hetkel olla enam võimalik ka pangateenuseid kasutada.

4. Turvalised autentimisvahendid

1. Mobiil-ID ja Smart-ID PIN-koode tohib sisesta vaid oma telefoni vastavas rakenduses! Teenusepakkujate ja pankade kodulehtedel ei küsita kunagi Mobiil-ID ega Smart-ID PIN-koodi.
2. Mobiil-ID ja Smart-ID kasutamisel jälgi alati, et telefonis enne kinnitamist näidatav kontrollkood vastaks interneti- või mobiilipanga lehel kuvatud koodile.
3. Mobiil-ID ja Smart-ID kasutamisel veendu alati, mis toimingut sa kinnitad: telefoni ekraanil on näha nii teenuse nimetus kui lühike toimingu kirjeldus. Kui sa ei ole kindel toimingu õigsuses, ära PIN-koodi sisesta!
4. Juhul, kui sa ei ole tehingut algatanud, kuid saad Mobiil-ID või Smart-ID parooli küsiva teavituse, ära kunagi sisesta oma PIN-koodi! Tõenäoliselt on tegemist kas pettuskatse või teise kasutaja veaga oma kasutajanime sisestamisel.
5. Smart-ID iseteenindusportaalis on võimalik näha ning vajadusel sulgeda oma kehtivaid Smart-ID lepinguid. Aeg-ajalt oleks mõistlik oma Smart-ID lepingutel silma peal hoida. Kahtlaste lepingute leidmisel tasuks kindlasti pöörduda Sertifitseerimiskeskuse või politsei poole.
7. ID-kaardi kaotamise või varguse(kahtluse) korral helista kohe ID-kaardi abiliinile 1777. Alustuseks peata sertifikaadid – siis ei saa keegi Sinu kaarti elektrooniliselt kasutada. Sulge kaart lõplikult, kui oled selle kadumises veendunud.
8. Kui kasutad Mobiil-IDs, siis helista telefoni kaotuse või varguse korral kohe ka ID-kaardi abiliinile 1777. Alustuseks peata sertifikaadid – siis ei saa keegi Sinu Mobiil-IDd kasutada. Sulge Mobiil-ID lõplikult, kui oled telefoni kadumises veendunud.
9. Ära vali ID-kaardi, Mobiil-ID või ID-kaardi PIN-koodiks iseenda või pereliikme sünnipäeva või muud lihtsalt ära arvatavat numbrit.
10. Ära hoia ID-kaarti ja selle PIN koode samas sahtlis või rahakotis.
11. Ära hoida Mobiil-ID või Smart-ID PIN-koode telefonis lihtsalt leitavana kontaktide seas.

5. Suhtlus pangaga

1. Ära usalda pimesi e-kirju, mis näivad tulevat pangalt ja paluvad mingile lingile klikkida või panka sisenemiseks vajalikke paroole sisestada. Kui Sul on pangast saadud kirja osas vähimgi kahtlus, helista panga klienditoele.
2. Pangaga suheldes krüpteeri edastatavad delikaatsed dokumendid ning palu panga töötajal sulle saadetavad delikaatse sisuga dokumendid samuti krüpteerida Sinu ID-kaardiga avamiseks. ID-kaardi veebilehelt https://www.id.ee/index.php?id=36034 leiad info, kuidas seda teha. Nii tagad andmete turvalise edastuse ning isegi kui vale adressaat peaks Sulle mõeldud kirja saama, ei pääse ta ligi sellele lisatud krüpteeritud andmetele.
3. Ära avalda oma salasõnu, PIN-koode või pangakaardi täielikke andmeid, kui suhtled pangaga telefoni teel. Eriti pea seda silmas siis, kui räägid pangaga telefonitsi avalikus kohas.

6. Seadmete turvalisus

1. Jälgi, et su internetiga ühendatud seadmed (arvutid, nutitelefonid, tahvelarvutid, tolmuimejad, turvakaamerad jne) omaksid alati kõige uuemat tarkvara. Ära ignoreeri seadme meeldetuletusi uus tarkvara alla laadida ega lükka pikalt edasi uuendusi, mida seade palub teha.
2. Võimalusel kasuta viirusetõrje tarkvara (eriti Windows'i arvutites). Kui aga juba kasutad, siis jälgi, et tarkvara uueneks automaatselt. Viirusetõrje uueneb reeglina mitu korda päevas!
3. Loo oma arvutites eraldi ilma administraatoriõigusteta kasutajakontod igapäevakasutuseks. Tee oma igapäevatoiminguid (veebis surfamine, e-kirjad, dokumendid) tavakasutaja õigustes – nii väheneb risk, et keegi Sinu seadmetesse sisse häkib ja Su andmeid kurjasti kasutab. Kui leibkonnas on vähem kogenud arvutikasutajaid (eriti lapsed, eakamad inimesed), on nende puhul selle reegli järgimine eriti oluline!
4. Kui paigaldad oma arvutisse tarkvara, jälgi selle päritolu: kommertstarkvara lae alla ainult tootja ametlikult veebilehelt. Vaba tarkvara kasutades usalda vaid selliseid, mille lähtekood on avalik (*open source*). Väldi vahendajaid, kelle seos tootjaga pole selge.