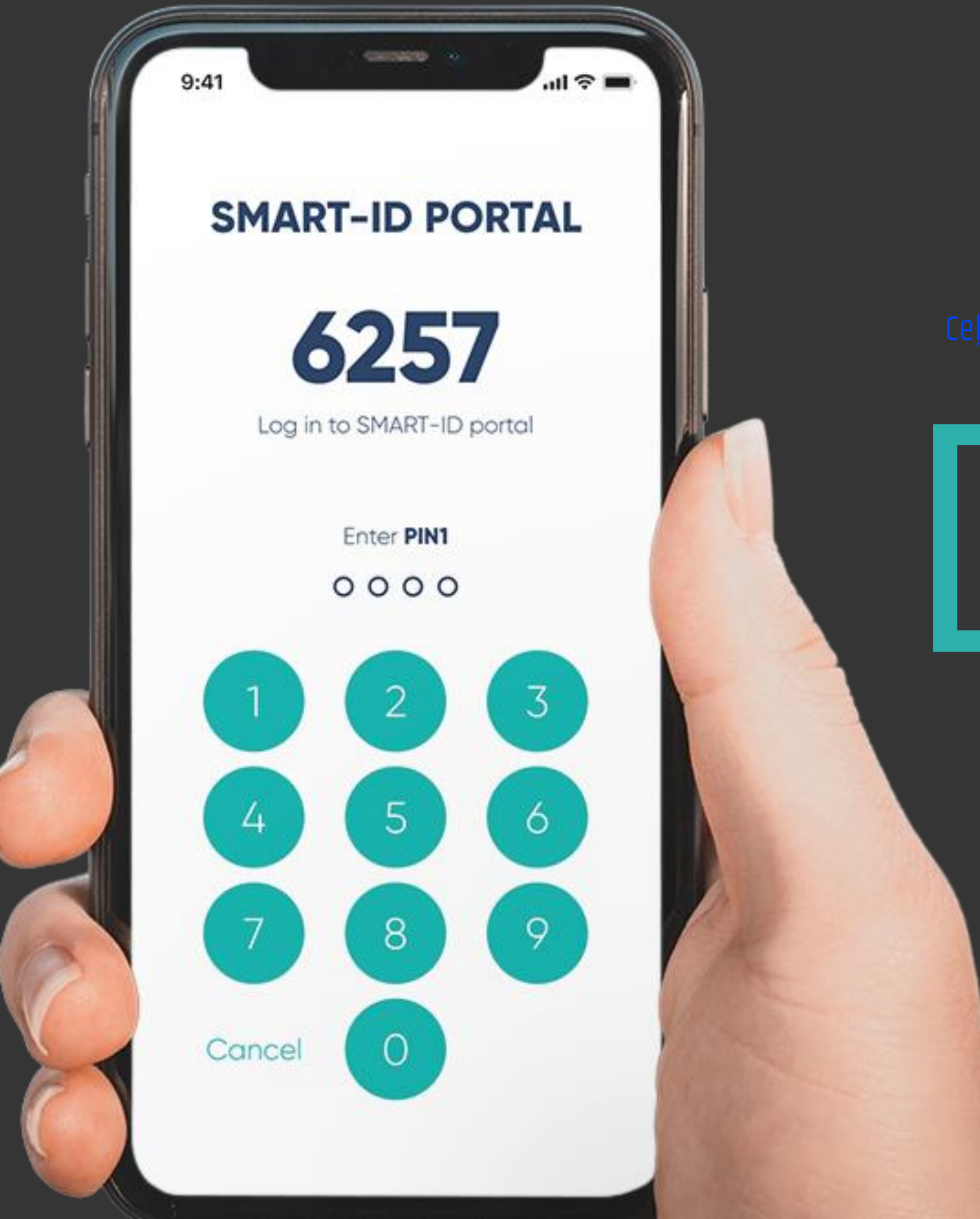


Celvedis jauniešiem, skolotājiem un vecākiem

TAVS DIGITĀLAIS ES

Šo materiālu sagatavoja digitālā
autentifikācijas rīka Smart-ID izstrādātājs SK ID
Solutions sadarbībā ar izglītības tehnoloģiju
uzņēmumu Datorium.



Materiāls ir veidots kā **palīgs skolotājiem sarunām mācību stundās** par jauniešu uzvedību digitālā vidē, savu datu drošu lietošanu un savas personības apliecināšanu.

Materiālā apkopotā informācija ir noderīga arī **pašiem jauniešiem** savu zināšanu un uzvedības pārbaudei, kā arī **vecākiem - pārrunājot ģimenē** digitālās identitātes drošu izmantošanu.

Šajā materiālā ietvertie piemēri, balstās uz **Smart-ID pieredzi, jo to lieto 78% jauniešu vecumā** no 16-19 gadiem. Tomēr drošības pamatprincipi, kodu apstiprināšana un citas nianse ir attiecināmas arī uz citiem autentifikācijas rīkiem.

Padomi balstās arī uz izglītības tehnoloģiju uzņēmuma **Datorium novērojumiem mācību stundās** par jauniešu zināšanām, uzvedību un attieksmi pret digitālajiem datiem.

KAS IR SMART-ID UN CITI AUTENTIFIKĀCIJAS RĪKI?

Smart-ID ir vienkāršs, drošs un ātrs veids, kā identificēt sevi tiešsaistē, reģistrēties e-pakalpojumu saņemšanai un parakstīt dokumentus.

Smart-ID darbojas saskaņā ar dubultās atpazīšanas principu: lietotājs tiek atpazīts pēc viedierīces (piemēram, mobilā tālruņa, kas lietotājam pieder) un PIN kodiem.

Atceries! Smart-ID un citi autentifikācijas rīki ir tikpat nozīmīgi kā Tava pase, pirkstu nospiedumi vai paraksts. Tie pieder tikai Tev! Izturies pret tiem rūpīgi, nedalies, nelieto pavirši!



AR KO **PIN1** ATŠKIRAS NO **PIN2**?

- **PIN1** izmanto, lai noteiktu personas identitāti: piemēram, piekļūstot e-pakalpojumam, PIN1 pierāda, ka **tu esi tu**.
- **PIN1** kods sastāv no **vismaz četriem** cipariem.
- Pirms ievadi savu **PIN1 - salīdzini** vai drošības kods ekrānā sakrīt ar pakalpojuma sniedzēja norādīto!



PIN1 jeb drošības kods nr. 1 ir Tavas digitālās identitātes apliecinājums. Tas ir kā Tava pase, kuru Tu uzrādi, lai apliecinātu, ka Tu esi Tu. Jeb atslēga uz Tavu māju! **To lieto tikai Tu, nedalies ar citiem un pārliedzies, vai durvis, kuras grasies atslēgt vispār ir Tavas durvis.**

AR KO **PIN1** ATŠKIRAS NO **PIN2**?

- **PIN2** izmanto, lai **apstiprinātu darījumu**, piemēram, naudas pārskaitījumu vai lietotu kā elektronisko parakstu.
- **PIN2** kods sastāv no **vismaz pieciem** cipariem.
- Pirms ievadi **PIN2 - pārliecinies**, ka drošības kods ekrānā sakrīt ar pakalpojuma sniedzēja norādīto!
- **Pēc PIN2 ievadīšanas transakcija jeb darījums kļūst neatgriezenisks!**



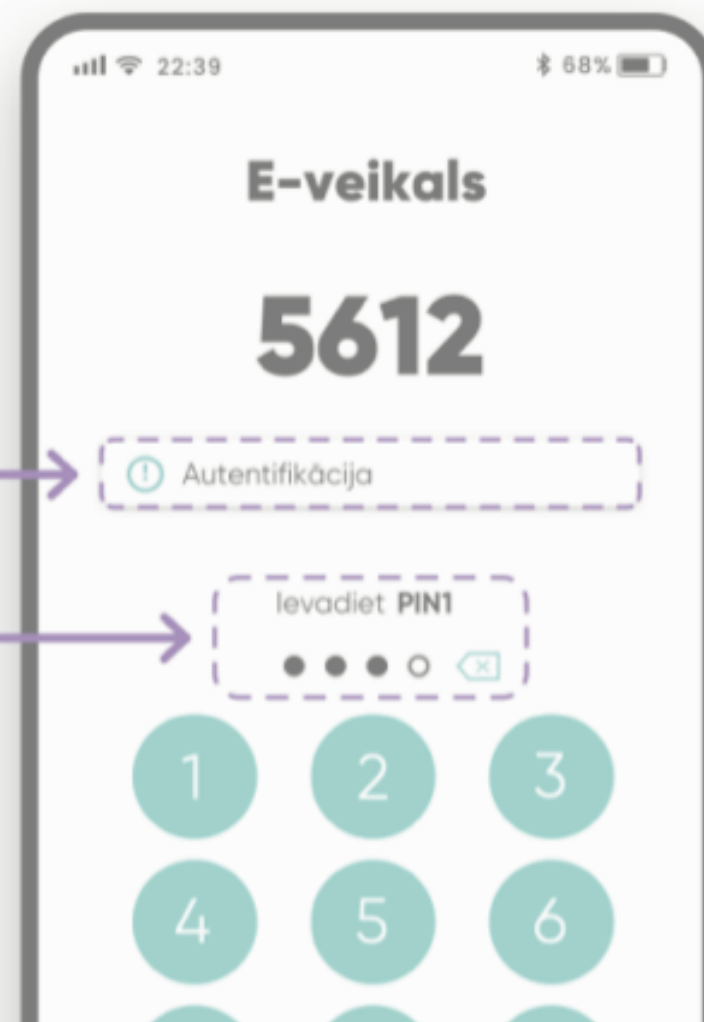
PIN2 jeb drošības kods nr. 2 ir Tavas digitālās paraksts. Izmantojot to, Tu apliecini, ka piekrīti darījumam, noteikumiem vai darbībai, kuru veic. Līdzīgi kā parakstot dokumentus, arī lietojot PIN2, **pārliecinies KO Tu paraksti!** Vai Tu vispār grib parakstīt tādu dokumentu, dot tādu atļauju, vai atpazīsti to. **Nekad nelieto PIN2 steigā un neiedziļinoties.**



PIN1

Ar PIN1 tu pierādi,
ka tieši tu konkrētā brīdī
esi internetā.

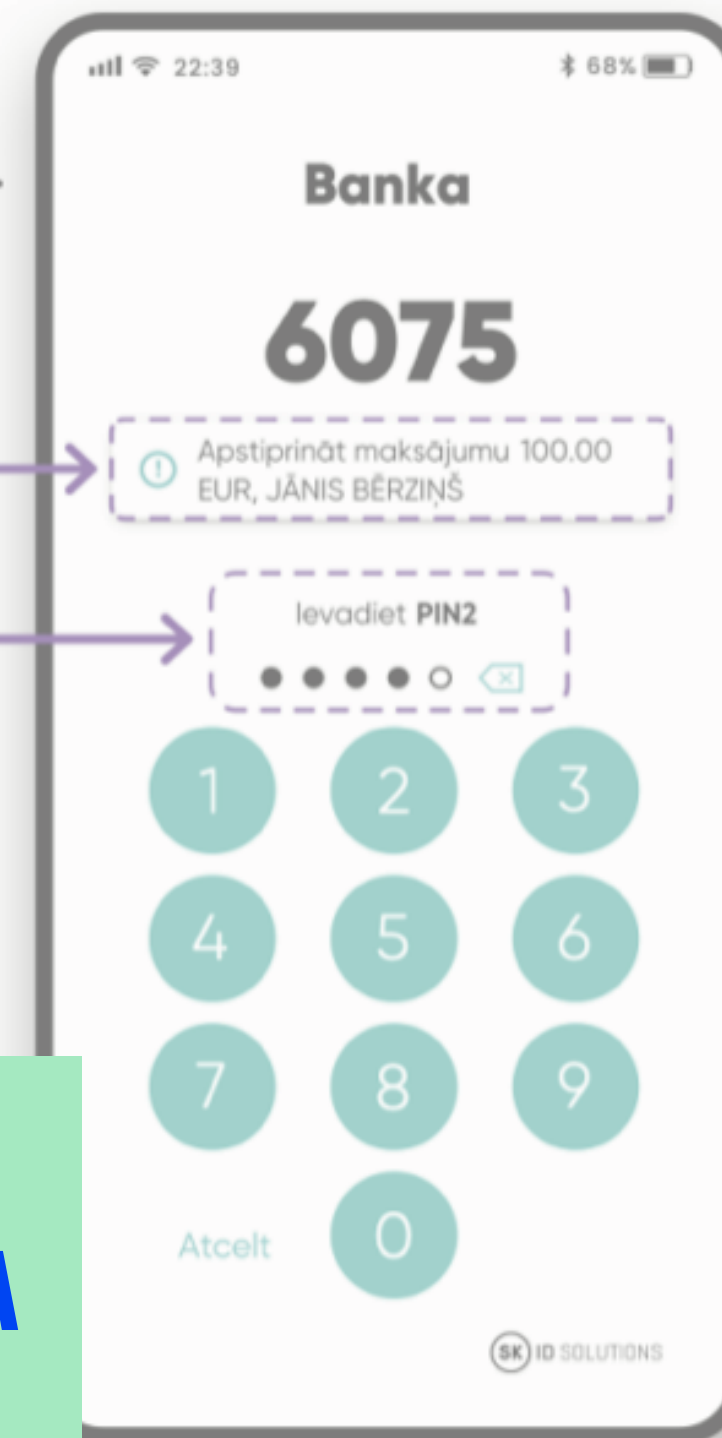
PIN1 kodā ir vismaz 4 cipari.



PIN2

Ar PIN2 tu apstiprini darījumu.
Piemēram, naudas pārskaitījumu.

PIN2 kodā ir vismaz 5 cipari.



**ŅEM VERĀ! VEICOT DARĪJUMUS VAI PIRKUMUS AR
BANKAS KARTI E-VEIKALOS, DAŽREIZ BŪS JĀIEVADA
TIKAI PIN2!**

PIN1 ir tava pazīšanās zīme internetā līdzīgi kā pase.

Pēc PIN2 ievadišanas darījumu atcelt vairs nevar!

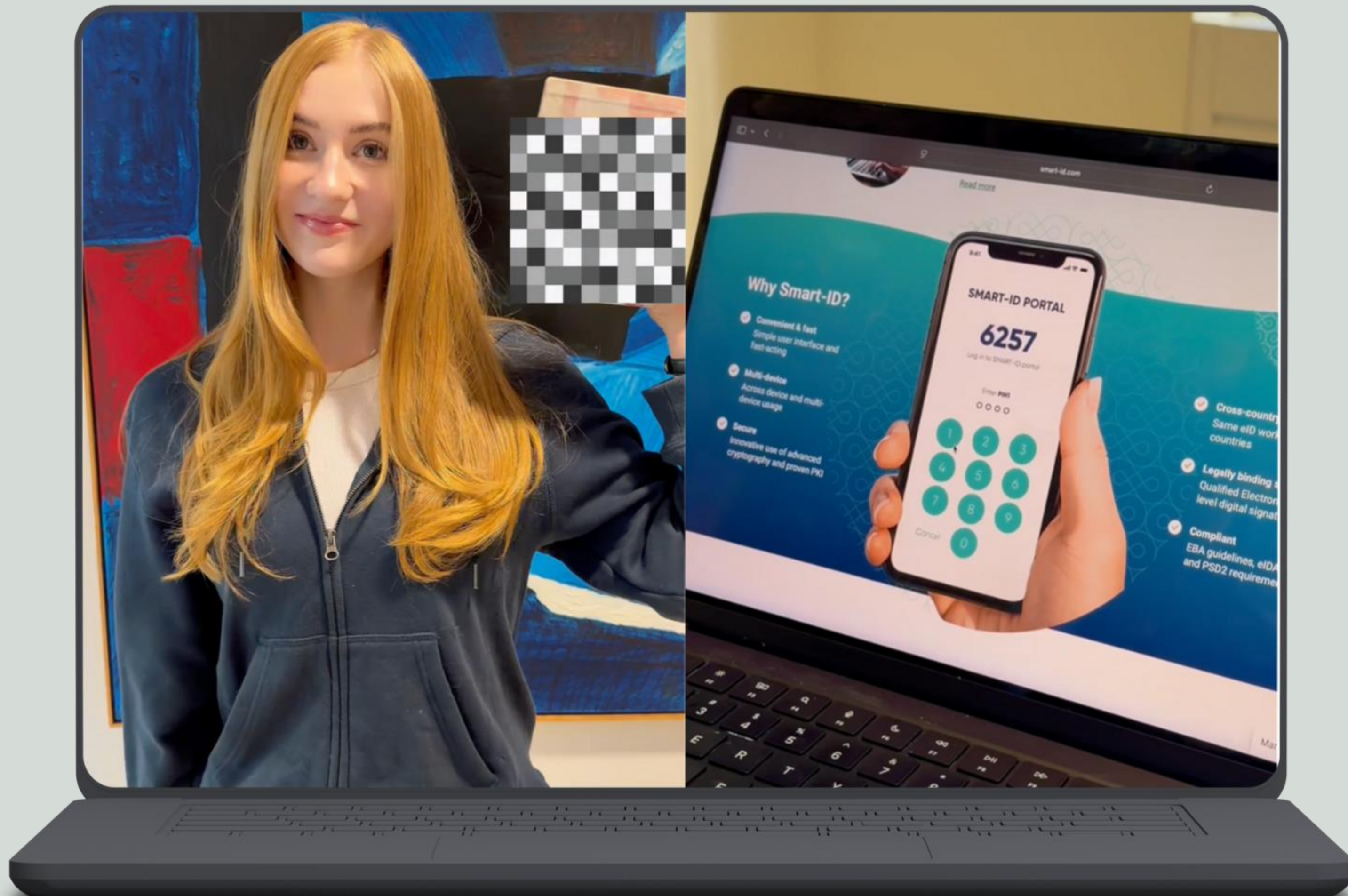
Visbiežāk jaunieši digitālās identitātes risinājumus izmanto, lai:

- V** iepirktos tiešsaistē – 82,7%,
- V** izmantotu finanšu pakalpojumus – 76,2%,
- V** skatītos izklaides platformas (filmas, mūziku, sportu) – 68,3%,
- V** spēlētu videospēles – 63,9%,
- V** piekļūtu e-veselības un mobilitātes pakalpojumiem – 28,2%,
- V** apmaksātu rēķinus – 25,7%.

KO DIGITĀLĀ PASAULĒ DARI TU?

Lai veiktu šos darījumus, būs nepieciešams apliecināt savu identitāti un apstiprināt darījumu!
Tāpēc dari to droši!

IESKATIES, KO **EVELĪNA PĀRKERE** IR NOVĒROJUSI UN IESAKA TEV, **LAI TU PASARGĀTU SEVI UN SAVU DIGITĀLO ES!**



LIETOJOT SMART-ID, NEAIZMIRSTI PĀRBAUDĪT:

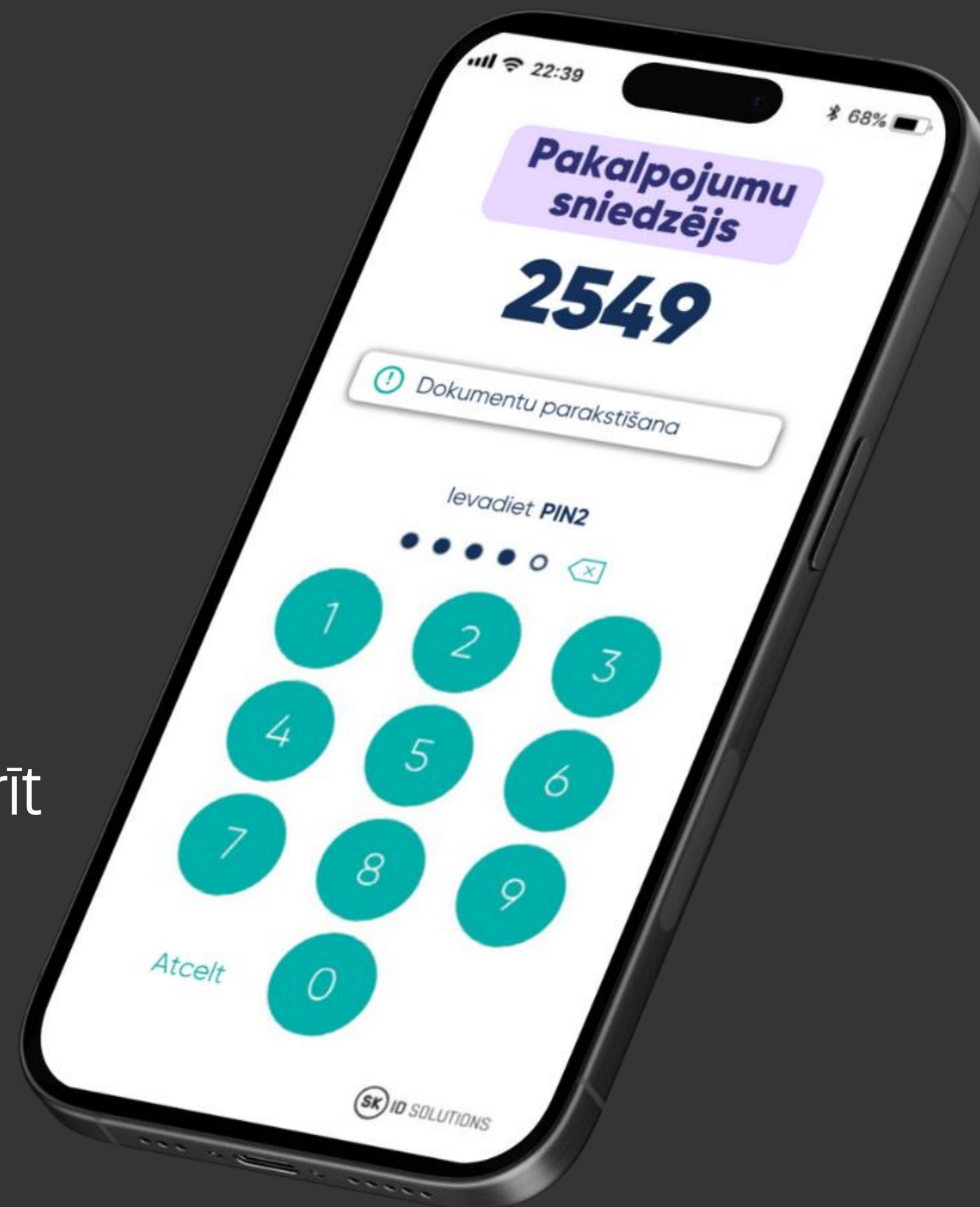
1. Vai tiešām esi uzsācis šo darījumu?

Ikdienas steigā nereti veicam darbības automātiski. Tomēr jautājumos, kas skar naudu, noteikti pārliedzinies, ka šo darījumu tiešām esi uzsācis Tu pats.

2. Vai pakalpojuma sniedzēja nosaukums vai naudas saņēmēja vārds un uzvārds ir īstais?

Pārliedzinies, vai pakalpojumu sniedzēja nosaukums, kura vietnē mēģini autentificēties vai saņemt pakalpojumus, sakrīt ar to, ko redzi lietotnē. Tas pats attiecas uz gadījumiem, kad vēlies pārskaitīt naudu kādam cilvēkam.

Ja informācija nesakrīt, atcel darījumu !!



LIETOJOT SMART-ID, NEAIZMIRSTI PĀRBAUDĪT:

3. Maksājumu jeb darījuma veidu

Nesteidzies un apskaties, kādu darbību veiksi: vai tā ir pieslēgšanās internetbankai, maksājuma apstiprināšana vai dokumenta parakstīšana ar elektronisko parakstu.



4. Maksājuma jeb darījuma summu

Tu taču nevēlētos 10 eiro vietā nejauši pārskatīt citai personai 100 vai 1000 eiro, vai ne? Arī šajā solī, apstiprinot darījumu ar PIN2, pievērs papildu uzmanību tam, cik liela ir darījuma summa.

Ja informācija nesakrīt, atcel darījumu !!

LIETOJOT SMART-ID, NEAIZMIRSTI PĀRBAUDĪT:

5. Vai maksājums jeb darījums ir veiksmīgi pabeigts

Noslēgumā pārliedzinies, ka viss ir kārtībā un ka pakalpojuma sniedzējs ir saņēmis apstiprinājumu. Visbiežāk tas tiek attēlots pakalpojuma sniedzēja vietnē. Pakalpojums var neizdoties tehnisku iemeslu dēļ, piemēram, vāja interneta signāla dēļ.



6. Vai netiek prasītas papildu darbības

Dažreiz e-pakalpojumu sniedzēji papildu drošībai ievieš arī t. s. “trīs kodu risinājumu”. Tas paredz, ka viedierīcē parādīsies papildu apstiprinājuma logs, kurā no trim kodiem vajadzēs izvēlēties pareizo jeb to, kas parādīts pakalpojuma sniedzēja vietnē.

2025. gadā Smart-ID ievieša kvadrātkodu reģistrācijas iespējas. QR koda izmantošana palielinās Tavu digitālo drošību! Šobrīd to pamazām ievieš arī bankas, internetveikali un citi pakalpojumu sniedzēji.



Ar Smart-ID+ piekļuve e-pakalpojumiem ir vēl vienkāršāka:
V vienkārši noskenē QR kodu,
V ievadi savu slepeno PIN1 kodu, un esi gatavs darbam.

V Nav nepieciešams ievadīt personas kodu vai salīdzināt apstiprinājuma kodus.

V Šis vienkāršotais process ne tikai ietaupa laiku, bet arī ievērojami apgrūtina pikšķerēšanu un citus uzbrukumus.

V Lai aizsargātu savu digitālo identitāti pret jaunām apdraudējumu formām, Smart-ID+ atbalsta visus jaunākos kriptogrāfiskos standartus.

VIENMĒR IEVĒRO ŠOS NOTEIKUMUS!

1

Neapstiprini darījumus automātiski!

Ja pats neesi uzsācis darījumu, bet tālrunī saņēmi pieprasījumu ievadīt PIN kodu, nedari to! Visticamāk, kāds krāpnieks mēģina ar taviem datiem piekļūt kādam pakalpojumam.

2

Neizpauž Smart-ID PIN kodus!

Savus personīgos PIN kodus turi slepenībā. Nenodod tos citiem cilvēkiem, pat ģimenes locekļiem. Iegaumē savus PIN kodus, jo tie netiek glabāti un tos nevar "atgādināt", ja būsi aizmirsis.

3

Neatstāj savu viedtālruni bez uzraudzības!

Papildu drošībai izmanto viedtālruņa ekrāna bloķēšanas iespēju, kas ir pieejama visos viedtālruņos.

4

Neaizmirsti regulāri atjaunināt lietotni!

Izmanto aplikācijas jaunāko versiju, lai pasargātu sevi no drošības apdraudējumiem. Regulāri to atjauno, izmantojot automātiskos atjauninājumus.

5

Neuzticies visām vietnēm!

Pārliecinies, ka pakalpojuma sniedzējs ir īsts. Šķietami nenožīmīgas nianšes kā pareizrakstības kļūdas, neprecīza uzņēmuma informācija, rekvizīti, domēna nosaukums var liecināt, ka vietne nav droša. Apmaksā pirkumus tikai tādās vietnēs, kur domēns sākas ar HTTPS.

UN ARĪ ŠOS NOTEIKUMUS...

1. Izmanto drošas un atšķirīgas paroles.

- Vislabāk ļauj sistēmai ģenerēt paroli.
- Maini tās regulāri.
- Neizmanto paroles, kuras satur Tavus personīgos datus, intereses vai ir saistītas ar Taviem hobijiem, mājdzīvniekiem un citām personīgām lietām. Hakeri tās var viegli uzminēt.
- Neizmanto vienu un to pašu paroli vairākām vietnēm!

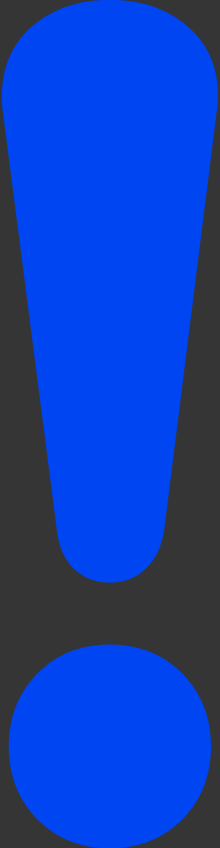
2. Ja izmanto skolas vai citu publiski pieejamu datoru:

- Centies nepieslēgties vietnēm ar saviem datiem
- Ja tomēr esi pieslēdzies - vienmēr, beidzot darbu, atslēdzies un pārlicinies, ka esi to izdarījis.
- Pametot datoru pat uz pavisam īsu pauzi, pārlicinies, ka citi nevar piekļūt Tavām vietnēm.
- Ja lieto bezmaksas publiski pieejamu wi-fi tīklu, piemēram, tirdzniecības centros, kafejnīcās u.c., esi īpaši uzmanīgs, nepieslēdzies svarīgām vietnēm.
- Pārlicinieties, ka Tavu datora vai telefona ekrānu neredz nevēlamas personas, un pieskatiet savu viedierīci, lai tā nenonāktu nepareizās rokās.

3. Nekad neizpauļ savus digitālos datus

- Telefonsarunās ar šķietamiem policijas, bankas vai citas valsts iestādes pārstāvjiem. Viņi NEKAD Tev neprasīs šādus datus!
- Neiesaisties darījumos, kuri prasa Tavus datus un kurus ierosina kāds cits, pat ja tas ir Tavs draugs. Piemēram, neveic pārskaitījumu nezināmiem cilvēkiem, pat ja to lūdz Tev labi pazīstams cilvēks. Neregistrējies vietnēs, par kurām neesi drošs, pat ja to lūdz Tavi draugi vai paziņas.

Tev varbūt liekas, ka šis ir elementārs ieteikums! Bet dati rāda, ka **tikai 10-20% jauniešu ievēro šo vienkāršo drošības prasību**. Realitātē - jaunieši lieto vienkāršas, viegli uzminamas paroles, tās maina reti, bieži vien tikai tad, kad to pieprasa sistēma, netiek izmantotas automātiski ģenerētas paroles. **Nepaslinko, esi digitāli drošs!**



Ja tomēr esi apstiprinājis kodu un veicis darījumu,
kad to nevēlējies, steidzami sazinies ar
banku un/vai policiju.

Savukārt, ja rodas aizdomas, ka vēl kāds zina tavus
Smart-ID PIN kodus, tev ir jāizdzēš savs Smart-ID
konts un jāizveido jauns ar citiem PIN kodiem.



PĀRBAUDI SAVAS ZINĀŠANAS, AIZPILDOT TESTU!



771 542 lietotāji Igaunijā



1 161 464 lietotāji Latvijā



1 775 508 lietotāji Lietuvā

PILDI TESTU ŠEIT!

VĒL VAIRĀK PAR DIGITĀLO IDENTITĀTI VARI UZZINĀT RESUME.LV VIDEO **EPIZODĒS “PAR IT AR SMART-ID”**.

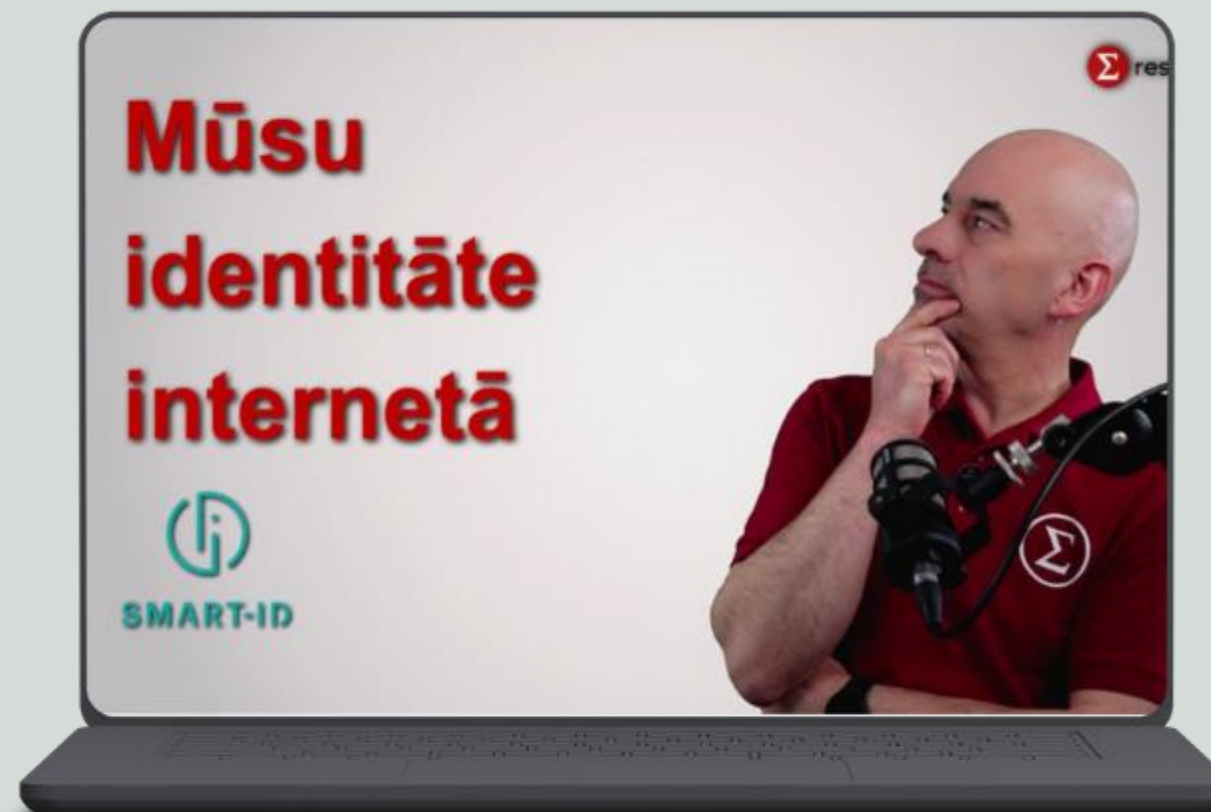
1. PAR **JAUNIEŠU UZVEDĪBU**
DIGITĀLAJĀ VIDĒ SKATIES RESUME.LV
RAIDIERAKSTĀ AR **DATORIUM**
VADĪTĀJU ANDŽELU.

[SKATIES ŠEIT!](#)



2. **IDENTITĀTES VEIDI UN DROŠĪBA**
INTERNETĀ. SARUNA IR IT DROŠĪBAS
EKSPERTU LAURI VĀVERI.

[SKATIES ŠEIT!](#)



3. **KĀ DARBOJAS KRĀPNIEKI?** SARUNA
AR CERT.LV KIBERDROŠĪBAS EKSPERTU
GINTU MĀKALNIETI.

[SKATIES ŠEIT!](#)

