

Scam and other frauds on the internet

(CC) 2021

Matej Kovačič

Institute of Forensics of
Information Technologies



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.*

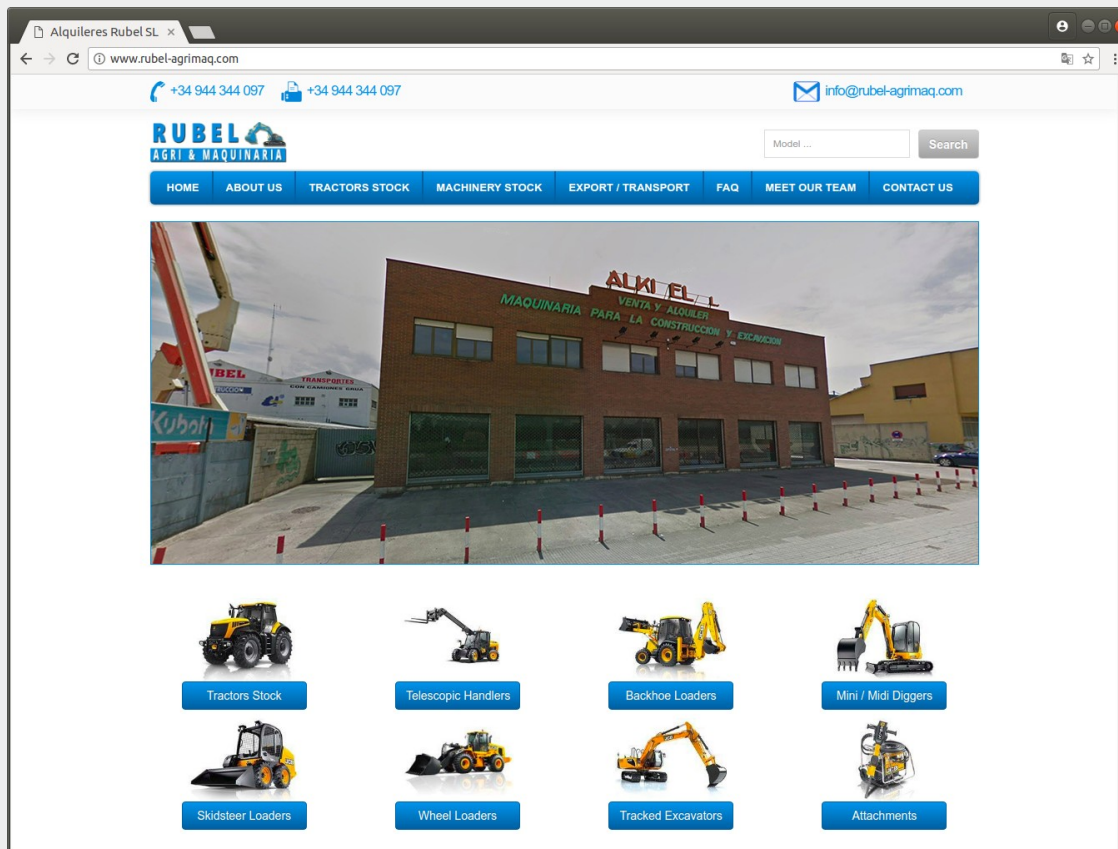
Type of scams

- 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:

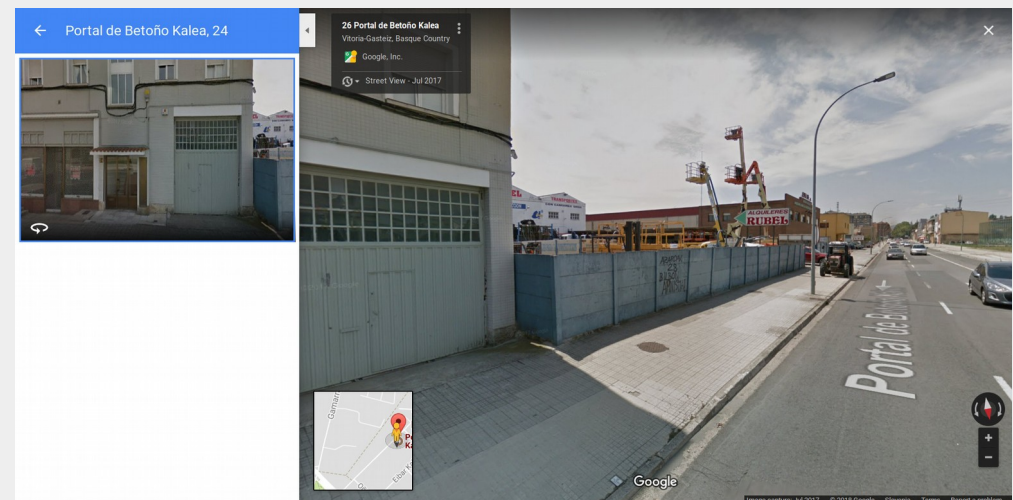
- User wanted to buy a small excavator and found online store with very good (low) prices.



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

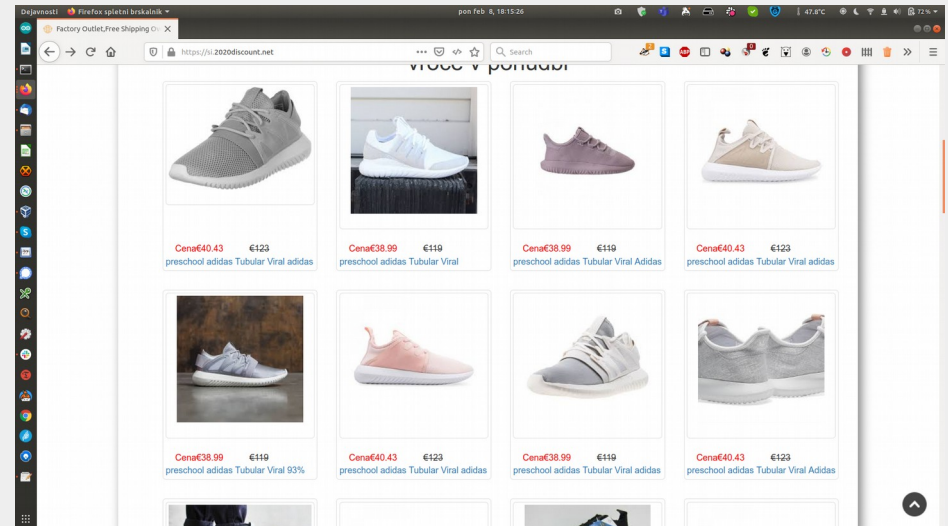
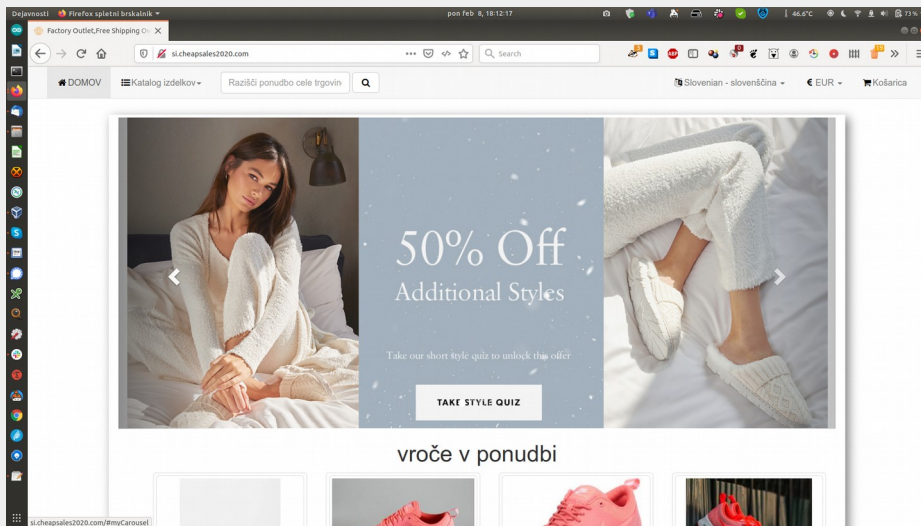
The analysis:

- 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"*).

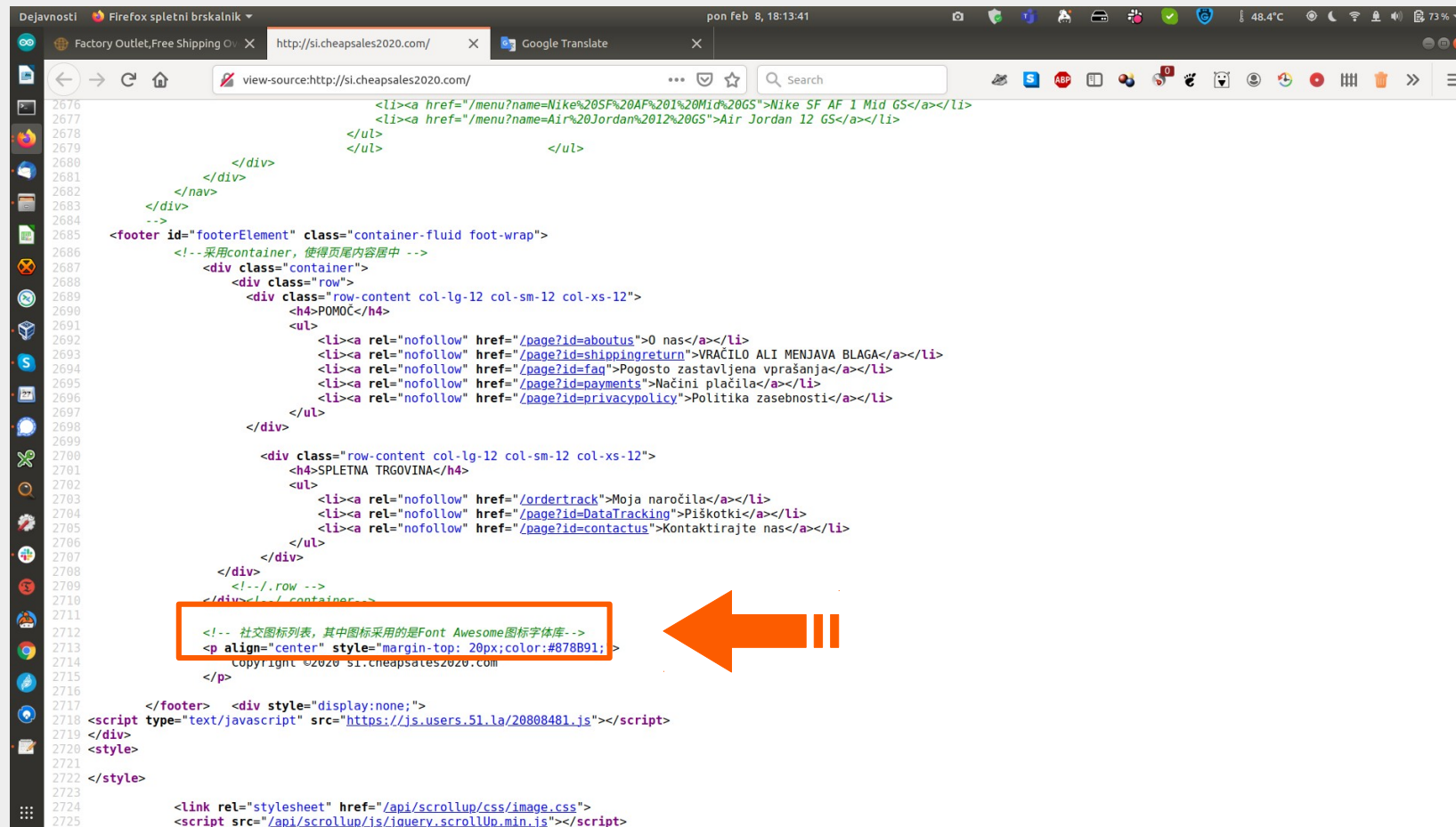
Deeper analysis:

- 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 <!-->
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>POMOČ</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=faq">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 </style>
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:

- ...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:~$
```

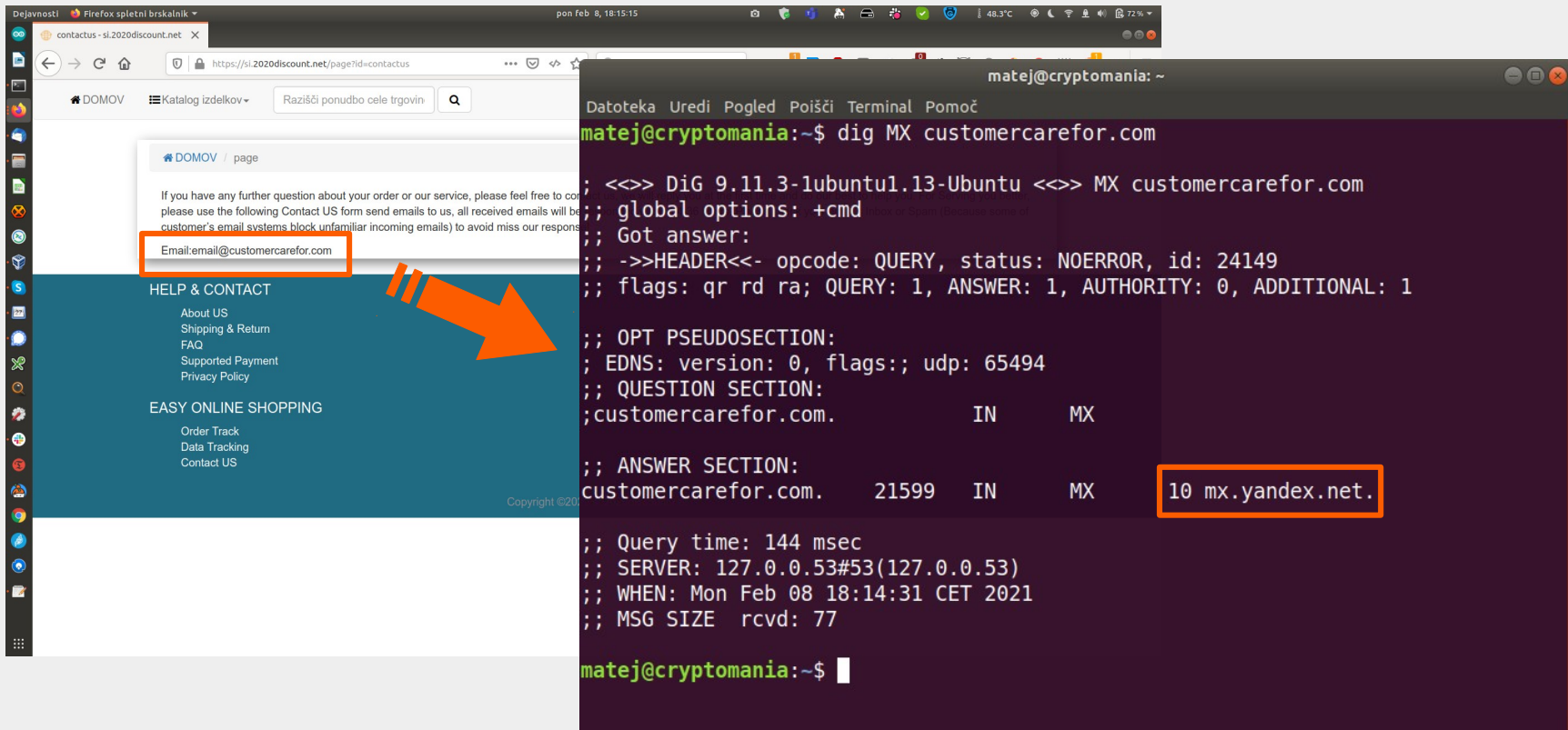
huaweisafedns.com
located on Swiss IP
address, domain registered
by Alibaba Cloud Computing
(Beijing)

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 the command 'dig MX customercarefor.com' and its output, which includes the MX record '10 mx.yandex.net' highlighted in a red box. An orange arrow points from the email address in the website footer to the terminal output.

Website contact information:

Email: email@customercarefor.com

HELP & CONTACT

- About US
- Shipping & Return
- FAQ
- Supported Payment
- Privacy Policy

EASY ONLINE SHOPPING

- Order Track
- Data Tracking
- Contact US

```
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 webserver.



The screenshot shows a web browser window with the URL https://s11o.github.io/set/#order_form. The page content is as follows:

POZOR!
Nacionalni program

Izpolnite obrazec in pridobite promotijsko ceno! **Oglasne enote so omejene!**

Obrazec za registracijo

CENA promotijski **39 EUR**

50 embalaža na zalogi!

Ime

Telefonska številka

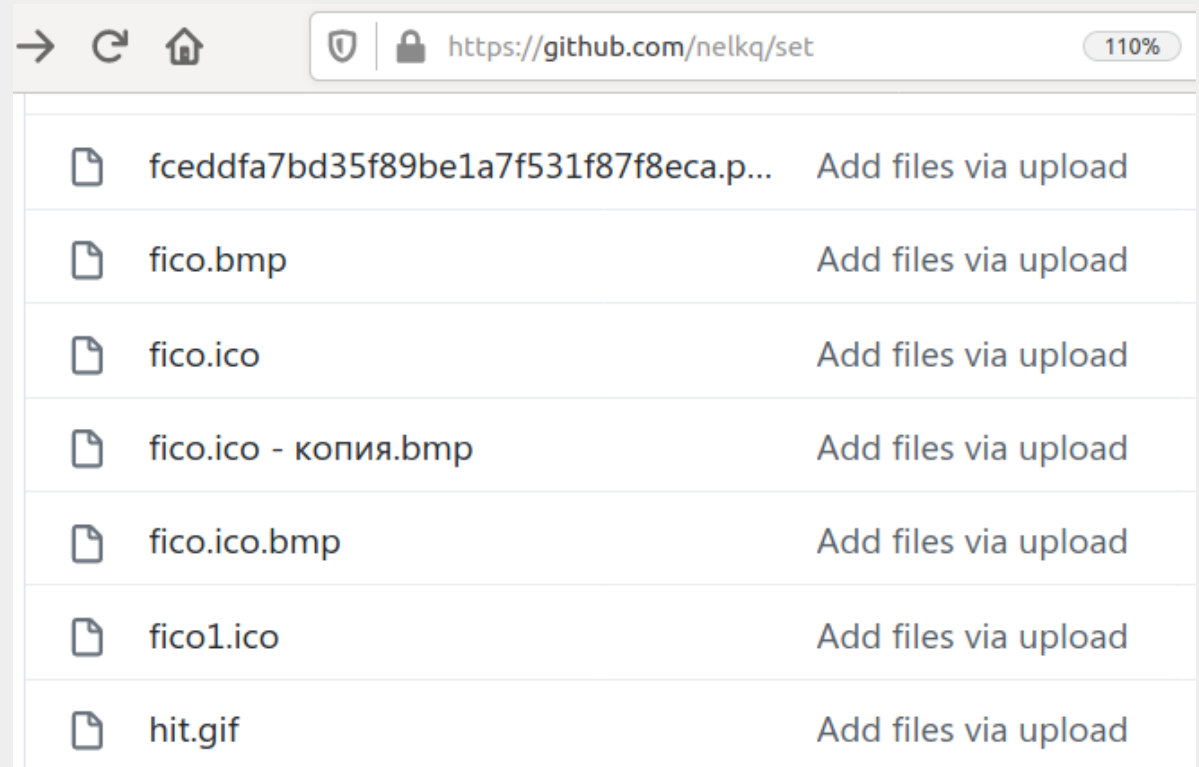
HOČEM!

* 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 language quality).

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,...).
- Similar fake articles are still appearing through Google Ads...

Targeted attack through Facebook

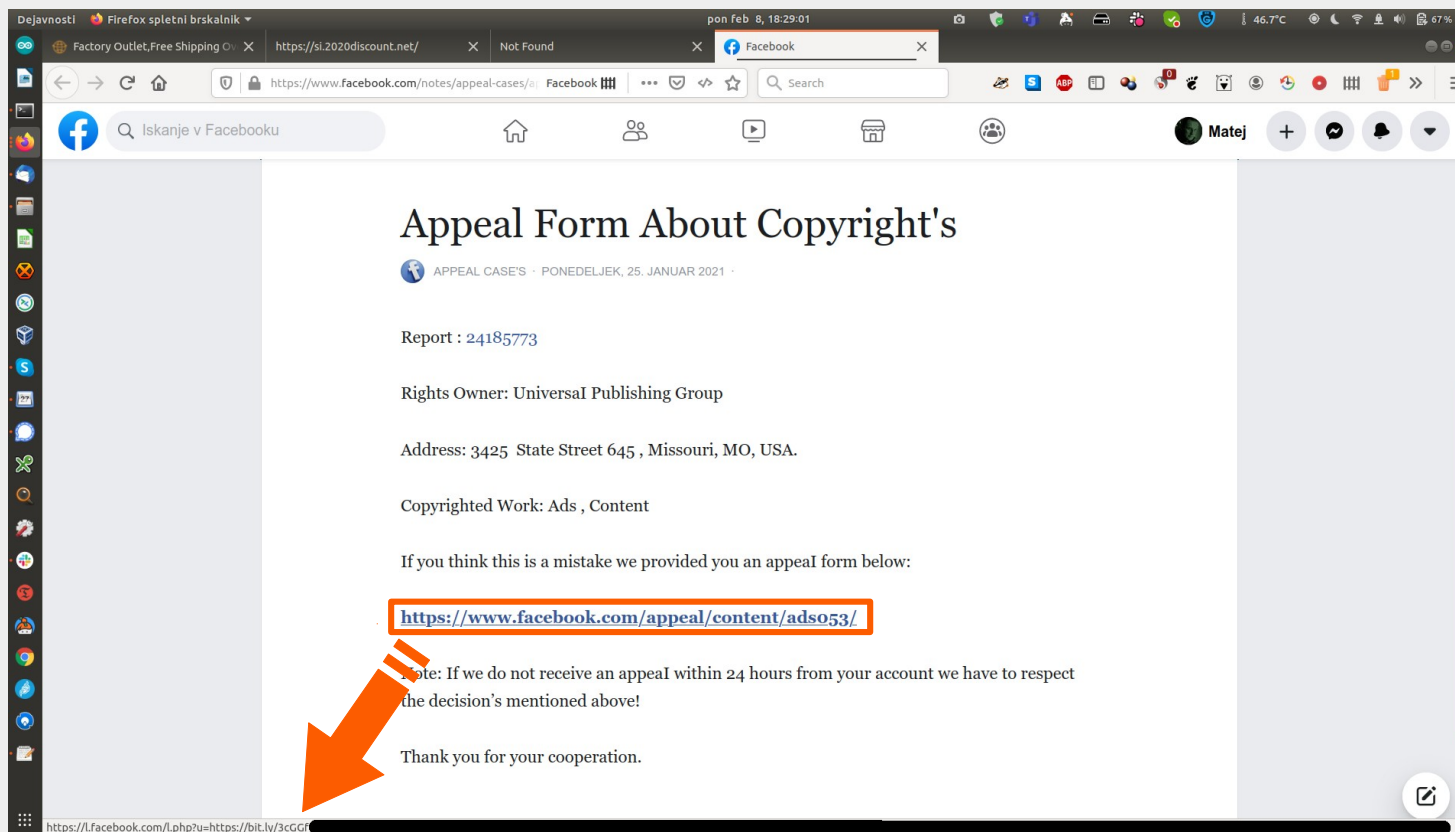
Story:

- 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 on a Facebook domain).

Targeted attack through Facebook

What happened:

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



The screenshot shows a Firefox browser window displaying a Facebook Notes page. The page title is "Appeal Form About Copyright's" and it is dated "PONEDELJEK, 25. JANUAR 2021". The content of the note includes:

- Report : 24185773
- Rights Owner: Universal Publishing Group
- Address: 3425 State Street 645 , Missouri, MO, USA.
- Copyrighted Work: Ads , Content

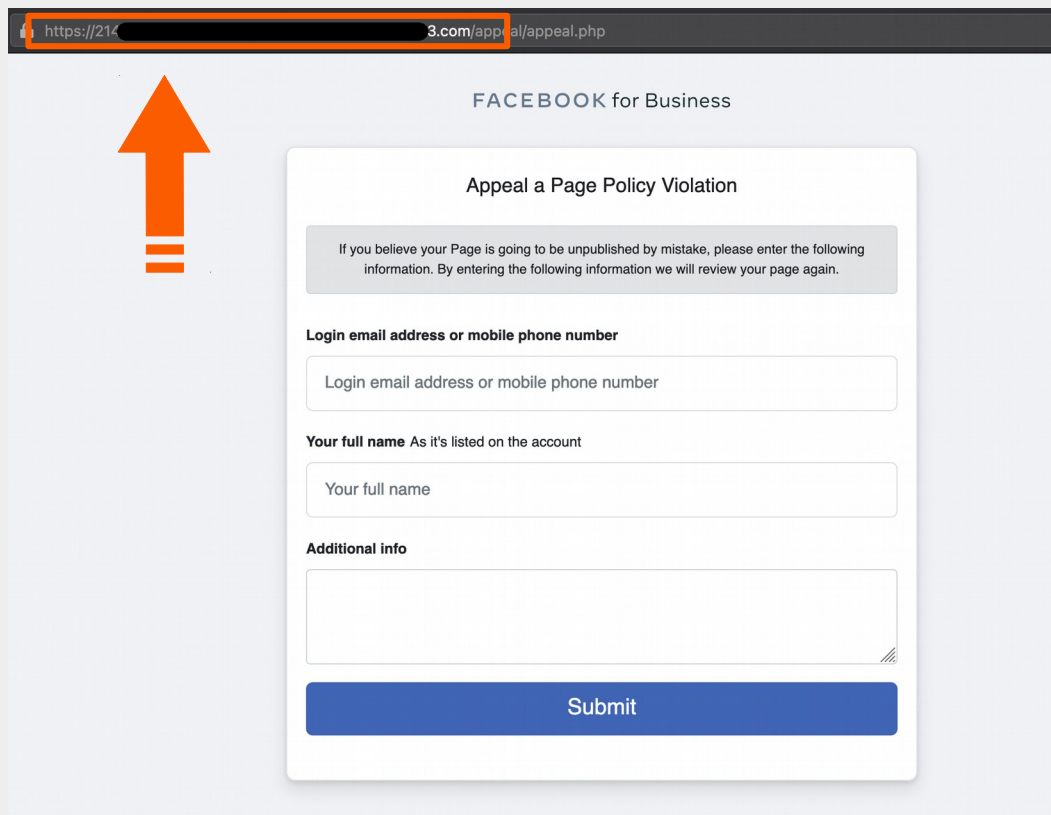
The note states: "If you think this is a mistake we provided you an appeal form below:" followed by a URL: <https://www.facebook.com/appeal/content/ads053/>. This URL is highlighted with a red box. A large red arrow points from the URL to the bottom of the page. Below the URL, the note says: "Note: If we do not receive an appeal within 24 hours from your account we have to respect the decision's mentioned above!" and "Thank you for your cooperation."

The browser's address bar shows the URL: <https://l.facebook.com/l.php?u=https://bit.ly/3cGG...>

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...al/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

Your full name As it's listed on the account

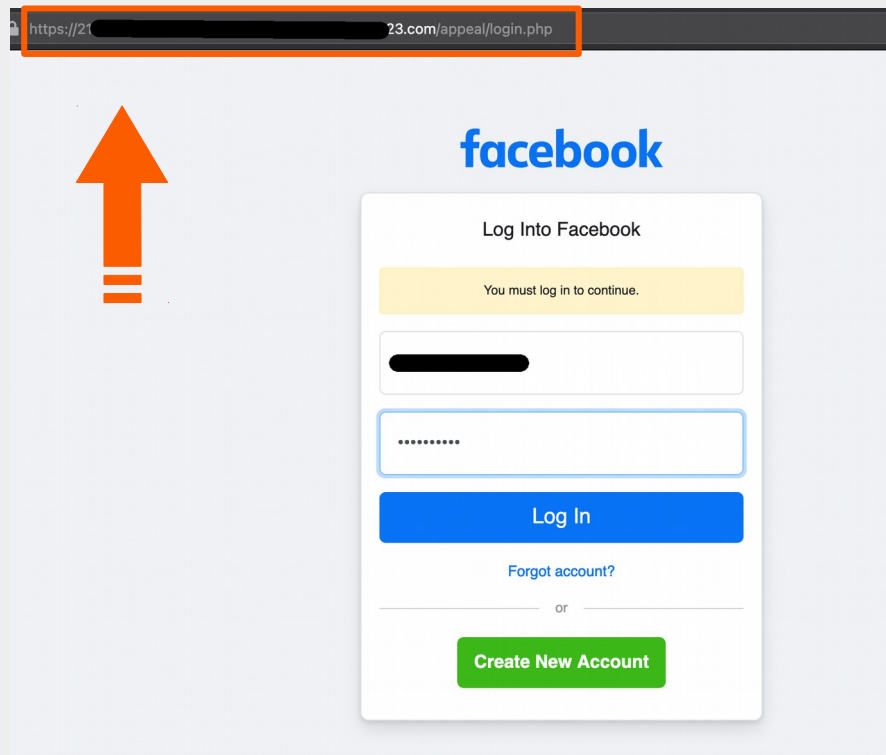
Additional info

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.



Calendar spam

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

To sporočilo vsebuje povabilo na dogodek. ✓ Sprejmi ? Neodločeno

Od fiacredepreville@gmail.com ☆ ↶ Odgovori → Posreduj 📁 Arhiviraj 🚫 Neželeno

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

Za Mene [redacted] ★

fiacredepreville@gmail.com vas je povabil(a) na Ponudba posojila med posamezniki

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 v...
bila njihova datoteka na banki zav...
Če iščete posojilo med posameznik...
Na voljo smo zadovoljiti naše stran...
Za več informacij nas kontaktirajte...
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&>

1 opomnik [close]

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

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

[Podrobnosti ...](#)

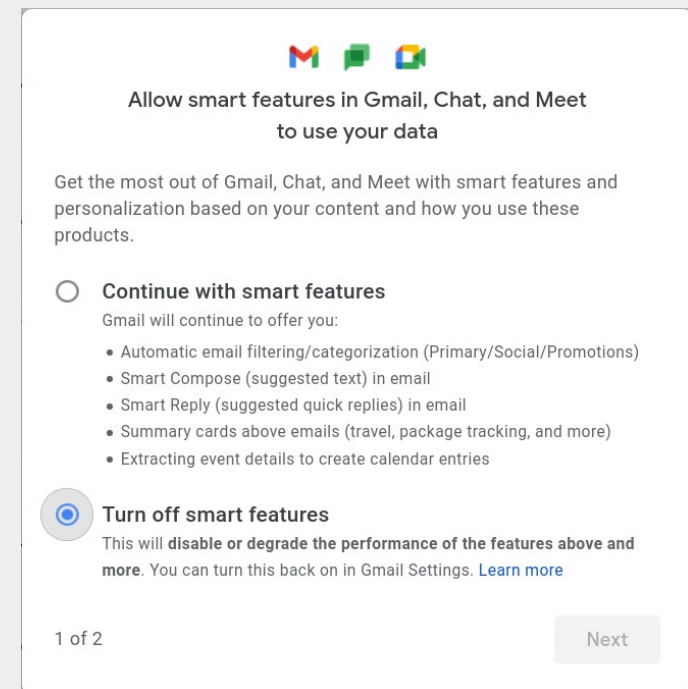
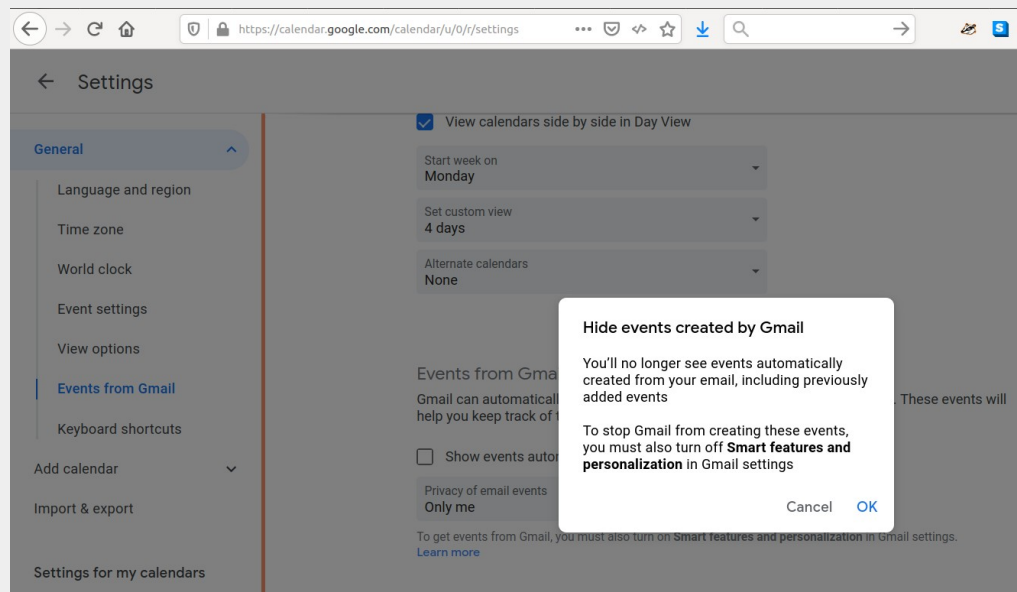
[Dremež vseh - v] [Izklopi vse]

, vendar je

Calendar spam

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

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

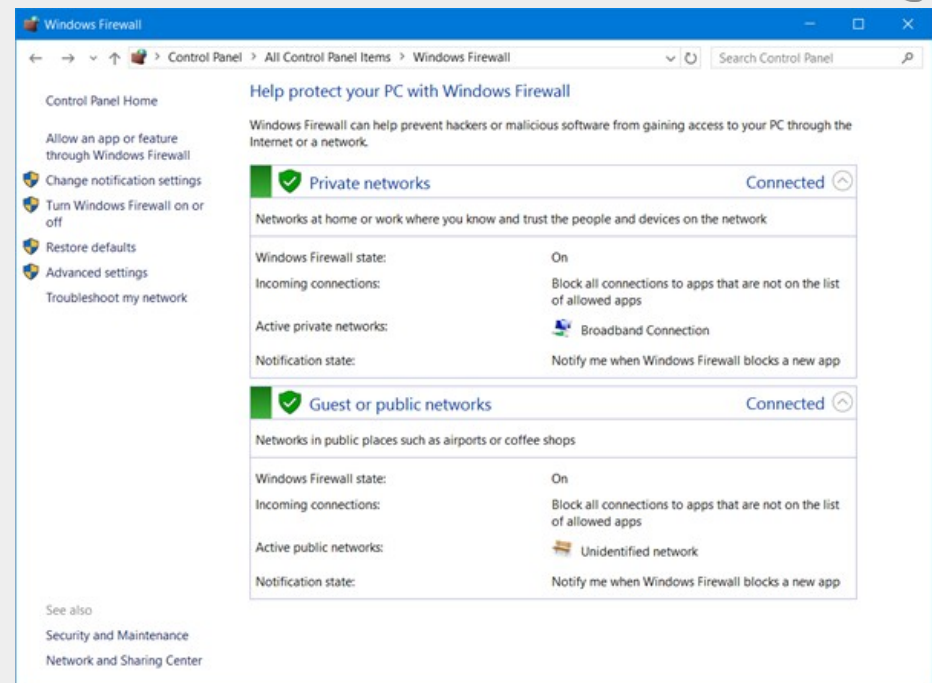
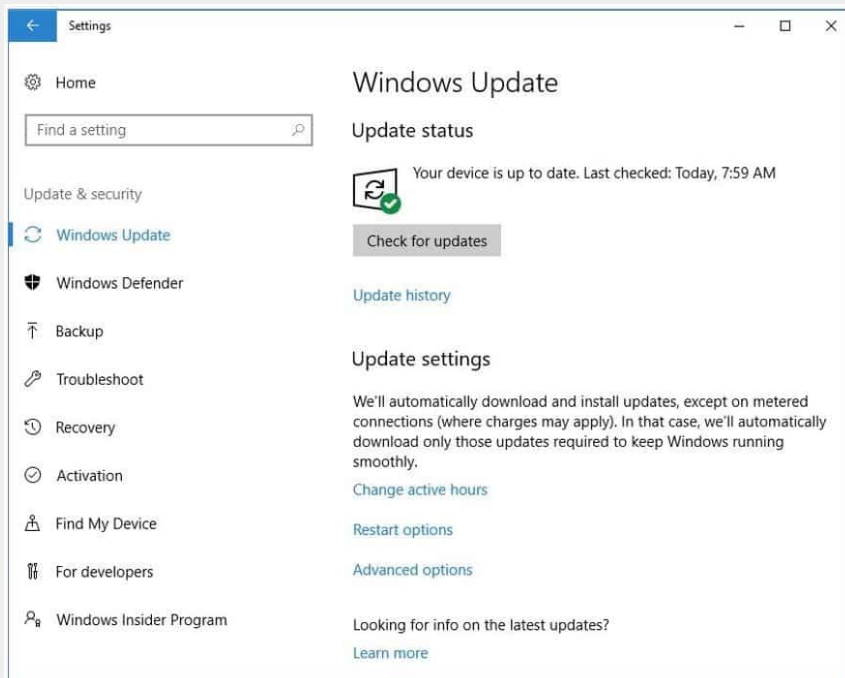
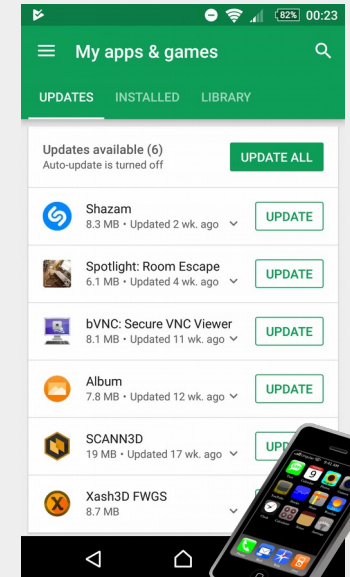
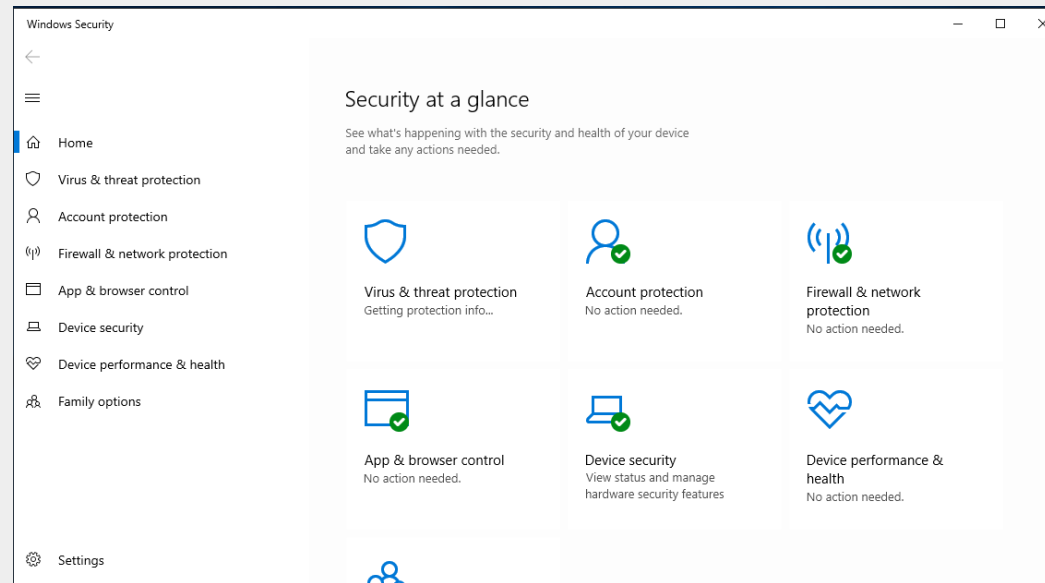


Protection

- 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.

Protection



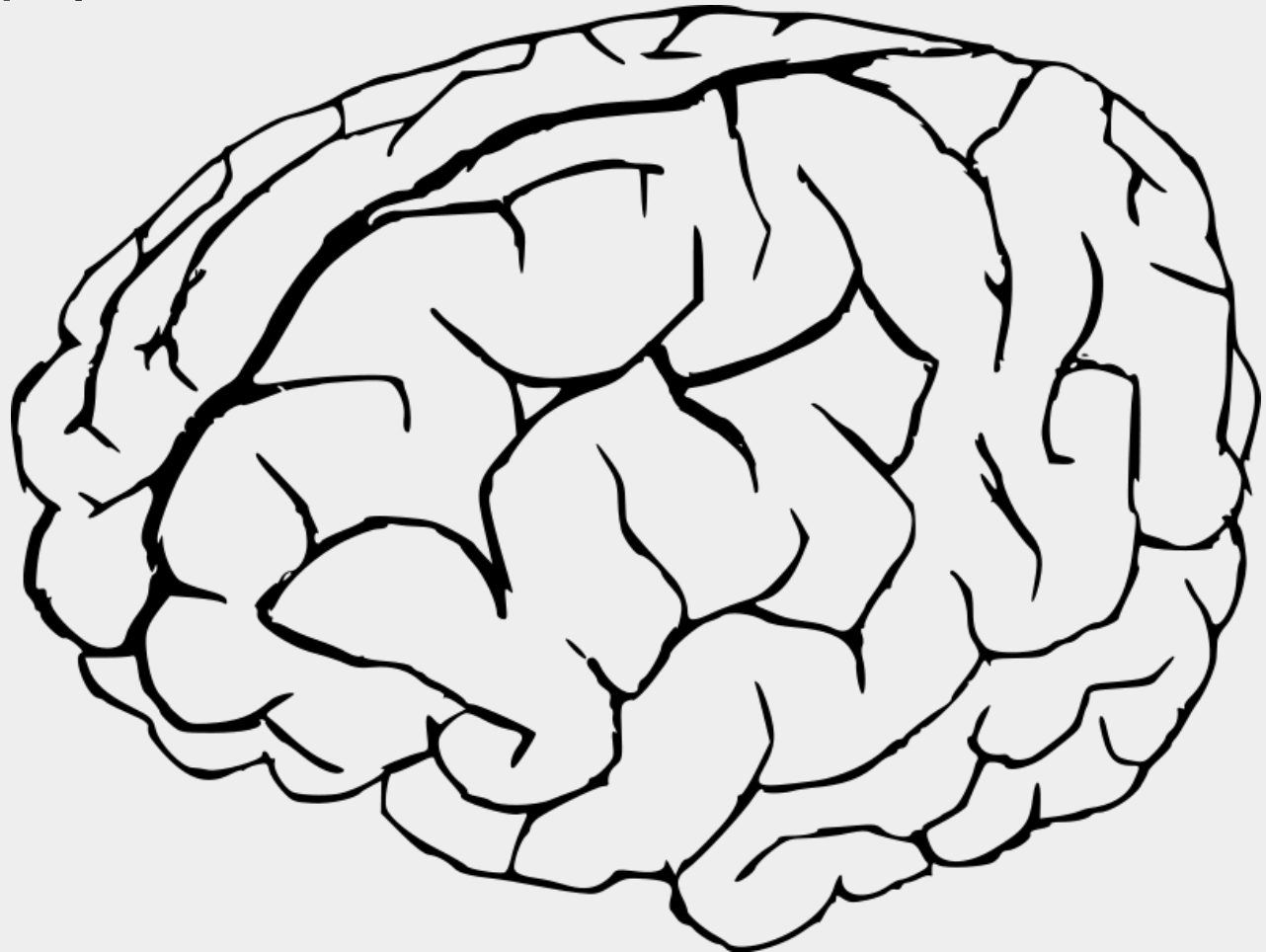
Protection

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.

Protection

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



Questions?



Questions for the audience

Od rmhashimi8@gmail.com ☆ Odgovori Posreduj Izbriši Več ▾

Zadeva **Partnership** 4. 01. 21 18:47

Za Mene <matej.kovacic@telefoncek.si> ☆

Hello,

My name is Reem E. Al-Hashimi, I am writing to you to stand as my partner to receive my share of gratification from foreign companies whom I helped during the bidding exercise towards the Dubai World Expo 2020 Committee.

Am a women and serving as a Minister, there is a limit to my personal income and investment level and For this reason, I cannot receive such a huge sum back to my country or my personal account, so an agreement was reached with the foreign companies to direct the gratifications to an open beneficiary account with a financial institution where it will be possible for me to instruct further transfer of the fund to a third party account for investment purpose which is the reason i contacted you to receive the fund as my partner for investment in your country.

The amount is valued at Eu 47,745,000.00 with a financial institution waiting my instruction for further transfer to a destination account as soon as I have your information indicating interest to receive and invest the fund, I will compensate you with 30% of the total amount and you will also get benefit from the investment.

If you can handle the fund in a good investment. reply on this email only: reem.alhashimi@kakao.com

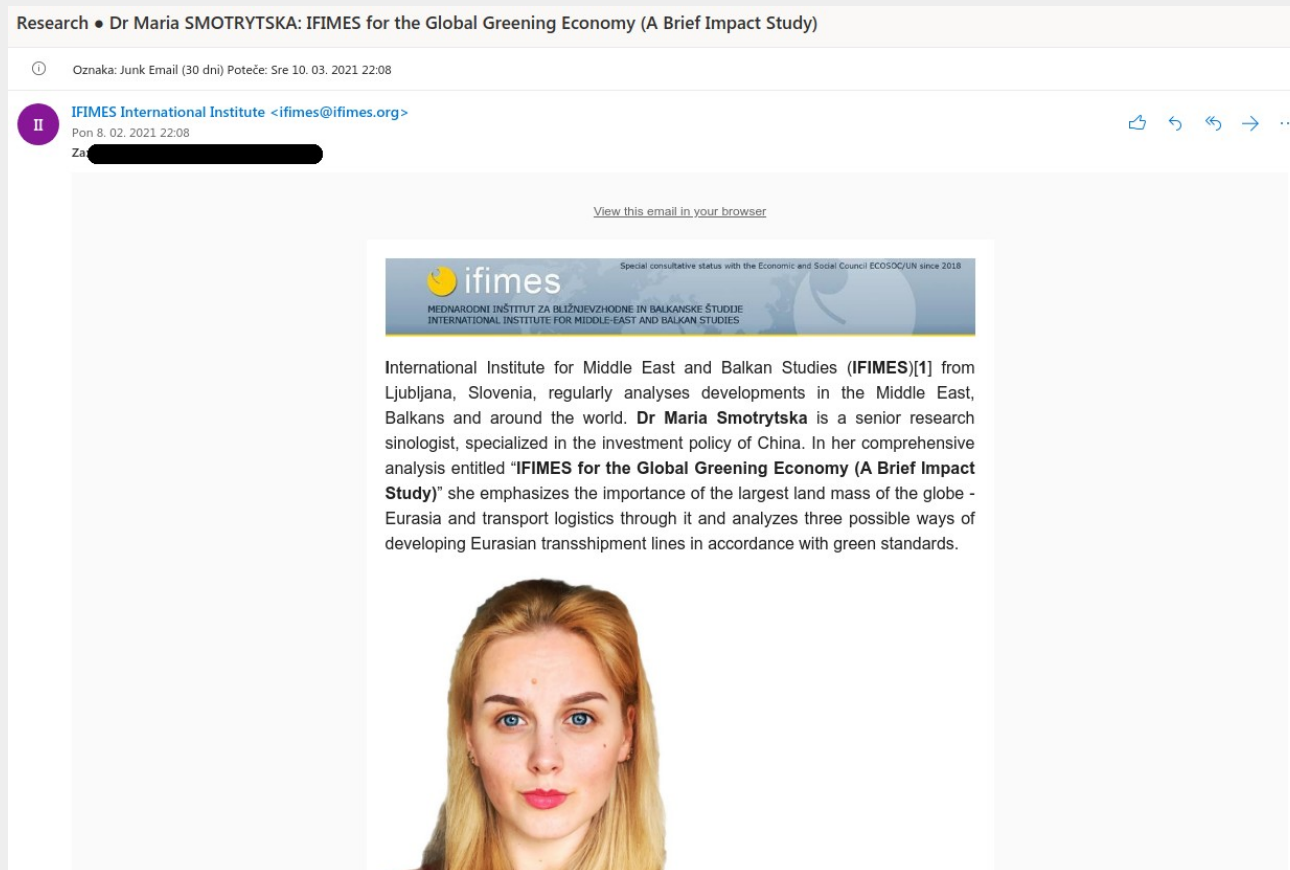
Regards,
Ms. Reem

[Untitled form](#)

[Fill out form](#)

- a) I can send contact mail, no harm in that.
- b) "30% of the compensation" looks too good to be true.
- c) Let's open the link in »incognito mode«.

Questions for the audience



- Looks suspicious, it must be a scam.
- It is just an ordinary spam.
- I subscribed to this mailing list, so it is legitimate mail.

Questions for the audience

Od Hans of Guardian★

Zadeva [guardian-dev] Important Alert 28. 01. 21 16:51

Za Guardian Dev★

You have received an important message.

Due to new covid19 security rules, you are required to update your account with further information.

follow this link to begin [Click Here To Begin](#)

Thank you.

List info: <https://lists.mayfirst.org/mailman/listinfo/guardian-dev>
To unsubscribe, email: guardian-dev-unsubscribe@lists.mayfirst.org

- a) It is sent by a person I know, so it must be true.
- b) The whole message smells like a scam.
- c) Let's click on the link to see what security updates are required.

Questions for the audience

Hello!

I am a hacker who has access to your operating system. I also have full access to your account.

I've been watching you for a few months now.

The fact is that you were infected with malware through an adult site that you visited.

If you are not familiar with this, I will explain.

Trojan Virus gives me full access and control over a computer or other device. This means that I can see everything on your screen, turn on the camera and microphone, but you do not know about it.

I also have access to all your contacts and all your correspondence.

I made a video showing how you masturbate on the left half of the screen, and in the right half you see the video that you watched. With one click of the mouse, I can send this video to all your emails and contacts on social networks.

If you want to prevent this, transfer the amount of \$950(USD) to my bitcoin address.

My bitcoin address (BTC Wallet) is: ...

- a) OMG, I am so embarrassed I was watching *that* porn yesterday.
- b) Well, in fact *I have been* watching porn, but I don't have a camera on my computer, so how did they got me?
- c) Nah, I will not pay, it is a scam.

Questions for the audience

The image shows a screenshot of an email from Greater Manchester Police. The header includes the Greater Manchester Police logo and the text 'YOUR PTN: 45UCZFQ46'. The main heading is 'Notice of Intended Prosecution (NIP)'. The body of the email states: 'In accordance with Section 1 of the Road Traffic Offenders Act 1988, we hereby inform you that it is mandatory to take proceedings against the driver of motor vehicle. This email is the part of GMP Notification Service.' Below this is a section titled 'Details of the Violation' containing a bulleted list: 'Fixed Speed Camera Number: 29YYR74', 'Time & Date: at 12:45 on 07/12/2016', 'Violation Location: A5067 Talbot Road, near jct Warwick Road, Trafford', 'Offence: EXCEED 25 MPH SPEED LIMIT', and 'Your Vehicle Speed: 89'. A red text box below the list says: 'We have photographic proof that the driver of motor vehicle failed to adhere with a speed limit at the date, time and location.' Further down, it says: 'In your own case the notice was served on the keeper of the vehicle as registered with the DVLA and your details have thereafter been supplied to us as being the driver at the moment. The registered owner, driver or legal representative may examine the photographic evidence now or later by appointment.' There is a red button labeled 'Check Fixed Speed Device Photo'. At the bottom, it says: 'Whether you agree with the NIP or not you have to complete the section 172 notice declaring who was driving the car at the time of the offence within 28 days. The NIP with the section 172 notice were sent to your mailing address.' The footer contains 'Copyright © Greater Manchester Police 2016'.

- a) Wow, police is now sending fines by e-mail, they got digital!
- b) I am driving fast occasionally, but this is not official notification.
- c) OMG, I am living in a police state, they are watching me everywhere and they do have my email address!

Matej Kovačič

Institute of Forensics of Information Technologies,
<http://www.ifit.si>



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

