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
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.
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.
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.
Fraudulent online store #2

Deeper analysis:

• JavaScript tracker code found...
Fraudulent online store #2

Deeper analysis:

- ...leading to Chinese servers.

huawei.safedns.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).
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.
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)
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.
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
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