Erasmus+

Līdzfinansē Eiropas Savienība

CIKLS 6

Kiberdrošība un datu aizsardzība

digitālajā vidē grāmatvedim

Kā grāmatvedim atpazīt krāpniecības mēģinājumus, droši rīkoties ar bankas datiem un personas datiem, kā arī ievērot kiberhigiēnas pamatprincipus ikdienas darbā.

LEKTORS

Mg. soc. Aiva Liakovičus

Alberta Koledža

Finansē Eiropas Savienība. Tomēr paustie uzskati un viedokļi ir tikai autora(-u) uzskati un viedokļi un ne vienmēr atspoguļo Eiropas Savienības vai Valsts izglītības un attīstības aģentūras (VIAA) uzskatus un viedokļus. Ne Eiropas Savienību, ne piešķīrēju iestādi (VIAA) nevar saukt pie atbildības par tiem.

Nodarbības mērķi

Pēc nodarbības students:

Atpazīs

izplatītākos digitālās krāpniecības veidus (phishing, vishing, smishing, CEO fraud, BEC, viltus rēķini) un to „sarkanos karogus".

Pielietos

VDAR principus personas datu apstrādei grāmatvedībā un zinās datu glabāšanas termiņus un incidentu paziņošanas kārtību.

Ievēros

kiberhigiēnas pamatprincipus — MFA, paroļu pārvaldnieks, droša e-pasta un internetbankas lietošana.

Veidos

drošu maksājumu kārtību ar „četru acu principu" un zinās, kā rīkoties krāpnieciska maksājuma gadījumā.

KONTEKSTS

Kāpēc tieši grāmatveži ir mērķis?

9,6 M€

izkrāpti no Latvijas banku klientiem 2025. gada pirmajos 10 mēnešos (FNA dati).

16 000 €

vidējā izkrāptā summa vienam uzņēmumam (FNA 2024. g. dati, 4 lielākās bankas).

90 %

krāpniecisko pārvedumu veikti ar drošu autentifikāciju — t.i., sociālā inženierija.

Profesija mainās

Grāmatvedim ir piekļuve uzņēmuma kontiem un maksājumu tiesības, ikdienā jāapstrādā liels rēķinu skaits — bieži vien steigā.

51% krāpšanas gadījumu uzņēmumos cēlonis — iekšējās kontroles trūkums vai apiešana (KPMG Latvia).

Avoti: FNA (financelatvia.eu), Latvijas Banka, CERT.LV ceturkšņa pārskati 2025/2026, KPMG Latvia.

Galvenie kiberdraudu veidi grāmatvedim

Krāpnieki izmanto cilvēka uzticību biežāk nekā tehnoloģiskas ievainojamības.

Sociālā inženierija

Pikšķerēšana (phishing) — viltus e-pasti it kā no bankas, VID, partnera.
Vikšķerēšana (vishing) — viltus zvani no „bankas drošības dienesta".
Smikšķerēšana (smishing) — viltus SMS no VID, kurjera, bankas.
CEO fraud — krāpnieks uzdodas par direktoru.
BEC — biznesa e-pasta kompromitēšana.

Tehniskie uzbrukumi

Izspiedējvīrusi (ransomware) — šifrē grāmatvedības failus, prasa izpirkumu.
Infostealer — zog paroles un sesijas (CERT.LV 12/2025).
ClickFix — lietotājs pats izpilda kaitīgu komandu.
Viltoti rēķini (invoice fraud) — ar nomainītu IBAN.
MI/deepfake — viltus balss un video (jauns risks 2025+).

PRINCIPS

Četri aizsardzības līmeņi

Drošība ir slāņveida — viens līmenis nepasargā, bet četri kopā atvaira lielāko daļu uzbrukumu.

1

Ierīce

Atjaunināta OS, antivīruss, BitLocker šifrēšana, DNS ugunsmūris (dnsmuris.lv).

2

Konts

Spēcīga parolfrāze, paroļu pārvaldnieks, MFA visiem kontiem.

3

Uzvedība

Pārbaudīt sūtītāju, neuzticēties steidzamībai, lasīt Smart-ID tekstu.

4

Process

Četru acu princips, VoP pārbaude, IBAN izmaiņas pēc zvana.

Krāpnieks meklē vājāko ķēdes posmu. Ja kāds no līmeņiem nedarbojas — uzbrukums izdosies.

PĪLĀRI

Trīs lietas, ko grāmatvedis nedrīkst aizmirst

01

Kiberhigiēna

Spēcīgas parolfrāzes, paroļu pārvaldnieks, MFA visiem darba kontiem.

MFA aktivizēts visiem finanšu un grāmatvedības kontiem

02

Personas datu apstrāde

VDAR principi, glabāšanas termiņi (5/10/75 gadi), incidentu paziņošana 72h DVI.

Personas datu apstrādes reģistrs (VDAR 30. pants)

03

Maksājumu drošība

Četru acu princips, VoP pārbaude (no 05.10.2025.), IBAN maiņa tikai pēc zvana.

Iekšējā maksājumu politika ar limitiem un eskalāciju

1. SOLIS

Krāpniecības atpazīšana: „sarkanie karogi”

Kā atpazīt aizdomīgu e-pastu, SMS vai zvanu pirms tas kļūst par incidentu?

- Steidzamība un laika spiediens („tikai šodien”)
- Neierasta komunikācijas forma (WhatsApp, privāts e-pasts)
- Sūtītāja adrese ar burtu izmaiņām (rn vietā m)
- Lūgums apstiprināt Smart-ID/PIN2 zvana laikā
- Pieprasījums mainīt IBAN bez oficiāla paziņojuma
- Gramatikas kļūdas, neierasts uzrunas stils

Uzmanību!

Banka NEKAD nezvana un neprasa:

- ✗ Smart-ID PIN1 vai PIN2 kodu
- ✗ Kodu kalkulatora kodus
- ✗ Internetbankas paroli
- ✗ Apstiprināt darījumu pa telefonu

Ja tā notiek — tas ir krāpnieks.

2. SOLIS

„Četru acu princips" maksājumiem

Maksājuma ievades un apstiprināšanas funkcijas vienmēr nodalītas (Valsts kases IKS vadlīnijas).

SAGATAVO

Grāmatvede

Ievada maksājuma uzdevumu internetbankā vai grāmatvedības sistēmā kā sagatavi.

- ✓ Pārbauda saņēmēja IBAN un summu
- ✓ Salīdzina ar oriģinālo rēķinu
- ✓ Ja IBAN mainīts — zvans partnerim

APSTIPRINA

Vadītājs vai 2. paraksta tiesīgais

Pirms Smart-ID/eParaksta apstiprināšanas pārbauda saņēmēju un summu uz ekrāna.

- ✓ Smart-ID tekstu izlasīt rūpīgi
- ✓ VoP pārbaude (no 05.10.2025.)
- ✓ Nesteidzīga apstiprināšana

Aizliegts vienai personai gan sagatavot, gan apstiprināt maksājumu.

3. SOLIS

Ja noticis krāpniecisks maksājums — pirmā stunda

Pirmās minūtes ir izšķirošas — SEPA Recall sekmīgums ir tieši atkarīgs no ātruma.

A	B	C	D	E
Banka	**Bloķē**	**Policija**	**CERT.LV**	**DVI**
Zvani bankas tālrunī: Swedbank 67444444, SEB 26668866, Citadele 67010000, Luminor 67171880	Bloķē karti, iesaldē kontu, atslēdz aizdomīgās ierīces no Smart-ID, maini paroli	Iesniegums Valsts policijai (caur e-adresi); saglabā e-pastus, SMS, ekrānuzņēmumus	Ziņo: , +371 67085888. SMS uz +371 23230444	Ja izkrāpti personas dati — paziņojums Datu valsts inspekcijai 72 stundu laikā

Pirmās 5–15 minūtes nosaka, vai naudu vēl var atgriezt.

DIAGNOSTIKA

Divi biežākie krāpniecības scenāriji 2025–2026

Saskaņā ar CERT.LV un FNA 2025. gada datiem šie ir izplatītākie pret grāmatvežiem vērsto uzbrukumu veidi.

„CEO fraud”

CĒLONIS

Krāpnieks no "gmail.com" adreses vai WhatsApp uzdodas par vadītāju un lūdz steidzami pārskaitīt naudu.

RISINĀJUMS

1. Zvani vadītājam pa zināmu darba numuru
2. Nekādi maksājumi caur WhatsApp/SMS
3. Saglabā ekrānuzņēmumus
4. Ziņo CERT.LV

„Viltus rēķins ar jaunu IBAN”

CĒLONIS

Pārtverta sarakste ar partneri vai homoglifu adrese (rn vietā m). Nosūtīts rēķins ar nomainītu IBAN.

RISINĀJUMS

1. Pārbaudi sūtītāja adresi burtu pa burtam
2. Zvani partnerim pa ZINĀMU numuru
3. VoP pārbaude internetbankā
4. Četru acu princips

PRAKTIKUMS

Jūsu uzdevums šodien

Posmi

1. Iepazīstieties ar uzdoto kāzusu (Kāzuss 1: Steidzamais rēķins) un identificējiet vismaz 5 „sarkanos karogus”.
2. Sagatavojiet rīcības plānu pirms maksājuma veikšanas — vismaz 5 soļi.
3. Aprakstiet pirmās stundas darbības, ja maksājums jau veikts (chronological order).
4. Grupās izveidojiet 1 lapas dokumentu „Maksājumu kārtība SIA „XYZ”.
5. Aizpildiet pašvērtējuma testu vietnē kibertests.lv un saglabājiet rezultātu.

Vērtēšana

Praktisko darbu vērtē četros kritērijos. Kopējais maksimums — 10 punkti.

3	Identificēti vismaz 5 „sarkanie karogi” ar pamatojumu
3	Pareizs rīcības plāns ar VDAR un CERT.LV atsaucēm
2	Loģisks „četru acu principa” pielietojums politikā
2	Skaidrs pamatojums par procesa loģiku

Video mācību materiāli (CERT.LV, bankas, Europol)

Pielikums patstāvīgai apguvei pirms un pēc nodarbības.

GRĀMATVEŽIEM
Kiberdrošības ekselences fonds – Grāmatvedība
youtube.com/watch?v=Vl32gEfh2ik

PHISHING
Kas ir pikšķerēšana?
youtube.com/watch?v=leiy14qgClM

VISHING
Kas ir vikšķerēšana? (telefonzvani)
youtube.com/watch?v=S4p2MKjp2UE

SMISHING
Kas ir smikšķerēšana? (SMS)
youtube.com/watch?v=JrJF7mzI9iE

RANSOMWARE
Kas ir izspiedējvīrusi?
youtube.com/watch?v=23yyZRG_ds8

INŽENIERIJA
Karstā sirds (sociālā inženierija)
youtube.com/watch?v=UwCDdtYXoSc

SWEDBANK
Uzmanies no krāpniekiem – sarunas piemērs
youtube.com/watch?v=fBvClVSr2oA

SWEDBANK
Krāpnieki uzdodas par Swedbank (Shorts)
youtube.com/shorts/xChMEGOPgxI

SEB
Smart-ID drošība
youtube.com/watch?v=pWkT0zNoQXk

EUROPOL
Beware scammers impersonating Europol officers
youtube.com/watch?v=xtipSzqNGRg

Papildus: cert.lv · esidross.lv · shemas.lv · dnsmuris.lv · kibertests.lv · dvi.gov.lv · bank.lv

KOPSAVILKUMS

Ko paturēt prātā?

01

Cilvēks ir svarīgākais aizsardzības līmenis

90% krāpniecisko maksājumu veikti ar drošu autentifikāciju — t.i., paši cilvēki tos apstiprina. Tehnoloģijas nevar pasargāt no nepārdomātām darbībām.

02

Četru acu princips — obligāts

Maksājuma ievades un apstiprināšanas funkcijas vienmēr nodalītas. IBAN izmaiņas — tikai pēc telefona zvana uz zināmu numuru.

03

Pirmās minūtes nosaka iznākumu

Ja noticis incidents — zvani bankai tūlīt, ziņo CERT.LV, dokumentē visu. Sliktais lēmums nav mēģināt slēpt — sliktākais ir vilcināties.

Jautājumi? Diskusija pirms praktiskā darba uzsākšanas.

Paldies par uzmanību!

Mg. soc. Aiva Liakovičus

Alberta Koledža · 28.05.2026

Alberta Koledža | Erasmus+ projekts Nr. 2024-2-LV01-KA210-VET-000280127

Finansē Eiropas Savienība. Tomēr paustie uzskati un viedokļi ir tikai autora(-u) uzskati un viedokļi un ne vienmēr atspoguļo Eiropas Savienības vai Valsts izglītības un attīstības aģentūras (VIAA) uzskatus un viedokļus. Ne Eiropas Savienību, ne piešķīrēju iestādi (VIAA) nevar saukt pie atbildības par tiem.