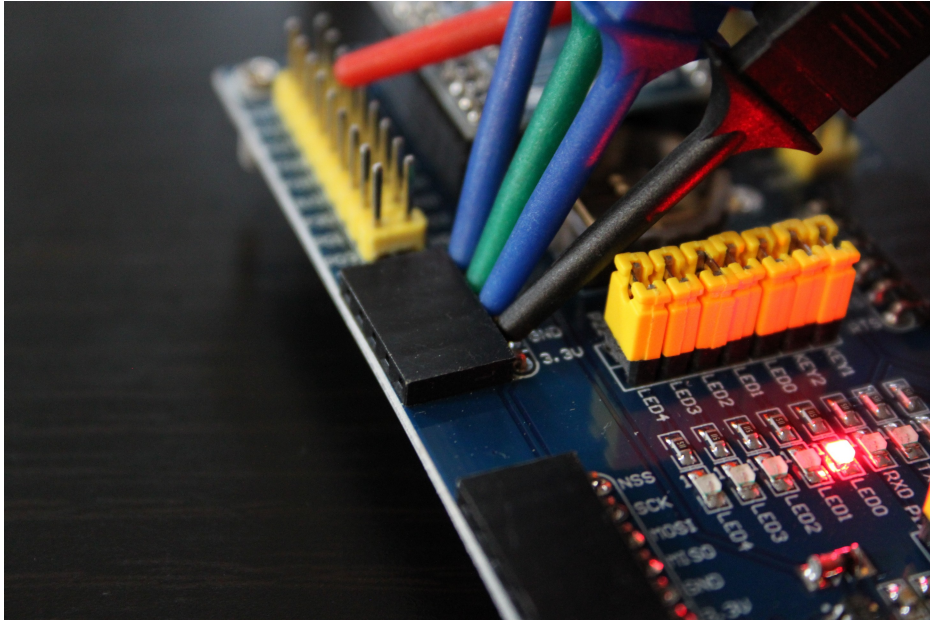


Everyday social-engineering in the Baltics

Kirils Solovjovs
26.10.2022.



Possible Security



- ◆ Penetration tests and audits
- ◆ Hardware and software security
- ◆ Consulting
- ◆ Premium-level service



- ◆ Possible Security Founder
- ◆ White-hat hacker
 - ◆ Network flow analysis
 - ◆ Reverse engineering
 - ◆ Social engineering
 - ◆ Consulting
- ◆ <https://kirils.org/>
- ◆ twitter / @KirilsSolovjovs



No: Fortis Global Venture <nurbaizura@johor.gov.my>
Atbildēt: fortisglobalventur@gmail.com
Temats: Aizdevuma piedāvājums
Datums: Fri, 30 Sep 2022 09:04:14 -0700 (2022.09.30. 19:04:14)

Mēs piedāvājam visu veidu aizdevumus, piemēram: - mājokļa aizdevumu, biznesa aizdevumu, personīgo aizdevumu. Sazinieties ar mums šodien, lai iegūtu vairāk informācijas.

Vilija Mačēnaites kundze
Fortis globālais uzņēmums


```
Received: from johor.gov.my [185.176.222.189] ([127.0.0.1]) by  
mail.johor.gov.my (12.3.0 build 2 RHEL7 x64) with ASMTTP (SSL) id  
1202210010006284627; Sat, 01 Oct 2022 00:06:28 +0800  
Date: Fri, 30 Sep 2022 09:04:14 -0700  
X-Barracuda-Effective-Source-IP: 263938.2cloud.eu[185.176.222.189]  
X-Barracuda-Apparent-Source-IP: 185.176.222.189  
From: "Fortis Global Venture" <nurbaizura@johor.gov.my>  
Subject: =?UTF-8?Q?Aizdevuma_pied=C4=81v=C4=81jums?=
```



From INTERPOLA POLICIJA <interieurgouv.bpm18@gmail.com> 

To policija@bpm.fr 

Subject **SŪDZĪBA**

 Thunderbird thinks this message is Junk mail.

PIEVIENOTA jūsu bis lapa — 227.-23. pants. Lūdzu, pēc iespējas ātrāk atbildiet uz šo adresi: interieurgouv.bpm18@gmail.com



No: mario-purkl@telering.at
Atbildēt: mario-purkl@telering.at
Kam: [redacted].lv, [redacted].lv
Temats: ZVIEBJF FBYCBSC VEUCTOOH
Datums: Thu, 09 Jun 2022 15:28:52 +0000 (2022.06.09. 18:28:52)

UQOHFKSDBDIEWXGAB
https://docs.google.com/presentation/d/e/2PACX-1vRPOa4NG-hYdhiW7qRvjqfam_O5TzTFQNBKuON4VHohSUi6sSP3eGUFKdB0R_O7Fl67gdPDHIFD5SVQ/pub?start=false&loop=false&delayms=3000#YHAXBEAQCGNQBSSESYEOCOQCLHSNBHEDCEXGPHDQYTOBWXVEREJEGO

VZOEHB ZVWCB



No: luminor Mobile AS <edward@yougotaticket.com>
Kam: ██████████
Temats: Ikmēneša maksas izraksts
Datums: Mon, 29 Aug 2022 02:02:23 -0700 (2022.08.29. 12:02:23)

luminor Bank AS

Konta parskats.

Konta izraksta elektroniskais veids ietver vairākus ziņojumus.

Turpināt

Informācija ir pieejama 24 stundas diennaktī , 7 dienas nedēļā.

Līga Lypina

Darbības atskaites



No: Swed Banka <aaron@nigeria-verified.theprocrete.com>
Kam: [redacted]
Temats: *** SPAM *** Bankas konta izraksts
Datums: Tue, 30 Aug 2022 01:04:44 -0700 (2022.08.30. 11:04:44)

Swedbank Support

Gada rēķins par samaksatajam nodevam
Jus varat izsekot visam jūsu kontu kustībam

Jūsu Datīem

Izmaksu pārskata tiek parādīti visi darījumi jūsu bankas kontā

Ināra Ozola
Darbības atskaite



No: Latvijas Pasts <info@mail.liepaja.edu.lv>

Kam: [redacted]

Temats: *** SPAM *** Jūsu paku nevarēja piegādāt 09 septembrī 2022, jo netika samaksāts muitas nodoklis (8,92 €).

Datums: Fri, 9 Sep 2022 11:56:39 -0700 (2022.09.09. 21:56:39)

Labdien

Jūsu paku nevarēja piegādāt **09 septembrī 2022**, jo netika samaksāts muitas nodoklis (**8,92 €**). izpildiet norādījumus

Lūdzu, aizpildiet šādu summu: 8,92 €
Aptuvenais piegādes datums ir : 10 septembris 2022

[Lai apstiprinātu pakas sūtījumu, klikšķiniet šeit](#)

Jūs saņemsiet e-pastu vai īsziņu, kad jūsu sūtījums nonāks jūsu mājas adresē. No pieejamības datuma jums ir 8 dienas, lai paņemtu iepakojumu. Izstāšanās brīdī jums tiks lūgts uzrādīt personu apliecinošu dokumentu.

Mēs pateicamies jums par uzticību,

Paldies, ka izmantojāt Latvijas Pasta pakalpojumu!

Pasts ir būtiski nozīmīgs katram cilvēkam un uzņēmumam, valstij un sabiedrībai.
Mūsu misija ir nodrošināt kvalitatīvus pasta pakalpojumus visā Latvijas teritorijā.
Mūsu pastnieki sasniedz attālākās viensētas un mēs spējam piegādāt sūtījumus uz jebkuru adresi pasaulē.
Mēs esam pieejami ikvienam, vienmēr un visur.
Papildus tradicionālajiem pasta pakalpojumiem mēs attīstām jaunus, mūsdienīgus piedāvājumus, lai kļūtu par klientu tuvāko palīgu ikdienas gaitās. Pie mums ir ērti, vienkārši un visu var nokārtot vienuviet.
Mēs īstenojam savu misiju ar atbildību pret klientiem, sabiedrību, valsti, apkārtējo vidi un saviem darbiniekiem.



Hello!

Unfortunately, I have some unpleasant news for you.

Roughly several months ago I have managed to get a complete access to all devices that you use to browse internet. Afterwards, I have proceeded with monitoring all internet activities of yours.

You can check out the sequence of events summarize below: Previously I have bought from hackers a special access to various email accounts (currently, it is rather a straightforward thing that can be done online).

Clearly, I could effortlessly log in to your email account as well.

One week after that, I proceeded with installing a Trojan virus in Operating Systems of all your devices, which are used by you to login to your email.

Actually, that was rather a simple thing to do (because you have opened a few links from your inbox emails previously).

Genius is in simplicity. (~_~)

Thanks to that software I can get access to all controllers inside your devices (such as your video camera, microphone, keyboard etc.). I could easily download all your data, photos, web browsing history and other information to my servers.

I can access all your social networks accounts, messengers, emails, including chat history as well as contacts list.

This virus of mine unceasingly keeps refreshing its signatures (since it is controlled by a driver), and as result stays unnoticed by antivirus software.



Atbildēt Pārsūtīt Atpakaļ Dzēst Ienākošie: Pārvietot ▼

Adresāti: [Adresātu saraksts](#)
Autors: ██████████ (skolēns), 8.a
Datums: 30.03.2022 14:22
Temats: darbs
Pielikumi:
[darbs.img](#)

Labdien. Lūdzu darbs pielikumā.
Piedodiet par kavējumu.

██████████

Sekojiēt E-klases pasta vēstulēm savā privātajā e-pastā! Šajā [Lietotāja dati](#) veiciet atbilstošus uzstādījumus.

Where does social engineering stand?

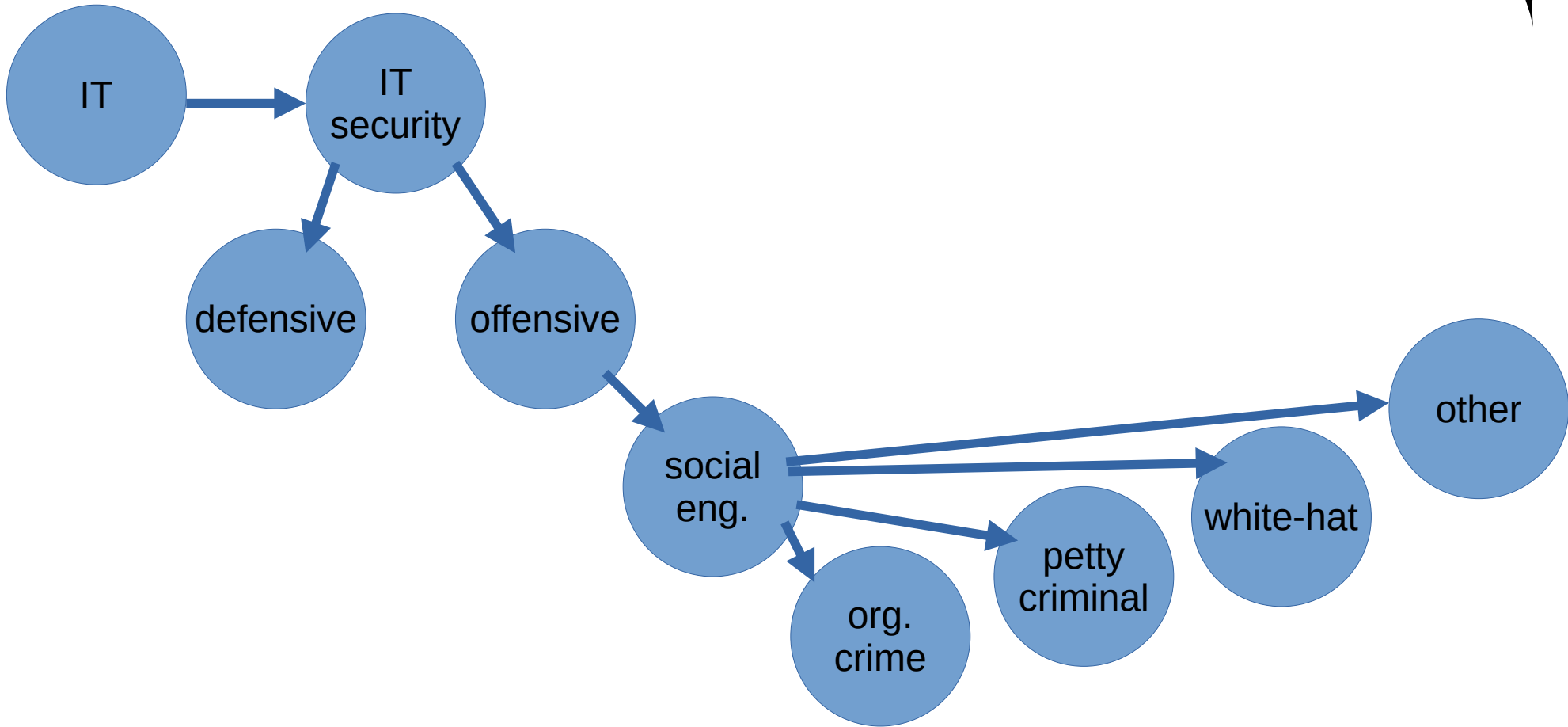




Foto: State Police (LV)



- ◆ SIM swapping
 - ◆ prepaid
 - ◆ post-paid
- ◆ CEO fraud



Simulation types

- ◆ SMiShing
- ◆ phishing
- ◆ vishing
- ◆ in-person attacks
 - ◆ device drops
- ◆ etc.

Advantages

- ◆ Verifies if your employees have the necessary knowledge and tools
- ◆ Helps identify gaps in employee training and defense procedures
- ◆ Allows to gauge your resilience to most popular type of cyber attacks

Thank you!

@KirilsSolovjovs
<https://kirils.org/>

