Kā pasargāt sevi un savu naudu no krāpniekiem?

Materiāls vieglajā valodā



Naudas skola
LATVIJAS BANKA

Materiāls tapis Latvijas Bankas sadarbībā ar
Vieglās valodas aģentūru.

LATVIJAS BANKA
EIROSISTĒMA

vieglās
valodas
aģentūra

Naudas
skola

naudasskola.lv

Krāpnieki katru dienu turpina izkrāpt no cilvēkiem naudu.
Krāpniecība ir cilvēku mānīšana.
Krāpniecība ir noziegums.

Šajā bukletā uzzini:

- Kā pazīt krāpnieku?
- Kā pasargāt savus personas datus, bankas datus un naudu no krāpnieka?

Bukleta beigās ir daži uzdevumi.
Tie ļaus nostiprināt iegūtās zināšanas.

Ko krāpnieks grib dabūt?

- **Tavu naudu.**
- **Pieeju tavam bankas kontam.**

Piemēram, internetbankas lietotāja numuru, kartes numuru, kartes PIN kodu, konta numuru, Smart-ID kodus.

Tas ir PIN 1 un PIN 2 kods.

Internetbankas lietotāja numuru sauc arī par lietotāja ID numuru.

- **Tavus personas datus.**

Personas dati ir tavs vārds, uzvārds,
personas kods un cita svarīga informācija par tevi.

Krāpnieks var izmantot šo informāciju sev par labu.

Piemēram, tavā vārdā aizņemties naudu bankā vai līdzīgā iestādē.

Kā pasargāt savu naudu?
Kā pasargāt savus personas datus?

- **Pārtrauc sarunu,**
  ja tev zvana svešinieks.
  Svešinieks var būt krāpnieks.
- **Neuzticies viltus ziņām!**
  Banka, policija, tiesa, pasts, slimnīcas un veselības centri nekad tev e-pastā, īsziņā vai pa telefonu neprasīs:
  - internetbankas lietotāja numuru;
  - bankas kartes numuru, bankas kartes drošības kodu;
  - bankas kartes PIN kodu;
  - konta numuru;
  - Smart-ID kodus.
- **Apstiprini ar Smart-ID PIN 1 un PIN 2 kodiem tikai tādus darījumus, kurus veic tu pats!**

- **Izmanto banku piedāvātos drošības risinājumus!**
  Piemēram, banka tev piedāvā samazināt limitus maksājumiem vai skaidrās naudas izņemšanai.
  Tu vari sadalīt savu naudu bankā vairākos kontos.
  Lielāko daļu naudas drošāk glabāt tādā bankas kontā, kura lietošanai tev nav bankas kartes.
- **Drošus internetbankas pakalpojumus var veikt banku filiālēs.**
  Izvairies lietot internetbanku ārpus mājām!
- **Nelieto internetbankas pakalpojumus citu cilvēku ierīcēs un publiskās vietās.**
  Datora programmas var saglabāt tavus datus.
- **Neļauj nevienam svešiniekam attālināti pieslēgties**
  tavam datoram, planšetei vai mobilajam telefonam.

  Nepiekrīti savā datorā, planšetē vai mobilajā telefonā uzlikt nezināmas programmas vai aplikācijas.
- **Vienmēr bloķē datora, planšetes un mobilā telefona ekrānu,**

  kad beidz lietot savu ierīci.

  Piemēram, bloķēt ekrānu tu vari ar tikai sev zināmu paroli.
- **Regulāri atjauno savu ierīču programmatūru.**

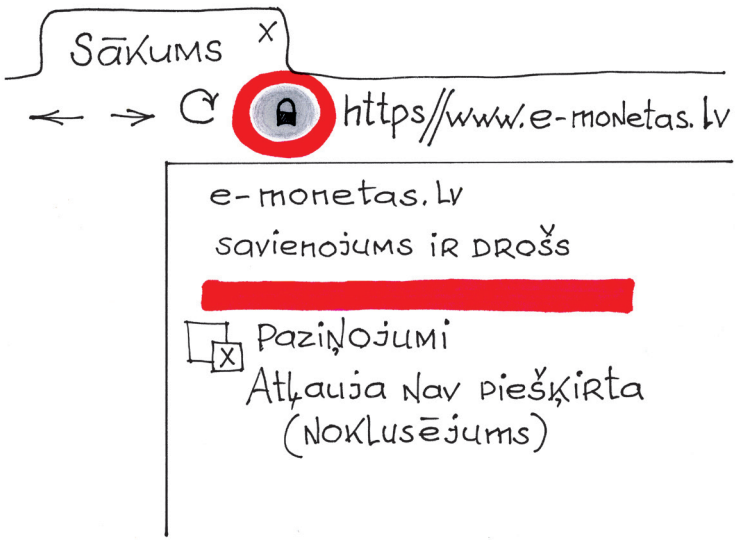
  Tas neļaus krāpniekam nozagt informāciju no tavas ierīces.

Tās ir programmas datorā vai mobilajā telefonā, kas ļauj droši saglabāt tavas paroles un lietotāja vārdus.

Sameklē informāciju internetā vai palūdz kādam no ģimenes, lai palīdz tev atjaunot tavu ierīču programmatūru.

- **Drošu mājas lapu var pazīt pēc:**

  – atslēgas simbola pie interneta adreses
  – nosaukuma pirmajiem burtiem https://



- **Ziņo savai bankai un policijai:**

  – par aizdomīgiem darījumiem ar tavu bankas kontu;

  – par aizdomīgiem svešiniekiem, kuri tevi uzrunā;

  – ja kāds svešinieks tevi jau piekrāpa.

- **Darījumiem internetā izmanto drošu paroli!**

  Drošā parolē ir vismaz 8 dažādas rakstu zīmes.

  Tie var būt lielie un mazie burti, cipari un simboli.

  Piemēram, zvaigznīte vai jautājuma zīme.

Drošas paroles veidošanas piemēri



Cilvēki mēdz izmantot parolēs sev tuvu cilvēku vai mājdzīvnieku vārdus, sev nozīmīgus datumus.
Taču šādas paroles nav drošas, jo tās var viegli uzminēt.
Drošības eksperti iesaka lietot paroles, ko grūti uzminēt.

Tādas paroles atcerēties ir grūtāk.
Labs palīgs ir īpaši paroļu pārvaldnieki.

Tās ir programmas datorā vai mobilajā telefonā,
kas ļauj droši saglabāt tavas paroles un lietotāja vārdus.

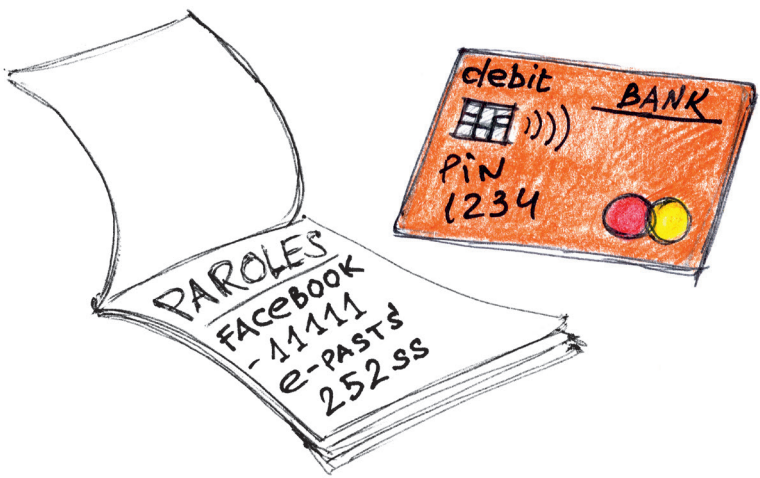
Sameklē informāciju internetā vai palūdz kādam no ģimenes,
lai palīdz tev apgūt paroļu pārvaldnieka programmu.

- **Nelieto vienu un to pašu paroli dažādiem mērķiem.**
  Piemēram, e-pastam, Facebook, Instagram u. c.

Nav droši:

- glabāt paroles un kodus savā piezīmju blociņā vai plānotājā;
- rakstīt bankas kartes PIN kodu uz bankas kartes;
- ielikt makā zīmīti ar bankas kartes PIN kodu;
- fotografēt un glabāt mobilajā telefonā drošības kodus un paroles;
- kādam sūtīt savus personas datus vai bankas kartes datus.

Nav droši!



Krāpnieciski telefona zvani

Svešinieki pa telefonu mēģina uzzināt tavus personas datus un dabūt tavu naudu.



- Tev piezvana svešinieks un izliekas par bankas, policijas vai pakalpojumu sniedzēja pārstāvi.
  Piemēram, par mobilo sakaru operatora pārstāvi.
- Krāpnieks bieži runā svešvalodā vai sliktā latviešu valodā.
- Svešinieks melo par aizdomīgu darījumu tavā bankas kontā.

  Svešinieks melo, ka tev ir nopietna problēma.

  Viņš uzbāzīgi piedāvā tev palīdzēt.

  Parasti svešinieks aicina tevi ieiet internetbankā ar taviem bankas datiem.
- Krāpnieks uzstājīgi piedāvā palīdzēt un mēģina dabūt no tevis pēc iespējas vairāk svarīgas informācijas.

  Piemēram, internetbankas lietotāja numuru, bankas kartes numuru, bankas kartes PIN kodu, konta numuru, Smart-ID kodus.

Kā sevi pasargāt?

- **Pārtrauc sarunu** ar svešinieku!
- Neatzvani uz numuru, no kura tev zvanīja.
- Sazvanies ar banku, policiju vai pakalpojumu sniedzēju, no kuras tev it kā zvanīja.

  Telefona numuru sameklē iestādes mājas lapā!

  Informē iestādi par saņemto zvanu!

  Sargā savu pieeju bankas kontam no svešiniekiem!

  Piemēram, internetbankas lietotāja numuru, bankas kartes numuru, bankas kartes PIN kodu, konta numuru, Smart-ID kodus.

  Nenosauc šādu informāciju svešiniekiem pa telefonu!
- Ziņo savai bankai un policijai:
  – par aizdomīgiem darījumiem ar tavu bankas kontu;
  – par aizdomīgiem svešiniekiem, kuri tevi uzrunā;
  – ja kāds svešinieks tevi jau piekrāpa.

Krāpnieciskas īsziņas

Krāpnieki tev sūta īsziņas uz mobilo telefonu.
Īsziņās viņi mēģina dabūt no tevis tavus personas datus un bankas datus.



- Krāpnieki īsziņās var aicināt tevi:
  - pieslēgties viltus mājas lapām;
  - ierakstīt mājas lapā tavus personas un bankas datus;
  - apstiprināt darījumu ar internetbankas pieeju;
  - apstiprināt darījumu ar informāciju par bankas karti.

- Šādas īsziņas parasti saņem uzreiz ļoti daudz cilvēku.

  Tu neatbildi uz īsziņu un nedari neko no īsziņā prasītā.

  Tad var gadīties, ka tev zvana cilvēks klientu apkalpošanas centra vārdā.

  Viņš pierunā tevi atvērt īsziņu un izdarīt īsziņā prasīto.

- Saite no īsziņas parasti ved uz viltus internetbanku.

  Tā izskatās ļoti līdzīga īstajai internetbankai.

  No šādas viltus internetbankas tava informācija uzreiz nokļūst pie krāpniekiem.

Kā sevi pasargāt?

- Neatver aizdomīgas īsziņas!
- Izdzēs aizdomīgās īsziņas un neatbildi uz tām!
- Sargā savu pieeju bankas kontam no svešiniekiem!

  Piemēram, internetbankas lietotāja numuru, bankas kartes numuru, bankas kartes PIN kodu, konta numuru, Smart-ID kodus.

  Nenosauc šādu informāciju svešiniekiem un neieraksti aizdomīgās mājas lapās!

- Sazvanies ar pakalpojumu sniedzēju, ja šaubies par saņemtās īsziņas patiesumu. Telefona numuru sameklē iestādes mājas lapā!
- Neļauj svešiniekiem uzlikt tavā datorā, planšetē vai mobilajā telefonā svešas programmas vai citu informāciju.

  Krāpnieku veidotās mājas lapās tev var nozagt personas datus, bankas datus un visu naudu!

- Ziņo savai bankai un policijai:
  - par aizdomīgiem darījumiem ar tavu bankas kontu;
  - par aizdomīgiem svešiniekiem, kuri tevi uzrunā;
  - ja kāds svešinieks tevi jau piekrāpa.

Krāpnieciska tavu datu izkrāpšana

Krāpnieks sūta ziņas uz tavu e-pastu.
Viņš mēģina dabūt tavus personas un bankas datus.

From: SEB Latvija <webmaster@salmalannoy.com>
To: [redacted]
Subject: Steidzami: mobilā tālruņa numurs nav apstiprināts

SIEB

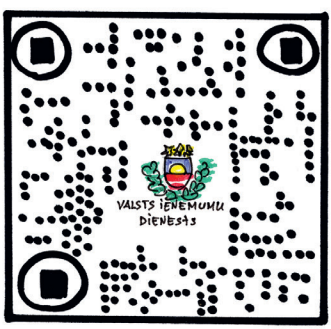
Cienījamais Klients [redacted]

Jūsu tālruņa numurs nav pārbaudīts, to varat apstiprināt, apmeklējot bankas filiāli. Vai arī varat tam piekļut tiešsaitē, izmantojot internetbanku.

Izmantojot internetbanku

Ja jums ir kādi jautājumi par mūsu pakalpojumiem vai produkti, lūdzu zvaniet mums uz bankas info tālruni 6708765

Konstitucijos ave. 24, LV-08105 Viļņa. Latvija
70440



- Krāpnieks sūta e-pastu labi pazīstama uzņēmuma vārdā.

  Piemēram, tavas bankas vārdā.

  E-pastā krāpnieks aicina steidzami atjaunot un apstiprināt tavus personas datus vai samaksāt rēķinu.

- Krāpnieka e-pasts izskatās ļoti līdzīgs īstajam. Krāpnieks tajā iekopē īsto uzņēmuma logo.

- E-pastā ir saite uz viltus mājas lapu.

  Mājas lapā krāpnieks tevi aicina apstiprināt maksājumu viltus internetbankā.

  Viltus internetbanka izskatās ļoti līdzīga īstajai internetbankai.

  No šādas viltus internetbankas tava informācija uzreiz nokļūst pie krāpniekiem.

Kā sevi pasargāt?

- Never vaļā aizdomīgus e-pastus!
- Neatver aizdomīgus e-pastiem pievienotos dokumentus un saites!
- Izdzēs aizdomīgus e-pastus un neatbildi uz tiem!
- Sazvanies ar uzņēmumu un noskaidro, vai tas tiešām sūta tev e-pastu. Telefona numuru sameklē uzņēmuma mājas lapā!
- Ziņo savai bankai un policijai:
  – par aizdomīgiem darījumiem ar tavu bankas kontu;
  – par aizdomīgiem svešiniekiem, kuri tevi uzrunā;
  – ja kāds svešinieks tevi jau piekrāpa.

Investīciju krāpšana

Tev piedāvā izdevīgi ieguldīt naudu.
Ieguldījums ļauj naudai pelnīt un palielināt uzkrāto naudu.

Ieguldījumus sauc arī par investīcijām.



- Parasti krāpnieki piedāvā nopirkt labi zināmu uzņēmumu akcijas, vērtspapīrus, fondus, zeltu vai kriptoaktīvus.

  Piemēram, visvairāk zināmi ir bitkoini.

- Investīciju krāpšana notiek viltus mājas lapās un sociālajos tīklos, kurus izveido paši krāpnieki.

- Krāpnieks piezvana bankas vai citas finanšu iestādes vārdā.
  Viņš piedāvā ieguldīt naudu un saņemt neticami lielu peļņu.
- Krāpnieks bieži runā svešvalodā vai sliktā latviešu valodā.
- Krāpnieks izmanto tavu pieredzes trūkumu un nelielās zināšanas par ieguldījumiem. Viņš kārdina ar iespēju ātri nopelnīt.
- Krāpnieks stāsta, ka darījums ir pilnīgi drošs un izdosies.
- Krāpnieks stāsta, ka pats labākais laiks ieguldīt naudu ir tieši tagad un steidzina tevi.
  Neļauj sevi steidzināt!
- Krāpnieki var tev rādīt viltus mājas lapu.

  Tajā var redzēt viltus informāciju par ieguldījumiem ar labu peļņu.
- Krāpnieks var aicināt tevi uzlikt datorā viltus programmu savu investīciju pārvaldīšanai.
- Krāpnieks var tev rādīt sabiedrībā pazīstamu cilvēku fotogrāfijas un melot par viņu iegūto peļņu.
- **Taču beigās tu nevari saņemt nopelnīto naudu.**
- **Tu zaudē arī visu savu ieguldīto naudu.**

Kā sevi pasargāt?

- Pārtrauc sarunu!
- Netici uzstājīgiem zvanītājiem pa telefonu!
- Sargā savu pieeju bankas kontam no svešiniekiem!

  Piemēram, internetbankas lietotāja numuru, bankas kartes numuru, bankas kartes PIN kodu, konta numuru, Smart-ID kodus.
- Nenosauc šādu informāciju svešiniekiem pa telefonu un neievadi aizdomīgās mājas lapās!

  Neļauj svešiniekiem uzlikt savā datorā svešas programmas vai citu informāciju.
  No šādas viltus mājas lapas tava informācija uzreiz nokļūst pie krāpniekiem.
- Pirms jebkura ieguldījuma pajautā savai bankai, vai tas ir droši.
- Pārbaudi Latvijas Bankas mājas lapā,
  vai krāpnieka nosauktajam uzņēmumam ir licence.
- Netici ieguldījumiem bez riska un ar lielu peļņu.
  Jebkurā ieguldījumā naudu var nopelnīt vai arī zaudēt.
- **Neaizņemies naudu, lai to ieguldītu nezināmā darījumā.**
- Ziņo savai bankai un policijai:
  - par aizdomīgiem darījumiem ar tavu bankas kontu;
  - par aizdomīgiem svešiniekiem, kuri tevi uzrunā;
  - ja kāds svešinieks tevi jau piekrāpa.

Vārdnīca

Bankas dati ir internetbankas lietotāja numurs, bankas kartes numurs, bankas kartes PIN kods, konta numurs, Smart-ID kodi, kodu kalkulators.

Bankas kartes PIN kods ir noteikta ciparu kombinācija.

Tavai bankas kartei kodu zini tikai tu, tas ļauj to pasargāt no citiem.

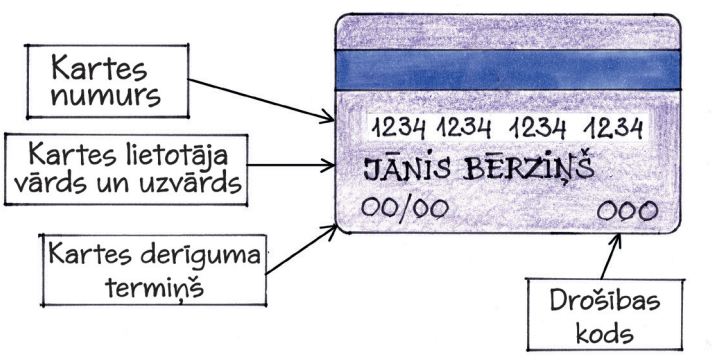
Bankas kartes PIN kods ļauj tev pierādīt sevi kā bankas kartes īpašnieku veikalā vai bankomātā.

Internetbankas lietotāja numurs.

To tev piešķir tava banka.

Kartes drošības kods ir 3 vai 4 ciparu kombinācija tavas bankas kartes otrajā pusē.

Šis drošības kods ļauj tev apstiprināt maksājumus ar karti.

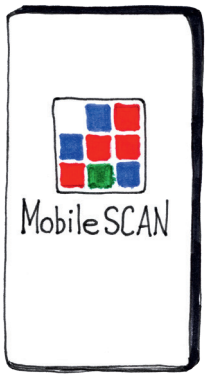


Kriptoaktīvi ir virtuāla nauda.

Piemēram, visvairāk zināmi ir bitkoini.

MobileSCAN ir bezmaksas autorizācijas ierīce Citadeles bankas mobilajā aplikācijā.

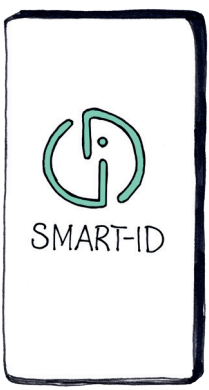
Tā ļauj attālināti tev pierādīt,
ka tieši tu konkrētā brīdī darbojies internetā.



Personas dati ir tavs vārds, uzvārds, personas kods un cita svarīga informācija par tevi.

Smart-ID ir bezmaksas mobilās ierīces programma.

Tā ļauj attālināti tev pierādīt,
ka tieši tu konkrētā brīdī darbojies internetā.



Smart-ID var būt tavā mobilajā telefonā
vai planšetē.

Vairāk par drošu Smart ID lietošanu lasi Latvijas Bankas mājas lapas sadaļā “Naudas skola”.

Padomus par digitālo drošību lietošanu var atrast internetā:

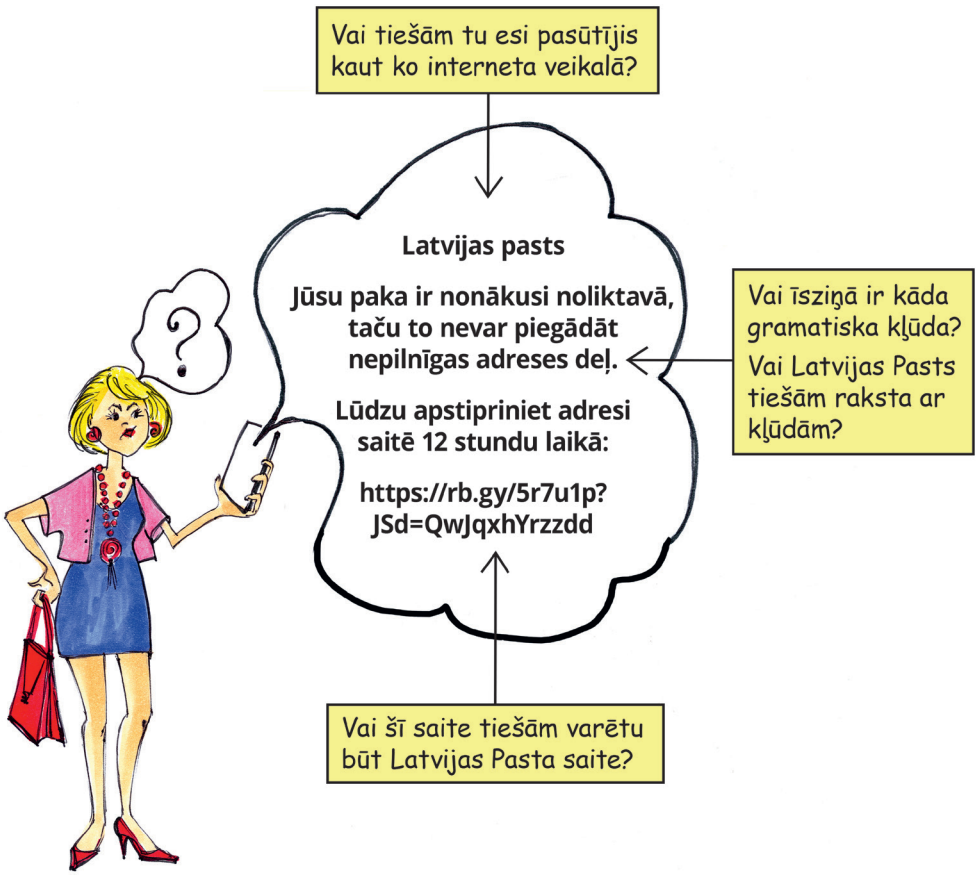
- **DROSSinternets.lv**
- **cert.lv**
- **https://dnsmuris.lv/**
- **neuzkeries.lv**
- **naudasskola.lv**

Sargā savus datus!
Tad arī tava nauda būs drošībā!

Nostiprini savas zināšanas!

1. uzdevums

Vēlreiz uzmanīgi aplūko šo attēlu!
Kā tu vari zināt, ka šo ziņu sūta krāpnieks?



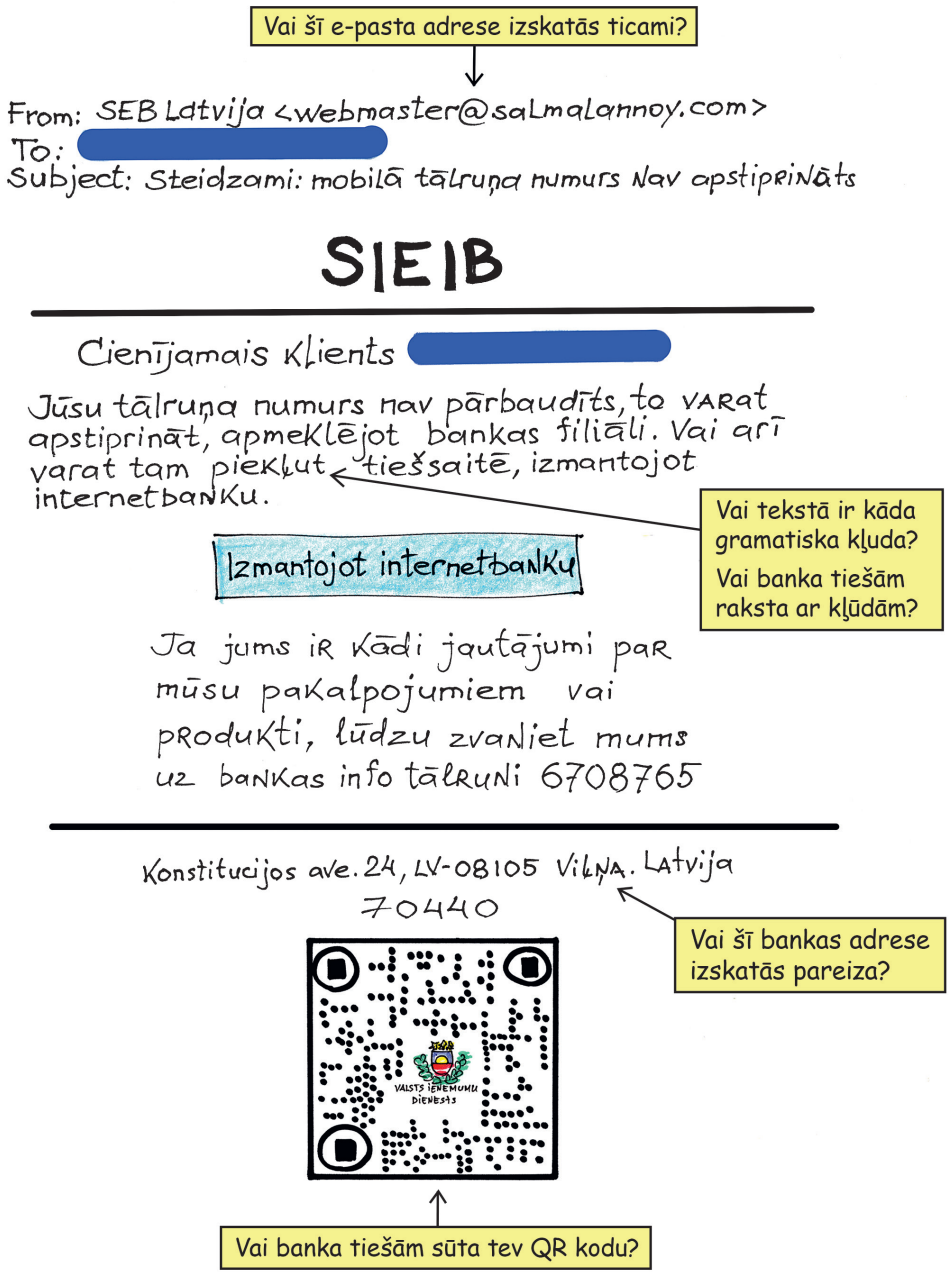
Kā rīkoties?

Zvani uz Latvijas Pastu pa publiski pieejamo tālruņa numuru.
Pārjautā, vai pasts sūtīja tev ziņu.

- Neatver atsūtīto saiti.
- Neatbildi uz īsziņu, izdzēs to.

2. uzdevums

Vēlreiz uzmanīgi aplūko šo attēlu!
Kā tu vari zināt, ka šo ziņu sūta krāpnieks?



Kā rīkoties?

- Sazinies ar banku pa publiski pieejamo telefona numuru.
  Pajautā, vai tiešām banka sūtīja tev ziņu.
  Neizmanto ziņā saņemto telefona numuru!
- Neskenē QR kodu.
- Sargā savus bankas datus no svešiniekiem!
  Nenosauc šādu informāciju svešiniekiem un neievadi aizdomīgās mājas lapās!

Ilustrācijas: **Zlata Ščerbakova**

Tava finanšu pratība sākas šeit!

Ienāc Latvijas Bankas “Naudas skolā”!
Tur atradīsi noderīgu informāciju un praktiskus padomus,
kā sakārtot savas naudas lietas.

www.naudasskola.lv



Kredīti



Drošība



Krāpšana



Budžeta plānošana



Apdrošināšana



Uzkrājumi



Ieguldījumi



Pensija



Klientu aizsardzība



Nauda un darījumi



Ilgtspējīgas finanses

LATVIJAS BANKA
EIROSISTĒMA

Naudas skola