



Kā atpazīt pikšķerēšanu

Uldis Lībietis
25.04.2023.



- Tēmas aktualitāte
- Kas ir pikšķerēšana
- Kāpēc pikšķerēt
- Vienmēr tālāk

The background features several abstract geometric shapes. A large beige shape is in the top-left corner. A yellow shape is in the top-right corner. A blue shape is in the bottom-right corner. A purple shape is in the bottom-left corner. A small beige shape is near the bottom center.

Cilvēks – vājākais posms kiberdrošībā

Mēs esam vareni, mēs esam bagāti

2021: zaudēti ~14,5M EUR
jeb vairāk nekā 270k EUR nedēļā

Arī 2022. gads sākās līdzvērtīgi, 111,3k EUR
pirmajās 3 dienās

2022: lietotāji krāpniekiem paši pārskaitījuši 12M EUR

Datu avots: Valsts policijas preses relīzes <https://www.vp.gov.lv/lv/jaunumi>

https://www.delfi.lv/bizness/bankas_un_finanses/latvijas-cetru-lielako-banku-klientiem-pern-izkrapti-12-04-miljoni-eiro.d?id=55122978



Kas ir pikšķerēšana

Kas ir sociālā inženierija?

Sociālā inženierija ir psiholoģisks un tehnisks process, kas tiek izmantots, lai manipulētu ar cilvēkiem



Mērķis:

iegūt informāciju vai likt veikt kādas darbības, ko citkārt persona nedarītu



Vides:

Sociālie tīkli, mājas lapas, mobilās lietotnes, e-pasts, SMS, WhatsApp, Telegram, Teams, arī balss zvani (voice phishing), krāpnieciskas reklāmas

Kas ir pikšķerēšana (phishing)?

**Pikšķerēšana ir sociālās inženierijas uzbrukuma veids,
kas ietver krāpniecisku ziņojumu sūtīšanu**



Mērķis:

iegūt informāciju vai likt veikt kādas darbības, ko citkārt persona nedarītu



Vides:

e-pasts, SMS, WhatsApp, Telegram, Teams, arī balss zvani (voice phishing)

Ko vēlas uzbrucēji

Piemēram, bet ne tikai:

Naudu

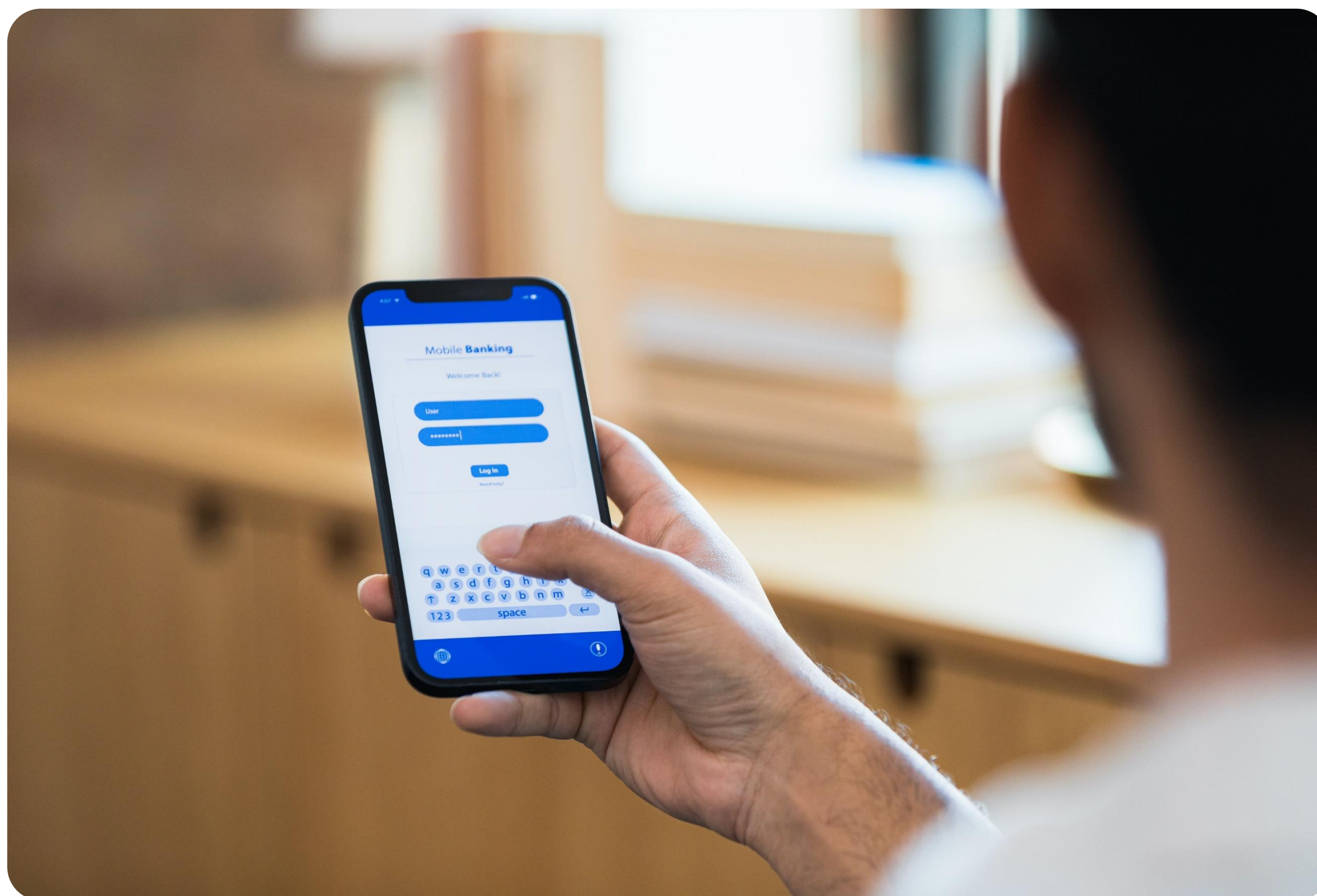
Piekļuvi datoram

Lietotājevārdus
un paroles

Informāciju

Kredītkartes numurus

Inficēt ar datorvīrusu



Mērķtiecīgs treniņš ir būtisks

Teorijas noklausīšanās neveido ieradumus

Organizācijas parasti grib:

- strādāt ātri & efektīvi
- 1 kibersdrošības kurss un 1-2 pikšķeri gadā

BET

Ieradumus veido tikai treniņš & atkārtojums



Kā sagatavoties

Testēšana nav iegāšana

Izveidojiet iespēju darbiniekiem ziņot par pikšķeri

Izvēlieties domēna vārdus testiem

Apmāciet darbiniekus, kā atpazīt un ziņot



Kā mēs to darām?

Burkānam jābūt līdzsvarā ar pātagu

E-pasts + lapa + lapa ar skaidrojumu

Radošs process

Darbības PĒC pikšķera ir pat svarīgākas
par pašu notikumu

Regulāri



Kā mēs to darām?

Burkānam jābūt līdzsvarā ar pātagu

Solīt – lidojumu kilometrus, prēmiju, jaunu datoru

Draudēt – atņemt datoru, bloķēt kontu*

Autoritāte – CEO, vadītāji un priekšnieki**



Kādi ir galvenie KPI?

Pusgads intensīva darba – un tad turpināt visu mūžu

2 galvenie KPI: datu ievade & Ziņošana


Nozares pieņemtais standarts – 5% datu ievade, sasniedzams ~ gada laikā

Pusgada laikā – samazinājums 5 reizes


Ziņošana – 1.5 reižu pieaugums



Kā mums izdodas?

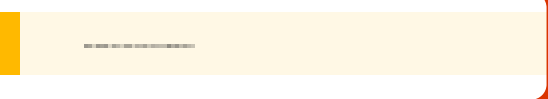



Uldis T <uldis.tatarcuks@tet-lv.lattelecom.ru>
To ✓ Kārlis Bergmanis

 This sender uldis.tatarcuks@tet-lv.lattelecom.ru is from outside your organization.

[Reply](#) [Reply All](#) [Forward](#)

otrd. 2022.





Jūs esat uzaicināts aizpildīt veidlapu **Kādus jaunus darba datus pirk?**, kas aizņems tikai 1 minūti. Lūdzu, iesniedziet savu atbildi līdz 28.07.2022.
Paldies!

<http://tet-lv.lattelecom.ru:443/forms?d=q3/p6un/z7gr0z/7>
Click or tap to follow link.

[Sākt tūlīt](#)

Jūs aizpildīsiet veidlapu, izmantojot pakalpojumu Microsoft Forms
[Noteikumi un nosacījumi](#) | [Konfidencialitātes politika](#)

Kā mums izdodas?



Hermes <hermes@palidziba.lattelekom.biz>

To  Kārlis Bergmanis



Reply



Reply All



Forward

piektd. 20.



This sender hermes@palidziba.lattelekom.biz is from outside your organization.



Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



TET DROŠĪBAS DAĻA: Šis e-pasts ir saņemts no droša sūtītāja.

Jums tika nosūtīts PD pieteikums Nr.284560 saskaņošanai

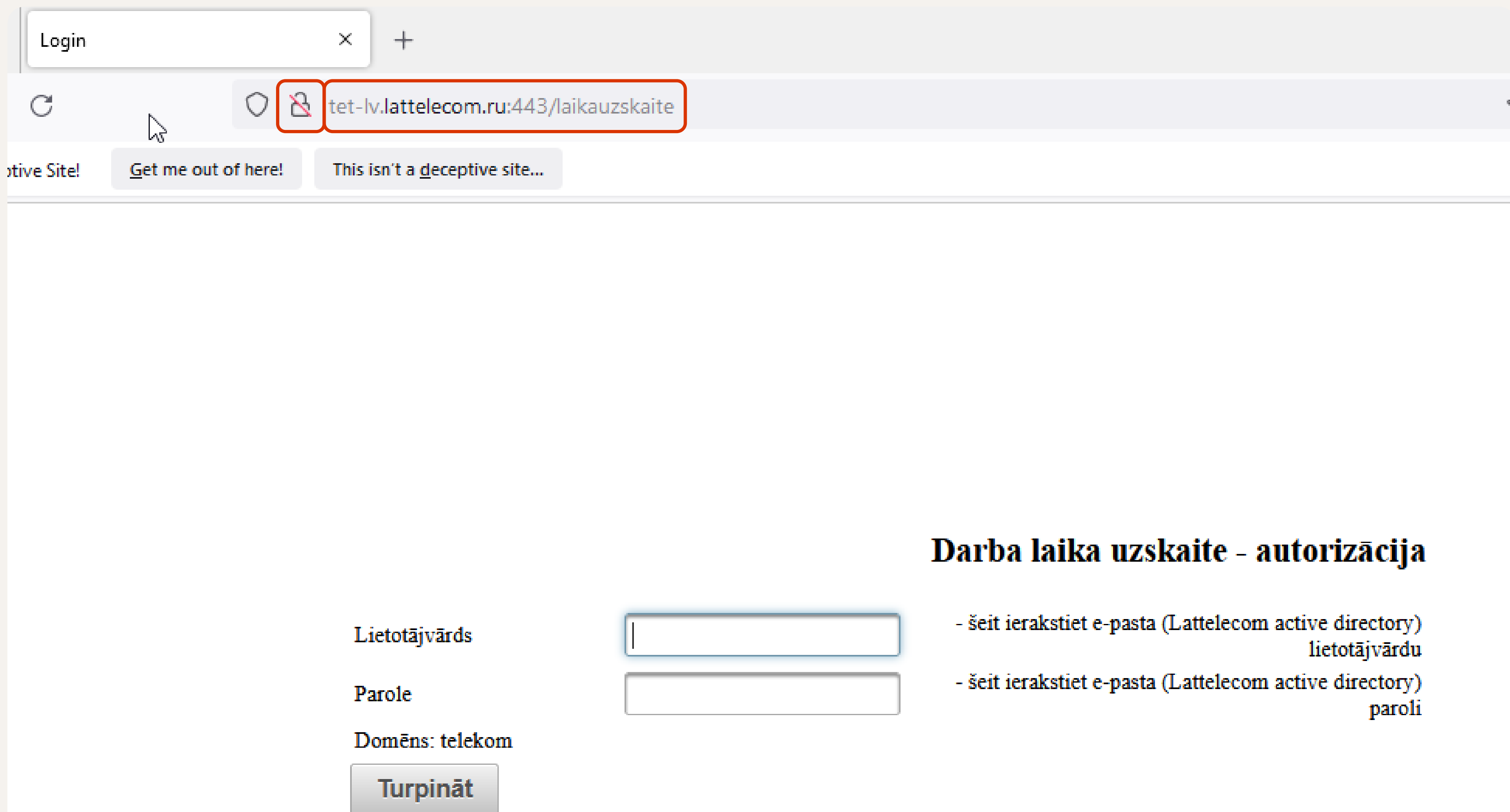
Spiediet uz zemāk norādīto saiti, lai atvērtu plānoto darbu:

<https://lasis.telekom.lv:8181/lasislogin/login.xhtml?open=HERMES&type=PD&ID=284560>

Ar cieņu,


Hermes (Produkcijas datu bāze)


Kā mums izdodas?



Kā mums izdodas?


BK

Biznesa Klientu Nodaļa <corporatecustomers@latekom.com>
To:  Kārlis Bergmanis

 This sender corporatecustomers@latekom.com is from outside your organization.

← Reply ← Reply All → Forward

otrd. 2022.



Labdien!

Jūs esat pievienots uzņēmuma TET SIA biznesa lietotāju sistēma, kas ļaus turpmākos lidojumus reģistrēt ātrāk un vieglāk, tikai norādot galamērķi un vēlamo lidojuma laiku!

Jums noteiktie limiti:

Lidojumu apjoms: **50 000 km/gadā**

Bagāžas klase: Bagāža Plus kas ietver, **1 soma 10kg + 1 soma 5kg**

Lidojuma klase: **Biznesa**

Kontu jāaktivizē līdz 31.12.2022:

<http://fileshare.latekom.com/korporativais-tet?d=q3/p8un/z7itzynm>
Click or tap to follow link.

Aktivizēt panākumus

Kā mums izdodas?

The screenshot shows a web browser window with the following elements:

- Browser Tab:** Labeled "Pieteikties" (Login).
- Address Bar:** Shows a "Not secure" warning and the URL "lietojumi.latekom.com:443/skola?Redirect=true&d=Q3%...".
- Language Selector:** Buttons for "LV" (Latvian) and "EN" (English).
- BDA Logo:** A red pixelated logo followed by the text "BDA".
- Navigation Menu:** Links for "KURSU GRAFIKS", "KURSU KATALOGS", "VIAA MĀCĪBAS PIEAUGUŠAJIEM", and "SISTĒMU TESTĒTĀJS".
- Left Sidebar:**
 - Par mums >
 - Mūsu pakalpojumi >
 - Autortiesības un preču zīmes >
- Main Content Area:**
 - Pieteikties** (Login) header with a user icon.
 - Text: "Lūdzu norādi savu epastu un paroli. [Reģistrējies](#), ja neesi kontu izveidojis jau agrāk."
 - Form fields for "Epasts" (Email) and "Parole" (Password).
 - Checkbox: "Nākošreiz pieteikties automātiski" (Log in automatically next time).
 - Pieteikties** (Login) button.
 - Links: "Aizmirsu paroli" (Forgot password).

Kā mums izdodas?

UZMANĪBU: piesakies TESLA 3 izlozei



TET darbiniekiem <darbiniekiem@lietojumi.latekom.com>

To Tīna Emīlija Gavare



This sender darbiniekiem@lietojumi.latekom.com is from outside your organization.



UZMANĪBU: Šis e-pasts ir saņemts no ārēja avota.

Laimē Bosa TESLA 3 arī Tu!

Esam priecīgi paziņot, ka domājot par saviem darbiniekiem, mainījām spēles noteikumus!

Tagad arī Tev ir iespēja piedalīties izlozē un ieripot vasarā ar jaunu elektroauto tikai aizpildot anketu.



Kā mums izdodas?

Pikšķerēšana iespējama ne tikai e-pastā – aptauja ar QR kodu



10:10 4G

tet

E-pasts:

Parole:

Pieteikties

AA Not Secure — tojumi.latekom.com

10:09 4G

tet

Kāds ir jūsu vecums?

Kādu kafiju birojā lietojat?

Vai kafijas kvalitāte apmierina?

Vai birojā vēlētos papīra krūzītes?

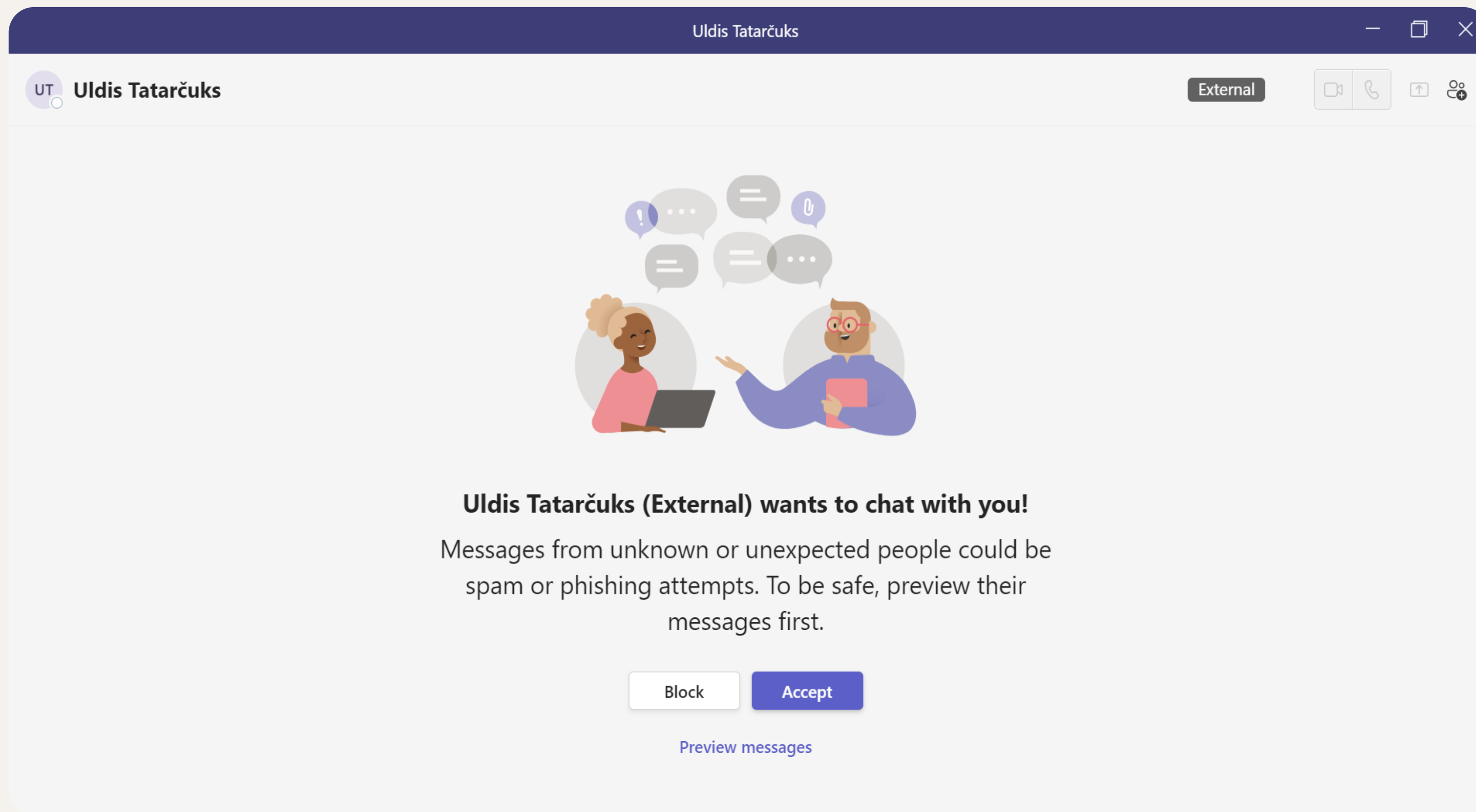
Komentāri

Iesniegt

AA Not Secure — tojumi.latekom.com

Kā mums izdodas?

Pikšķerēšana iespējama ne tikai e-pastā – Teams čats



Ko mēs nedarām

Ievērojam ētiku un privātumu

Mērķtiecīgi privāto kontu pikšķeri

Slēpta pikšķrēšana

Pikšerēšana sociālos tīkos

SmartID pikšķeri

Banku pikšķeri



Vienmēr tālāk!

**Lielās uzvaras vienmēr ir maratons,
nevis sprints**

Procesu nekad nevar apturēt – darbinieku rotācija

Arī 5%, 2.5% vai 1% kompromitētu kontu var novest pie uzbrukuma visam uzņēmumam

Reaģēt uz uzbrukumu ir tikpat būtiski kā to nepieļaut



THE SKY'S THE LIMIT

IT REALLY IS. IF YOU GO ABOVE THE SKY, THERE IS NO OXYGEN, AND YOU'LL SUFFOCATE AND DIE. SO STOP CLIMBING WHILE YOU CAN.

tet

Lai droši!

