

Scam and other frauds on the internet

(CC) 2021

Matej Kovačič



Personal blog:
<https://telefoncek.si>



This work is published under
CC BY-NC-SA 4.0 license

Scam

A scam is a deceptive scheme or trick used to cheat someone out of something, especially money. Scam is also a verb meaning to cheat someone in such a way.

noun: *a confidence game or other fraudulent scheme, especially for making a quick profit; swindle.*

verb (*scammed, scamming*): *to cheat or defraud (someone) with a scam.*

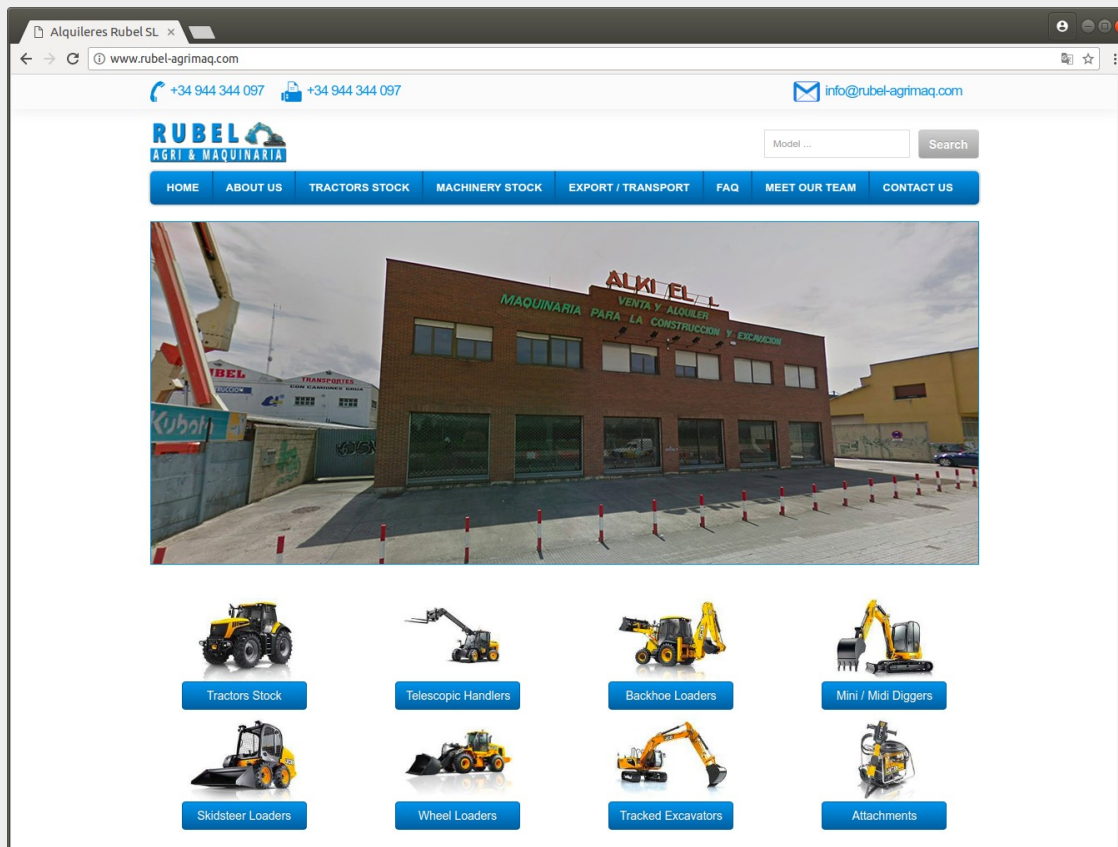
Type of scams

- Attempts to gain your personal information
- Buying or selling
- Dating and romance
- Fake charities
- Investments
- Jobs & employment
- Threats & extortion
- Unexpected money (inheritance,...) and winnings
- Pyramid schemes
- Government impersonation scams

Fraudulent online store #1

Story:

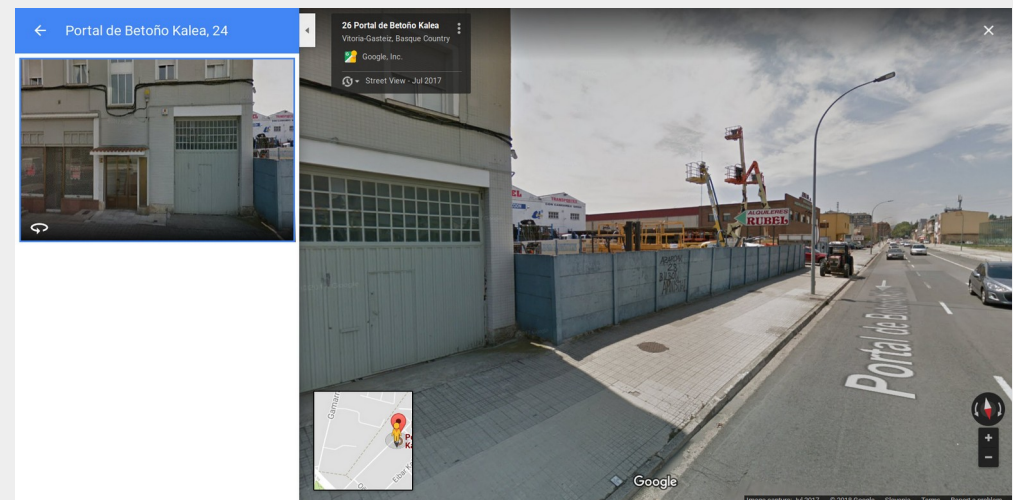
- User wanted to buy a small excavator and found online store with very good (low) prices.



Fraudulent online store #1

Story:

- Low prices were suspicious, so he decided for some additional checks.
- He checked the existence of company and obtained a business balance sheet containing share capital, annual turnover, profit, number of employees...
- He also checked company headquarters on Google StreetView.



Fraudulent online store #1

Story:

- He also contacted company representative through an e-mail. Communication has been quick, professional and in good English.
- However, the company wanted that he pays to their subsidiary's bank account in Portugal "in order to avoid some taxes".
- He also wanted to check VIN number of the machine, but received no answer.

Fraudulent online store #1

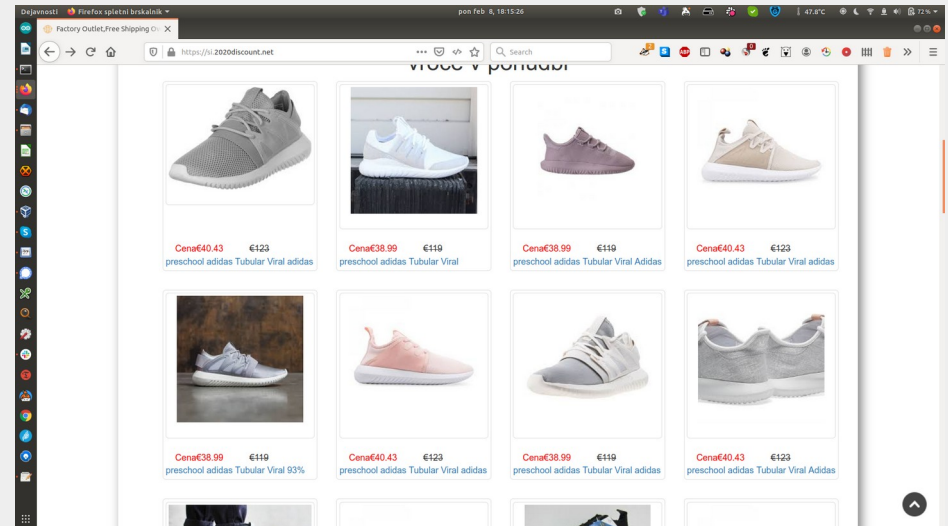
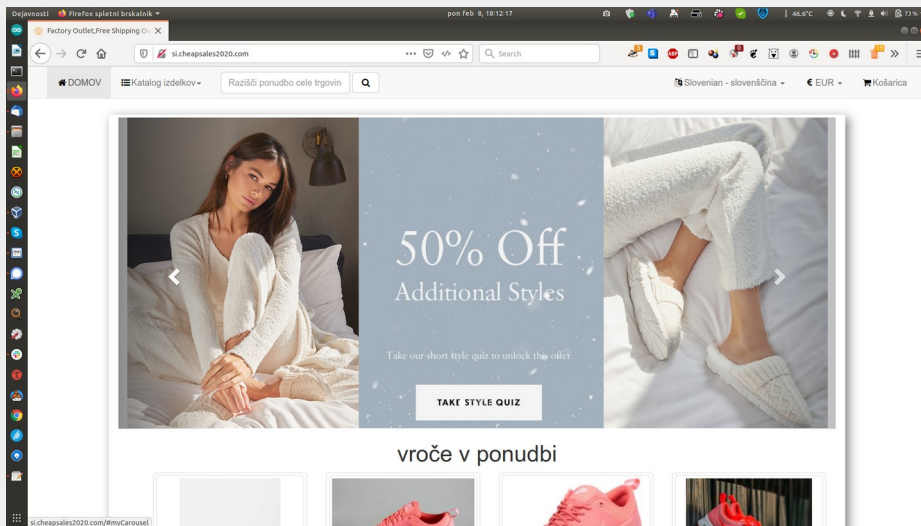
The analysis:

- Webserver has been located in Russia (*nic.ru* network). Domain has also been registered in Russia (by *nic.ru*).
- Searching also revealed that similar domain (*rubel-maquinaria.com*) has been previously registered in Malaysia. Perpetrators had also run another scam store with construction machinery on domain *budo-maszyny.com* (pretending to be store from Poland). They were using the same web design template. Both sites have been exposed and shut down.
- Today *rubel-agrimaq.com* is not accessible anymore.

Fraudulent online store #2

A set of fraudulent stores in Slovenian language, advertised through spam mail, offering cheap goods.

Various, but similar domain names:
si.2020discount.net, *sisale2021.com*,
si.cheapsales2020.com, etc.



Fraudulent online store #2

First warning sign:

- Very cheap products (*"If it is too good to be true, it is very likely not true"*).

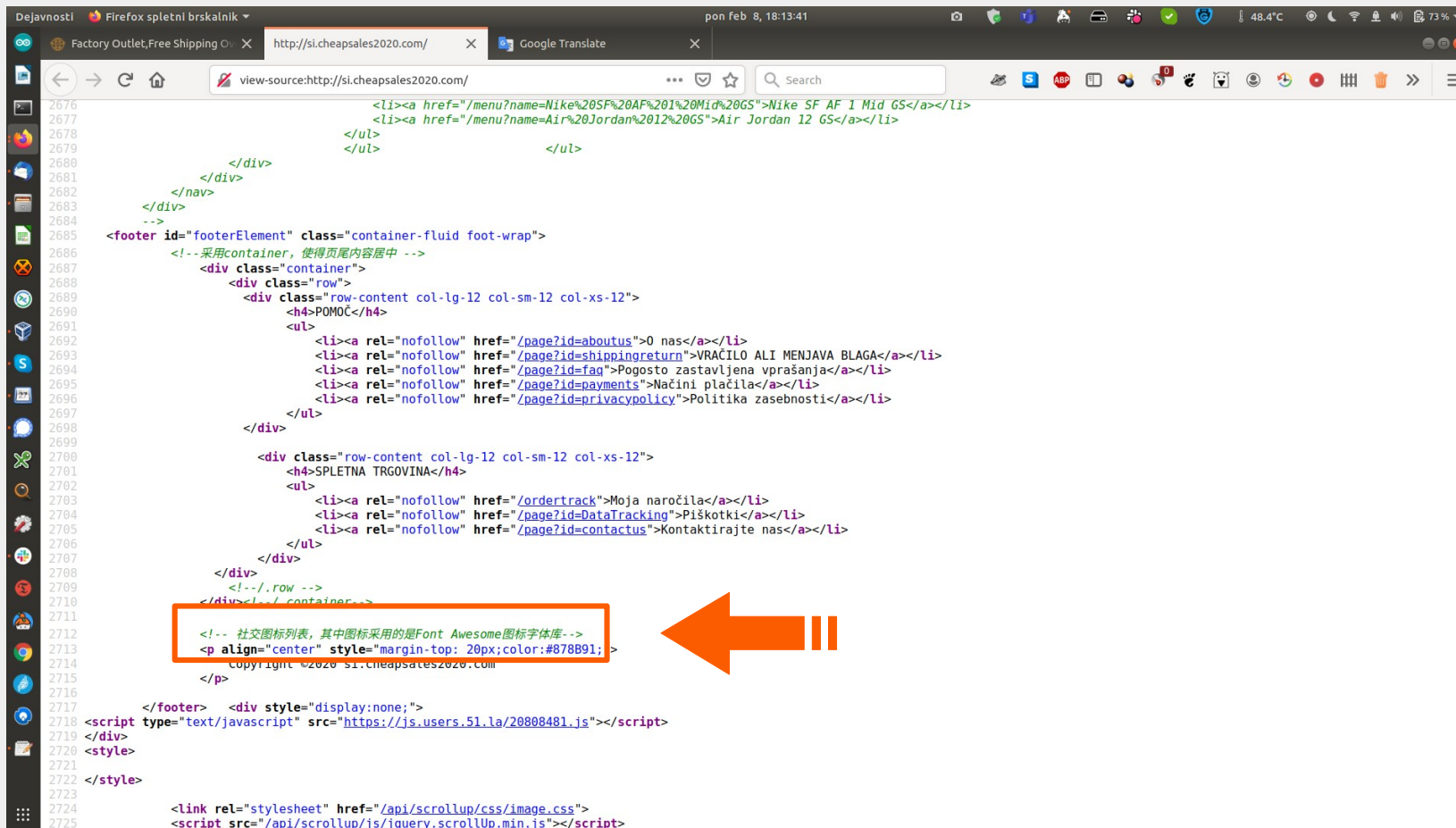
Deeper analysis:

- IP address hidden behind Cloudflare.
- HTTPS is available (provided by Cloudflare).

Fraudulent online store #2

Deeper analysis:

- HTML code comments in Chinese.

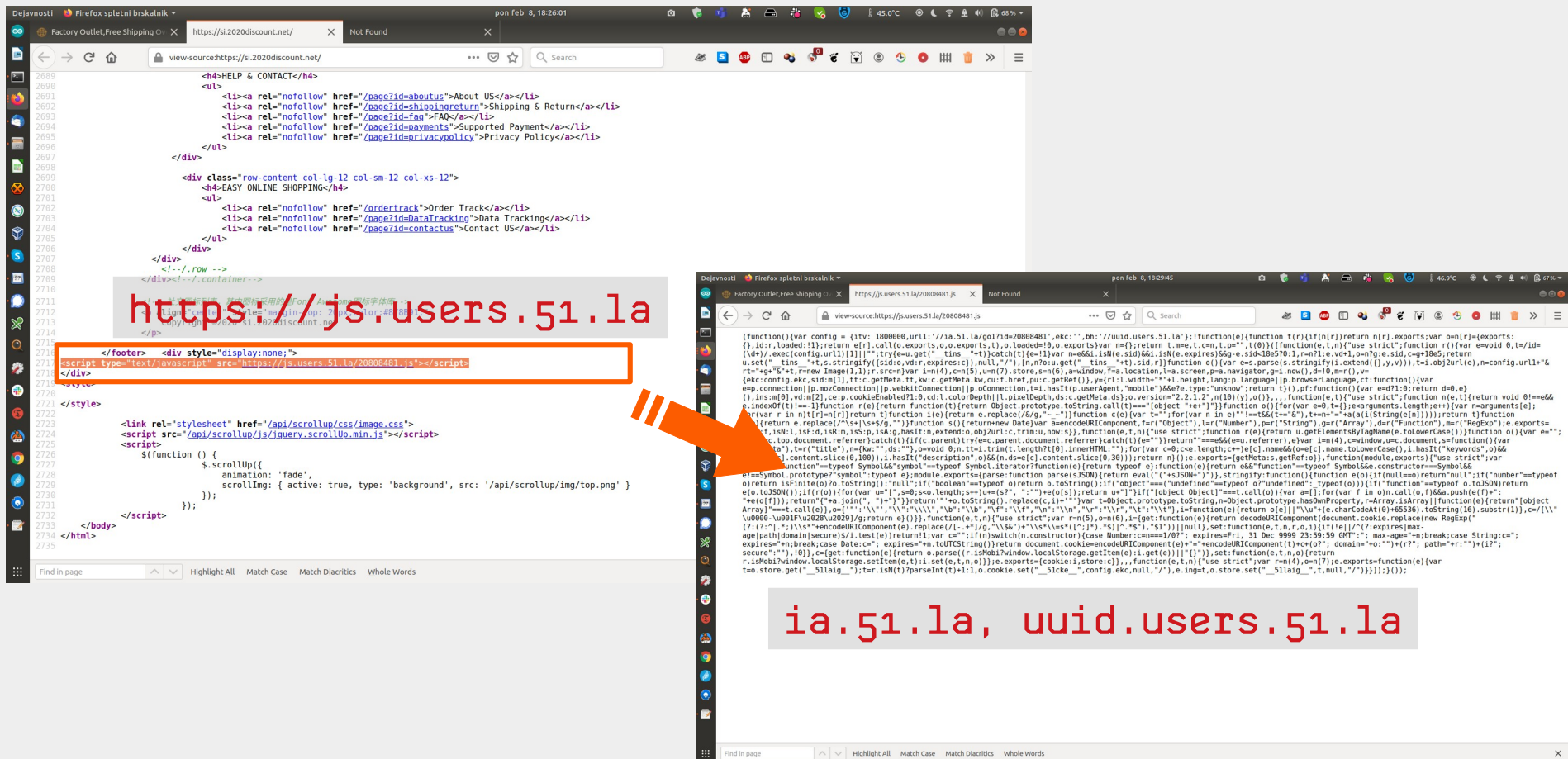


```
2676 <li><a href="/menu?name=Nike%20SF%20AF%201%20Mid%20GS">Nike SF AF 1 Mid GS</a></li>
2677 <li><a href="/menu?name=Air%20Jordan%2012%20GS">Air Jordan 12 GS</a></li>
2678 </ul>
2679 </ul>
2680 </div>
2681 </nav>
2682 </div>
2683 </div>
2684 -->
2685 <footer id="footerElement" class="container-fluid foot-wrap">
2686 <!-- 采用container, 使得页尾内容居中 -->
2687 <div class="container">
2688 <div class="row">
2689 <div class="row-content col-lg-12 col-sm-12 col-xs-12">
2690 <h4>POMOĆ</h4>
2691 <ul>
2692 <li><a rel="nofollow" href="/page?id=aboutus">0 nas</a></li>
2693 <li><a rel="nofollow" href="/page?id=shippingreturn">VRACILO ALI MENJAVA BLAGA</a></li>
2694 <li><a rel="nofollow" href="/page?id=fag">Pogosto zastavljena vprašanja</a></li>
2695 <li><a rel="nofollow" href="/page?id=payments">Načini plačila</a></li>
2696 <li><a rel="nofollow" href="/page?id=privacypolicy">Politika zasebnosti</a></li>
2697 </ul>
2698 </div>
2699 <div class="row-content col-lg-12 col-sm-12 col-xs-12">
2700 <h4>SPLETNA TRGOVINA</h4>
2701 <ul>
2702 <li><a rel="nofollow" href="/ordertrack">Moja naročila</a></li>
2703 <li><a rel="nofollow" href="/page?id=DataTracking">Piškotki</a></li>
2704 <li><a rel="nofollow" href="/page?id=contactus">Kontaktirajte nas</a></li>
2705 </ul>
2706 </div>
2707 </div>
2708 <!-- /.row -->
2709 </div></div>
2710 </div>
2711 <!-- 社交图标列表, 其中图标采用的是Font Awesome图标字体库 -->
2712 <p align="center" style="margin-top: 20px;color:#878B91;">
2713 Copyright ©2020 SI.cheapsales2020.com
2714 </p>
2715 </div>
2716 </div>
2717 <script type="text/javascript" src="https://js.users.51.la/20808481.js"></script>
2718 </div>
2719 <style>
2720 </style>
2721 </div>
2722 </div>
2723 <link rel="stylesheet" href="/api/scrollup/css/image.css">
2724 <script src="/api/scrollup/js/jquery.scrollUp.min.js"></script>
2725
```

Fraudulent online store #2

Deeper analysis:

- JavaScript tracker code found...



Fraudulent online store #2

Deeper analysis:

- ...leading to Chinese servers.

```
matej@cryptomania: ~  
Datoteka Uredi Pogled Poišči Terminal Pomoč  
  
matej@cryptomania:~$ ping -c1 ia.51.la  
PING d2cb5ad7002c4066.huaweisafedns.com (183.131.207.66) 56(84) bytes of data.  
64 bytes from 183.131.207.66 (183.131.207.66): icmp_seq=1 ttl=48 time=282 ms  
  
--- d2cb5ad7002c4066.huaweisafedns.com ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 282.793/282.793/282.793/0.000 ms  
matej@cryptomania:~$ ping -c1 51.la  
PING 51.la (14.17.102.104) 56(84) bytes of data.  
  
--- 51.la ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms  
  
matej@cryptomania:~$ ^C  
matej@cryptomania:~$ ping -c1 uuid.users.51.la  
PING uuid.users.51.la (14.17.102.107) 56(84) bytes of data.  
64 bytes from 14.17.102.107 (14.17.102.107): icmp_seq=1 ttl=47 time=232 ms  
  
--- uuid.users.51.la ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 232.272/232.272/232.272/0.000 ms  
matej@cryptomania:~$
```

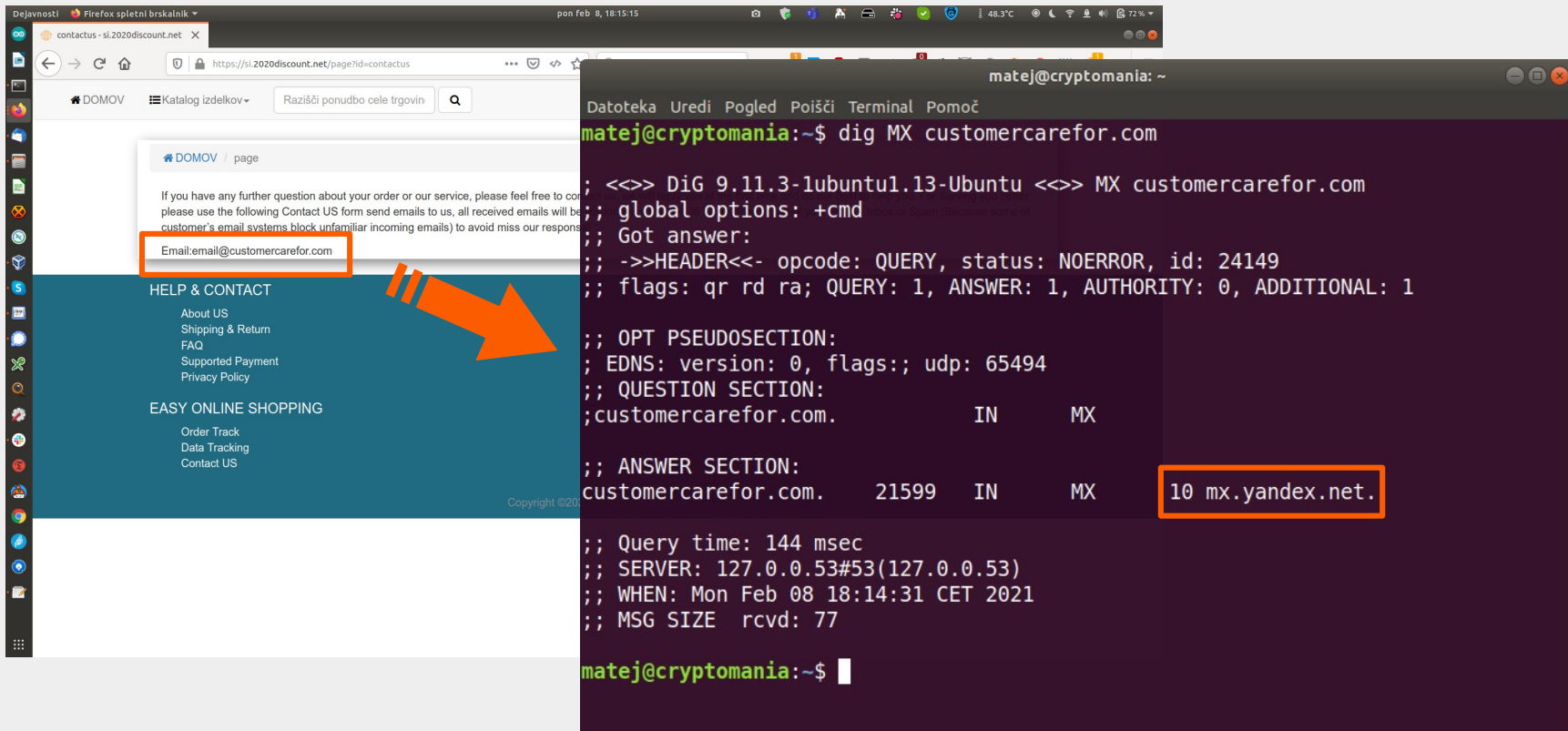
huaweisafedns.com
located on Swiss IP
address, domain registered
by Alibaba Cloud Computing
(Beijing)

IP addresses 14.17.100.0/22
allocated to CT-FOSHAN-IDC
CHINANET Guangdong province
network, CN

Fraudulent online store #2

Deeper analysis:

- Contact e-mail (email@customercarefor.com) points to Russia (Yandex.net).



The image shows a screenshot of a website and a terminal window. The website is a contact page for 'DOMOV' with a contact form and a footer menu. The terminal window shows a command to dig MX records for 'customercarefor.com', which returns '10 mx.yandex.net'.

Website Screenshot:

- URL: <https://sl.2020discount.net/page?id=contactus>
- Page Title: DOMOV / page
- Contact Form: "If you have any further question about your order or our service, please feel free to contact us. Please use the following Contact US form send emails to us, all received emails will be forwarded to our customer's email systems block unfamiliar incoming emails) to avoid miss our responses." Email: email@customercarefor.com
- Footer Menu:
 - HELP & CONTACT
 - About US
 - Shipping & Return
 - FAQ
 - Supported Payment
 - Privacy Policy
 - EASY ONLINE SHOPPING
 - Order Track
 - Data Tracking
 - Contact US

Terminal Screenshot:

```
matej@cryptomania:~$ dig MX customercarefor.com
;<>> DiG 9.11.3-lubuntu1.13-Ubuntu <>> MX customercarefor.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24149
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags::; udp: 65494
;; QUESTION SECTION:
;customercarefor.com.          IN      MX

;; ANSWER SECTION:
customercarefor.com.  21599  IN      MX      10 mx.yandex.net.

;; Query time: 144 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Feb 08 18:14:31 CET 2021
;; MSG SIZE rcvd: 77

matej@cryptomania:~$
```

Collecting personal data

Plot:

- Google Ads on Slovenian media websites promoting interview with known Slovenian journalists about her medical problems and fake medicine which supposedly helped her.
- Fake interview visually looked like news article on popular news website.
- Linguistically correct (much better than Google translate).

Collecting personal data

Plot:

- Contained mostly positive (but also some negative!) comments from fake users with pictures and Slovenian sounding names.



Collecting personal data

Analysis:

- Fake website hosted on Github Pages.
- Visitors were invited to register for free medicine.
- Input form has been collecting personal data, but **no credit cards data**.
- Input form hosted on Russian web server.



The screenshot shows a web browser window with the URL https://s1lo.github.io/set/#order_form. The page content is as follows:

POZOR!
Nacionalni program

Izpolnite obrazec in pridobite promocijsko ceno! Oglasne enote so omejene!

Obrazec za registracijo

CENA promocijski **39 EUR**

50 embalaža na zalogi!

Ime

Telefonska številka

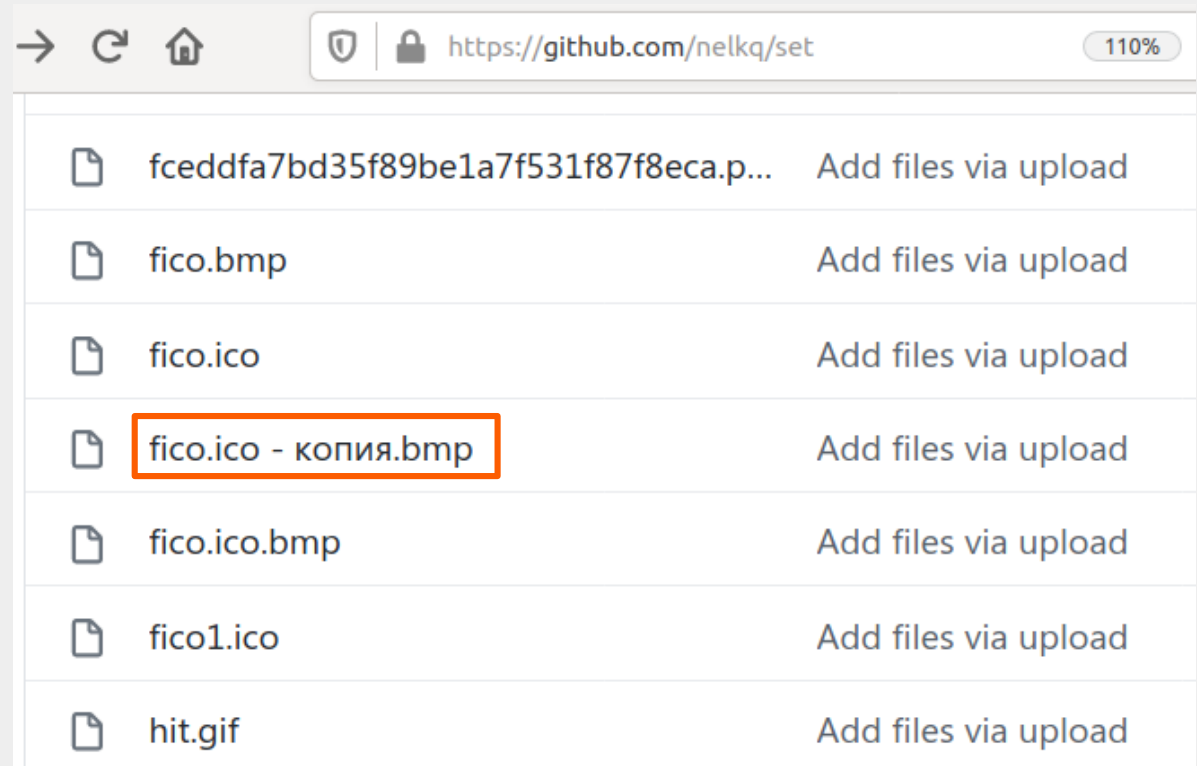
HOČEM!

* cena na porcijo

Collecting personal data

Analysis:

- Filename in Russian language (“fico.ico – копия.bmp”) has been found on a fake website.
- Comments in HTML code in Russian language have been found.



Collecting personal data

Analysis:

- Contact information (e-mail, mobile phone) of person who registered scammer's domain has been found and pointed to Russian citizen living in Moscow.
- This person was thanking the translators on *kwork.ru* website for quick and accurate translations to various languages of eastern Europe (this explains the quality of language on scam websites).

Collecting personal data

Analysis:

- Similar scams were found targeting audience in Poland and Czech Republic (in fake interview are appearing their local celebrities, website is in their local language,...).
- Github Pages has been notified of this, and fake websites have been removed, however similar fake articles are still appearing through Google Ads and scammers are opening new accounts on Github Pages...

Targeted attack through Facebook

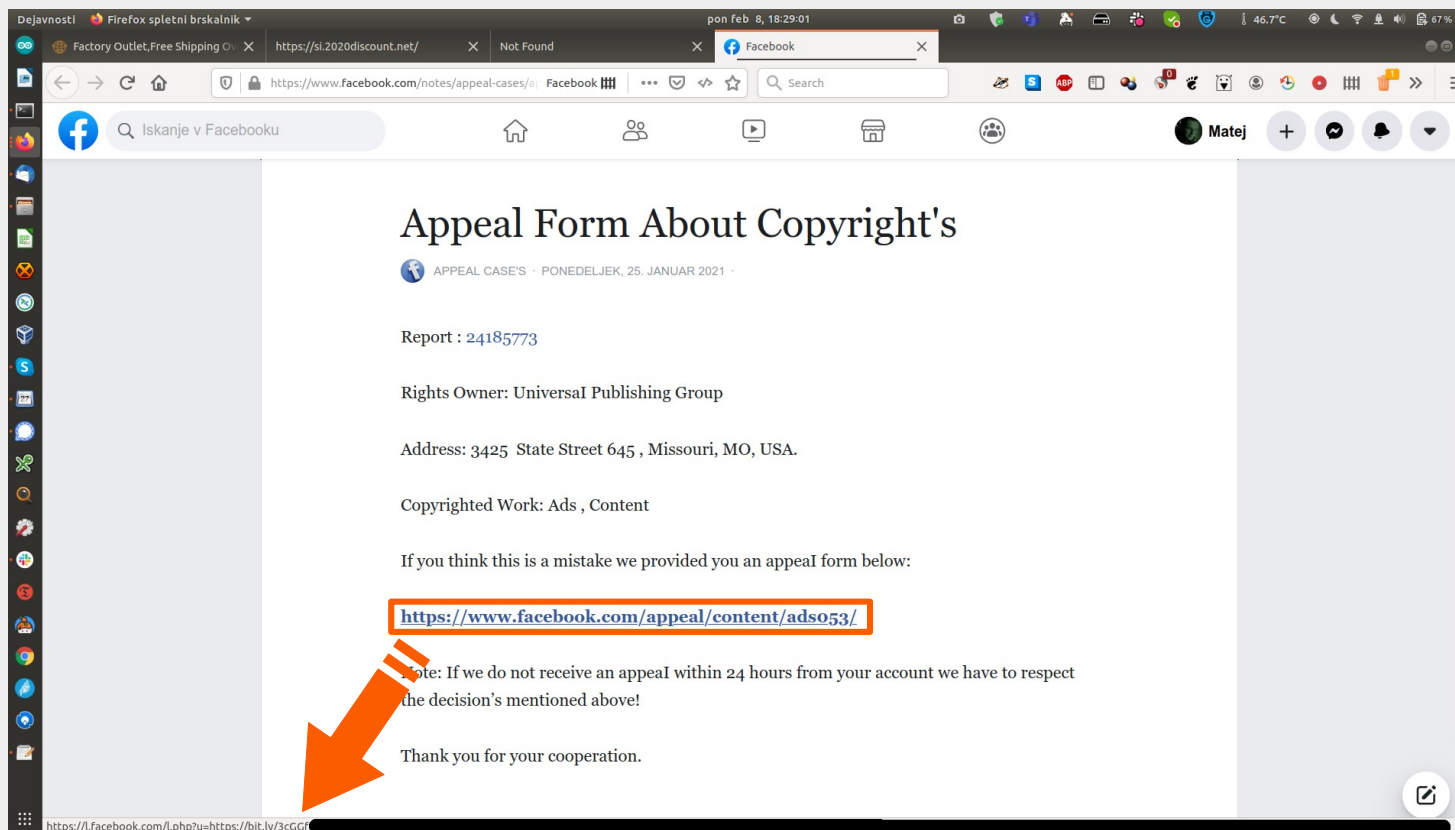
Story:

- User posted a picture on his Facebook profile.
- Few days after that (on February 8th, 2021), user receives an e-mail notifying him that he conducted copyright infringement and needs to respond.
- E-mail message contained (a legitimate) link to Facebook.
- However, link has been pointing to Facebook Notes, which is created by users (but resides on a Facebook domain).

Targeted attack through Facebook

What happened:

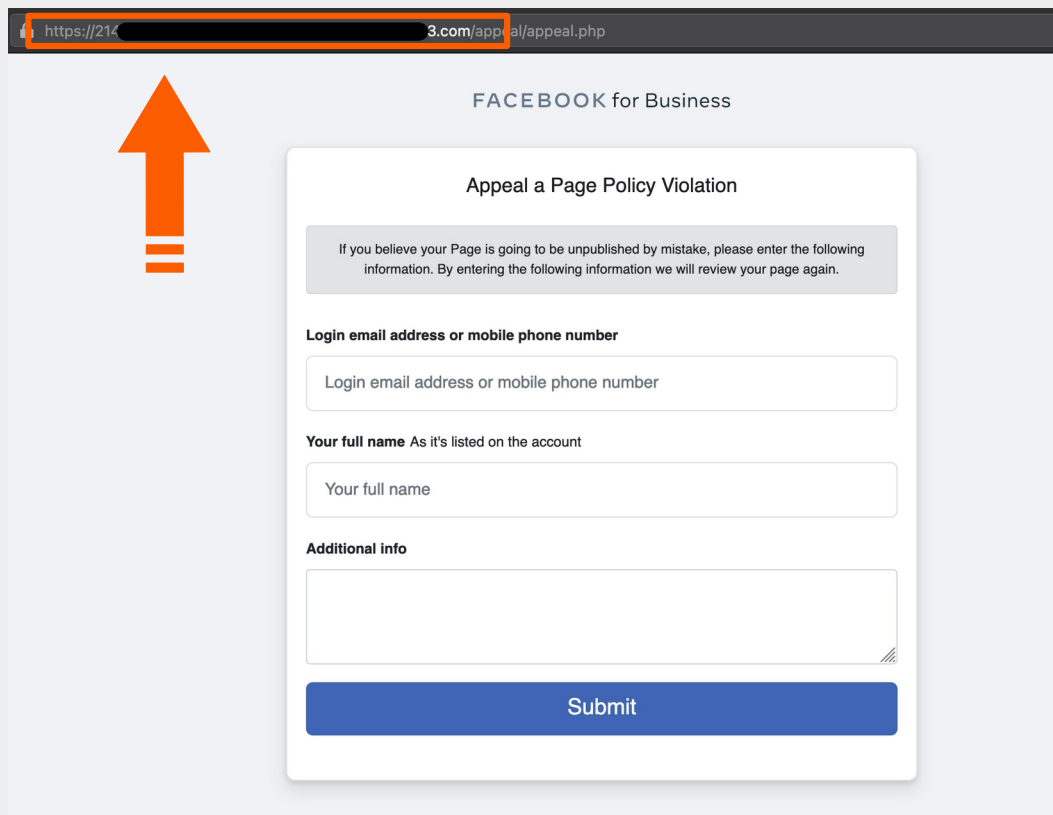
- Facebook Notes page contained “appeal” link, which pointed to bit.ly URL shortener...



Targeted attack through Facebook

What happened:

- ...bit.ly URL shortener redirected to scammer's domain registered in USA (on 3rd February 2021)



https://21... 3.com/appl.../appeal.php

FACEBOOK for Business

Appeal a Page Policy Violation

If you believe your Page is going to be unpublished by mistake, please enter the following information. By entering the following information we will review your page again.

Login email address or mobile phone number

Login email address or mobile phone number

Your full name As it's listed on the account

Your full name

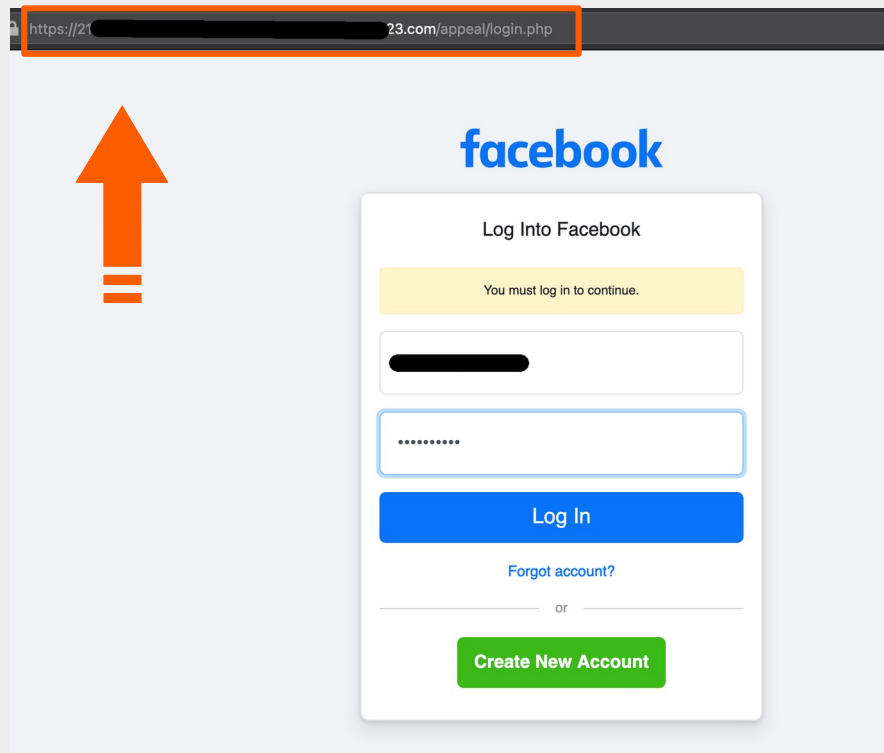
Additional info

Submit

Targeted attack through Facebook

What happened:

- ...after user submitted his appeal, user was asked to “login” to Facebook again and his credentials were stolen.



Targeted person was a local businessman and the incident has been reported to the police, which opened the investigation.

Calendar spam

GMail can automatically add events from Gmail to calendar...

...and scammers began sending calendar invitations to random people.

To sporočilo vsebuje povabilo na dogodek. [Sprejmi] [? Neodločeno]

Od fiacredepreville@gmail.com ☆ [Odgovori] [Posreduj] [Arhiviraj] [Nezeleno]

Zadeva **Invitation: Ponudba posojila med posamezniki @ Sat Feb 13, 2021 19:00 - 20:00 (CET)** [1 opomnik]

Za Mene [redacted] ★

fiacredepreville@gmail.com vas je povabilo

Naziv: Ponudba posojila med posamezniki
Kdaj: sobota, 13. februar 2021 19:00 – 20:00
Organizator: 📧 fiacredepreville@gmail.com <fiacredepreville@gmail.com>
Opis: zdravo

Osebna posojila vam dajemo na voljo z 3-odstotno obrestvino, če njihova datoteka na banki zavržena.

Če iščete posojilo med posamezniki za obnovo dejavnosti, smo vam na voljo. Na voljo smo zadovoljiti naše stranke v rekordnem času.

Za več informacij nas kontaktirajte neposredno na ta e-pošto.

Hvala vam
prisrčno

~~~~~  
Please do not edit this section of the description.

This event has a video call.  
Join: <https://meet.google.com/rvo-vkne-ayt>

View your event at <https://calendar.google.com/calendar/event?action=VIEW&>

**Ponudba posojila med posamezniki** [Dremež - v] [Izklopi]

sobota, 13. februar 2021 19:00 – 20:00

[Podrobnosti ...](#)

[Dremež vsi]

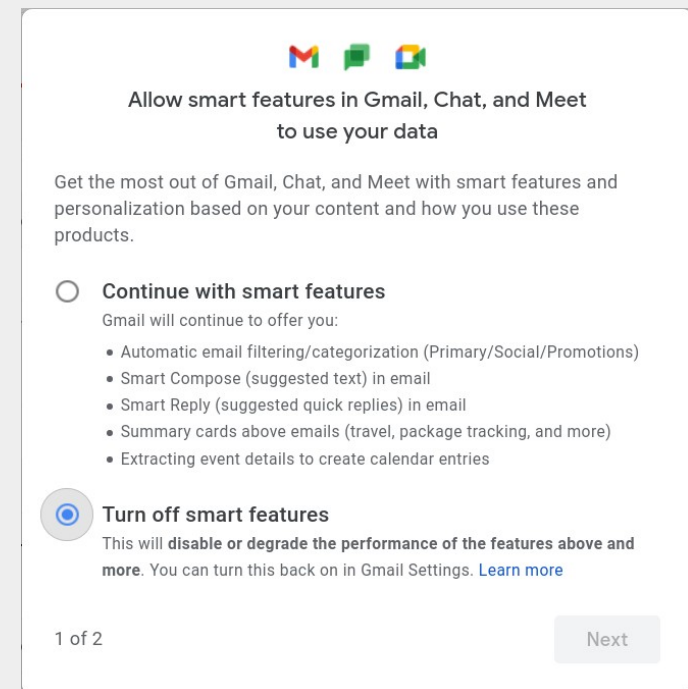
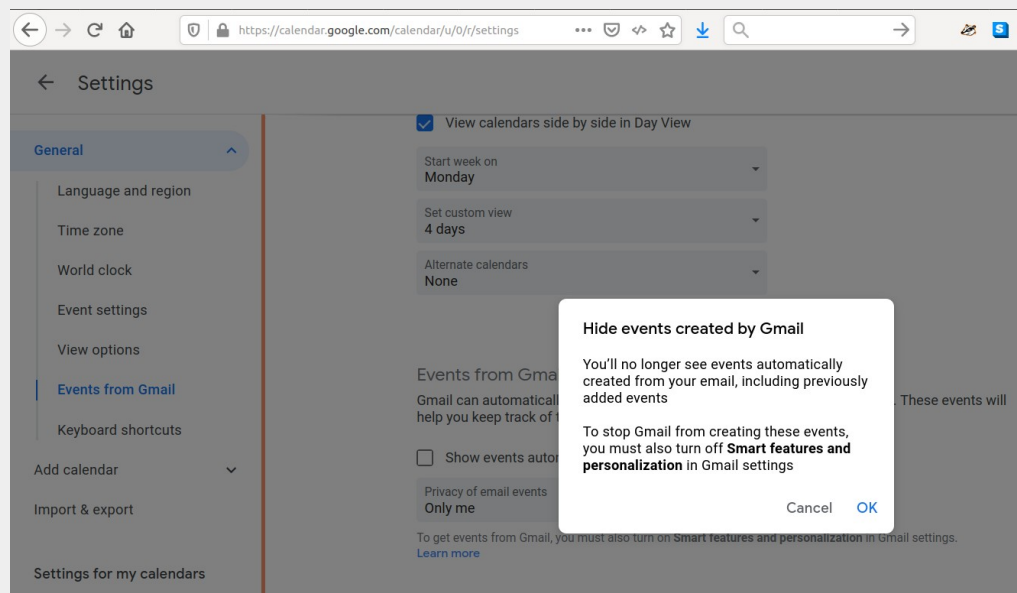
Calendar event offering financial loan



# Calendar spam

In Google Calendar settings uncheck “*Automatically add events from Gmail to my calendar*”.

In Gmail settings turn off “*Smart features and personalization*”.



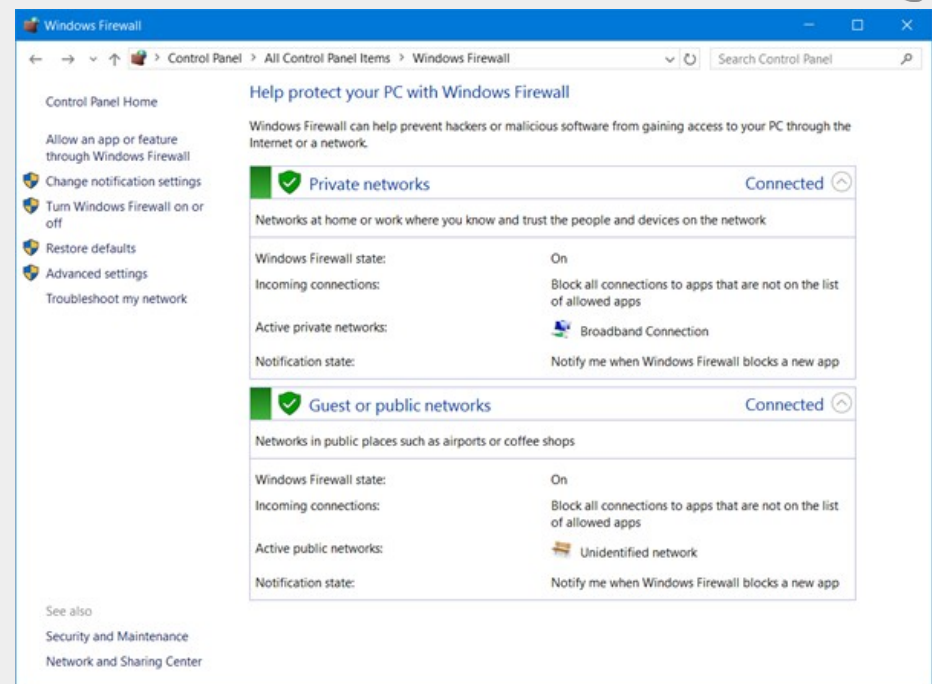
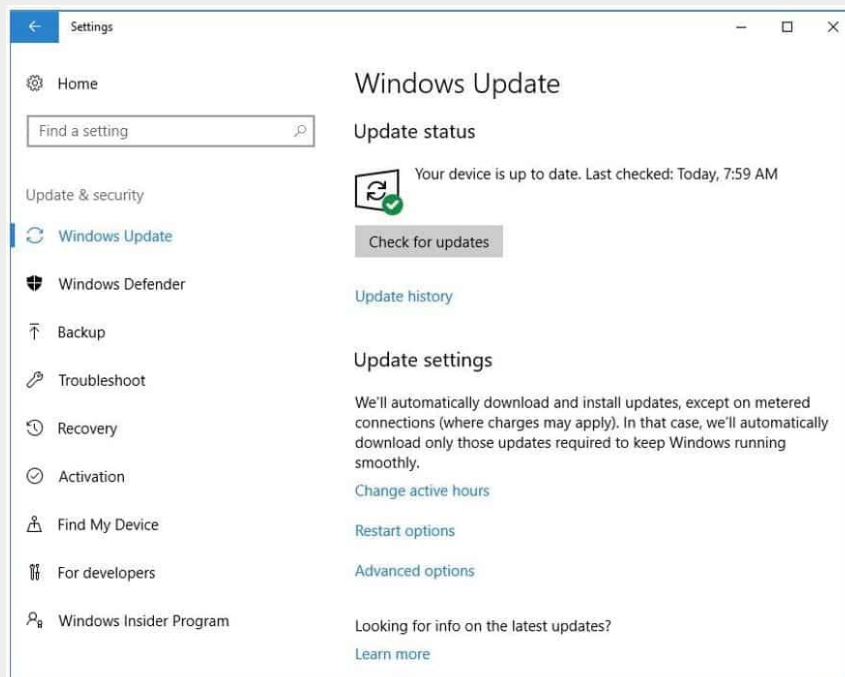
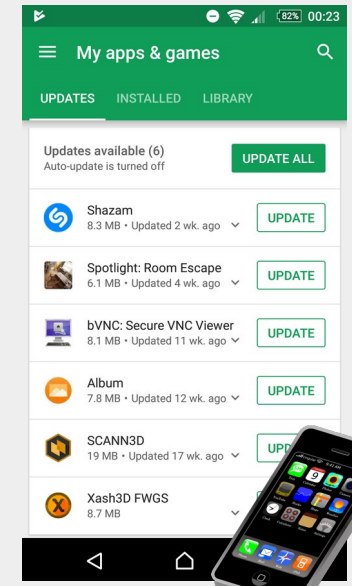
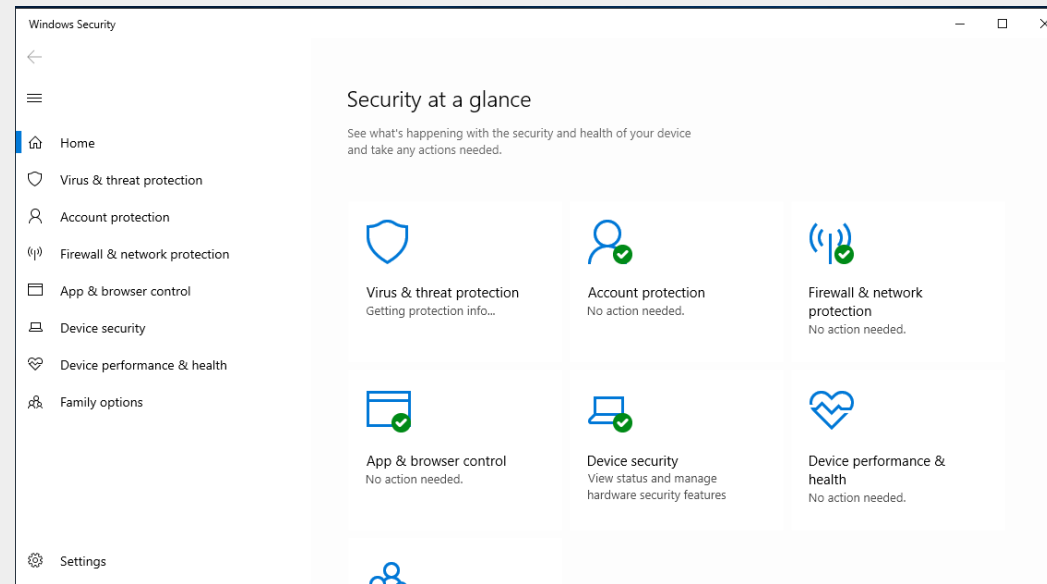
# Scam protection

---

- Be alert to the fact that scams exist.
- Know who you're dealing with.
- Do not open suspicious links or attachments in emails.
- Be careful when shopping online.
- Before making a payment or entering your passwords, always check that you are on a secure website and that website has the correct address.
- Don't respond to messages or phone calls asking for remote access to your computer.
- Don't respond to text messages or missed calls that come from numbers you do not recognise.
- Keep your personal details (including bank account info) secure.
- Keep your mobile devices and computers secure.
- Review and keep strict privacy and security settings on social media.
- Beware of any requests for your details or money.

**If an offer looks too good to be true, it probably is not true.**

# General security guidelines



# General security guidelines

---

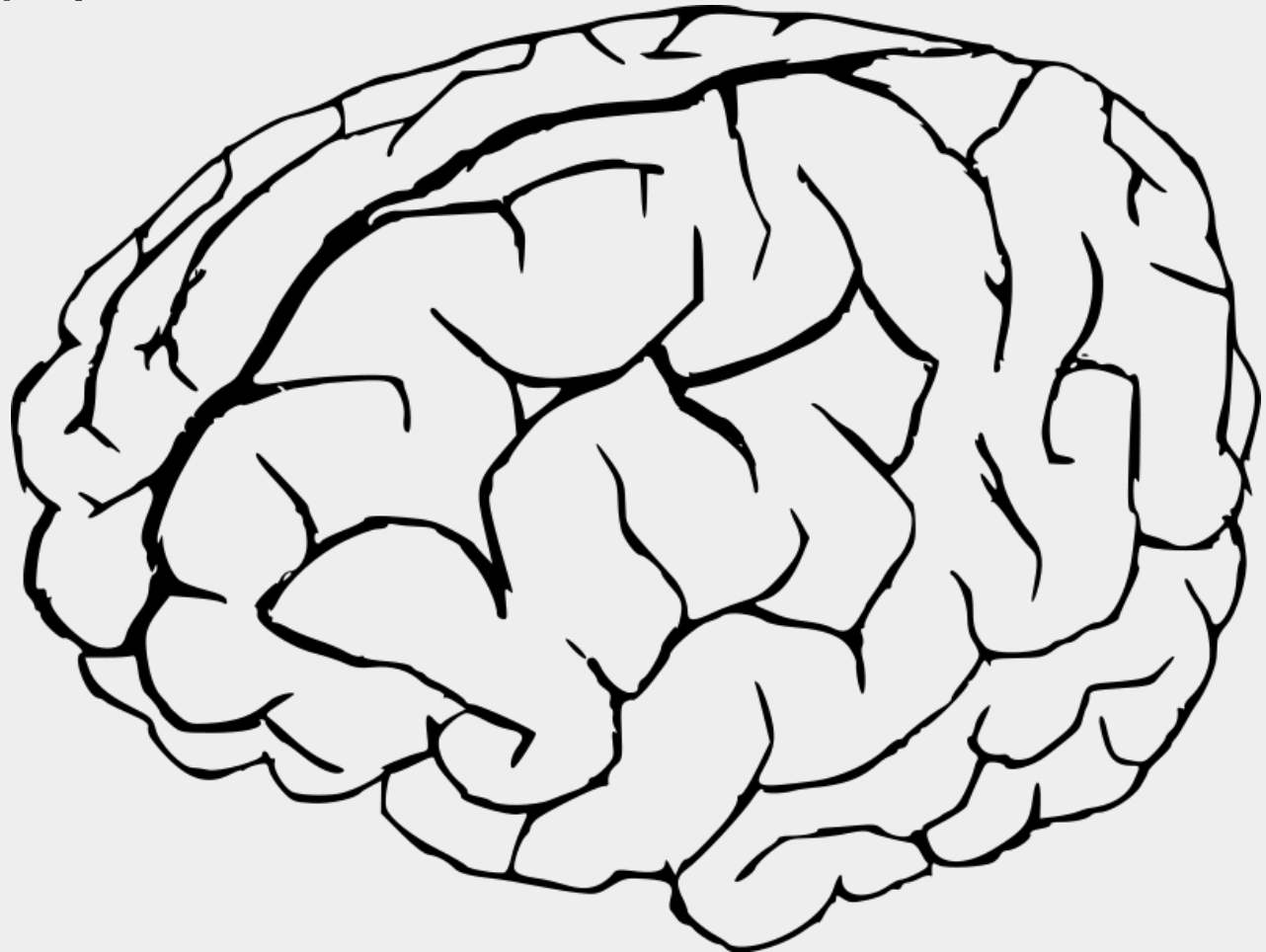
Some other protection techniques:

- choose good passwords and do not recycle them;
- use 2FA or multifactor authentication wherever possible;
- regularly update all your software on all your devices;
- enable firewall;
- use antivirus, tracking and spyware removing technology, block telemetry;
- backup;
- install only apps you need;
- use encryption wherever possible;
- physical security.

# General security guidelines

---

Develop “security culture”, be alerted and use common sense. ;-)



# Questions?

**Matej Kovačič**



Personal blog:  
<https://telefoncek.si>



This work is published under  
CC BY-NC-SA 4.0 license