Funded by the Erasmus+ Programme of the European Union

Kiberuzbrukumi: Sociālā inženierija un pikšķerēšana

Dažādi pikšķerēšanas uzbrukumu veidi un paņēmieni

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Apmācību mērķis

Izskaidrot dažādus pikšķerēšanas uzbrukumu veidus un iemācieties tos atpazīt

Pikšķerēšanas (personas datu izmānīšanas) uzbrukumi:

- Uz notikumiem balstīti uzbrukumi, e-pasti, mirkļsaziņa, sociālie tīkli, vietnes, izlozes, SMS, telefona zvani, klātienes tikšanās, datu noskatīšanās pār plecu.

Metožu kombinācija:

- Izkrāpšanas centieni uz labu laimi, mērķēta pikšķerēšana, lielo zivju pikšķerēšana, tālruņa un balss ziņu pikšķerēšana, īsziņu pikšķerēšana, sociālo tīklu pikšķerēšana, klonu pikšķerēšana, ļaunprātīga reklāmu izplatīšana.

Funded by the Erasmus+ Programme of the European Union

Kursantu darba slodze

Lekcija	4 st.
Audio un video materiāli	2 st.
Pētījumi	2 st.
Papildu lasīšana	2 st.
Sagatavošanās eksāmenam	2 st.

Krāpniecība pa e-pastu

Viltus vinnesti

Datu noskatīšanās pār plecu

Viltus aptaujas

Krāpniecība īsziņās

Ēsmas izlikšana

Viltus mājaslapas

Krāpniecība sociālajos tīklos

Tālruņa un balss ziņu pikšķerēšana

Distances neievērošana

Krāpniecība, izmantojot tūlītējo ziņojumapmaiņu

CyberPhish


Telefona zvani
SMS (īsziņas)
E-pasti
Klātienes
iekļūšana
uzņēmumā
CyberPhish

Veiksmīga pikšķerēšanas uzbrukuma rezultāti

- Sensitīvu datu zaudēšana
- Akreditācijas datu zaudēšana
- (lietotājvārdi un paroles)
- Identitātes zādzības
- Klienta informācijas zādzība
- Līdzekļu zaudēšana no uzņēmumu un klientu kontiem
- Piekļuve iekšējām sistēmām, lai uzsāktu turpmākus uzbrukumus
- Neautorizēti darījumi
- Intelektuālā īpašuma zaudēšana
- Dati, kas sniegti vai pārdoti noziedzīgām trešajām personām
- Operatīvās darbības traucējumi
- Reakcija uz incidentu
- Izskaušana un atgūšanās
- Zaudēts darba laiks sistēmas atveseļošanai
- Reputācijas kaitējums
- Peļņas atrāvums
- Sodi, juridiskās izmaksas
- …

Funded by the Erasmus+ Programme of the European Union

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Uz notikumiem balstīti uzbrukumi

- Liela mēroga notikumi, kari, pandēmijas, piemēram, COVID-19, liek cilvēkiem rīkoties impulsīvāk nekā parastos apstākļos

- Visbiežāk izmantotie paņēmieni: e-pasti, mērķēta pikšķerēšana, SMS, sekošana, tālruņa un balss ziņu pikšķerēšana utt.

Funded by the
Erasmus+ Programme
of the European Union

Ar GDPR saistīti uzbrukumi

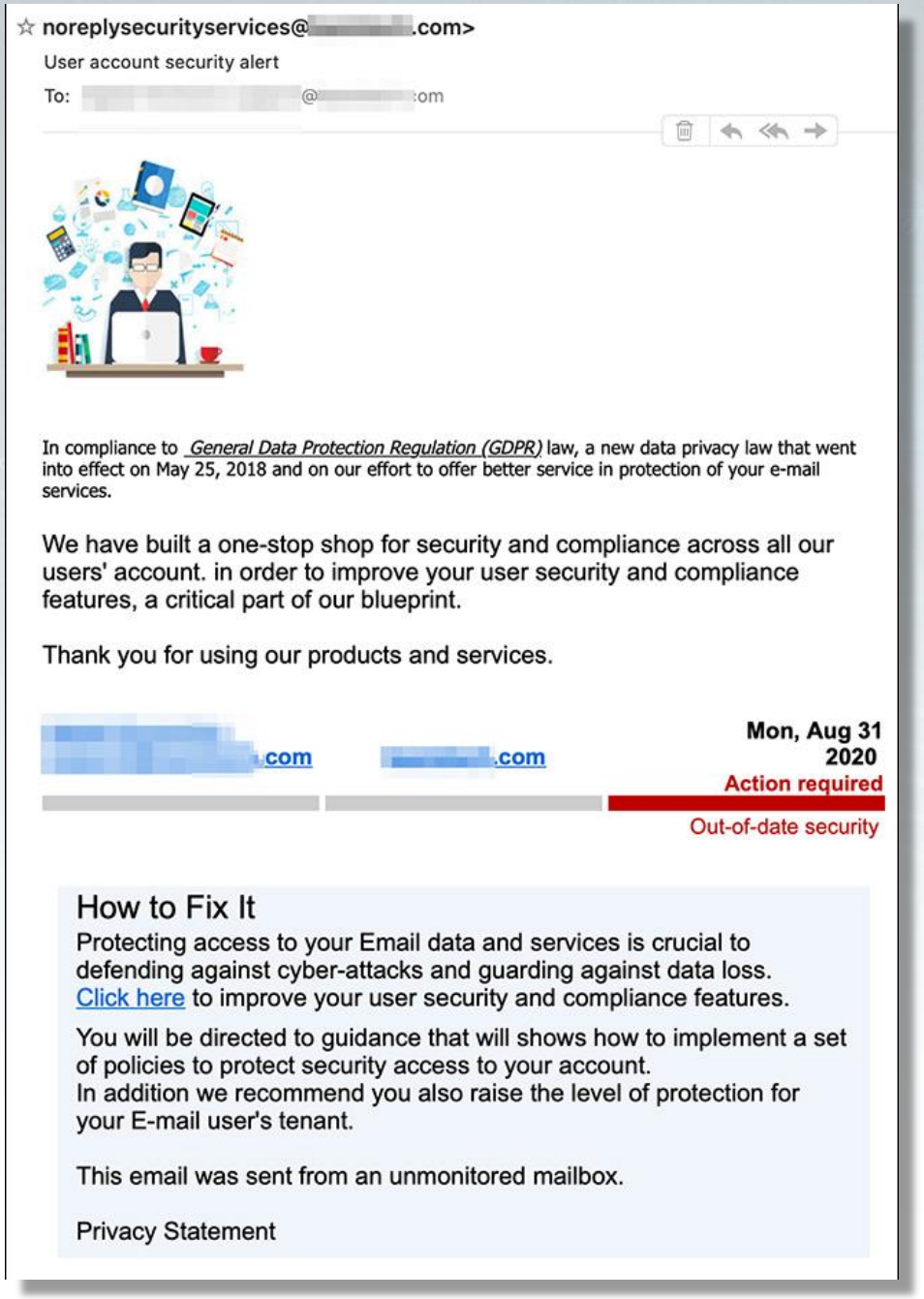
- **Vispārīgā datu aizsardzības regula** (GDPR vai VDAR) ir regula, kas nosaka datu aizsardzību un privātumu Eiropas Savienības valstīs, kas ir spēkā kopš 2018. gada, un kontrolē uzņēmumus un organizācijas, kas apstrādā personas datus.
- Uzņēmumiem, kas veic automatizētu vai daļēji automatizētu personas datu apstrādi, ir jāievēro GDPR
- 2018. gadā notika daudzi GDPR uzbrukumi, jo visiem uzņēmumiem un organizācijām bija jāievieš GDPR savās organizācijās.

Ar GDPR saistīts uzbrukums organizācijām

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Uzņēmumiem nebija pietiekami daudz zināšanu par GDPR.
- **Mērķis:** organizāciju darbinieki, parasti, lai
  - uzņēmuma e-pasti, kas ir pieejami internetā vai
  - vērsties pie uzņēmumu vadītājiem vai augstākajiem vadītājiem (kuriem, cerams, ir piekļuve klientu datiem vai kuri ir atbildīgi par atbilstību GDPR)
- **Draudi:** e-pasta ziņojumi no "drošības organizācijām", kas sniedz pakalpojumus, lai uzlabotu lietotāju drošību un atbilstību GDPR
- **Uzbrukuma metode:** e-pasta ziņojumi (mērķēta pikšķerēšana).
- **Pikšķerēšanas taktika:** Izstrādātie un formatētie e-pasta ziņojumi izskatās likumīgi. Uzbrucēji rada iespaidu, ka e-pasta ziņojumi ir sūtīti no likumīga avota
- **Pikšķerēšanas faktors:**
  - **bailes no likuma pārkāpumiem**
  - **Tiek iedvesta steidzamības sajūta:** uzbrucēji izmantoja laika grafiku iedomātai GDPR pieprasītajai atbilstībai, ko uzbrucēji regulāri atjaunināja, lai palielinātu spiedienu uz mērķi.
- **Ievainojamības:**
  - Neapmācīts personāls (kas noklikšķina uz saites e-pastā un sniedz datus)

Funded by the Erasmus+ Programme of the European Union

Ar GDPR saistīts uzbrukums: lietotāju drošības un GDPR atbilstības uzlabošana



- Pikšķerēšanas vietne tiek atvērta, kad upuris noklikšķina uz saites
- Vietne var būt personalizēta ar upura e-pasta adresi
- Cietušajam var lūgt pieteikties (sniedzot pieteikšanās datus) viltotajā vietnē, kas izskatās kā īsta vietne
- **Rezultāts:**
  - Nozagti upuru e-pasta pieteikšanās dati, lai piekļūtu e-pastam
  - Sensitīvi dati var tikt nozagti no upura e-pasta vai nozagtie kontakti var tikt izmantoti turpmākiem kiberuzbrukumiem

Avots: https://www.helpnetsecurity.com/2020/09/24/phishers-targeting-employees-fake-gdpr-compliance-reminders/

Funded by the Erasmus+ Programme of the European Union

Ar GDPR saistīts uzbrukums klientiem

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Uzņēmumi nosūta klientiem e-pasta ziņojumus par GDPR atjauninājumiem attiecībā uz klientu datu konfidencialitātes politikām.
- **Mērķi:** dažādu organizāciju klienti, parasti IT pakalpojumu sniedzēji, finanšu organizāciju klienti
- **Draudi:** e-pasti no "organizācijām", lūdzot apstiprināt atļauju uzglabāt un apstrādāt personas datus
- **Uzbrukuma metode:** e-pasti.

- **Pikšķerēšanas taktika:**
  - izveidoti un formatēti e-pasta ziņojumi, kas izskatās kā īsts organizācijas e-pasts. Uzbrucēji rada iespaidu, ka e-pasta ziņojumi ir sūtīti no likumīga avota.
  - Uzbrucēji izmanto uzticamus zīmolus un simbolus.
- **Pikšķerēšanas faktors:**
  - **Attiecības ar saistībām vai konsekvence**
  - **Lojalitāte organizācijai**
- **Ievainojamības:**
  - Klienti ar ierobežotām vai bez zināšanām par pikšķerēšanu (kas noklikšķina uz saites e-pastā un sniedz datus)

Funded by the Erasmus+ Programme of the European Union

Ar GDPR saistīts uzbrukums: Pieņemiet jauno privātuma politiku

From: Airbnb! <important@mail.airbnb.work>
Sent: 18 April 2018 10:41
To: Info [redacted]
Subject: [redacted] New Policy - Act now
Importance: High

airbnb

Your account ([redacted]) needs an update

Hi [redacted]

You (Airbnb host [redacted] are currently not able to accept new bookings or send messages until you accept our new Privacy Policy.

Airbnb has updated his Privacy Policy for European users on 18 Apr 2018.

This update is mandatory because of the new changes in the EU Digital privacy legislation that acts upon United States based companies, like Airbnb in order to protect European citizens and companies.

In order to log back in, you need to accept our new Privacy Policy.

Click here to accept the new Privacy Policy

- Pikšķerēšanas vietne tiek atvērta, kad upuris noklikšķina uz saites
- Upurim, iespējams, tiek lūgts sniegt savu personisko informāciju, tostarp konta akreditācijas datus un maksājumu kartes informāciju viltotajai vietnei, kas izskatās kā īsta vietne.
- **Rezultāts:**
  - Nozagti upuru e-pasta pieteikšanās dati, lai piekļūtu e-pastam Sensitīvi dati var tikt nozagti no upura e-pasta vai nozagtie kontakti var tikt izmantoti turpmākiem kiberuzbrukumiem
  - Nozagti finanšu dati.
  - Inficētas ierīces (t.i., taustiņu reģistratori, izspiedējprogrammatūras utt.)

Avots: https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/, Redscan

Ar COVID saistīti uzbrukumi

- Covid-19 pandēmijas laikā daudzi cilvēki strādā no mājām. Darbinieki izmantoja savus personālos datorus darba uzdevumu veikšanai attālinātā režīmā, pamata saziņa notika ar e-pastiem – tas nozīmē, ka darbinieki kļuva neaizsargātāki pret kiberuzbrukumiem
- Covid-19 laikā tika novērots ar pandēmiju saistītu krāpniecību pieaugums, piemēram, viltoti Slimību kontroles un profilakses centra (CDC) vai veselības organizāciju e-pasta ziņojumi, e-pasti par vakcinācijas segumu, kur var iegūt vakcīnu, vakcinācijas statistiku, darbinieku vakcinācijas statusu utt.

Covid uzbrukumi: E-pasti

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** COVID-19 izraisīja cilvēkos nestabilitātes un nenoteiktības sajūtu, biežas politiķu lēmumu izmaiņas attiecībā uz karantīnu, vakcināciju, vakcināciju apliecinošiem dokumentiem utt.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - e-pasta ziņojumi ar lūgumu sniegt sensitīvu informāciju viltotā vietnē;
  - e-pasta vēstules ar aicinājumu noklikšķināt uz saites.
- **Uzbrukuma metode:** e-pasti.

- **Pikšķerēšanas taktika:**
  - izveidoti un formatēti e-pasta ziņojumi, kas izskatās kā īsts organizācijas e-pasts.
  - Uzbrucēji parasti iesaka lejupielādēt dokumentu, lai pārskatītu COVID-19 statistiku, lejupielādētu Covid veidlapu, aizpildītu tiešsaistes veidlapu vai aizpildītu lejupielādētos dokumentus par vakcinācijas statusu, augšupielādētu negatīvu testu utt.
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Tiek lūgts izpildīt nestandarta procesu**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu (iedzīvotāji, kuri veic pikšķerēšanas e-pastos prasītās darbības)

Funded by the Erasmus+ Programme of the European Union

Covid uzbrukumi: Veselības konsultāciju e-pasti

Singapore Specialist : Corona Virus Safety Measures

DT

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

Safety Measures.pdf

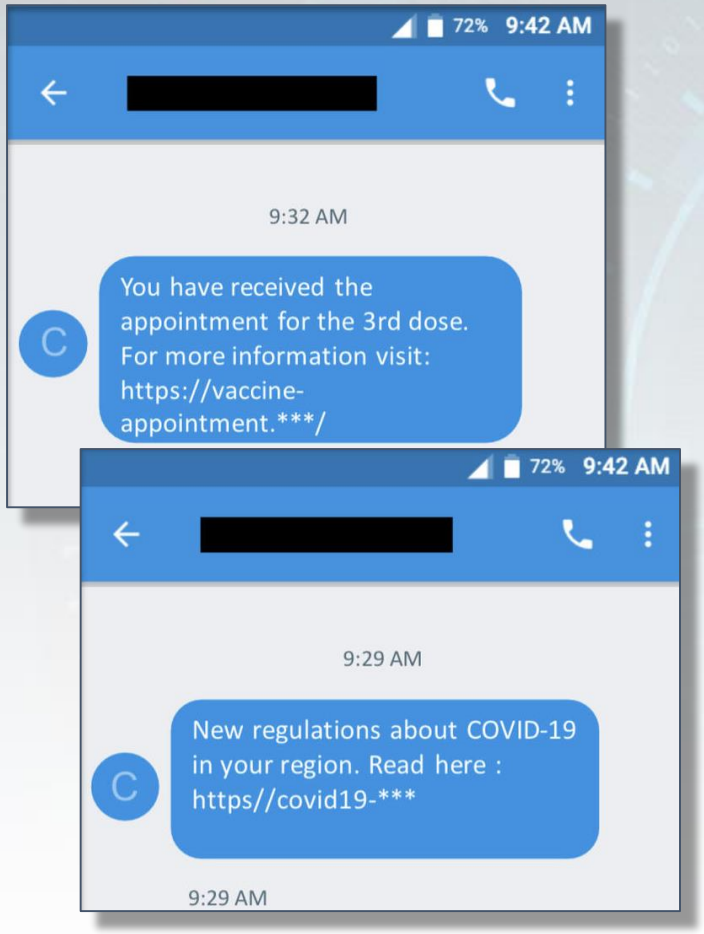
Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

- Pikšķerēšanas vietne tiek atvērta, kad upuris noklikšķina uz saites, kas izskatās kā saite uz PDF failu
- Upurim, iespējams, tiek lūgts sniegt savu personisko informāciju, tostarp konta akreditācijas datus un maksājumu kartes informāciju, lai "autentificētu identitāti" viltotajā vietnē.
- **Rezultāts:**
  - Nozagti upuru e-pasta pieteikšanās dati, lai piekļūtu e-pastam
  - Nozagti finanšu dati.
  - Inficētas ierīces (t.i., taustiņu reģistratori, izspiedējprogrammatūras utt.)

Avots: https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

Covid uzbrukumi: Informācija par vakcīnām, izmantojot SMS



- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Iestādes iedzīvotājiem nosūta SMS par vakcināciju.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - SMS ar aicinājumu noklikšķināt uz norādītās saites
- **Uzbrukuma metode:** SMS (īsziņas)
- **Pikšķerēšanas taktika:**
  - SMS ir īsas. Viens vai divi teikumi. Saite uz viltotu vietni parasti tiek sniegta īsziņā
- **Pikšķerēšanas faktors:**
  - nestabilitātes un nenoteiktības sajūta
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu (iedzīvotāji, kuri veic pikšķerēšanas e-pastos prasītās darbības)

Avots: www.techrepublic.com/article/new-sms-malware-targets-android-users-through-fake-covid-messages

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pasta ziņojumi

- Viens no vispazīstamākajiem pikšķerēšanas veidiem
- Uzbrucēji pikšķerēšanas e-pastos var izmantot šādu taktiku:
  - Pieprasa nosūtīt sensitīvu informāciju pa e-pastu
  - Lūdz noklikšķināt uz norādītās saites e-pastā
  - Lūdz atvērt pielikumu, parasti PDF vai DOC formātā
- Parastās pikšķerēšanas e-pasta tēmas:
  - Problēmas ar e-pasta vai cita pakalpojuma kontu
  - Tehniskā atbalsta problēmas
  - Romantiskas attiecības
  - Mērķētas pikšķerēšanas e-pasta ziņojumi direktoriem un vadītājiem
  - Lai atgūtu datus, atmaksātu naudu vai saņemtu finansiālu atbalstu no iestādes

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pasta ziņojumi

Lietotājs var saskarties ar vairākiem terminiem, kas saistīti ar pikšķerēšanas e-pastiem:

- **Izkrāpšanas centieni uz labu laimi** – ļaunprātīgas e-pasta ziņas, kas tiek sūtītas uz jebkuru e-pasta adresi, mēģinot nozagt sensitīvu informāciju
- **Iepriekš samaksātās nodevas krāpniecība** – izplatīta krāpšana, kas saistīta ar Nigērijas pilsoņiem, piemēram, palīdzības lūgšana lielas naudas summas pārvietošanai
- **Mērķēta pikšķerēšana** – ļaunprātīgi e-pasta ziņojumi, kas ir īpaši izstrādāti un nosūtīti konkrētai personai vai organizācijai, lai mēģinātu nozagt sensitīvu informāciju
- **Lielo zivju pikšķerēšana** – mēģinājums nozagt sensitīvu informāciju, kas bieži ir vērsts uz augstāko vadību
- **Sociālo tīklu pikšķerēšana** – salīdzinoši jauns veids, kas attiecas uz uzbrukumiem sociālajos medijos, izmantojot viltus vietrāžus URL, klonētas vietnes, ziņas un tvītus, kā arī tūlītējo ziņojumapmaiņu.
- **Klonētā pikšķerēšana** – pikšķerēšanas veids, kurā tiek izmantots likumīgs un iepriekš piegādāts e-pasts, lai izveidotu identisku e-pasta ziņojumu ar ļaunprātīgu saturu
- **Ļaunprātīga reklāmu izplatīšana** – šis pikšķerēšanas veids izmanto tiešsaistes reklāmas vai uznirstošos logus, lai liktu cilvēkiem noklikšķināt uz derīga izskata saites, kas pēc tam instalē ļaunprātīgu programmatūru lietotāja datorā.

Pikšķerēšanas e-pasta ziņojumi: Pieprasa nosūtīt sensitīvu informāciju pa e-pastu

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Pikšķerēšanas uzbrukumi izskatās pārliecinoši, ņemot vērā iespaidu, ka tie nāk no uzticama avota. Organizācijas neveic pietiekamu uzticamības pārbaudi. Uzbrucēji izmanto sarežģītākus pikšķerēšanas uzbrukumus, kurus ir grūti atklāt utt.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - e-pasti, kuros tiek lūgts nosūtīt atbildi
  - e-pasta ziņojumi ar lūgumu sniegt sensitīvu informāciju e-pastā
- **Pikšķerēšanas taktika:**
  - meklē partnerus, ir labas ziņas upurim, piedāvā naudu, informē par laimestu, kāds uzdodas par draugu un lūdz aizdot naudu negaidītas nelaimes dēļ utt.
  - piedāvā naudu, informē par konkursa uzvarētāju utt.
- **Pikšķerēšanas faktors:**
  - **Upurim rada iespaidu, ka sūtītājs ir noderīgs**
  - **Iedvesmo uz alkatību**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu (iedzīvotāji, kuri atbild, veic pikšķerēšanas e-pastos prasītās darbības)
- **Rezultāts:**
  - Identitātes zādzība, naudas zaudēšana

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pastu piemēri: Pieprasa nosūtīt sensitīvu informāciju pa e-pastu

Nosūtītājs: eduardorodriguez <andreasjohnson874@gmail.com>

Saņēmējs: andreasjohnson847@gmail.com

Tēma:

Sveiks, draugs!

Mans vārds ir ANTONIJS FĒLIKSS *[ANTONI FELIKS]* no Polijas, man ir labas ziņas.
APSVEICU!!!
Nekavējoties sazinies ar mani pa šo e-pastu:
homebankpln@gmail.com or
homebankpln@polandmail.com lai saņemtu labas ziņas

Nosūtītājs: administrator <admin@www-professionals.online>

Saņēmējs:

Tēma: Apsveicam!!!

Mēs esam priecīgi jūs informēt, ka jūsu e-pasts ir laimējis $ 7500 no www tiešsaistes loterijas balvas. Lai saņemtu šo balvu, jums ir jāsniedz šāda informācija:
Saņēmēja vārds un uzvārds:_____
Saņēmēja adrese:_____
Saņēmēja valsts: _____
Saņēmēja kredītkartes numurs: _____
Saņēmēja kredītkarte un drošības kods (CVC2):
_____

PIEZĪME: saglabājiet laimesta informācijas konfidencialitāti.

Paraksts:

Nosūtītājs: Eiva Viljamsa *[Ava Williams]* <avawilliamsj@gmail.com>

Saņēmējs: avawilliamsj@gmail.com

Tēma: Sveiks…

Sveicieni tev

Es zinu, ka būsi pārsteigts, saņemot šo ziņu no manis, jo mēs iepriekš neesam tikušies. Es ieguvu tavu e-pastu no Google pētniecības. Es rakstu tev no slimnīcas, kurā es ārstējos, jo tagad esmu ļoti slima vēža dēļ.

Es sazinos ar tevi šodien, jo man ir nepieciešama tava palīdzība, lai ieguldītu līdzekļus, ko mantoju no sava mirušā vīra.
Es tev kompensēšu 30% no naudas, ja piekritīsi man palīdzēt šajā jautājumā.
Es pastāstīšu vairāk par sevi un saviem plāniem, kad saņemšu atbildi.

Ar sveicieniem,
Eiva Viljamsas k-dze *[Mrs. Ava Williams]*

Nosūtītājs: manyrib7@gmail.com

Saņēmējs:

Tēma: Sveiks…

Mani sauc Riabs Manjangs *[Rihab Manyang]*. Esmu šeit, lai atrastu biznesa partneri vai draugu, kas palīdzētu man investēt savus fondus jūsu valstī.

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pasta ziņojumi: Lūdz noklikšķināt uz norādītās saites e-pastā

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Pikšķerēšanas uzbrukumi izskatās pārliecinoši, ņemot vērā iespaidu, ka tie nāk no uzticama avota. Organizācijas neveic pietiekamu uzticamības pārbaudi. Uzbrucēji izmanto sarežģītākus pikšķerēšanas uzbrukumus, kurus ir grūti atklāt: viņi var izmantot satura, konteksta un emocionālo stimulu kombināciju, kas veicina pikšķerēšanas uzbrukuma panākumus utt.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - pikšķerēšanas uzbrukumi kopē mūsu esošās darbplūsmas
  - uzbrucēji lūdz noklikšķināt uz e-pastā norādīto saiti
- **Pikšķerēšanas taktika:**
  - E-pasta ziņojumi par uzlauztām e-pasta adresēm vai parolēm
  - E-pasta ziņojumi par koplietotiem dokumentiem sadarbībai
  - E-pasta ziņojumi par tehniskām problēmām

- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Uzbrucēji izmanto upura emocijas un instinktus**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu (iedzīvotāji, kuri atbild, veic pikšķerēšanas e-pastos prasītās darbības)
- **Rezultāts:**
  - Identitātes zādzība, naudas zaudēšana

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pastu galvenās funkcijas

- Izmantot cienījamu organizāciju vai personu vārdus
- Izmantot datus no cienījamiem avotiem
- Lūgt sniegt sensitīvu informāciju
- E-pastiem var būt pielikumi
- Parasti nezināms adresāts
- Saites uz vietnēm (saites var būt saīsinātas)
- Saites tradicionāli novirza uz ļaunprātīgām vietnēm
- Izmanto bailes vai tiek pausta steidzamības sajūta
- Neticams ieganststs (loterija, atlaides, mantojums,...)

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Pikšķerēšanas e-pastos izmantotās saites

- Uzbrucēji pikšķerēšanas e-pastos parasti izmanto saites uz viltotām vietnēm:
  - Uzbrucēji var reģistrēt viltotu domēnu. URL nosaukums var būt līdzīgs reālai organizācijai, tie vienkārši maina vienu vai vairākus burtus domēna nosaukumā, piemēram, burta "l" vietā var izmantot burtu "i", vai "m" vietā lietot "rn" utt. Piemēram, viņi varētu reģistrēt šādu viltotu domēna vārdu***www.exarnple.com*** (patiesā URL saite ***www.example.com***)
  - Uzbrucēji var reģistrēt domēnu, URL izmantojot reālu organizācijas nosaukumu, piemēram, ***www.sales-organization.com*** (patiesā URL saite ***www.organization.com***)
  - Uzbrucēji varētu izmantot saīsinātus URL, piemēram, ***Bitly***, ***TinyURL***, ***Short.io*** (vairāk informācijas sadaļā saīsināšanas pakalpojumi)
  - Uzbrucēji var izmantot uzlauztas vietnes saiti (izmantojot īstu domēna nosaukumu, bet citu URL daļu veidojot no hakeru puses)
  - Uzbrucēji ietver ļaunprātīgu kodu likumīgā tīmekļa lapā (injekcijas uzbrukums). Kad upuris atver šo vietni, tiks izpildīts ļaunprātīgs skripts. Šāda veida uzbrukuma rezultāts būtu datu zādzība, taustiņu reģistrācija, sīkfailu zādzība utt.

Nosūtītājs: Uzmanību! Tiešsaistes krāpšanas novēršana <info@nat1onalbank.com>

Saņēmējs: undisclosed-recipients

Tēma: Jūsu Nacionālās bankas konta darbība ir apturēta

CyberPhish

National Bank

Cienītais klient,

Mēs nesen pamanījām, ka dažādas ierīces no dažādām vietām mēģināja pieteikties jūsu Nacionālās bankas kontā.

Mēs piedāvājam to IP adrešu sarakstu, no kurām nesen tika mēģināts pieteikties jūsu kontā:
12.55.155.6:8080
32.44.789.99:3128
54.22.124.44:8080
78.44.457.14:80

Pašlaik jūsu konta darbība ir APTURETA. Jums tas jāaktivizē 7 dienu laikā, pretējā gadījumā konts tiks bloķēts.
Lai apstiprinātu, ka esat sākotnējais lietotājs, un aktivizētu kontu, noklikšķiniet uz HTTP://WWW.NAT1ONALBANK.COM?PROFILE
Vairāk informācijas pieejams šeit.

http://www.nat1onalbank.com/?PROFILE

Ar cieņu,
Nacionālās bankas tiešsaistes krāpšanas novēršanas vadītājs
JohnBank@gmail.com

Report-of-attempts-to-login.zip

Pikšķerēšanas e-pasta ziņojumi ar pielikumu vai failu lejupielādi

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Pikšķerēšanas uzbrukumi izskatās pārliecinoši, ņemot vērā iespaidu, ka tie nāk no uzticama avota. Organizācijas neveic pietiekamu uzticamības pārbaudi. Uzbrucēji izmanto sarežģītākus pikšķerēšanas uzbrukumus, kurus ir grūti atklāt: viņi var izmantot satura, konteksta un emocionālo stimulu kombināciju, kas veicina pikšķerēšanas uzbrukuma panākumus utt.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - pikšķerēšanas uzbrukumi kopē mūsu esošās darbplūsmas
  - uzbrucēji lūdz atvērt pievienotos attēlus, mūziku, filmas, dokumentus (piemēram, PDF, DOC, ZIP), kuros ir iegulta ļaunprātīga programmatūra
  - uzbrucēji pievieno HTML failus, kas ir pilnībā funkcionāli – tajos ir visi pikšķerēšanai nepieciešamie elementi, uzbrucējiem tie nemaz nav jāpublicē internetā
- **Pikšķerēšanas taktika:**
  - E-pasta ziņojumi ar pielikumiem: fails ar biznesa vai individuālu piedāvājumu, fails ar “konfidenciālu” vai “ļoti svarīgu” informāciju, pārdošanas vai finanšu (neapmaksāti rēķini, pirkuma pasūtījums) informācija, steidzams balss e-pasts, atjaunināta organizatoriskā politika, faili par tehniskām problēmām, konkrētā laika perioda informācija, piemēram, pandēmija utt.
  - E-pasta ziņojumi ar lūgumu aizpildīt pievienoto dokumentu svarīgām darbplūsmām
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Uzbrucēji izmanto upura emocijas un instinktus**
- **Ievainojamības:**
  - lietotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu (iedzīvotāji, kuri atver pielikumu)
- **Rezultāts:**
  - Inficēti datori, identitātes zādzības, naudas zaudēšana

Funded by the Erasmus+ Programme of the European Union

Pikšķerēšanas e-pastu piemēri:
Pikšķerēšanas e-pasta ziņojumi ar pielikumu vai failu lejupielādi

Neuzticieties saitēm un pielikumiem e-pastā, pat ja tas ir no uzticamas personas

Nosūtītājs: Jana Džordana *[Jaana Jordan]*<cdg446@comcast.net>
Saņēmējs: Una Vilime *[Una Vilime]* <una.vilime@organisationname.com>
Tēma: Sveika, Una

Jums steidzami jāapstrādā ātrāks rēķina maksājums, lūdzu, informējiet mani, ja esat pēc iespējas ātrāk pieejama.

Ar sveicieniem,
Jana Džordana *[Jaana Jordan]*

Nosūtīts no mana IPhone

Nosūtītājs: ABC Banka<noreply@support-abcbank.com>
Saņēmējs:
Tēma: ABC bankas kontu atbalsta nodaļa

Cienījamais ABC bankas lietotāj!

Mēs pamanījām neparastu darbību jūsu kredīta/debeta kontā. Rezultātā man ir jāierobežo piekļuve jūsu bankas kontam. Jūsu ierobežotā piekļuve paliks spēkā, līdz problēma tiks atrisināta.

Mēs strādājam, lai nodrošinātu jūsu konta drošību, tāpēc novērtējam jūsu sapratni.

Lai nodrošinātu Jūsu drošību, pievienojam dokumentu, kas jāatver interneta pārlūkprogrammā. Lai atjaunotu kontu, veiciet atvērtajā tīmekļa lapā norādītās darbības.

Ar cieņu,
ABC bankas kontu atbalsta nodaļa

Pikšķerēšanas e-pastu piemēri:
Pikšķerēšanas e-pasta ziņojumi ar pielikumu vai failu lejupielādi

CyberPhish

Nosūtītājs: WeTransfer <noreply@wetransfering-files.net>

Saņēmējs: es

Tēma: info@wetransfering-files.net **nosūtīja jums politika.doc, izmantojot WeTransfer**

we

info@wetransfering-files.net nosūtīja jums politika.doc, izmantojot WeTransfer

1 vienība, 25.6 KB kopā · Izbeidzas pēc 2 dienām

Svarīga informācija darbiniekiem!

Lūdzu, skatiet pievienoto konfidenciālo failu – atjaunināto organizācijas politiku. Lejupielādējiet to un uzmanīgi izlasiet, pretējā gadījumā jūs nevarēsiet piekļūt savām darba vietas telpām vai informācijas sistēmām. Sistēmu drošības komanda

Iegūt failu

Nosūtītājs: Microsoft drošības komanda <support@digi-support.com>

Saņēmējs:

Tēma: Svarīgi: datu drošības brīdinājums

Microsoft

Cienījamais Microsoft lietotāj!

Rūpējoties par jūsu tiešsaistes drošību, mēs nosūtām jums drošības ziņojumu. Mēs pamanījām, ka jūsu dokuments ar sensitīviem datiem ir brīvi pieejams internetā.

Atgādinām, ka, daloties ar citu personu sensitīvu informāciju, jūs pārkāpjat GDPR. Par to var uzlikt pamatīgu naudas sodu.

Lūdzu, lejupielādējiet dokumentu un mainiet koplietošanas opcijas.

Lejupielādēt dokumentu.

Microsoft drošības komanda

Mērķēta pikšķerēšana

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Mērķētas pikšķerēšanas ziņojumi ir vērsti uz katru paredzēto upuri, mērķētas pikšķerēšanas uzbrukumi notiek ilgā laika gaitā, mērķēta pikšķerēšana izmanto nulles dienas izmantojamības, uzņēmumiem trūkst vai tie neīsteno datoru lietošanas politikas, katrs pikšķerēšanas e-pasts izskatās autentisks, upuris izpilda pieprasījumu utt.
- **Mērķis:** darbinieki: Personāla priekšnieki C-komandā, grāmatvežu komanda, personāla nodaļa, algu nodaļa, utt.
- **Draudi:**
  - pikšķerēšanas uzbrukumi kopē mūsu esošās darbplūsmas
- **Pikšķerēšanas taktika:**
  - E-pasta ziņojumi ar pielikumiem: fails ar biznesa vai individuālu piedāvājumu, fails ar "konfidenciālu" vai "ļoti svarīgu" informāciju, pārdošanas vai finanšu (neapmaksāti rēķini, pirkuma pasūtījums) informācija, steidzams balss e-pasts
  - E-pasta ziņojumi ar saitēm uz viltotu vietni
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Uzbrucēji izmanto upura emocijas un instinktus**
- **Ievainojamības:**
  - darbinieki ar ierobežotām vai neesošām zināšanām par pikšķerēšanu
- **Rezultāts:**
  - Konfidenciālas informācijas zaudēšana, intelektuālā īpašuma zaudēšana, biznesa noslēpumu zaudēšana, inficētas digitālās ierīces utt.

Funded by the Erasmus+ Programme of the European Union

Mērķētas pikšķerēšanas e-pasta piemērs (priekšnieks/izpilddirektors): Pikšķerēšanas e-pasta ziņojumi ar pielikumu vai failu lejupielādi

CyberPhish

Nosūtītājs: Direktors <bill.jonson99@hotmail.com>

Saņēmējs: es

Tēma: Steidzami maksājums

Sveika, Džeina *[Jane]*,

Tagad esmu sapulcē dažas stundas, un man ir ierobežota piekļuve savam darba e-pastam un mobilajam tālrunim. Tikko saņēmu ziņu, ka esam nokavējuši maksājumu savam ekskluzīvajam partnerim.

Lai preces saņemtu laikā, lūdzu veic steidzamu maksājumu jau šodien tieši partnerim – piegādātājam.
Bankas rekvizīti, kas norādīti zemāk:
AA 12 3000 9852 0001 0020.

Maksājuma mērķis: par precēm

Paļaujos uz tevi.
Bils Džonsons *[Bill Jonson]*

Nosūtītājs: Rīkotājdirektors <Eva.Stivens53@yahoo.com>

Saņēmējs: es

Tēma: Pašreizējā mēneša algas

Sveiks, Tom *[Tom]*,

Es šodien strādāju no mājām, tāpēc rakstu no sava personīgā e-pasta.

Atjaunināju kārtējā mēneša algas un veicu vairākas izmaiņas. Atvainojos par šo pārpratumu, ceru, ka varēsi veikt izmaiņas un visiem darbiniekiem tiks samaksāts laikā.

Sazinies ar mani, ja ir kādi jautājumi.

Ar sveicieniem,
Eva Stīvensa *[Eva Stivens]*, Rīkotājdirektore

Updated-Salaries.xls

Tehniskā atbalsta pikšķerēšanas e-pasta ziņojumi

CyberPhish
Safeguarding your digital future

Pikšķerēšana: Tehniskais atbalsts

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?**
  Izmantojot digitālās ierīces, lietotāji parasti saņem dažādas kļūdas vai brīdinājumus. Tāpēc krāpnieki var pieprasīt tehnisko atbalstu un piedāvāt palīdzību drošības pārkāpumu novēršanā, izmantojot attālās piekļuves programmatūru vai noklikšķinot uz saites e-pastā.
- **Mērķis:** visi iedzīvotāji, īpaši cilvēki bez digitālajām prasmēm, vecāka gadagājuma cilvēki
- **Draudi:**
  - pikšķerēšanas uzbrukumi kopē mūsu esošās darbplūsmas
  - Uzbrucēji lūdz noklikšķināt uz e-pastā norādīto saiti vai zvanīt uz norādīto tālruņa numuru
- **Pikšķerēšanas taktika:**
  - E-pasta ziņojumi par uzlauztām e-pasta adresēm vai parolēm
  - E-pasta ziņojumi par koplietotiem dokumentiem sadarbībai
  - E-pasta ziņojumi par tehniskām problēmām
- **Pikšķerēšanas faktors:**
  - Tiek iedvesta steidzamības sajūta
  - Tiek iedvesta baiļu sajūta
  - Uzbrucēji izmanto upura emocijas un instinktus
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu
- **Rezultāts:**
  - Izspiedējprogrammatūra, inficēta digitālā ierīce, iegūta piekļuve digitālajai ierīcei, jo, piekļūstot ierīcei, krāpnieki vat to izmantot vēlākiem uzbrukumiem, mainīti ierīces iestatījumi,var nozagt sensitīvus datus, lietotājs var zaudēt naudu utt.

Uzbrucēji var izmantot arī cita veida paņēmienus:

Uznirstošie ziņojumi
Viltus vietnes (Par viltotām vietnēm skatiet sadaļu Vietņu pikšķerēšana)
Negaidīti zvani (par tālruņa un balss ziņu pikšķerēšanu skatīt sadaļā Tālruņa un balss ziņu pikšķerēšana)

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Tehniskā atbalsta pikšķerēšanas e-pasta piemērs

Nosūtītājs: Pasta iestatījumi <tech-support.954mail-delivery352477@cloud.website.com>

Saņēmējs: Lūsija Bredsone *[Lucy Bradson]*

Tēma: E-pasta piegādes kļūme

Sveiki, lucy.bradson

E-pasta serverim ir problēmas ar jūsu e-pasta apstiprināšanu.

Jūs nevarēsit saņemt jaunus e-pasta ziņojumus, kamēr nebūsiet verificējusi šo pastkasti.

Automātiski verificējiet savu pastkasti tūlīt, izmantojot tālāk sniegtos norādījumus.

UTO-VERIFICĒT PASTKASTI TAGAD

Ja netiks veiktas nekādas derīgas darbības, jūsu e-pasta konts tiks PĀRTRAUKTS pēc 24 stundām.

Ar cieņu, pastkastes administrators

Tehniskā atbalsta pikšķerēšanas telefona zvani

Tehniskā atbalsta pikšķerēšanas uznirstošā loga piemērs

Microsoft drošības brīdinājums

X

Jūsu datorā var būt vīruss.

Jums nekavējoties jāzvana
1 877 00 11 00 145, lai saņemtu palīdzību.

Jūsu IP adrese:
147.254.114.741

Datums:
2021. gada
11. oktobris

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Pikšķerēšanas e-pasta ziņojumi: Romantiskas attiecības (mincīšu pikšķerēšana)

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Ir cilvēki, kuri ir vieni, šķīrušies. Viņi var saņemt pikšķerēšanas e-pasta ziņojumus vai sociālo mediju ziņojumus no krāpniekiem vai arī no iepazīšanās vietnēm.
- **Mērķis:** vieni, šķīrušies cilvēki, cilvēki, kas meklē jaunas attiecības, sociālo tīklu lietotājus
- **Draudi:**
  - Krāpnieki ar viltotu identitāti ātri uzsāk attiecības un iegūst upura uzticību. Pēc tam krāpnieki pieprasa naudu un pēc tās saņemšanas pazūd.
- **Pikšķerēšanas taktika:**
  - E-pasts no nezināmas personas
  - Īsziņa, izmantojot sociālos tīklus, tūlītējās ziņojumapmaiņas programma
- **Pikšķerēšanas faktors:**
  - **Ātra nokļūšana attiecībās**
  - **Upura uzticības iegūšana pēc iespējas ātrāk**
- **Ievainojamības:**
  - emocionāli ievainojami pilsoņi
- **Rezultāts:**
  - finansiāli zaudējumi.

Funded by the Erasmus+ Programme of the European Union

Piemērs: Romantiskas attiecības (mincīšu pikšķerēšana)

Nosūtītājs: Džons Džons *[John John]* <john.19850215@gmail.com>
Saņēmējs: es

Tēma: manai mīlai

Mana mīļā,

Esmu ļoti priecīgs, ka man ir iespēja tevi atrast, jo tikai tu visā pasaulē vari mani saprast. Jūtu, ka tu esi mana otrā pusīte. Zinu, ka tūkstoš kilometru mūsu ciešās attiecības neietekmēs.
Es darīšu visu iespējamo, lai ierastos tavā valstī, mainītu savu darba vietu un pavadītu visu savu atlikušo dzīvi lielā laimē kopā ar tevi.

Es gaidu tavu ziņojumu.

Tava mīlestība – Džons *[John]*

Ilustrāciju nodrošina Freepik Storyset

Nosūtītājs: Džons Džons *[John John]* <john.19850215@gmail.com>
Saņēmējs: es

Tēma: manai mīlai

Sveika, mana mīla,

Tu neticēsi, bet es gribēju pārsteigt un satikt tevi tavā pilsētā. Kad nolaidos Frankfurtē, uz citu lidmašīnu bija jāgaida 18 stundas. Tāpēc es devos uz pilsētas viesnīcu, un šeit man tika nozagta soma. Vai tu varētu man palīdzēt, lūdzu. Es paliku viesnīcā, un rīt man jāsedz viesnīcas rēķins. Vai tu, lūdzu, varētu segt manas uzturēšanās izmaksas?

Ar nepacietību gaidu satikt tevi pēc iespējas ātrāk, mana dārgā.

Tava mīlestība – Džons *[John]*

Ēsmas izlikšana

Ēsmas izlikšana

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Cilvēki mēdz uzticēties un tic, ka varētu kaut ko dabūt bez maksas, kaut ko nopirkt ar atlaidi, saņemt naudu vai laimestus.
- **Mērķis:** visi pilsoņi, tostarp darbinieki
- **Draudi:**
  - krāpnieki piedāvā kaut ko ļoti pievilcīgu, piemēram, mūzikas lejupielādi, filmas, negaidītas uzvaras vai balvas, milzīgas atlaides un tā tālāk.
- **Pikšķerēšanas taktika:**
  - E-pasts, uznirstošie logi, īsziņas, ieraksti sociālajos tīklos ar ļoti pievilcīgiem piedāvājumiem
  - Biroja telpu tuvumā pazaudēti USB diskdziņi
- **Pikšķerēšanas faktors:**
  - **Viltus solījumi**
  - **Tiek iedvesta alkatības sajūta**
  - **Tiek iedvesta ziņkārība**
- **Ievainojamības:**
  - Mantkārīgi vai ziņkārīgi pilsoņi, neuzmanīgi darbinieki
- **Rezultāts:**
  - Iegūta sensitīva informācija, identitātes zādzība, intelektuālā īpašuma zādzība, sabotāža, naudas zaudēšana, instalēta ļaunprātīgu programmatūru.

Funded by the Erasmus+ Programme of the European Union

Ēsmas izlikšanas pikšķerēšanas e-pasts: Atlaižu krāpniecība

Nosūtītājs: Melnās piektdienas piedāvājums <Black-Friday-Proposal@trust-fridays.com>

Saņēmējs: es

Tēma: Apsveicam! Jūs esat ieguvis slepenās cenas

www.trust-fridays.com/discounts/sdtuyx5D7rtkh6

Neticami milzīgas atlaides vai zemas cenas ļoti labi zināmiem zīmoliem un produktiem

Ēsmas izlikšanas pikšķerēšanas e-pasts: Nodokļu atmaksa un Covid-19

Nosūtītājs: Valdības iestāde <do-not-reply@online-gateway.com>
Saņēmējs: es
Tēma: Valsts atmaksa par Covid-19

Iesniegšanai pēc pieprasījuma

Valdība ir veikusi pasākumus, lai palīdzētu iedzīvotājiem un organizācijām, kas cieš no Covid-19.

Informējam, ka jums ir tiesības saņemt vienreizēju atmaksu USD 2500 apmērā. Lai saņemtu šo atmaksu, jums ir jāaizpilda šī tiešsaistes veidlapa.

Šo ziņojumu automātiski ģenerēja valdības vārteja

Krāpnieki var sekot līdzi reāliem notikumiem un izmantot tos uzbrukumiem, kā arī piedāvāt pieprasītus produktus vai atgūt nodokļus, kā tas ir šajā piemērā.

Funded by the Erasmus+ Programme of the European Union

Ēsmas izlikšanas piemēri. Pikšķerēšanas e-pasts: Laimesti, godalgas

Nosūtītājs: Eida Gudčailda *[Ade Goodchild]* <admin>

Saņēmējs: es

Tēma: Dārgais,

Dārgais,

Jūsu e-pastu nejauši izvēlējās mans fonds, jums ir jāsaņem ziedojums 1 000 000,00 (viens miljons mārciņu), kas jums ir jāizmanto vismaz 20% apmērā, lai ietekmētu mazāk priviliģēto cilvēku dzīves ap jums.
Es tikko uzsāku fonda darbību.

Lasiet vairāk par to, kā es kļuvu par miljonāri. https://www.bbc.cominews/uk-england-hereford-worcester-47637306

Lūdzu, apstipriniet sava e-pasta īpašumtiesības, nekavējoties nosūtot man atbildi, un es jums detalizēti paskaidrošu, kas jums jāzina.

Ar cieņu,
Eida Gudčailda *[Ade Goodchild]*
Gudčaildas fonds

Ēsmu izlikšanas krāpnieki var nosūtīt e-pasta ziņojumus, informējot upurus par laimestu, balvām un vieglu naudu.

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

Funded by the Erasmus+ Programme of the European Union

Teksta īsziņas

- Īsziņas, kas nosūtītas pa tālruņiem, lietotnēm vai sociālo mediju platformām.
- Uzbrucēji var izmantot šādu taktiku:
  - Pieprasa nosūtīt sensitīvu informāciju īsziņās
  - Lūdz noklikšķināt uz īsziņā norādītās saites
  - Lūdz atvērt pielikumu
  - Zvanīt uz norādīto tālruņa numuru
- Parastās pikšķerēšanas īsziņu tēmas:
  - Atjauniniet personīgo vai preču piegādes informāciju
  - Saņemiet milzīgu atlaidi vai piedalieties konkursā par balvu
  - Problēmas ar e-pasta vai cita pakalpojuma kontu
  - Romantiskas attiecības
  - Finansiālu atbalsta sniegšana

Funded by the Erasmus+ Programme of the European Union

Teksta īsziņas

- Īsziņas var tikt maskētas kā no uzticamiem avotiem
- Pikšķerēšanas īsziņas var saņemt, izmantojot dažādas platformas:
  - **Tūlītējā ziņapmaiņa** (Hangouts, Skype u.c.)
  - **Sociālo mediju platformas vai lietotnes** (Instagram, Facebook, LinkedIn, Snapchat, Twitter u.c.)
  - **SMS pikšķerēšana –** *angl.* **smishing** (ieskaitot WhatsApp, Telegram, Viber)
- Tiek izmantoti saīsināšanas URL pakalpojumi

Funded by the Erasmus+ Programme of the European Union

Teksta īsziņas
Sociālie mediji un tūlītējā ziņapmaiņa (IM)

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Grūti atšķirt no īstiem ziņojumiem (parasti krāpnieki izmanto tūlītējās ziņojumapmaiņas tārpus, kas inficē ierīces pēc noklikšķināšanas uz saites vai pielikuma atvēršanas) utt.
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - ziņas ar pielikumiem, ar saitēm, ziņojumi ar lūgumu sniegt finansiālu atbalstu, ziņas no romantiskiem krāpniekiem utt.
- **Uzbrukuma metode:** īsziņas no tērzēšanas vai sociālo tīklu kontaktpersonām vai nezināmām personām.
- **Pikšķerēšanas taktika:**
  - Īsa ziņa (parasti viens vai divi teikumi) ar saiti. Ziņojumos tiek lūgts atjaunināt kontu, mainīt iestatījumus, atvērt dokumentus vai attēlus, ieteikt labas atlaides utt.
  - Īsa ziņa (parasti viens vai divi teikumi) ar pielikumu.
  - Īsziņas ar lūgumu sniegt finansiālu atbalstu
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu un tādi, kas nesagaida, ka notiks pikšķerēšanas mēģinājumi pret viņiem, izmantojot tūlītējo ziņapmaiņu
- **Rezultāts:**
  - Inficētas digitālās ierīces, identitātes zādzība, akreditācijas datu zādzība, naudas zaudēšana

Īsziņas
Tūlītējās ziņojumapmaiņas (IM) pikšķerēšanas piemēri

CyberPhish

Džons Džons *[John John]*

Vai redzēji?

Tas esi tu bildē?

http://livegogle.com/images/family15.jpg

Loren_18

Sveiks, noskatieties manu privāto video. Nedalies tajā ar nevienu.
http://y2u-videos.info/Y7zNlEMDmI4

Samanta *[Samantha]*

Es kopīgoju ar tevi tiešsaistes dokumentu:
https://docs.google.com/document/d/ba?usp=sharing

Drošības administrators

Jūsu kontam šodien beigsies derīguma termiņš. Lūdzu, noklikšķiniet uz saites un aktivizējiet savu kontu
www.skype-admin.info/account-update?ID=7844156

Debija Borna *[BDebbie Buorn]*

Vai vēlies uzzināt, kas ir apskatījis tavu Facebook profilu?

Tagad tas ir iespējams. Jums tikai jāinstalē lietotne savā ierīcē.

Saite uz lietotni:
http://bit.ly/38fCIdxS

Džims Loans *[Jim Lohan]*

Jūs laimējāt dāvanu karti 1000 eiro vērtībā. Aktivizējiet to
https://bit.ly/3ALiAkE

Teksta īsziņas
Sociālo mediju pikšķerēšanas piemēri

Instagram

Sveiki! Kāds vairākas reizes nesekmīgi mēģināja pieteikties jūsu kontā. Drošības apsvērumu dēļ jūsu konts ir bloķēts.
Lai atbloķētu, lūdzu, pierakstieties šeit un ievadiet šo kodu:
753147

Instagram

Mēs atklājām, ka esat ievietojis saturu, uz kuru attiecas autortiesības. Jūsu konts tika deaktivizēts.

Noklikšķiniet šeit, lai aktivizētu savu kontu.

Instagram

https://www.livegogle.com/images/family15.jpg

SMS pikšķerēšana

CyberPhish

Teksta īsziņas: SMS (SMS pikšķerēšana)

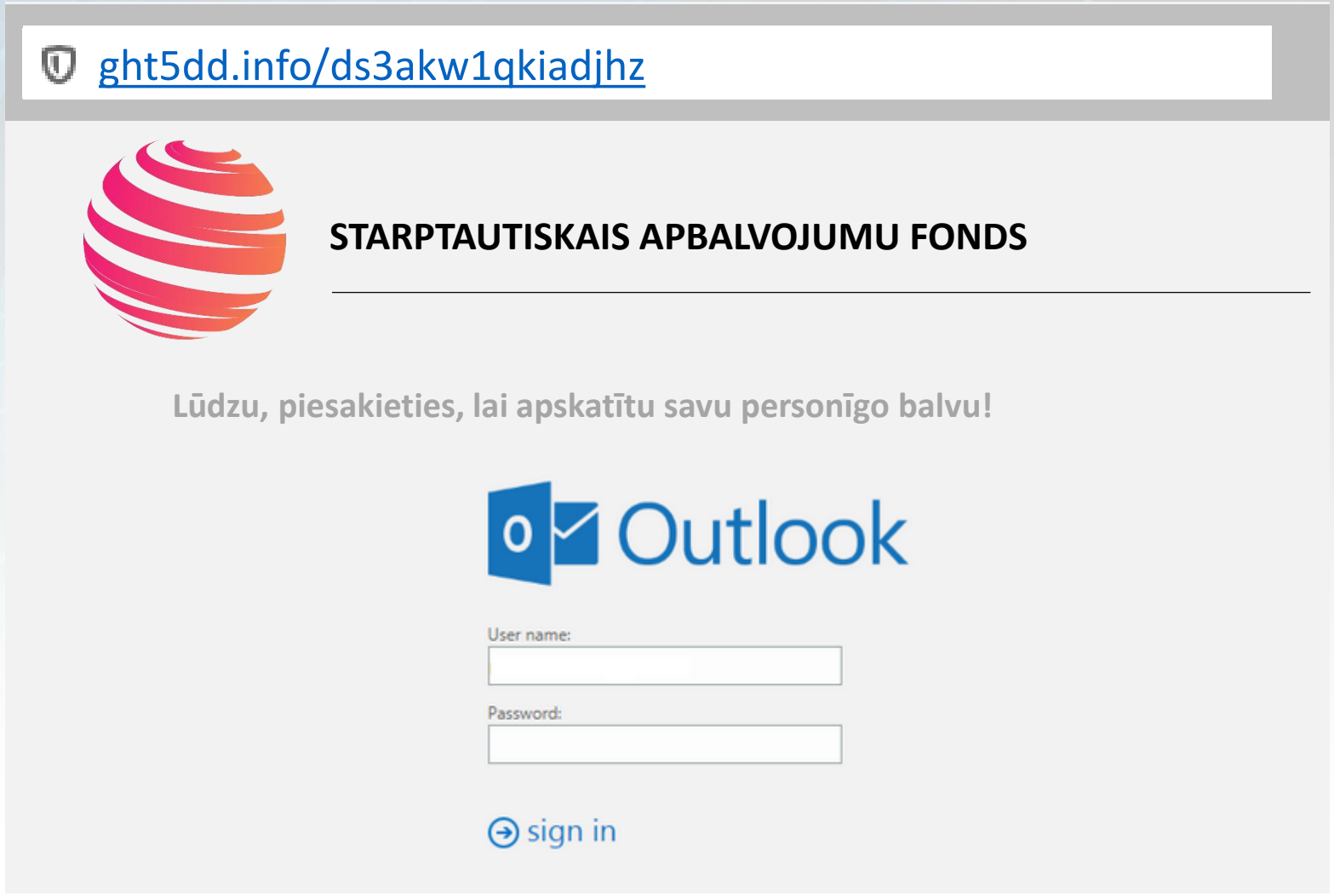
- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** To ir grūti atšķirt no īstajiem ziņojumiem
-

  (parasti krāpnieki izmanto reālus iestāžu nosaukumus)
- **Mērķis:** visi iedzīvotāji
- **Draudi:**
  - ziņas ar saitēm, ziņas ar lūgumiem sniegt finansiālu atbalstu, lūgumi atbildēt vai piezvanīt
- **Uzbrukuma metode:** SMS teksta īsziņas.
- **Pikšķerēšanas taktika:**
  - Īsa ziņa (parasti viens vai divi teikumi) ar saiti. Ziņojumos tiek lūgts mainīt iestatījumus, atjaunināt kontus, mainīt sūtījuma datus utt.
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu un tādi, kas nesagaida, ka notiks pikšķerēšanas mēģinājumi pret viņiem, izmantojot SMS
- **Rezultāts:**
  - Inficētas digitālās ierīces, identitātes zādzība, akreditācijas datu zādzība, naudas zaudēšana

Teksta īsziņas: SMS pikšķerēšanas taktika

http://www.nat1onalbank.com?profile

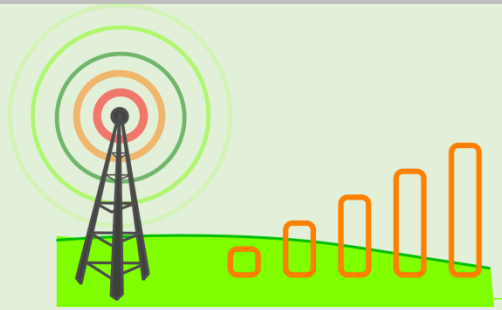
Teksta īsziņas: SMS pikšķerēšanas piemēri



Teksta īsziņas. SMS pikšķerēšanas piemēri

CyberPhish

https://bit.ly/2YI6BY6



Lūdzu, norādiet pieteikšanās informāciju, lai redzētu atjauninājumu informācijas paneli

Lietotājvārds

Parole

Lūdzu, atjauniniet savu maksājumu informāciju

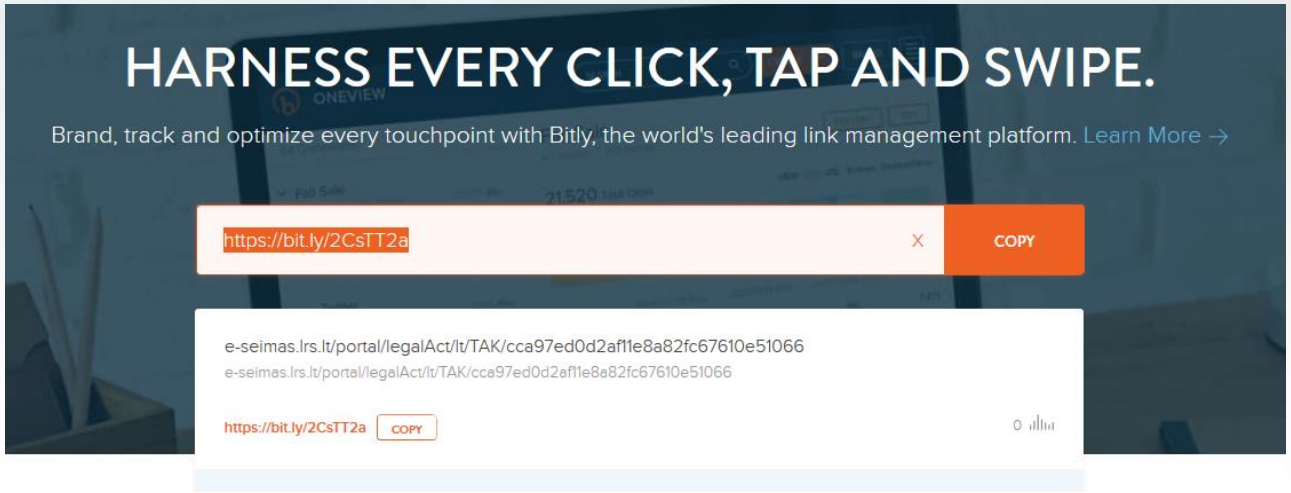
Kredītkartes numurs

CSV drošības kods

Teksta īsziņas: SMS pikšķerēšanas piemēri

URL saīsināšanas pakalpojumi

- URL (interneta saišu) saīsināšanas pakalpojumi tiek plaši izmantoti. Šādu pakalpojumu piemēri:
  - Bitly
  - youtu.be
  - Rebrandly
  - TinyURL
  - BL.INK
  - URL Shortener by Zapier
  - Shorby
  - Short.io



CyberPhish
Safeguarding your digital future

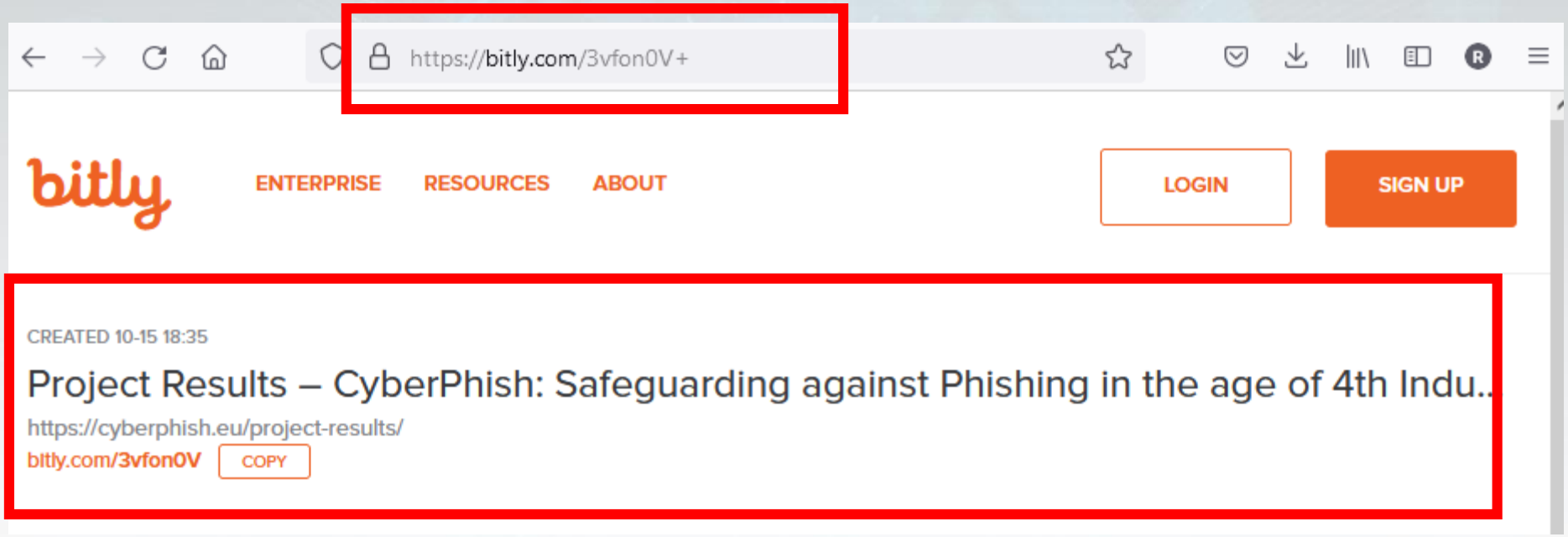
Funded by the Erasmus+ Programme of the European Union

URL saīsināšanas pakalpojumu izmantošanas mērķi

- Grūti iegaumēt garu URL saiti
- Ērta lietošana tīmekļa vietnēs, sociālajos medijos, drukātajos izdevumos
- Īsa URL saite ir ērta, sūtot SMS, tūlītējās ziņapmaiņas ietvaros
- Ir saīsināšanas pakalpojumu sniedzēji, kas var ģenerēt cilvēku salasāmas URL saites.

Funded by the Erasmus+ Programme of the European Union

Apskatiet bit.ly saiti: saites galā iespējams pierakstīt +



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pārbaudiet informāciju par vietni

CyberPhish

http://checkshorturl.com

Get long URL from hundreds of URL shortening services

Ensure your safety and prevent unsuitable content while surfing on the World Wide Web

https://bitly.com/3vfon0V | Expand

Long URL	https://cyberphish.eu/project-results/
Delay	0.96 second(s)
Short URL	https://bitly.com/3vfon0V
Redirection	301
Search long URL on	Yahoo | Google | Bing
Check if safe on	Web Of Trust | SiteAdvisor | Google | Sucuri | Norton
Title	Project Results – CyberPhish: Safeguarding against Phishing in the age of 4th Industrial Revolution
Description	N/A
Keywords	N/A
Author	N/A

Pārbaudiet informāciju par vietni

- http://www.getlinkinfo.com: Noskaidrojiet, vai vietnē nav ietverta ļaunprātīga programmatūra vai tā ir pikšķerēšanas vietne

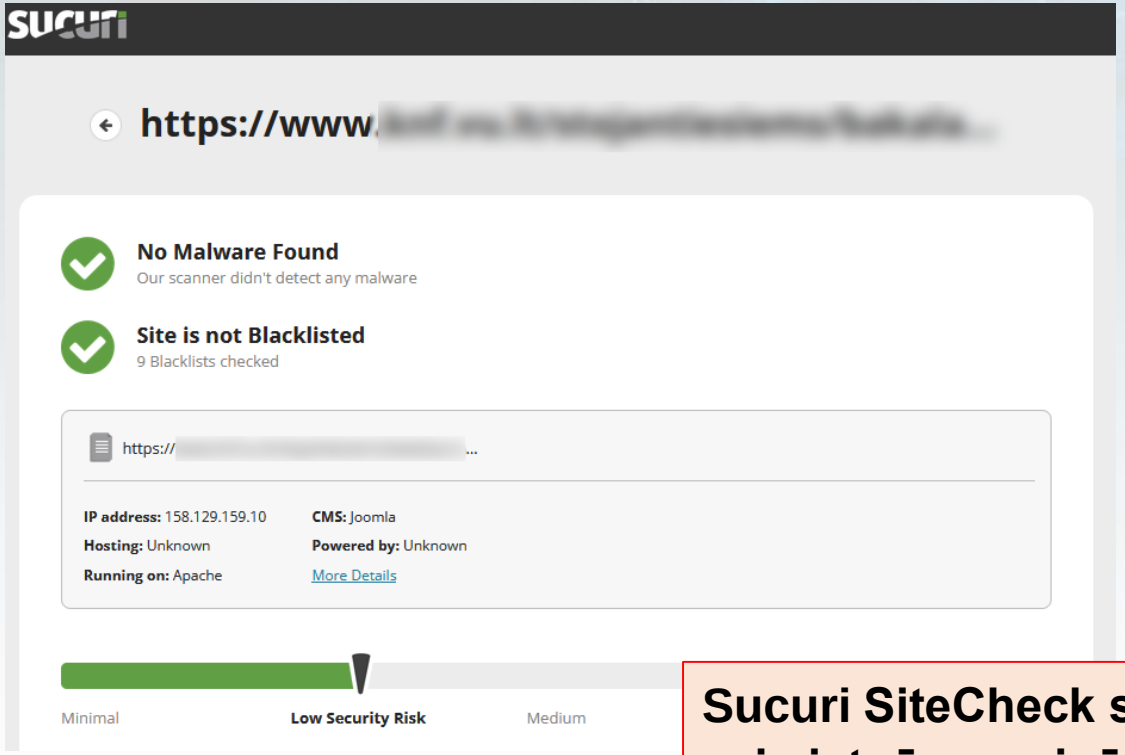
CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

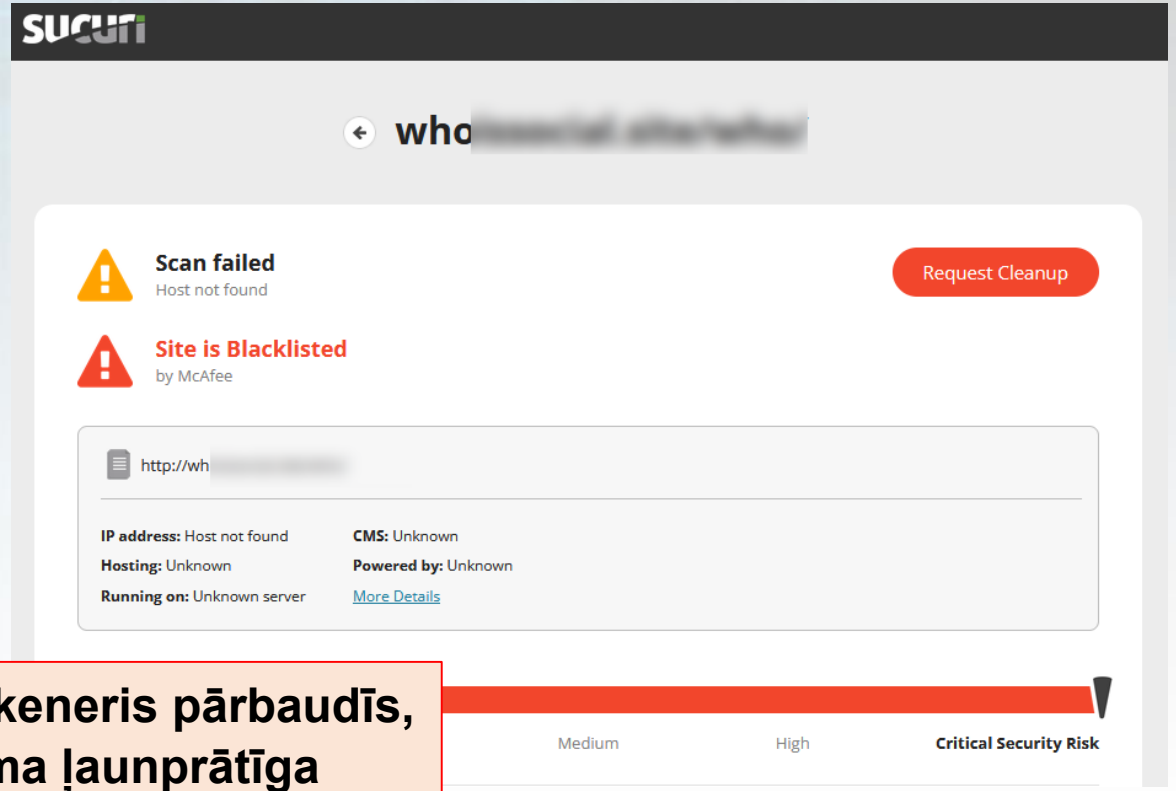
Pārbaudiet informāciju par vietni

https://sitecheck.sucuri.net

Droša noskenēta vietne



Nedroša noskenēta vietne



Sucuri SiteCheck skeneris pārbaudīs, vai vietnē nav zināma ļaunprātīga programmatūra, vīrusi, melnajā sarakstā iekļautības statuss, vietnes kļūdas, novecojusi programmatūra un ļaunprātīgs kods.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana

- Vietņu pikšķerēšanu sauc arī par viltošanu
- Ir vairāki veidi, kā vietnēs tiek izmantota pikšķerēšana
  - **Viltus vietnes ar viltotu URL** – ļoti labi zināmu iestāžu vai organizāciju vietņu viltotas kopijas, kurām lietotāji uzticas *
  - **Pašpārvaldītas tīmekļa vietnes** – krāpnieki izstrādājuši savas tīmekļa vietnes, piemēram, viltus interneta veikalus, investīciju portālus *
  - Bezmaksas hostinga pakalpojumi
  - Uznirstošie logi vietnēs
  - **Sludinājumu bloki**, kas tiek izmantoti portālos, pat uzticamās vietnēs
- Saites uz viltus vietnēm tiek izmantotas pikšķerēšanas e-pastos, SMS, tūlītējās ziņojumos, sociālajos saziņas līdzekļos utt.
- Meklētājprogrammas var arī nodrošināt saites uz bīstamām vietnēm *

* www.uni-mannheim.de/en/information-security/security-tips/spam-and-phishing/examples-and-current-warnings/#c230018

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana

- Šādu viltus vietņu galvenais mērķis:
  - Iegūt pieteikšanās akreditācijas datus informācijas sistēmās, e-pastos
  - Iegūt finanšu informāciju, piemēram, bankas karšu datus un drošības kodus
  - Inficēt lietotāju ierīces, jo šādas vietnes var saturēt ļaunprātīgu kodu
- Krāpnieki var izmantot līdzīgus domēna nosaukumus, lai piešķirtu maldinošu likumību tīmekļa lapai, parasti domēna nosaukumā aizstājot vienu vai vairākus burtus, piemēram, izmantojot burtu “l”, nevis “i”; piemērs:
  - Oriģinālā vietne: www.website.eu
  - Viltus vietne: www.webslte.eu

Vairāk par HTTPS:
https://www.cloudflare.com/learning/ssl/what-is-https

https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana

- Viltus tīmekļa vietnēs tiek izmantots tāds pats dizains, logotipi un krāsas kā likumīgai vietnei, tāpēc tās ir grūti atpazīt. Tāpēc ir jāpārbauda citi rādītāji, piemēram:
  - URL adrese,
  - Kontaktdati;
  - Esiet piesardzīgi, sniedzot akreditācijas datus vai finanšu datus, atverot jebkuru saiti no e-pasta.

Viltus vietnes adrese

- Viltus vietņu URL saites parasti sākas ar HTTP
- Viltus vietnes arī var sākties ar HTTPS
- HTTPS izmanto SSL sertifikātu, pārbauda vietnes īpašumtiesības un nodrošina lietotāja datu drošību: nodrošina drošu datu pārraidi starp klientu un serveri, bet nenorāda, ka vietne ir likumīga

Vairāk par HTTPS:
https://www.cloudflare.com/learning/ssl/what-is-https

https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Viltus vietnes ir grūti atšķirt no īstām vietnēm, tiek izmantoti citi pikšķerēšanas faktori, lai mudinātu lietotājus atvērt vietnes, veikt noteiktas darbības.
- **Mērķis:** visi iedzīvotāji
- **Uzbrukuma metode:** e-pasti, SMS, tūlītējās ziņas, ieraksti sociālajos tīklos, kombinētās metodes.
- **Pikšķerēšanas taktika:**
  - E-pasts vai ziņa ar saiti. Ziņojumos tiek lūgts atjaunināt kontu, mainīt iestatījumus, atvērt dokumentus vai attēlus, ieteikt labas atlaides utt.
  - Lietotāji var atrast viltotas vietnes, izmantojot meklētājprogrammu: tās var būt interneta veikala preces ar labām atlaidēm
  - Krāpnieki var piezvanīt upuriem, aicinot viņus veikt veiksmīgus ieguldījumus
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Iedvesmo uz alkatību**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu un tādi, kas nesagaida, ka notiks pikšķerēšanas mēģinājumi pret viņiem
- **Rezultāts:**
  - Inficētas digitālās ierīces, identitātes zādzība, akreditācijas datu zādzība, naudas zaudēšana

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana: Vietņu pikšķerēšanas piemēri

http://sale-branding.store

Dr iepirkšanās tiešsaistē

LABĀKĀS CENAS! VISI ZĪMOLI VIENĀ VIETĀ AR 90% ATLAIDI TIKAI ŠODIEN!

Funded by the Erasmus+ Programme of the European Union

Vietņu pikšķerēšana: Vietņu pikšķerēšanas piemēri

CyberPhish

http://mobile-company.online/prizes

APSVEICAM!
Mūsu uzņēmums šogad svin savu jubileju, tāpēc mēs dalāmies priekā ar saviem klientiem un aicinām jūs saņemt savu balvu pilnīgi bez maksas.

Laimējiet kādu no tālāk norādītajām balvām: Samsung Galaxy S21, Apple iPhone 13 Pro vai Samsung Watch 4 LTE.

Jau 153 dalībnieki šobrīd priecājas par balvām. Balvu skaits ir ierobežots!

Jums rezervēts laiks: 1 min. 29 sekundes.

GRIBU SAŅEMT SAVU BALVU!

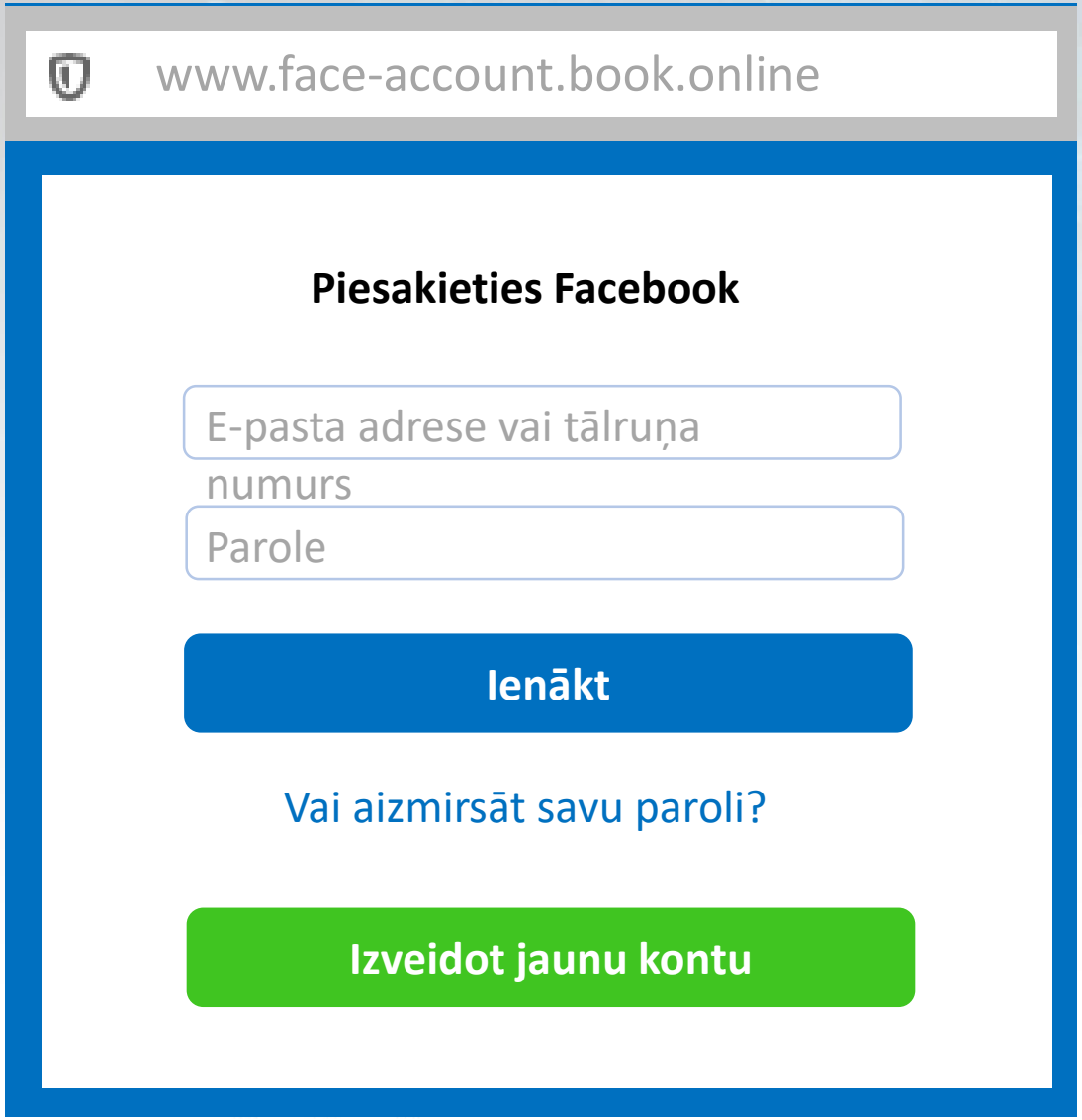
http://mobile-company.online/iwantget

Samsung Galaxy S21
Cena: EUR 780
Izpārdots
Nav pieejams

Apple iPhone 13 Pro
Cena: EUR 920
Pieejamas tikai 2 preces
Saņemt tūlīt!

Samsung Watch 4 LTE
Cena: EUR 320
Izpārdots
Nav pieejams

Vietņu pikšķerēšana: Vietņu pikšķerēšanas piemēri



Funded by the Erasmus+ Programme of the European Union

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

Funded by the Erasmus+ Programme of the European Union

Viltus loterijas

- Loteriju krāpnieki izmanto dažādus rīkus, lai notvertu savus upurus:
  - E-pasts
  - SMS vai ziņas, izmantojot tūlītējās ziņojumapmaiņas programmas
  - Ziņa sociālajos tīklos no viltota vai uzlauzta konta
  - Zvans pa tālruni
  - Tīmekļa lapas
- Upuri tiek vilināti ar milzīgu naudas summu, lielu balvu, piemēram, automašīnām, digitālajām ierīcēm vai citām dārgām precēm
- Tās var atsaukties uz likumīgu loteriju, aģentiem vai mantiniekiem, kam nepieciešama palīdzība

Funded by the Erasmus+ Programme of the European Union

Viltus loterijas

- Galvenās pazīmes, kas liecina par izkrāpšanu loterijā *
  - Ir jāsniedz personiskā un finanšu informācija
  - Ja krāpnieki pieprasa samaksāt noteiktu naudas summu, lai palielinātu iespēju laimēt
  - Lai saņemtu balvu, ir jāmaksā īpaša maksa
- Loteriju krāpnieki sagaida personas un finanšu informācijas izgūšanu vai izmanto viltību, lai saņemtu naudu, piemēram, honorārus, nodokļus, piegādes maksas, neatbilstības starp valūtām vai naudu citu izdevumu segšanai, apmaksas ar dāvanu kartēm, lai saņemtu balvas utt.
- Tās var lūgt veikt noteiktas darbības un kādu laiku neizpaust informāciju par laimestu, t.i. paturēt to noslēpumā.

* www.consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

Funded by the Erasmus+ Programme of the European Union

Loteriju krāpniecība

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Viltus vietnes ir grūti atšķirt no īstām vietnēm, tiek izmantoti citi pikšķerēšanas faktori, lai mudinātu lietotājus atvērt vietnes, veikt noteiktas darbības.
- **Mērķis:** visi iedzīvotāji
- **Uzbrukuma metode:** e-pasti, SMS, tūlītējās ziņas, ieraksti sociālajos tīklos, kombinētās metodes.
- **Pikšķerēšanas taktika:**
  - E-pasts vai ziņa ar saiti. Ziņojumos tiek lūgts atjaunināt kontu, mainīt iestatījumus, atvērt dokumentus vai attēlus, ieteikt labas atlaides utt.
  - Lietotāji var atrast viltotas vietnes, izmantojot meklētājprogrammu: tās var būt interneta veikala preces ar labām atlaidēm
  - Krāpnieki var piezvanīt upuriem, aicinot viņus veikt veiksmīgus ieguldījumus
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Iedvesmo uz alkatību**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par pikšķerēšanu un tādi, kas nesagaida, ka notiks pikšķerēšanas mēģinājumi pret viņiem
- **Rezultāts:**
  - Inficētas digitālās ierīces, identitātes zādzība, akreditācijas datu zādzība, naudas zaudēšana

Piemērs: Loteriju krāpniecība

Nosūtītājs: Nacionālā loterija <jim-*Stanley*@info-winlottery.online>

Saņēmējs: es

Tēma: Apsveicam!

Cien. lietotāj!

Vēlamies informēt, ka jūsu e-pasts tika izvēlēts, lai varētu pieprasīt summu 150 000 EUR apmērā.

Lai saņemtu naudu, lūdzu, izpildiet pievienotos norādījumus.

Nacionālā loterijas komanda
Izpilddirektors Džims Stenlijs [Jim Stanley]

Norādījumi-uzvarētājiem.pdf

Citi loteriju piemēri, kas sniegti šādos slaidos:

- E-pastu sadaļa
- Tūlītējās ziņojumapmaiņas slaids
- SMS pikšķerēšanas slaids
- Vietņu pikšķerēšanas sadaļa

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Telefona zvani: Tālruņa un balss ziņu pikšķerēšana

- Tālruņa un balss ziņu pikšķerēšanu var izskaidrot kā balss pikšķerēšanu
- Uzbrucēji izmanto rūpīgi izstrādātus scenārijus un metodes, lai iegūtu upuru pārliecību
- Tālruņa un balss ziņu pikšķerēšanu var apvienot ar citām sociālās inženierijas metodēm
- Dažreiz uzbrucējs pirms zvanīšanas upurim var veikt izpēti, lai iegūtu lielāku pārliecību

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Telefona zvani: Tālruņa un balss ziņu pikšķerēšana

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Viltus zvanus ir grūti atšķirt no īstiem. Uzbrucējs pārstāv sevi kā citu personu vai juridiskas institūcijas, piemēram, policijas vai bankas, pārstāvi, neizmantojot citus tehniskos rīkus, izņemot tālruni, izmanto manipulācijas, izmanto cilvēku bailes, autoritāti vai vēlmes, lai iegūtu sensitīvu informāciju .
- **Mērķis:** visi iedzīvotāji
- **Uzbrukuma metode:** zvani pa tālruni, zvani, izmantojot tūlītējās ziņojumapmaiņas programmas, piemēram, Viber. Uzbrucēji var izmantot citas metodes, piemēram, viltotas vietnes.
- **Tālruņa un balss ziņu pikšķerēšanas taktika:**
  - Krāpnieks, kurš uzdodas par juridiskas organizācijas darbinieku, parasti piezvana upurim un nodrošina investīciju iespējas; krāpnieki var izlikties par policijas pārstāvi, iebiedēt upuri ar finanšu mahinācijām viņa kontā, lai piekļūtu upura bankas kontam.
- **Pikšķerēšanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta baiļu sajūta**
  - **Iedvesmo uz alkatību**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par tālruņa un balss ziņu pikšķerēšanu
- **Rezultāts:**
  - naudas līdzekļu zaudējumi

Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Klātienes tikšanās: Distances neievērošana

- Distances neievērošanas uzbrukumi, ko dēvē arī par “parazitēšanu”, tiek izmantoti, ja kibernoziedznieks izmanto uzņēmuma darbiniekus, lai iekļūtu organizācijas ierobežotas piekļuves telpās.
- Piekļuve ierobežotajai zonai ir atļauta tikai pilnvarotam personālam

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Klātienes tikšanās: Distances neievērošana

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Milzīgās organizācijās darbinieki varēja nepazīt citus kolēģus, cilvēki mēdz uzticēties svešiniekiem.
- **Mērķis:** darbinieki lielās organizācijās
- **Uzbrukuma metode:** uzbrucējs var izlikties par jaunu darbinieku, par pakalpojumu sniedzēju, par preču piegādes palīgu utt.
- **Distances neievērošanas taktika:**
  - Kibernoziedznieki vienkārši piemāna un apmuļķo vienu no pilnvarotajiem darbiniekiem, sekojot viņam aiz muguras, lai iekļūtu telpās.
  - Uzbrucējs var izlikties par piegādes aģentu, kuram rokās ir vairākas kastes, par ēdienu piegādātāju un lūgt personālam atvērt durvis.
  - Vēl viens šī uzbrukuma piemērs varētu būt izlikšanās par uzņēmuma darbinieku un sarunu uzsākšana valsts uzņēmumu zonās, piemēram, smēķēšanas zonās. Pēc pārtraukuma viltvārdis var doties ēkā kopā ar izvēlēto darbinieku, kas ļāvies sarunām, sekojot viņam aizliegtajā zonā.
- **Distances neievērošanas faktors:**
  - **Tiek iedvesta steidzamības sajūta**
  - **Tiek iedvesta pašpārliecinātība**
  - **Naivuma izmantošana**
- **Ievainojamības:**
  - darbinieki ar ierobežotām vai neesošām zināšanām par distances neievērošanas uzbrukumu
- **Rezultāts:**
  - Nepiederošai personai nokļūstot aizliegtajā zonā, var tikt nodarīts milzīgs kaitējums.
  - Kad nepiederošā persona nokļūst ierobežotajā zonā, viņš var veikt uzbrukumu, piemēram, datu zādzību, datu pārkāpumu, ļaunprātīgas programmatūras uzbrukumus un tā tālāk.

Funded by the Erasmus+ Programme of the European Union

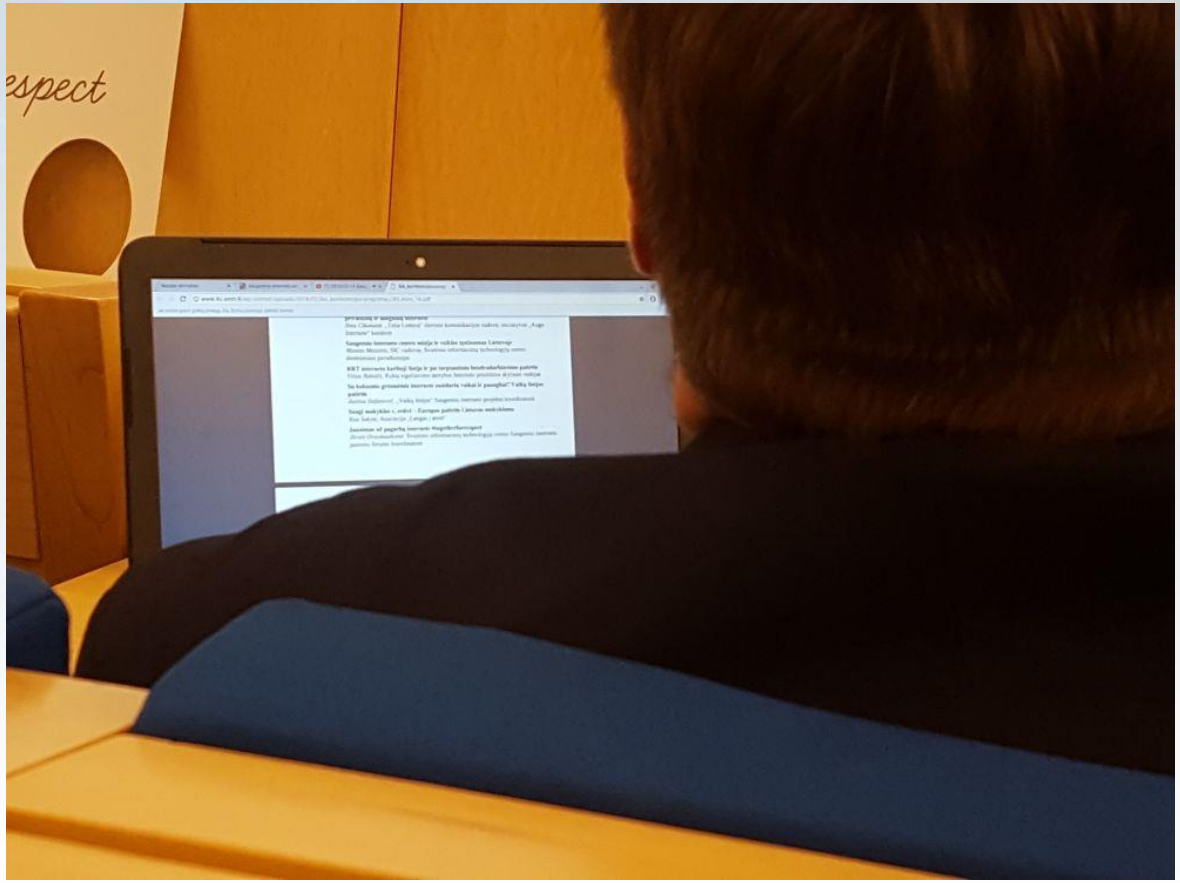
Saturs

Uz notikumiem balstīti uzbrukumi	E-pasti	Teksta īsziņas	Mājaslapas
Viltus loterijas	Telefona zvani	Tikšanās klātienē	Datu noskatīšanās pār plecu

Funded by the Erasmus+ Programme of the European Union

Datu noskatīšanās pār plecu

- Datu noskatīšanās pār plecu ir efektīvs veids, kā uzraudzīt kāda datora, viedtālruņa vai bankomāta ekrānu, lai personīgi piekļūtu sistēmas datiem, piemēram, pieteikšanās vārdiem un parolēm, PIN kodiem vai citai sensitīvai informācijai.
- Uzbrucējs var novērot, stāvot cieši pie ekrāna, klausoties mutiski sniegtos sensitīvos datus, vai arī uzbrucējs var izmantot tīmekļa kameras, lai ievāktu nepieciešamos datus



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Klātienes tikšanās: Datu noskatīšanās pār plecu

- **Kāpēc šāda veida uzbrukumi ir sekmīgi?** Cilvēki, kuri parasti strādā ar portatīvajiem datoriem un viedierīcēm sabiedriskās vietās, sabiedriskos pasākumos, sabiedriskajā transportā, neaizdomājas par to, ka kāds varētu novērot viņa ekrānu, un nedomā par sekām.
- **Mērķis:** visi iedzīvotāji
- **Uzbrukuma metode un taktika:** uzbrucējs var izlikties par parastu cilvēku, kas sēž vai stāv blakus upurim, bet patiesībā skatās upura ekrānā un ievāc sensitīvus lietotāja datus. Lai neradītu aizdomas, krāpnieki var izmantot tīmekļa kameras.
- **Distances neievērošanas faktors:**
  - **mērķis ir iedvesmot pārliecību**
- **Ievainojamības:**
  - iedzīvotāji ar ierobežotām vai neesošām zināšanām par datu noskatīšanos pār plecu
- **Rezultāts:**
  - nozagti personīgās pieteikšanās sistēmas dati, piemēram, pieteikšanās vārdi un paroles, PIN kodi vai cita sensitīva informācija.

Funded by the Erasmus+ Programme of the European Union

Kopsavilkums: Pikšķerēšanas (personas datu izmānīšanas) uzbrukumi

Uz notikumiem balstīti uzbrukumi	E-pasti	Tūlītējā ziņapmaiņa (mirkļsaziņa)	Sociālie tīkli
Mājaslapas	Viltus loterijas	SMS (īsziņas)	Telefona zvani
	Tikšanās klātienē	Datu noskatīšanās pār plecu	

Krāpnieki un uzbrucēji apzināti uzlabo savus izmantotos paņēmienus vai izmanto paņēmienu kombināciju

CyberPhish
Safeguarding your digital future

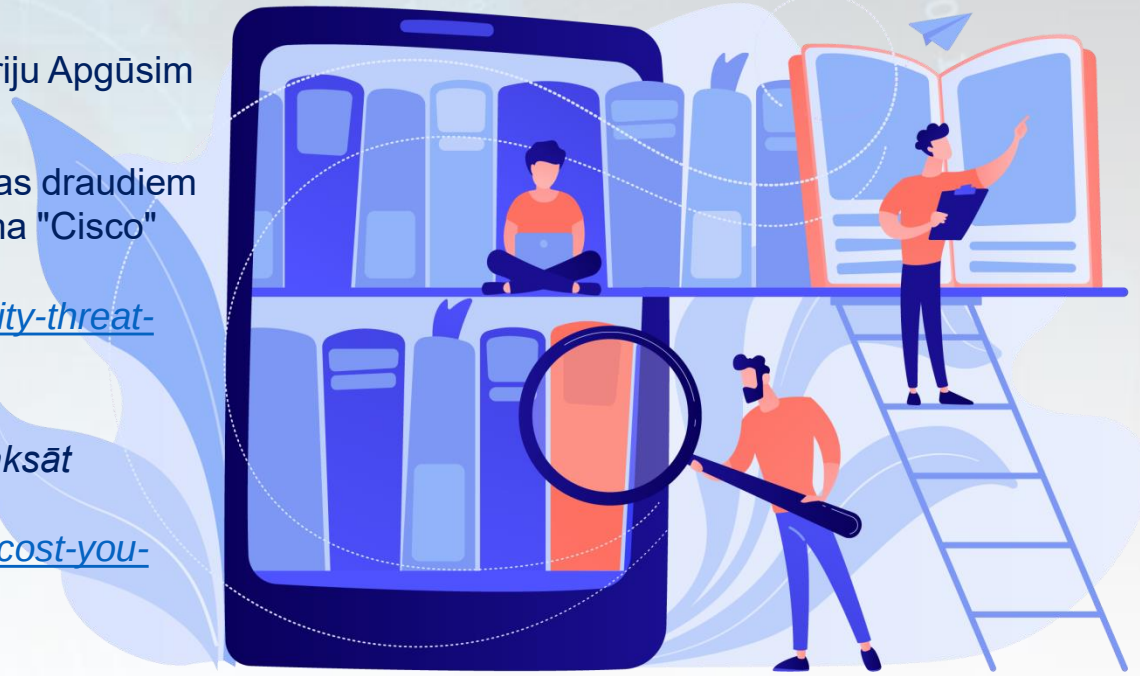
Funded by the Erasmus+ Programme of the European Union

Piešķiršana

- Apspriediet, kādus pikšķerēšanas uzbrukumu veidus zināt
- Vai esat kādreiz saskāries ar pikšķerēšanas uzbrukumu? Kāda veida uzbrukums tas bija?
- Kā jūs domājat, kurš pikšķerēšanas uzbrukuma veids ir vispopulārākais?
- Kādi varētu būt veiksmīga pikšķerēšanas uzbrukuma rezultāti?
- Norādiet vismaz četrus dažādus pikšķerēšanas faktorus

Papildu lasīšana

- **Kristofers Hednegijs** *[Christopher Hadnagy]* (2018. gads). Sociālā inženierija: Zinātne par cilvēku hakerismu, 2. izdevums.
- **Erdals Ozkaja** *[Erdal Ozkaya]* (2018. gads) Apgūsim sociālo inženieriju Apgūsim cilvēku uzlaušanas mākslu kopā ar starptautiski atzītu ekspertu.
- **Martinezs Klaudijs** *[Martinez, Claudia]*. Aizsardzība pret kiberdrošības draudiem 5 miljardu dolāru apmērā – uzņēmuma e-pasta uzbrukumi. Uzņēmuma "Cisco" emuāri pieejami *https://blogs.cisco.com/security/defending-against-the-5b-cybersecurity-threat-business-email-compromise*
- **Tjūzena, Kristīna** *[Tusan, Christina]*. *Viltus e-pasta ziņojumi var izmaksāt tūkstošus*. ASV Federālā tirdzniecības komisija ir pieejama vietnē *https://www.consumer.ftc.gov/blog/2017/05/fake-emails-could-cost-you-thousands*
- **US-CERT.** Drošības padoms (ST04-014) Izvairīšanās no sociālās inženierijas un pikšķerēšanas uzbrukumiem. ASV Iekšzemes drošības ministrija pieejama vietnē*https://www.us-cert.gov/ncas/tips/ST04-014*



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Īsi video

- Kas ir pikšķerēšana? Uzziniet, kā darbojas šis uzbrukums
  https://youtu.be/Y7zNlEMDmI4
- Kas ir pikšķerēšanas uzbrukums? Kā no tā izvairīties?
  https://youtu.be/j3nE8JQATXo
- Uzziniet, kā pamanīt pikšķerēšanas un surogātpasta e-pastu
  https://youtu.be/AmPX4DdBz-k
- Kas ir mērķētā pikšķerēšana | Atšķirība starp pikšķerēšanu un lielo zivju pikšķerēšanu
  https://youtu.be/JzoJeJBdhuI
- Kas irSMS pikšķerēšana? Kā darbojas pikšķerēšana, izmantojot īsziņas?
  https://youtu.be/ZOZGQeG8avQ
- Kas tālruņa un balss ziņu pikšķerēšana? Izpratne par šo augsto tehnoloģiju tālruņa krāpniecību
  https://youtu.be/DysFLnOf4Nw
- Kas man jādara, ja nejauši noklikšķinu uz pikšķerēšanas saites?
  https://youtu.be/d21-z8wsO7c

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Pateicamies!

Prezentācijā izmantoto attēlu resursi no:

- www.pixabay.com
- Personīgiem arhīviem

Ekrānuzņēmumi no vietnēm