ZINI NAUDAS LI(Ī)KUMUS!

Finanšu izlūkošanas dienests

# metodiskais materiāls skolām

Finanšu izlūkošanas dienesta veidotā metodiskā materiāla skolotājiem „Zini naudas li(ī)kumus" mērķis ir informēt vidusskolēnus un veicināt viņu izpratni par finanšu noziegumu veidiem, riskiem un rīcību, lai no tiem izvairītos.

Materiālā ir pieci izglītojoši video par dažādām tēmām. Komplektā ar video ir pieejami uzdevumi, kurus var pildīt patstāvīgi vai grupā, tiešsaistē vai izdrukātā veidā. Metodiskais materiāls pieejams vietnē www.fid.gov.lv

## 3. Kā nekļūt par „naudas mūli"? Krāpšanas pamanīšana digitālajā vidē

Viens no pēdējo gadu populārākajiem krāpšanas veidiem internetā ir **pikšķerēšana** jeb fišings (angliski – *phishing*), kas ir kiberuzbrukuma veids ar nolūku nozagt lietotāja datus, paroles vai kredītkaršu numurus.

Pikšķerēšana var izpausties **krāpniecisku** e-pasta vēstuļu vai banku īsziņu (sms) veidā:

- pikšķerēšanas e-vēstules nozīmē krāpnieciskas **e-pasta vēstules,** kas saņēmēju mudina dalīties ar personas, finansiālu vai drošības informāciju;
- pikšķerēšanas sms jeb smikšķerēšana (sms un pikšķerēšana apvienojums) ir krāpnieku mēģinājums iegūt personīgu, finansiālu vai drošības informāciju, izmantojot **īsziņas.**

Šie noziegumi tiek veikti organizētās grupās, uzturot slēptus saziņas veidus, tai skaitā, uzstādot automātiskās dzēšanas saturam, netiekoties un pat nezinot grupas dalībnieka patiesos datus. Grupas organizē un vada personas, kas atrodas dažādās pasaules valstīs.

Tas ne tikai liek pievērst uzmanību tam, kādu informāciju jaunieši glabā **digitālajā vidē,** bet arī, kā seko līdzi dažādiem piesardzības pasākumiem un kādu uzmanību pievērš ienākošiem e-pasta paziņojumiem no svešiem adresātiem vai ar aizdomīgu saturu, vai saņemtajām īsziņām mobilajā ierīcē.

Saņemtās e-pasta **mēstules** var saturēt norādes uz pikšķerēšanas lapām vai krāpšanas shēmas, piemēram, darba piedāvājumus ar vilinošu atalgojumu. Lai to saņemtu, nepieciešams bankas konts un internetbankas pieslēgums, kura dati jānodod potenciālajam darba devējam. Citi **uzbrukumi** ir saistīti ne tikai ar internetbankas un karšu informāciju, bet arī piekļuves datiem *Facebook*, *PayPal* utt.

Šādu noziegumu organizatori izmanto segvārdus, veic nepieciešamās darbības slēpti, lai netiktu identificēti, kā arī izmanto virtuālo valūtu noziedzīgi iegūto līdzekļu saņemšanai atpakaļ. Noziedzīgi iegūtu līdzekļu legalizācijas izmeklēšana un nozieguma atklāšana ir īpaši sarežģīta, un to veido tādi faktori kā nepieciešamā starptautiskā sadarbība, īpašas zināšanas informācijas tehnoloģijās, apjomīgs analītiskais darbs lielo datu apjomu apstrādē.

Taču šāda veida **krāpšanu var iemācīties atpazīt** pēc vairākām raksturīgām pazīmēm, piemēram:

- saites, pielikumi vai attēli, kas steidzami jāatver;
- atbildes pieprasījums, kurā jānorāda PIN kods, parole vai citi dati;
- pareizrakstības, drukas un gramatikas kļūdas;
- aizdomīga sūtītāja e-pasta adrese un e-vēstules vizuālais noformējums.

ZINĀŠANU TESTS

# KRĀPŠANA DIGITĀLAJĀ VIDĒ

***Uzdevuma apraksts:*** *pārbaudi savas zināšanas, izpildot testu, kas sastāv no 5 slēgta tipa jautājumiem. Katram jautājumam ir 4 atbilžu varianti. Viena atbilde ir pareiza. Atzīmē tīkamo atbilžu variantu un pārbaudi, vai atbildēji pareizi.*

***Izpildes laiks:*** *no 3 līdz 5 minūtēm*

***Ieteicamās mācību jomas:*** *ekonomika un uzņēmējdarbības pamati, politika un tiesības, sociālās zinības un vēsture*

**1. Kiberuzbrukuma veids ar nolūku nozagt lietotāja datus, paroles vai kredītkaršu numurus ir:**

- ☐ e-laupīšana
- ☐ zvejošana jeb fišings
- ☐ pikšķerēšana jeb fišings
- ☐ naudas atmazgāšana jeb noziedzīgi iegūtu līdzekļu legalizācija

**2. Biežākās pikšķerēšanas pazīmes ir:**

- ☐ pareiza gramatika un ievērota pareizrakstība
- ☐ pievilcīgs dizains un vizuālā grafika
- ☐ sūtītājam atbilstīga e-pasta adrese
- ☐ nezināms sūtītājs, steidzamība, nesaprotami pielikumi, aizdomīgas saites vai obligātas atbildes pieprasījums

**3. Cik miljonu krāpniecisku e-pasta vēstuļu vidēji dienā izsūta pasaulē?**

- ☐ 10 miljoni
- ☐ 25 miljoni
- ☐ 75 miljoni
- ☐ 150 miljoni

**4. Ar kādām sekām jārēķinās, atverot saiti vai pielikumu krāpnieciskā e-vēstulē?**

- ☐ var tikt nozagti personas dati
- ☐ var tikt nozagti bankas dati un piekļuves
- ☐ var tikt nozagtas pieejas *Netflix*, *Facebook*, *PayPal* un citiem kontiem
- ☐ visas atbildes ir pareizas

ZINI NAUDAS LIETKUMUS!

**Atceries!** Pikšķerēšana jeb fišings ir viens no populārākajiem kiberuzbrukuma veidiem ar nolūku nozagt lietotāja datus, paroles vai kredītkaršu numurus. Pikšķerēšana izpaužas krāpniecisku e-pasta vēstuļu vai banku īsziņu (sms) veidā. Tāpēc domā līdzi un pamani brīdinājuma zīmes jeb **„sarkanos" karogus.**

## NĀKOTNE IR TAVĀS ROKĀS ...

Mācies atpazīt noziedzīgas shēmas

Kritiski izvērtē katra darījuma apstākļus

Palīdzi citiem izvairīties no krāpniecības

**5. Viena no svarīgām prasmēm, kuru attīstīt, lai identificētu krāpnieciskas darbības, ir:**

- ☐ izcila angļu valoda
- ☐ ātra reakcija
- ☐ kritiskā domāšana
- ☐ humora izjūta

## Pareizās atbildes

1. jautājums: pikšķerēšana jeb fišings
2. jautājums: nezināms sūtītājs, steidzamība, nesaprotami pielikumi, aizdomīgas saites vai obligātas atbildes pieprasījums
3. jautājums: 150 miljoni
4. jautājums: visas atbildes pareizas
5. jautājums: kritiskā domāšana

Finanšu izlūkošanas dienests

Finanšu izlūkošanas dienests apkopo un analizēt finanšu datus, saņemtos ziņojumus par aizdomīgiem darījumiem, lai iegūto informāciju nodotu Latvijas tiesībaizsardzības iestādēm noziedzīgi iegūtu līdzekļu legalizācijas, terorisma un proliferācijas finansēšanas lietu izmeklēšanai.

**Sociālie tīkli**

FIU Latvia
Naudas Likumi
@naudas_likumi

www.fid.gov.lv