Računalniška/Informacijska/Kibernetska/Digitalna varnost
Computer/Information/Cyber/Digital security

Matjaž Kljun matjaz.kljun@upr.si

2. del / Part 2

- …

- …

Socialni inženiring

Social engineering

Kaj je? / What is it?

- Psihološko manipuliranje z ljudmi, da nekaj naredijo ali razkrijejo zaupne informacije.
- Vse tehnike socialnega inženiringa temeljijo na lastnostih človeškega odločanja, ki so znane kot kognitivne pristranskosti.
- Bodimo pozorni na igrano karto:
  - Čustev
  - Nujnostu
  - Ukrepanja

- Psychological manipulation of people into performing actions or divulging confidential information.
- All social engineering techniques are based on attributes of human decision-making known as cognitive biases.
- Be aware of playing on:
  - Emotions
  - Emergency
  - Call to actions

Tehnike / Techniques

- Ribarjenje
- Ribarjenje s kopijem
- Lovljenje kitov
- SMS ribarjenje
- Glasovno ribarjenje
- Zavajanje z zgodbo
- Romantično zavajanje
- Zavajanje z vabo
- Vodna zajetja
- Quid Pro Quo
- Sledenje
- Deskanje za ramo
- Potapljanje v smetnjaku
- Pharming
- ...

- Phishing
- Spear Phishing
- Whailing
- Smishing (SMS phishing)
- Vishing (voice phishing)
- Pretexting
- Catfishing
- Baiting
- Water holing
- Quid Pro Quo
- Tailgating
- Shoulder surfing
- Dumpster diving
- Pharming
- …

Ribarjenje

Phishing

Ribarjenje / Phishing

Oblika prevare, pri kateri napadalci ljudi zavajajo, da razkrijejo občutljive podatke ali namestijo zlonamerno programsko opremo, kot je izsiljevalska programska oprema.

To se pogosto zgodi prek:

- elektronske pošte
- programov za takojšnje sporočanje
- sporočil SMS
- po telefonu (vishing)
- storitve družabnih omrežij
- …

A form of scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

It often occurs over:

- Email (phishing)
- Instant messaging software
- SMS messaging (smishing)
- Phone (vishing)
- Social networking services
- …

TOOLBOX

PHISHING VS. SPEAR PHISHING VS. WHALING

PARAMETER	PHISHING	SPEAR PHISHING	WHALING
TARGET 	Hackers go after a large number of targets	The target is usually one organization. Fraudulent emails are sent to a handful of well-researched employees.	The target is a top executive who is in direct contact with the organization's CEO and high-value customers.
VALUE 	Phishing targets are low-yield, with not many organizational assets at stake	Phishing targets are high-yield. In personalized attacks, victims willingly compromise extra-sensitive data.	Whaling yields immediate high-value results, considering the ranking of the people involved. It may leak trade secrets.
TECHNOLOGY 	Phishing attacks are generic and use very low-key technology. There are many off-the-shelf phishing kits available on the dark web.	Spear phishing attacks research targets on the internet. The attack may use slightly more sophisticated technology.	Whaling is similar to spear phishing with respect to the reconnaissance phase and sophisticated technology.
EXAMPLE 	Sending out mass emails stating that a specific bank's online accounts have been compromised and passwords need to be reset.	An email stating that a specific vendor-related payment has failed due to incomplete details, and a fake link is shared to retry the payment process.	Sending a carefully crafted email that appears to be from the organization's CEO asking executives to share employee payroll details.

Ribarjenje ali Smetenje / Phishing or Spam

Ribarjenje

- Vrsta napada, ki uporabnike zvabi k razkritju občutljivih ali dragocenih podatkov, kot so prijavni ali finančni.
- Sporočila uporabljajo socialni inženiring za ustvarjanje občutka nujnosti ali pomembnosti in dajejo občutek da gre za zaupanja vredne osebe ali organizacije, da bi pridobili zaupanje žrtve.
- Ukrepi: Sporočiti IT službi, saj gre lahko za širši kibernetski napad in jih je treba raziskati.

Smetje

- Nezaželena sporočila, ki se običajno pošiljajo v velikem obsegu, so komercialne narave in promovirajo izdelek ali storitev.
- Smetje je nadleženo, vendar običajno ni zlonamerno in ne poskuša prejemniku ukrasti podatkov.
- Ukrepi: Izbrišite, odjavite, filtrirajte med neželeno pošto ali blokirajte.

Phishing

- A type of cyberattack that lures users into disclosing sensitive or valuable information such as login credentials or financial information.
- Messages typically use social engineering to create a sense of urgency or importance and may impersonate a trusted individual or organization to gain the victim's trust.
- Actions: Report to IT/Security, as they could be part of a wider cyber attack and should be investigated.

Spam

- Spam are unsolicited messages, typically sent in bulk, often commercial in nature, promoting a product or service.
- Spam is annoying, but typically not malicious or attempting to steal information from the recipient.
- Actions: Delete, unsubscribe, filter to junk mail, or block.

Primeri e-pošte / Examples of e-mail

- Čustva, nujnost, ukrepanje.
- Poglejmo si nekaj primerov.
- Poskusimo ugotoviti za kaj gre.

- Emotions, emergency, call to action
- Let’s look at some examples.
- Try finding out what they are.

Pazimo na / Take care of

- Berimo e-pošto v čistem besedilu, če je možno.
- Izklopimo nalaganje slik, če je možno - https://en.wikipedia.org/wiki/Spy_pixel.
- Preverimo pošiljatelja.
- Preverimo naslovnike.
- Preverimo “Reply to” polje.
- Poglejmo kam peljejo povezave, preden nanje kliknemo.
- Ne odpiramo priponk neznanih pošiljateljev.
- Če se nam e-pošta znanih pošiljateljev zdi sumljiva, vprašamo o čem je.
- Brišemo neželeno pošto.
- Uporabimo filter neželene pošte. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/spam-filtering-tips-outlook-email-inboxes

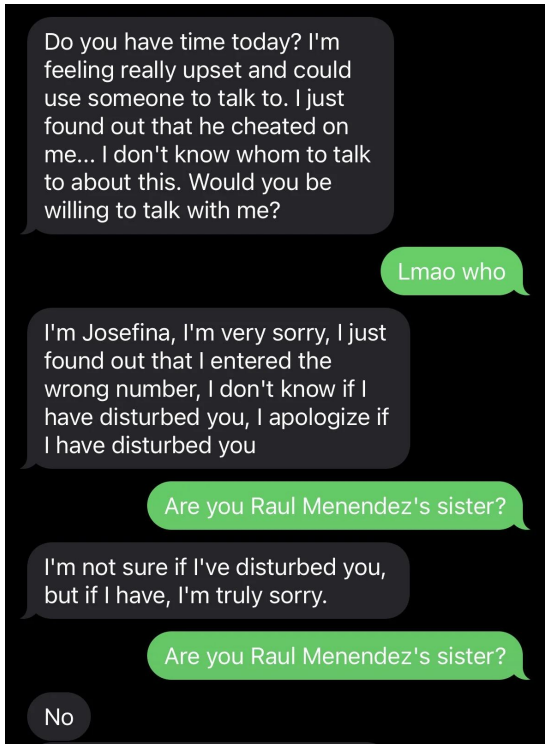
- Read emails in plain text if possible.
- Turn off image loading if possible - https://en.wikipedia.org/wiki/Spy_pixel
- Check the sender.
- check the addressees.
- Check the “Reply to” field.
- Check where the links lead before we click on them.
- Do not open attachments from unknown senders.
- If we think an email from known senders is suspicious, ask what’s the message about.
- Delete spam and other unwanted email.
- Use spam filter https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/spam-filtering-tips-outlook-email-inboxes

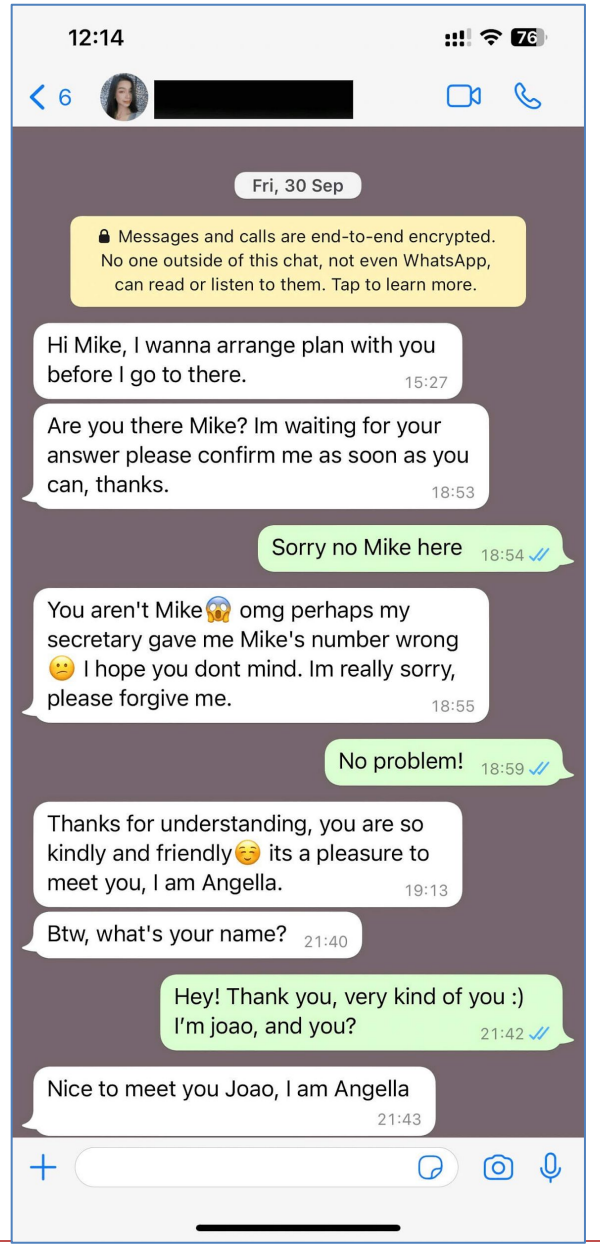
Romantično zavajanje

Catfishing

Catfishing

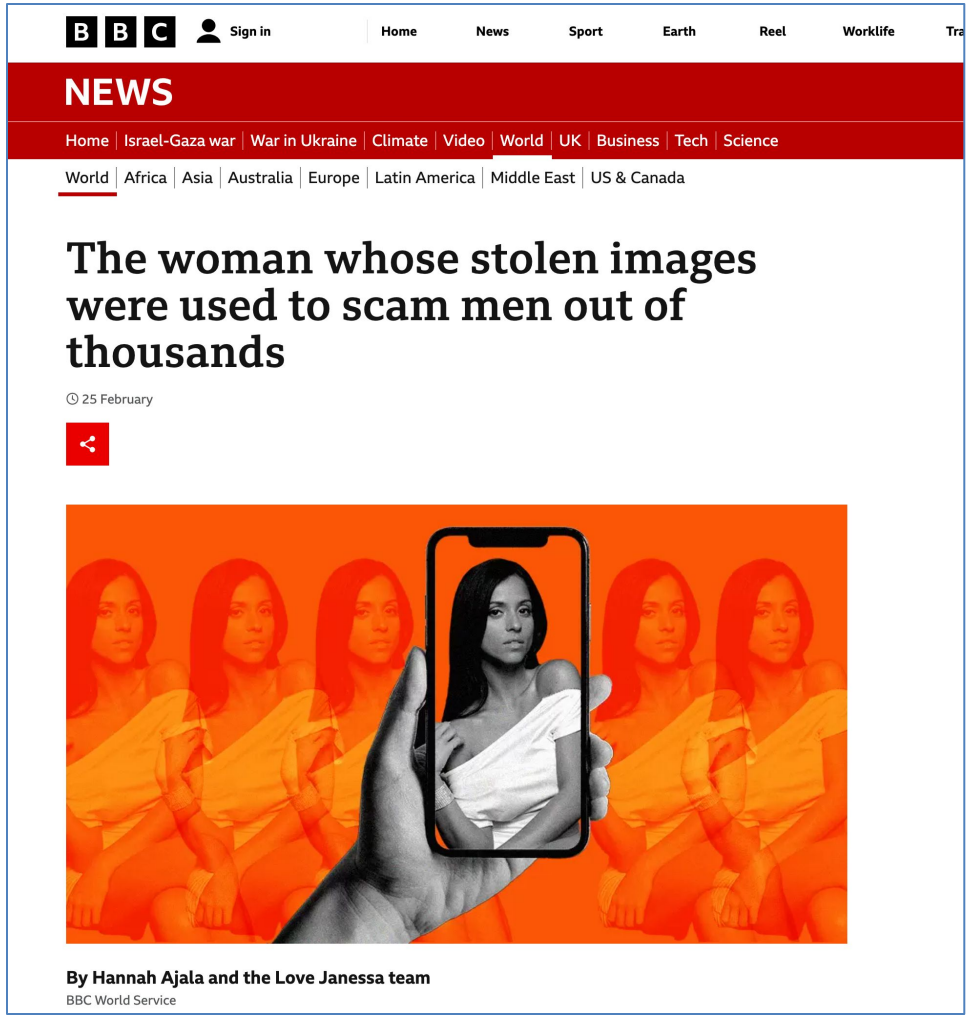
Catfishing je tehnika zavajanja, pri kateri napadalec uporabi izmišljeno osebo ali lažno identiteto na družabnem omrežju ali programih za takojšnje sporočanje, pri čemer običajno cilja na določeno žrtev.





Catfishing is a deceptive activity in which a person creates a fictional persona or fake identity on a social networking service or instant messaging, usually targeting a specific victim.

V branje / To read



The woman whose stolen images were used to scam men out of thousands

Published 25 February, 2023
By Hannah Ajala and the Love Janessa team
BBC World Service

https://www.bbc.com/news/world-64720239

Skripte za prevaro / Scam scripts

- Nigerian scammers playbook https://scamfishcdn.socialcatfish.com/2019/03/Nigerian-scammers-playbook.pdf

- Tricking English translators for ShaZhuPan Scripts, Jan 20, 2022 https://www.globalantiscam.org/post/tricking-english-translators-for-shazhupan-scripts

- Romance scam script (Part 1/18), Posted by u/Scammerce, 2022 https://www.reddit.com/r/Scams/comments/w1pxy4/romance_scam_script_part_118/

==========
Ways of saying hi to a client Pick one below
==========

Hi, how was your weekend?

Hey, how's your week going so far?

Hi. What have you been up to lately?

Hey, how are things with you today?

Hi, any fun plans for the weekend?

Hi, I hope your week is going well.

Hi, how are you? ??

Hi there. How's life treating you today?

Hey, what are you up to today?

Just stopping by to say hello. Hello!

I just had to say hi to you. Hi!

What's up? How are you?

How's your day going so far?

I hope you're having a nice day ??

Bodimo pozorni / Be careful

- Če pri pogovoru prek videa zvok ne deluje in se s sogovornikom ne moremo pogovarjati, oseba na drugi strani lahko ni resnična. Prosimo, da na list napišejo naše ime in ga pokažejo v kamero.
- Izgovori, da imajo težave s povezavo.
- Fotografijo sogovornika poiščemo na spletu. Lahko se iste fotografije uporabijo v različnih goljufijah ali pa je na fotografiji druga oseba.
- Imamo občutek,
  - da se pogovarjamo z več različnimi osebami,
  - so njihove zgodbe polne lukenj in neujemanj.

- Takšne goljufije v mnogih državah v razvoju predstavljajo pomemben del zaslužka in lahko potekajo v obliki organiziranega kriminala. Žrtev tako ne govori ves čas z isto osebo in bolj kot se romanca zapleta, težje vzdržujejo nivo doslednosti.

- If the sound does not work during a video conversation and we cannot talk to the person, the person on the other end may not be real. Ask them to write our name on the paper and show it to the camera.
- If the person often claim they are having connection problems.
- We check for a photo of the person online. The same photo may be used in different scams, or the photo may be of a different person.
- We have a feeling
  - to talk to several different people,
  - their stories are full of holes and inconsistencies.

- Such frauds represent a significant part of earnings in many developing countries and can take the form of organized crime. Thus, the victim does not talk to the same person all the time, and the more complicated the romance becomes, the harder it is for them to maintain a level of consistency.

Zgodba iz Pirana / The story from Piran

Ljubezen in financiranje terorizma

Love and financing terorism

https://en.wikipedia.org/wiki/Piran#/media/File:Panoramics_of_Piran_2015.jpg

Izsiljevanje z intimnimi posnetki / Sextortion

Suicide of Amanda Todd

13 languages

Article Talk | Read View source View history Tools

From Wikipedia, the free encyclopedia

Amanda Michelle Todd (November 27, 1996 – October 10, 2012)[7][8] was a 15-year-old Canadian student and victim of cyberbullying who hanged herself at her home in Port Coquitlam, British Columbia. A month before her death, Todd posted a video on YouTube in which she used a series of flashcards to tell her experience of being blackmailed into exposing her breasts via webcam,[5] and of being bullied and physically assaulted. The video went viral after her death,[9] resulting in international media attention. The original video has had more than 15 million views as of May 2023,[10] although mirrored copies of the video had received tens of millions of additional views shortly after her death; additionally, a YouTube video by React has a video of teens reacting to Todd's video which has garnered 44.7 million views as of May 2023,[11] and various videos from news agencies around the world regarding the case have registered countless millions more.[12][13][14][15] The Royal Canadian Mounted Police and British Columbia Coroners Service launched investigations into the suicide.

Suicide of Amanda Todd

A screenshot of Todd's YouTube video

Date October 10, 2012

Scenarij / Scenario

- Predstavljajmo si, da nas na Facebooku (ali na drugi storitvo socialnega omrežja) kot prijatelja doda privlačna/privlačen neznanka/neznanec.
- Po začetnem klepetu ali kar nekaj klepetih (pridobivanje zaupanja, igranje na karto zaljubljenosti) nas povabi na Skype (ali katerikoli drugi program ki ponuja enako funkcionalnost), in ko prižgemo kamero, je na drugi strani brez oblačil.
- Povabi nas, da se tudi mi slečemo, in nam obljubi, da bo to najina skrivnost.
- Ko dobi slike/video grozi z njihovo objavo, če ji ne bomo nakazali denarja.

- Imagine that an attractive stranger adds us as a friend on Facebook (or other SNS).
- After initial chat or several chats (gaining trust, playing the love card), they invite us to Skype (or any other program that offers the same functionality), and when we turn on the camera, they are naked.
- They invite us to show us our nakedness and promise us that it will be our secret.
- When they get the pictures/videos, they threaten to publish them if we don't transfer the money to them.

V branje / To read

Boys as young as 13 being targeted in sextortion scams

Published 12 September, 2023


BBC Sign in Home News Sport Earth Reel Worklife

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science

Scotland | Scotland Politics | Scotland Business | Edinburgh, Fife & East | Glasgow & West | Highlands & Islands | NE

Boys as young as 13 being targeted in sextortion scams

12 September

Boys as young as 13 are increasingly being targeted by so-called sextortion scammers, Police Scotland figures reveal.

The victims are typically enticed into sending explicit photos and videos to strangers they have befriended online.

They are then blackmailed into paying to make sure the images are not made public.

Rising numbers of cases have been identified in **Police Scotland's latest performance report.**

The Scotland-wide analysis shows "the vast majority" of threats and extortions recorded last year related to sextortion-style crimes against males.

BBC Sign in Home News Sport Earth Reel Worklife

NEWS

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science

N. Ireland | N. Ireland Politics

Sextortion on Snapchat is not the end of my world, says victim

8 September

Nathan McErlean was left with an ultimatum last year, either pay thousands or have his nudes leaked

By Auryn Cox

BBC News NI

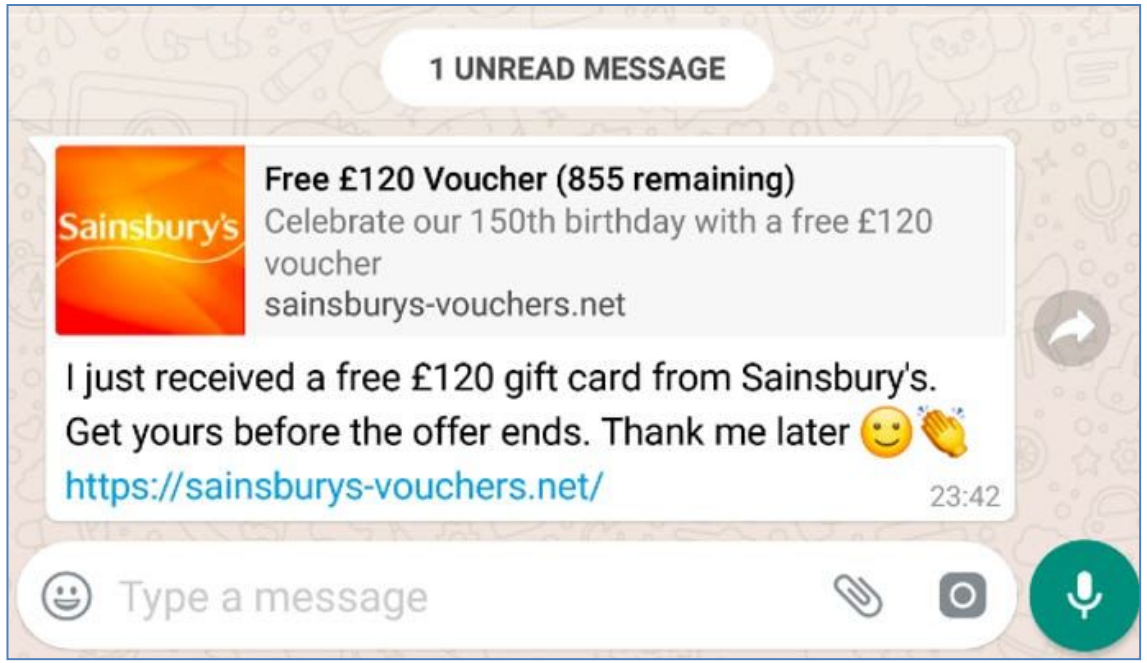
What started off as a bit of flirting on Snapchat ended in an ultimatum for Nathan McErlean - either he could pay thousands of pounds or explicit photos of him would be shared on social media.

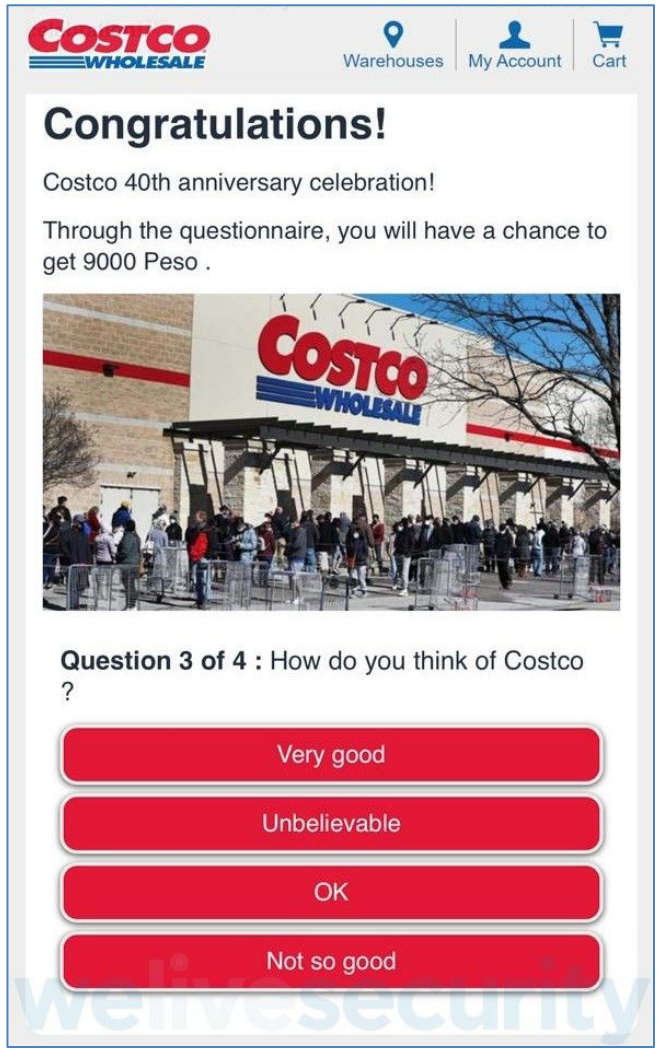
https://www.bbc.com/news/uk-scotland-66785583 and https://www.bbc.com/news/uk-northern-ireland-66736462

Zavajanje z vabo

Baiting

Ankete, kuponi in loterije / Surveys, vouchers and lotteries

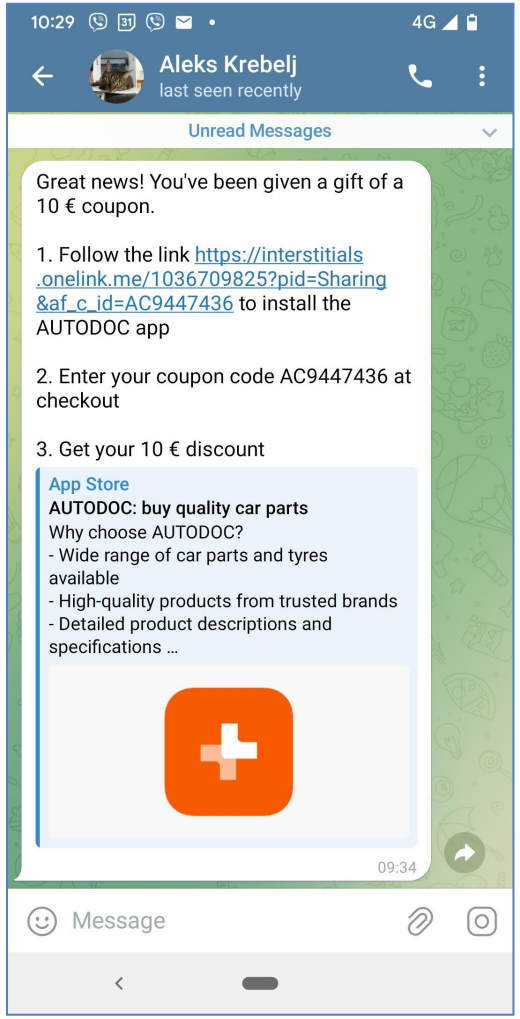


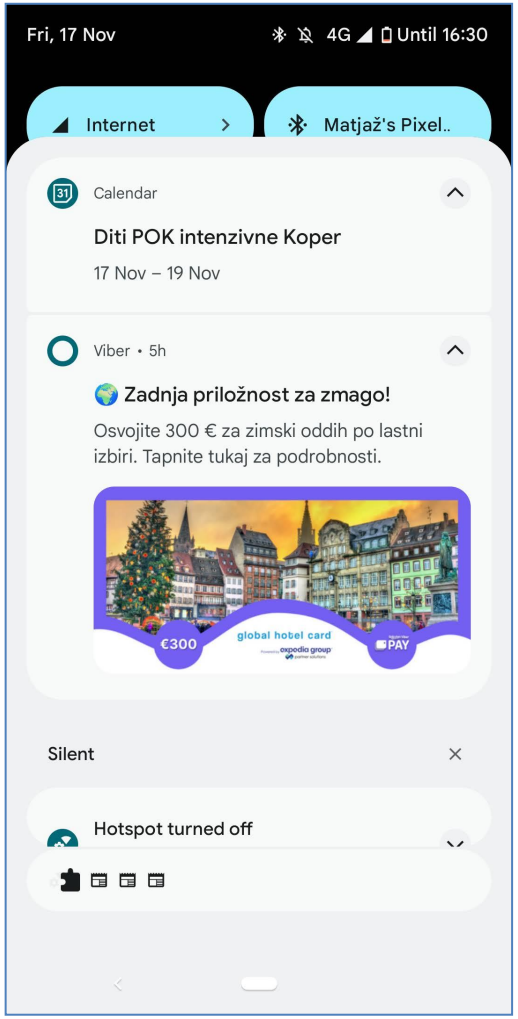


- Čustva
- Nujnost
- Poziv k ukrepanju

- Emotions
- Emergency
- Call to actions

Nagrade, darila / Prizes, gifts





- Čustva
- Nujnost
- Poziv k ukrepanju

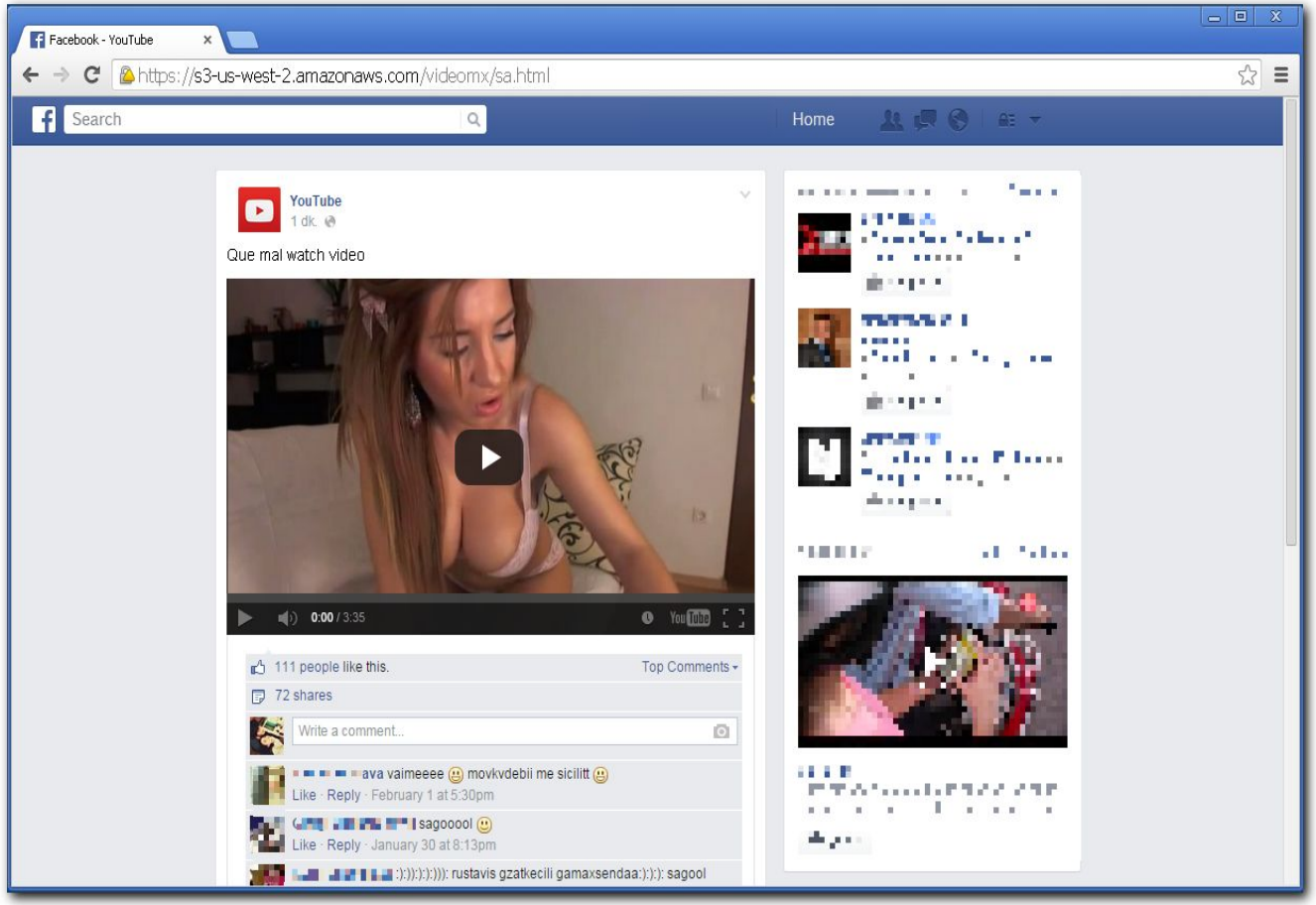
- Emotions
- Emergency
- Call to actions

Možen potek "nagradne igre" / Possible course of the "prize draw"

- Po končanem žrebanju prejmemo obvestilo z navodilom: **‘Pošlji SMS sporočilo "psc kupim 50" na številko 6888‘.**
- S tem smo pričeli nakup za predplačniško kartico Pay Safe Card v vrednosti 50 EUR. Ko kodo nakupa kopiramo na Facebook stran, nas tam blokirajo, da ne moremo opozoriti drugih.
- Predpogoj za sodelovanje v lažnih nagradnih igrah je lahko, da jih najprej delimo s svojimi prijatelji. S tem lahko tudi njih spravimo v nevarnost.
- Slovenska zakonodaja zelo natančno opredeljuje pogoje nagradne igre. Objavljeni morajo biti podatki o organizatorju, času trajanja, pogojih sodelovanja, načinu žrebanja, obveščanja …

- After the draw is over, we receive a notification with the instruction: **'Send the SMS message "psc kupim 50" to the number 6888'**.
- With this, we have started the purchase for a prepaid Pay Safe Card worth EUR 50. When we copy the purchase code to the Facebook page, we are blocked so that we cannot alert others.
- A prerequisite for participating in fake lotteries may be to share them with your friends first. This can also put them in danger.
- Slovenian legislation defines the terms of prize games very precisely. Information about the organizer, duration, conditions of participation, method of drawing, notification... must be published.

Radovednost / Curiosity



"Šokantno, kača pojedla človeka!", "Ekskluzivni posnetki letalske nesreče", "Prijatelj XY je označen v seksi videu!", "OMG, ne morem verjeti, da si ti v videu!".

“Za ogled namestite …”

Curiosity

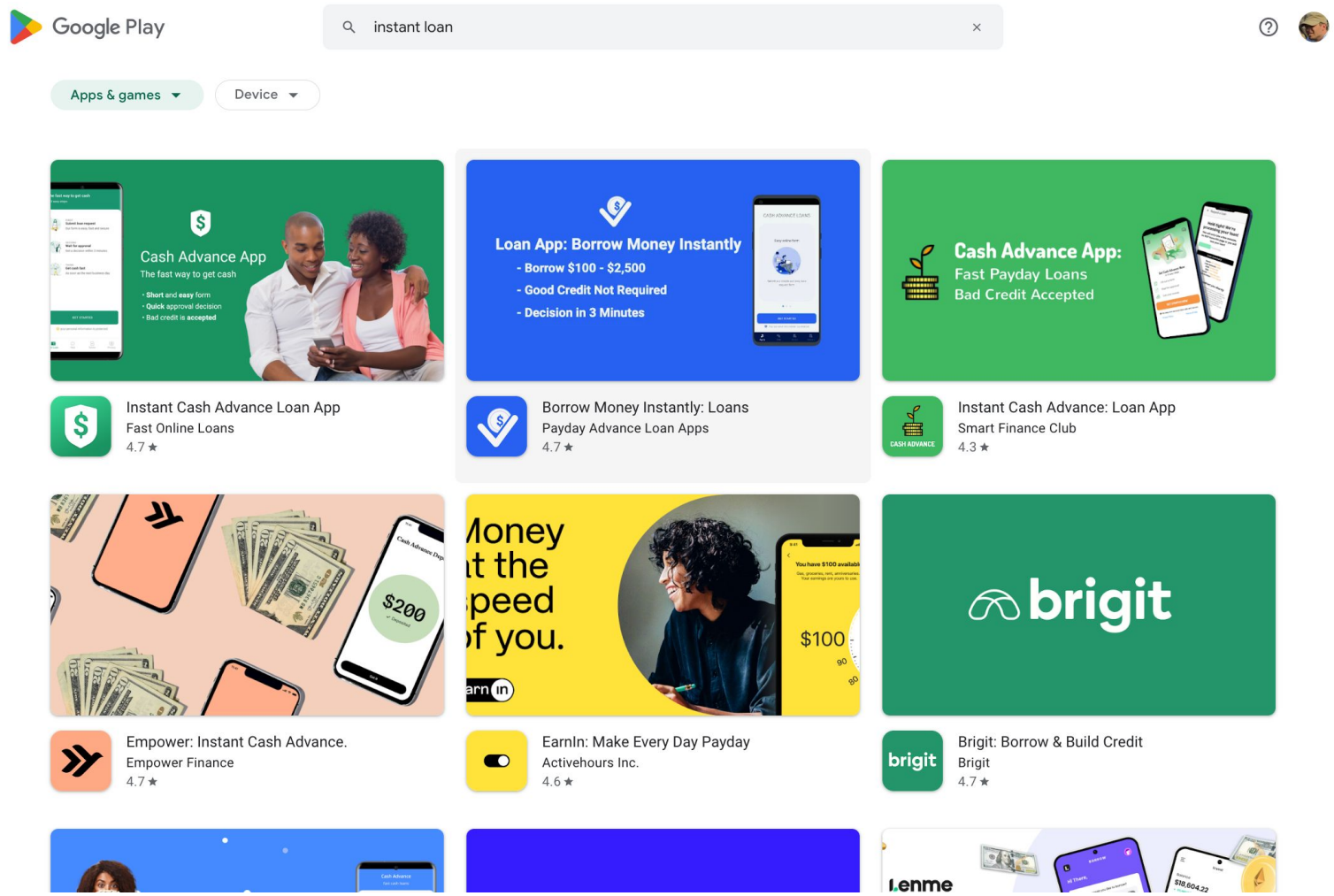
"Shocking, snake ate a man!", "Exclusive footage of plane crash", "XY's friend is tagged in this sexy video!", "OMG I can't believe you're in the video!".

"To view … install ..."

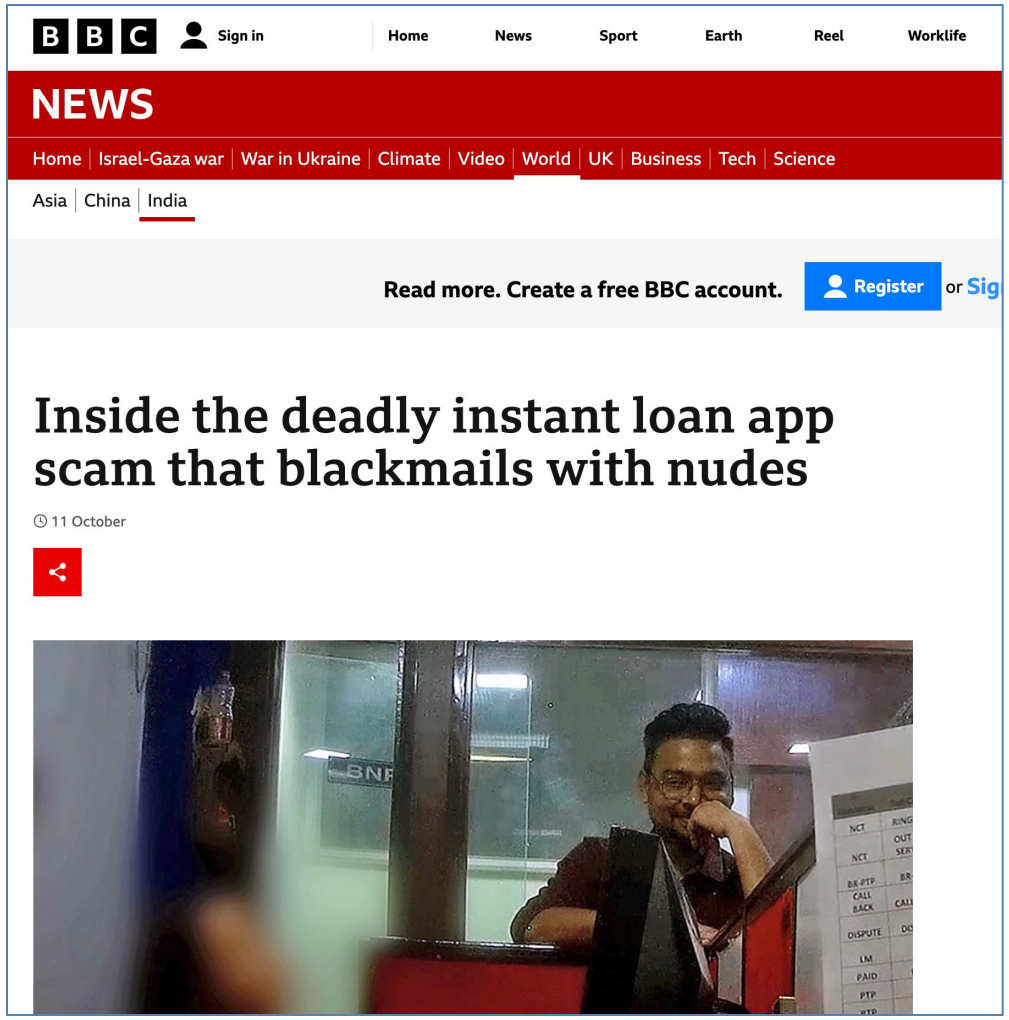
Pravice, ki jih damo applikacijam / Rights we give applications

Ali te aplikacije potrebujejo dostop do slik?

Do these applications need access to your photos?



V branje / To read



Inside the deadly instant loan app scam that blackmails with nudes

11 October, 2003

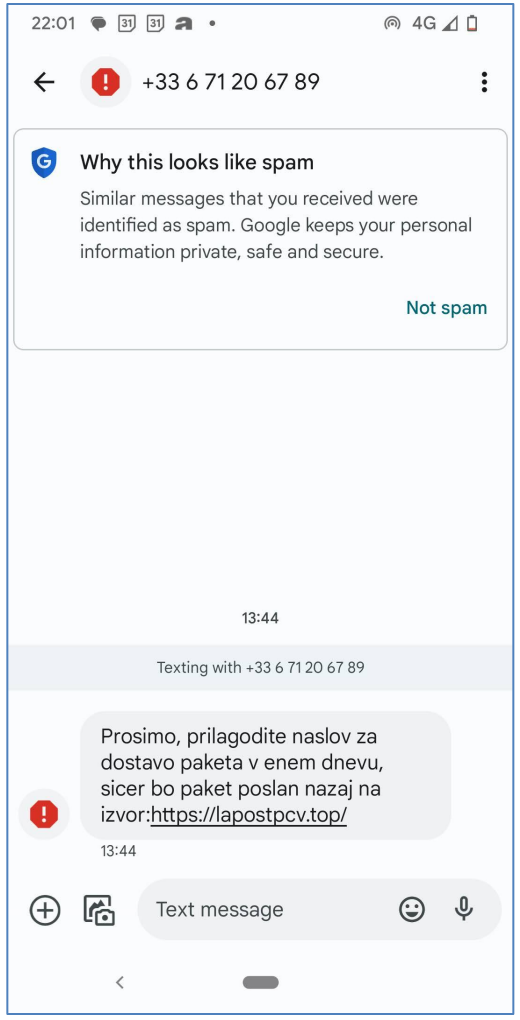
By Poonam Agarwal, Nupur Sonar and Stephanie Hegarty

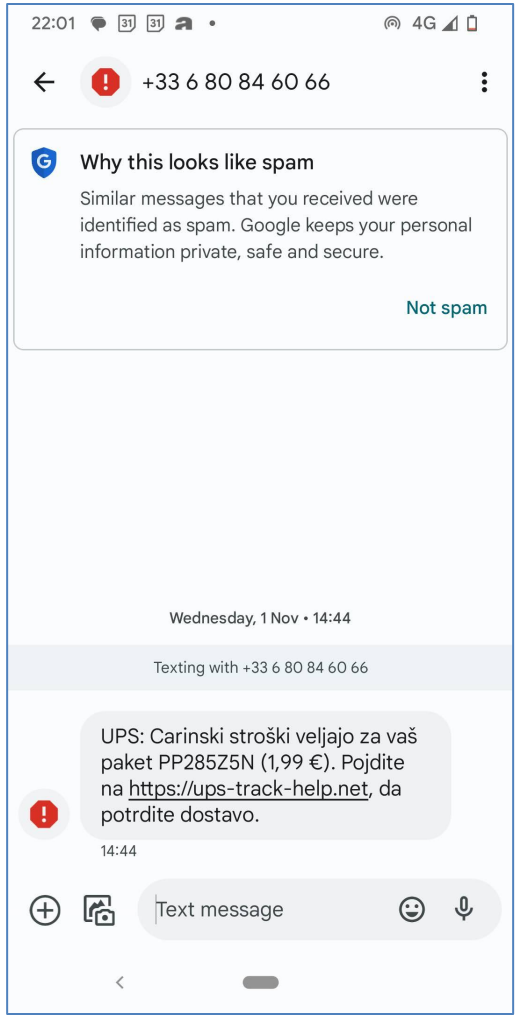
BBC World Service Eye Investigations

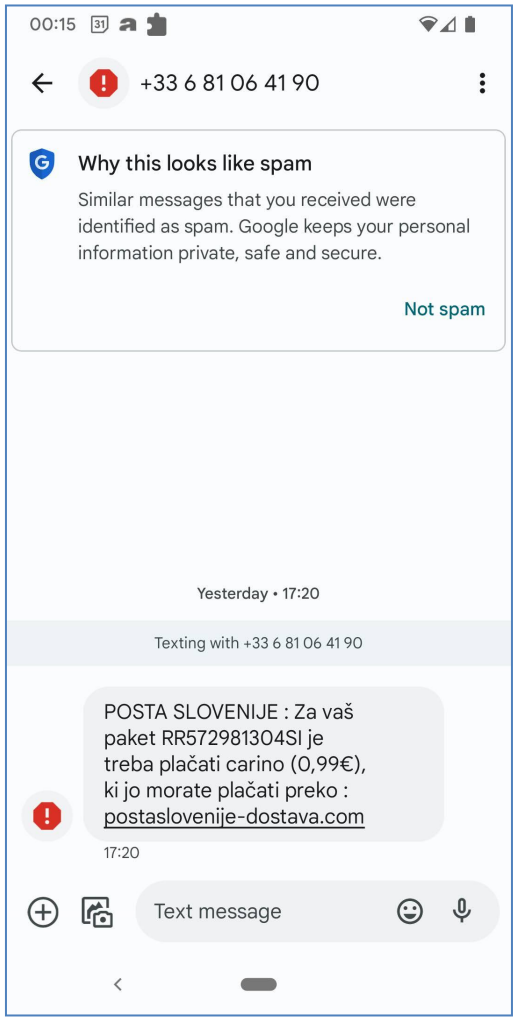
SMS in Glasovno ribarjenje

Smishing, Vishing

SMS ribarjenje / Smishing





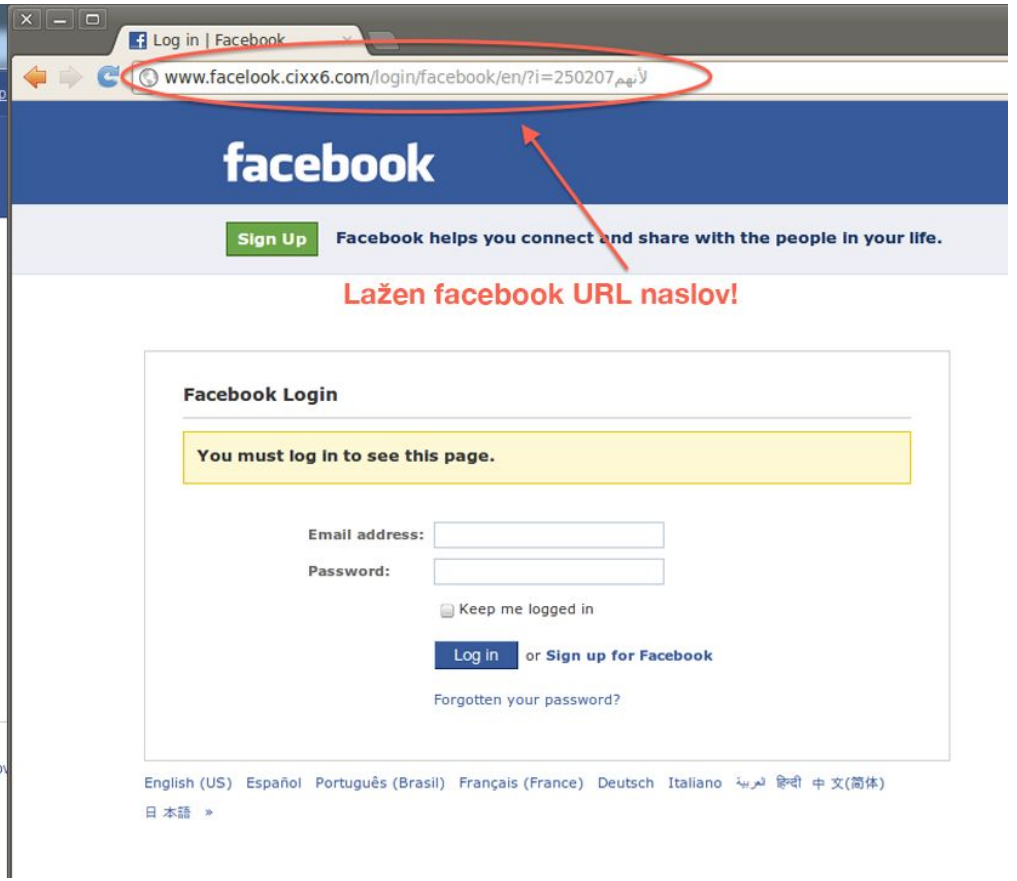


- Radovednost

- Curiosity

Lažne spletne strani / Fake web pages

- NUJNO POGLEDAMO NASLOV
- WE NEED TO CHECK THE ADDRESS



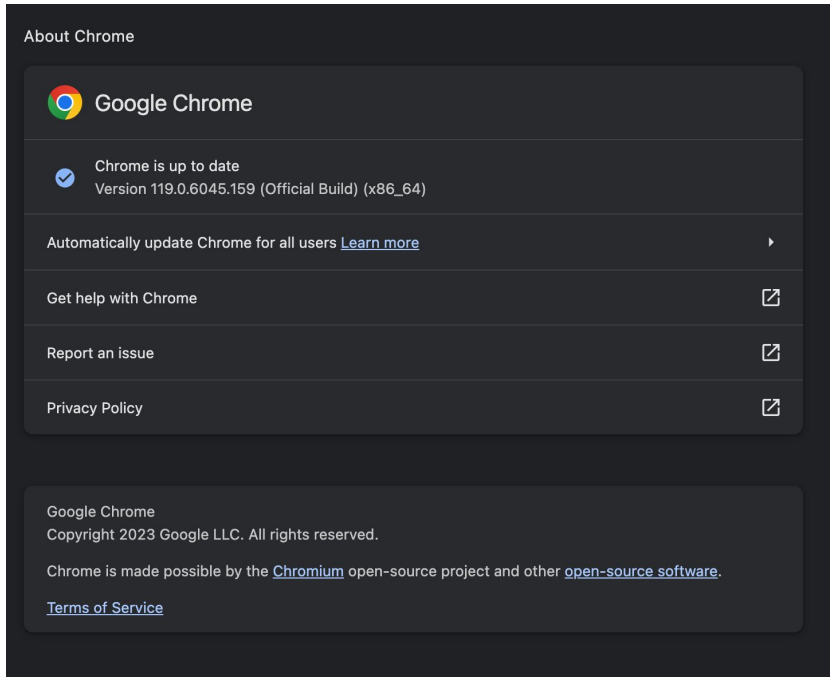
Poskusimo narediti lažno spletno stran / Let’s make a fake page

- Snamemo obstoječo stran
  - Na primer https://bankanet.otpbanka.si/auth/prijava
- Poglejmo, če lahko registriramo podobno domeno.
  - Na primer https://www.hitrost.com/domene/registracija-domene/
- Dajmo spletno stran na strežnik osebje.famnit.upr.si, ker domene ne bomo registrirali.
- Pošljemo HTML e-pošto enemu od nas.

- Download an existing page
  - For example https://bankanet.otpbanka.si/auth/prijava
- Check if we can register a similar domain.
  - For example https://www.hitrost.com/domene/registracija-domene/
- Upload the website on the server osebje.famnit.upr.si, because we will not register the domain.
- Let's send an HTML email to one of us.

Bodimo pozorni / Be careful

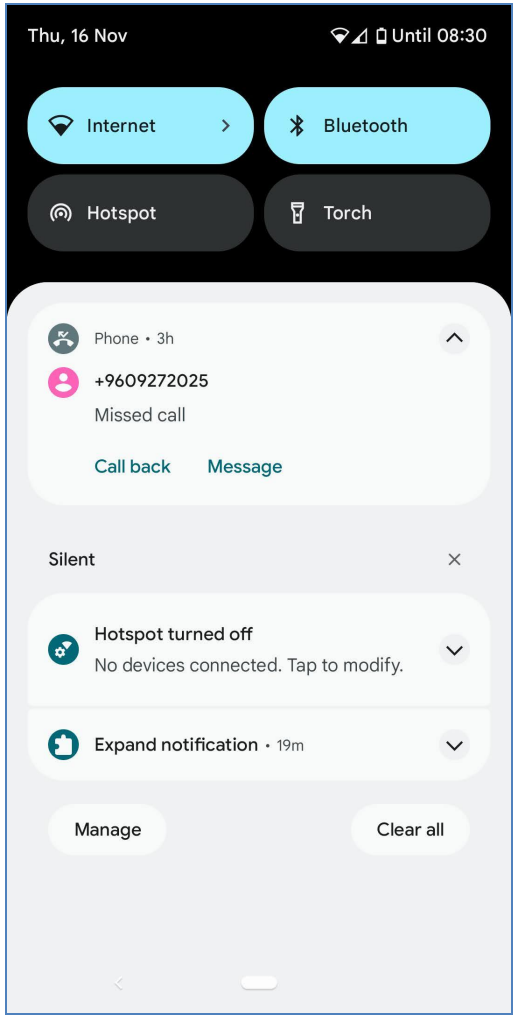
- HTTP in HTTPS – poglejmo v različnih brskalnikih.
  - Firefox, Chrome (Chromium), Edge, Opera, Vivaldi, Brave
  - https://www.google.com/search?q=the+most+popular+browsers
- Ali uporabljamo zadnjo različico brskalnika? Varnostni popravki v vsaki verziji. Poglejte vse brskalnike na računalniku
  - E.g. chrome://settings/help
- Zaseben/Inkognito način.
- Dodatki v brskalniku
  - Poglejmo, če so kakšni, ki jih ne poznamo
  - Namestimo take, ki blokirajo beleženje prometa, reklame, …
  - https://www.google.com/search?q=best+extenstions+for+private+browsing



- HTTP and HTTPS - let's see in different browsers.
  - Firefox, Chrome (Chromium), Edge, Opera, Vivaldi, Brave
  - https://www.google.com/search?q=the+most+popular+browsers
- Are we using the latest version of the browser? Security fixes in every version. See all browsers on your computer
  - E.g. chrome://settings/help
- Private/Incognito browsing mode
- Add-ons or extensions:
  - Check if there are any that we don't know about
  - Install ones that block traffic tracking, advertisements,...
  - https://www.google.com/search?q=best+extenstions+for+private+browsing

Glasovno ribarjenje / Vishing

Glasovno ribarjenje je vrsta napada socialnega inženiringa, ki se izvaja prek telefona. Klicatelji skušajo pridobiti naše osebne podatke, da bi jih uporabili pri izvedbi drugega kaznivega dejanja. Pogosto je cilj pridobiti dostop do našega bančnega računa.



Vishing is a type of social engineering attack that happens over the phone. Callers try to extract your personally identifying details to use in perpetrating another crime. The goal is often to gain access to your bank account.

Lažni klici / Fake calls

- Klicatelj zahteva, da odpremo programe, ki so del operacijskega sistema Windows (npr. Event Viewer), ki prikazujejo neke napake.
- Želijo nas prepričati, da imamo računalnik okužen. Dejansko pa gre za povsem običajne napake.
- V nadaljevanju želijo, da obiščemo določeno spletno stran in namestimo dolčen program (Team Viewer, AnyDesk, Ultraviewer ipd.).
- Preko tega programa omogočimo popoln nadzor nad našim računalnikom.

- The caller asks us to open programs that are part of Windows (e.g. Event Viewer) that show some errors.
- They want to convince us that our computer is infected. In fact, these are quite normal errors.
- Next, they want us to go to a certain website and install a program (Team Viewer, AnyDesk, Ultraviewer, etc.).
- This programme allows them to take full control of our computer.

https://www.varninainternetu.si/klici-lazne-microsoftove-tehnicne-pomoci/

Še ena poučna zgodba / Another educational story

Eva Wolfangel

... novinarka, govornica in moderatorka, ki se osredotoča na tehnologije prihodnosti, kot so ... kibernetska varnost ...

Eva Wolfangel

... a **journalist, speaker and moderator**, focusing on future technologies such as … cyber security ...

CHI 2023 Opening Keynote – Eva Wolfangel "The Human Element in Cybercrime and Cybersecurity"

https://www.youtube.com/live/LKUMRTLV49g?si=WZVt4Y0zox9__Haf&t=2607

Podobna zgodba iz Bukarešte / A similar story from Bucharest

- STRAH

- FEAR

- STRAH

- FEAR

INTERPOL

GENERALNI DIREKTORAT POLICIJE

VABILO NA SODIŠČE

Za sodno preiskavo

((člen 331-18 Mednarodnega kazenskega zakonika))

Jaz sem Mag. SENAD JUŠIĆ, generalni direktor nacionalne policije v sodelovanju z Evropskim policijskim uradom (Europol). Obračam se na vas kmalu po tem, ko je bil vaš računalnik daljinsko nadzorovan s kibernetsko infiltracijo (ta ukrep je dovoljen v primerih otroške pornografije, pornografske strani, kibernetske pornografije), da vas obvestim, da ste predmet več tekočih pravnih postopkov:

*** PORNOGRAFSKA SPLETNA STRAN**
*** KIBERNETSKA PORNOGRAFIJA**
*** EXHIBITIONIZEM**
*** ZLORABA MLADOLETNIKOV**

Na razgovor boste povabljeni po elektronski pošti, pošljite nam svoje razloge, da jih bomo lahko pregledali in preverili ter upoštevali sankcije; v strogem roku 48 ur. Po preteku tega roka bomo morali naše poročilo posredovati M. Drago ŠKETA, generalnemu državnemu tožilcu in specialist za kibernetsko kriminaliteto, da izda nalog za vašo aretacijo in vas registrira kot spolnega prestopnika .

Vaš spis bo posredovan tudi organom pregona, ki so najbližje vašemu prebivališču, da vas aretirajo. Registrirani boste kot spolni prestopnik, vaša fotografija bo objavljena v medijih, tako da bodo vaša družina in prijatelji vedeli, kaj počnete na računalniku.
Veselim se vaših razlogov.

Mag. SENAD JUŠIĆ
Direktor Uprave kriminalistične policije - SI
GENERALNI DIREKTORAT POLICIJE - SI

RheinlandPfalz
POLIZEIPRÄSIDIUM RHEINPFALZ
ZENTRALE BUßGELDSTELLE

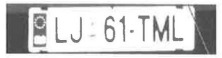
Zentrale Bußgeldstelle - 67346 Speyer
22 2FC5 D900 2E 7000 C1C4
DV 11.23 1,10

25.3387243.6
Univerza na Primorskem Univerista Del Litorale
Titov Trg 004
6000 Koper
SLOWENIEN
Re

Frau Wimberger
+49 6232 8720-600
+49 6131 4868-9700
https://www.polizei.rlp.de/kontakt-zbs
https://www.polizei.rlp.de/zbs
15.11.2023

eferenčnega znaka: **25.3387243.6**

Pisno obvestilo
po 27. čl. Zakona o cestnem prometu[1]
o cestnoprometnem prekršku, storjenem v Nemčiji



Spoštovane dame in gospodje,

dne 06.10.2023, ab 14:07 v Münchweiler, Gem. Münchweiler a.d.R., B 10, km 1,100, Walmersbach FR Landau je bil z vozilom z registrsko številko LJ–61–TML (SLO) storjen sledeči cestnoprometni prekršek po § 24 Zakona o cestnem prometu (StVG):

Prekoračitev dovoljene zunaj zaprtega naselja za 6 km/h.
Dovoljena hitrost 100 km/h.
Ugotovljena hitrost (po tolerančnem odbitku) 106 km/h.

Prekršen cestnovarnostni predpis: § 41 Abs. 1 iVm Anlage 2, § 49 StVO; § 24 Abs. 1, 3 Nr. 5 StVG; 11.3.1 BKat

Dokazna sredstva: laserska meritev, fotografija, priča

Priča: PHK Scheuermann, PASt KL - ZVD

V kolikor je bil za ugotovitev prekrška uporabljen merilni aparat, se potrdi, da je bil kalibriran.

Kot imetnik prometnega dovoljenja za omenjeno vozilo ste pozvani kot priča, da nam sporočite ime voznika, ki je odgovoren za zgoraj omenjeni prekršek, in njegove/njene osebne podatke

Te podatke ste dolžni dati po 46. čl. 1. od. Zakona o prekrških (OWiG), v povezavi s 161a čl. 1. od. 1. stavek Zakona o kazenskem postopku (StPO).

Kot priča lahko odklonite odgovore samo na tista vprašanja, s katerimi bi spravili samega sebe – ali nekoga, ki po 52. čl. 1. od. StPO šteje med sorodnike – v nevarnost pregona zaradi kaznivega dejan-ja ali prekrška.

3102 / 3225_1 / 3

Zaslišanje prek spleta	Koda QR	Na voljo so naslednje možnosti	Številkatekoče garačuna
https://zbs-onlineportal.polizei.rlp.de/oaweb/07300000 Prijava: 25.3387243.6 Geslo: !MfpHy)t8qaT		✓ Vpogled v dokazne slike ✓ Navedba voznika/voznice ✓ Izjava o domnevnem kaznivem dejanju ✓ Dodajte priloge	

Polizeipräsidium Rheinpfalz, Zentrale Bußgeldstelle, Maximilianstraße 6, 67346 Speyer, Telefax: 06131 4868-9700, Telefon: 06232 / 8720-600,
Für Anfragen nutzen Sie bitte das Kontaktformular auf unserer Homepage: https://www.polizei.rlp.de/kontakt-zbs
Öffnungszeiten: Mo.-Do. 09:00 - 12:00 & 13:00 - 14:30 Uhr, Fr. 09:00 - 12:00 Uhr
Kontoinhaber: LOK Koblenz; IBAN entnehmen Sie ggfls. dem Fließtext; BIC: PBNKDEFFXXX

- STRAH

- FEAR

INTERPOL

GENERALNI DIREKTORAT POLICIJE

VABILO NA SODIŠČE

Za sodno preiskavo

((člen 331-18 Mednarodnega kazenskega zakonika))

Jaz sem Mag. SENAD JUŠIĆ, generalni direktor nacionalne policije v sodelovanju z Evropskim policijskim uradom (Europol). Obračam se na vas kmalu po tem, ko je bil vaš računalnik daljinsko nadzorovan s kibernetsko infiltracijo (ta ukrep je dovoljen v primerih otroške pornografije, pornografske strani, kibernetske pornografije), da vas obvestim, da ste predmet več tekočih pravnih postopkov:

*** PORNOGRAFSKA SPLETNA STRAN**
*** KIBERNETSKA PORNOGRAFIJA**
*** EXHIBITIONIZEM**
*** ZLORABA MLADOLETNIKOV**

Na razgovor boste povabljeni po elektronski pošti, pošljite nam svoje razloge, da jih bomo lahko pregledali in preverili ter upoštevali sankcije; v strogem roku 48 ur. Po preteku tega roka bomo morali naše poročilo posredovati M. Drago ŠKETA, generalnemu državnemu tožilcu in specialist za kibernetsko kriminaliteto, da izda nalog za vašo aretacijo in vas registrira kot spolnega prestopnika .

Vaš spis bo posredovan tudi organom pregona, ki so najbližje vašemu prebivališču, da vas aretirajo. Registrirani boste kot spolni prestopnik, vaša fotografija bo objavljena v medijih, tako da bodo vaša družina in prijatelji vedeli, kaj počnete na računalniku.
Veselim se vaših razlogov.

SENAD JUŠIĆ
Direktor U[illegible]ve kriminalistične policije - SI
GENER[illegible]NI DIREKTORAT POLICIJE - SI

FAKE

RheinlandPfalz
POLIZEIPRÄSIDIUM RHEINPFALZ
ZENTRALE BUßGELDSTELLE

Zentrale Bußgeldstelle - 67346 Speyer
22 2FC5 D900 2E 7000 C1C4
DV 11.23 1,10

25.3387243.6
Univerza na Primorskem Univerista Del Litorale
Titov Trg 004
6000 Koper
SLOWENIEN
Re

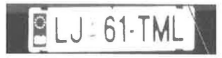
Frau Wimberger
+49 6232 8720-600
+49 6131 4868-9700
https://www.polizei.rlp.de/kontakt-zbs
https://www.polizei.rlp.de/zbs
15.11.2023

eferenčnega znaka: **25.3387243.6**

Pisno obvestilo
po 27. čl. Zakona o cestnem prometu[1]
o cestnoprometnem prekršku, storjenem v Nemčiji

Spoštovane dame in gospodje,

dne 06.10.2023, ab 14:07 v Münchweiler, Gem. Münchweiler a.d.R., B 10, km 1,100, Walmersbach FR Landau je bil z vozilom z registrsko številko LJ–61–TML (SLO) storjen sledeči cestnoprometni prekršek po § 24 Zakona o cestnem prometu (StVG):



Prekoračitev dovoljene zunaj zaprtega naselja za 6 km/h.
Dovoljena hitrost 100 km/h.
Ugotovljena hitrost (po tolerančnem odbitku) 106 km/h.

Prekršen cestnovarnostni predpis: § 41 Abs. 1 iVm Anlage 2, § 49 StVO; § 24 Abs. 1, 3 Nr. 5 StVG; 11.3.1 BKat

Dokazna sredstva: laserska meritev, fotografija, priča

Priča: PHK Scheuermann, PASt KL - ZVD

V kolikor je bil za ugotovitev prekrška uporabljen merilni aparat, se potrdi, da je bil kalibriran.

Kot imetnik prometnega dovoljenja za omenjeno vozilo ste pozvani kot priča, da nam sporočite ime voznika, ki je odgovoren za zgoraj omenjeni prekršek, in njegove/njene osebne podatke

Te podatke ste dolžni dati po 46. čl. 1. od. Zakona o prekrških (OWiG), v povezavi s 161a čl. 1. od. 1. stavek Zakona o kazenskem postopku (StPO).

Kot priča lahko odklonite odgovore samo na tista vprašanja, s katerimi bi spravili samega sebe – ali nekoga, ki po 52. čl. 1. od. StPO šteje med sorodnike – v nevarnost pregona zaradi kaznivega dejan-ja ali prekrška.

3102 / 3225_1 / 3

Zaslišanje prek spleta	Koda QR	Na voljo so naslednje možnosti	Številkatekoče garačuna
https://zbs-onlineportal.polizei.rlp.de/oaweb/07300000 Prijava: 25.3387243.6 Geslo: !MfpHy)t8qaT		✓ Vpogled v dokazne slike ✓ Navedba voznika/voznice ✓ Izjava o domnevnem kaznivem dejanju ✓ Dodajte priloge	

Polizeipräsidium Rheinpfalz, Zentrale Bußgelds[illegible]Maximili[illegible]raße [illegible]346 Speyer, Telefax: 06131 4868-9700, Telefon: 06232 / 8720-600,
Für Anfragen nutzen Sie bitte d[illegible]Kontaktfor[illegible]r auf uns[illegible]r Homepage: https://www.polizei.rlp.de/kontakt-zbs
Öffnungszeiten[illegible]o.-Do. 09[illegible]0 - 1[illegible] Uhr, Fr. 09:00 - 12:00 Uhr
Kontoinhaber: LOK Koblenz; IBA[illegible]ntne[illegible]g ggfl[illegible]m Fließtext; BIC: PBNKDEFFXXX

TRUE

Kraja identitete

Identity theft

Kaj je? / What is it?

- Do kraje identitete pride, ko nekdo ukrade naše osebne podatke ter le-te uporabi za nečedne namene.
- Obstajajo različne oblike kraje identitete, najpogostejša pa je finančna kraja.

- Zaščita pred krajo identitete je rastoča računalniška panoga, ki spremlja kreditna poročila posameznika, njegove finančne dejavnosti ...

- Identity theft occurs when someone steals your personal information and credentials to commit fraud.
- There are various forms of identity theft, but the most common is financial.

- Identity theft protection is a growing computer industry that keeps track of people's credit reports, financial activity …

Načini / Techniques

- Vdiranje v računalnike ali omrežja za dostop do podatkovnih zbirk in odvzem podatkov o strankah.
- Dostop do računalniških javnih evidenc.
- Uporaba zlonamernega programja za zbiranje informacij za okužbo računalnikov.
- Brskanje po spletnih straneh družabnih omrežij.
- Uporaba zavajajoče e-poštne ali SMS sporočil, preko katerih delimo podatke.
- Brskanje po smetnjaku in iskanje izpiskov bančnih računov in kreditnih kartic.
- ...

- Hack into computers or computer networks to access databases and steal customer information.
- Access computer-based public records.
- Use information-gathering malware to infect computers.
- Browse social networking sites.
- Use deceptive emails or text messages to gain our information.
- Sift through litter bins looking for bank account and credit card statements.
- …

V branje / To Read

Previdno! Kraja identitete vas lahko drago stane!

T. K. B., 13. april 2011,
MMC RTV Slovenija

https://www.rtvslo.si/slovenija/previdno-kraja-identitete-vas-lahko-drago-stane/255297

Dvignili kredit v Izoli za 20k

Podatke dobijo na straneh/aplikacijah, kjer se identificiramo (slikamo) z osebnim dokumentom. Tako kot na Revolut, N26, kripto marketi … ipd.

Zgodbe Slovencev, ki so jim ukradli identiteto

Nina Simič

13.03.2018 22:00

Moje finance

Si predstavljate, da bi, ne da bi vedeli, kupili štiri plazemske televizorje, odprli podjetje v Veliki Britaniji, všečkali žgečkljive slike na instagramu, pa bi vas pri tem zalotila žena, ali pa da bi kot direktor podjetja obljubljali nore popuste? To ni Hollywood, to so zgodbe Slovencev, ki so jim ukradli identiteto.

Scammers get your data on pages/applications where we identify ourselves (take a picture) with a personal document. Just like on Revolut, N26, crypto markets... etc.

Fizične nevarnosti

Physical hazards

Kraja opreme ali informacij / Theft of equipment or information,

Jenny Radcliffe - fizična testna vdiralka

- Vdor v banko v Hamburgu

Jenny Radcliffe - physical penetration tester

- Hamburg bank penetration

Internet stvari / Internet of things (IoT)

Home CCTV systems hacked and streamed online

Poglejmo nekaj kamer / Check some cameras

- http://insecam.org/en/bycountry/IT/

ICS

WHO WE ARE | BECOME A MEMBER | NEWS & EVENTS | ACTIVITIES | CONTACT US

NEWS

Home CCTV systems hacked and streamed online

It has been revealed that hackers are now spying on people through webcams, home CCTV and baby monitors, and streaming the footage online.

As many people fail to change the default passwords on the devices when they're bought, this leaves them vulnerable to attack and open to privacy breaches.

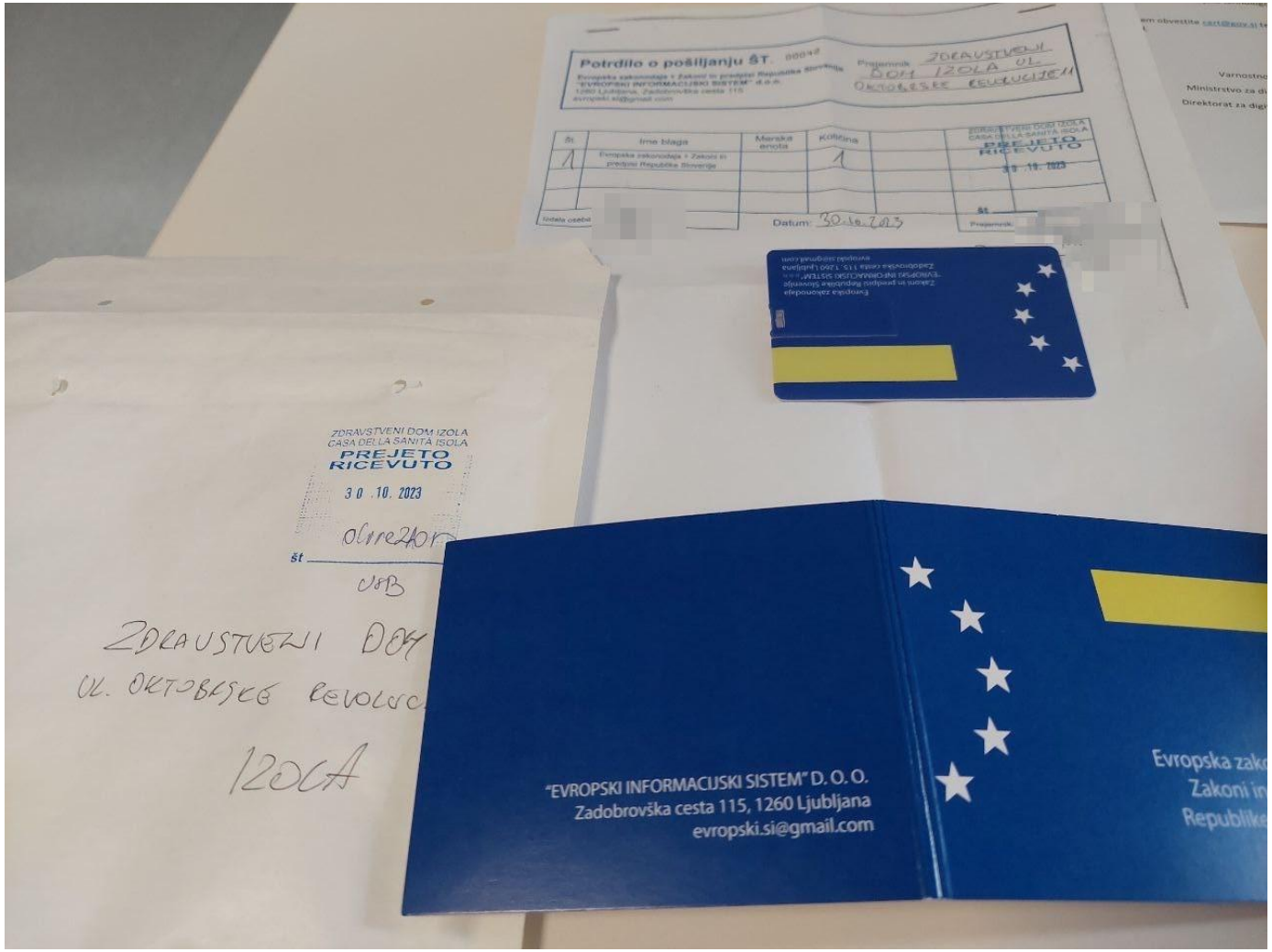
An investigation by the The Mail on Sunday newspaper showed security camera footage from inside homes, offices and shops across the UK being intercepted and broadcast live on the internet.

According to The Mail on Sunday, during a two-hour period last week investigators watched an internet website – available to anyone in the world – and saw footage from British locations, including:

- Babies in cots
- A schoolboy playing on his computer at home in North London
- Another boy asleep in bed
- The inside of a Surrey vicar's church changing room
- An elderly woman relaxing in an armchair
- Two men in a kitchen sharing a meal

https://www.ics.ie/news/view/1204

USB ključki / USB thumbdrives



OBVESTILO: dostava sumljivih USB ključkov

Spoštovani!

Obveščamo vas, da se je po podjetjih v Sloveniji pojavlja sumljiva distribucija USB ključkov. Napadalci delujejo na način, da želijo izvesti vročitev nenapovedanega blaga.

Opaženi primeri imajo naslednji način delovanja:

- dostavljavec se ne želi identificirati oz. se predstavi s prirejeno izkaznico;
- vztraja pri osebnem prevzemu pošiljke s strani vodstvenega kadra (direktor, predsednik uprave);
- lahko deluje agresivno, poskuša vstopiti tudi v območja z omejenim dostopom.

V sklopu preiskave je bilo ugotovljeno, da gre po vsej verjetnosti za način prevare, da napadalec želi finančno korist. Sumimo, da podjetje, ki dostavlja USB ključke, kasneje izstavi račun za naročilo blaga, v primeru neplačila le-tega pa tudi vloži izvršbo.

Po naših informacijah oseba, ki dostavi USB ključke, zahteva podpis obrazca, ki vsebuje elemente naročilnice (in ne zgolj vročilnice):
- ime podjetja ("Evropski informacijski sistem" d.o.o.);
- ime prejemnika;
- ime blaga (Evropska zakonodaja + Zakoni in predpisi Republike Slovenije);
- količina blaga.

Analiza omenjenih USB ključkov ni pokazala elementov, da njihova uporaba predstavlja varnostno tveganje npr. da vsebujejo zlonamerno kodo kot je virus ali črv. Vseeno odsvetujemo njihovo uporabo in v kolikor pridobite vzorec – ga prosimo posredujte za analizo na SIGOV-CERT.

V sklopu obvladovanja tovrstnih prevar predlagamo naslednji protokol:

- organi državne uprave, prosim da s to zadevo seznanite pristojno osebo za informacijsko varnost na vašem organu, ki nato naprej o zadevi seznani vse deležnike, še posebej službe, ki so najbolj izpostavljene tovrstnih prevaram,
- izpostavljene službe so tiste, ki sprejemajo stranke in prevzemajo tovrstno blago (npr. varnostniki, receptorji, tajništva, odnosi z javnostmi in informacijska tehnologija) – le-te prosim, da se po možnosti osebno obvesti.

V primeru prevzema pošiljke USB ključkov prosimo, da o tem obvestite cert@gov.si ter jim na varen način npr. po kurirju dostavite vzorec za forenzični pregled.

V naprej hvala za sodelovanje in lep pozdrav!

SOC MDP

Varnostno-operativni center

Ministrstvo za digitalno preobrazbo

Direktorat za digitalno infrastrukturo

Davčna ulica 1

SI-1000 Ljubljana

Slovenija

Najden ali prinešen! /
Found or Delivered!

Wifi napadi / Wifi attacks

Napad "zlobnega dvojčka" - hekerji ustvarijo lasten signal Wi-Fi, ki je videti kot signal, ki ga zagotavlja hotel, kavarna ali restavracija. Ko se prijavimo v ta nepooblaščeni Wi-Fi, lahko napadalec spremlja vse, kar počnemo na internetu, če komunikacija ni kriptirana.

Posledice so lahko kot v vsakem napadu:

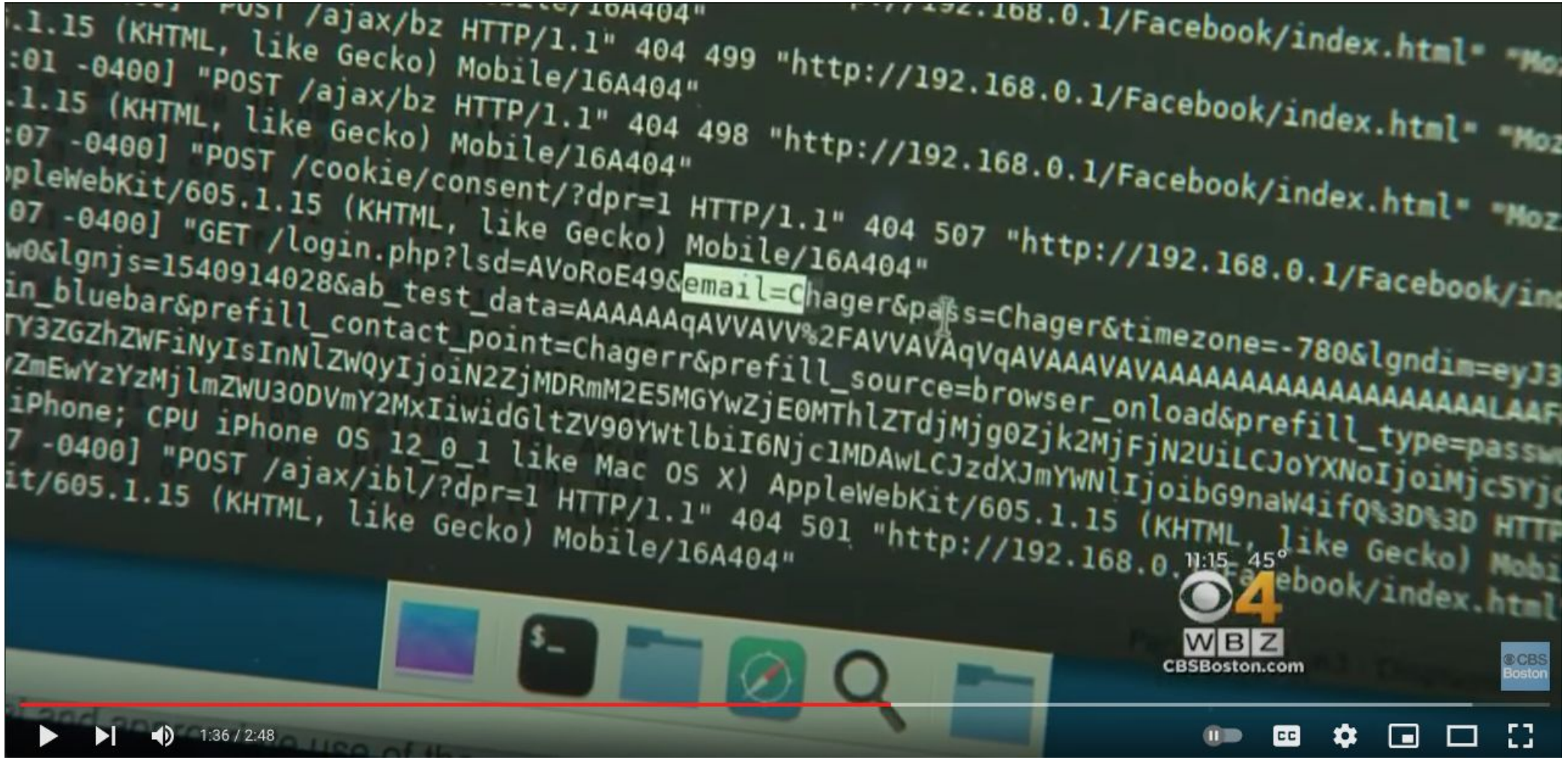
- ukradeni podatki o bančnih računih,
- ukradena uporabniška imena in gesla,
- okužba računalnika z zlonamerno programsko opremo,
- prisluškovanje našim dejavnostim na netu.

Evil Twin attack - hackers create their own Wi-Fi signal that looks like the one provided by a hotel, coffee shop or restaurant. When you log onto this unauthorized Wi-Fi, the cyberthief can monitor everything you do online, if communication is not encrypted.

Line in every attack this can result in:

- Stolen bank account information
- Stolen usernames and passwords
- Infecting your computer with malware
- Eavesdropping on your online activities

Hacker Demonstrates Security Risks Of Free Public Wi-Fi

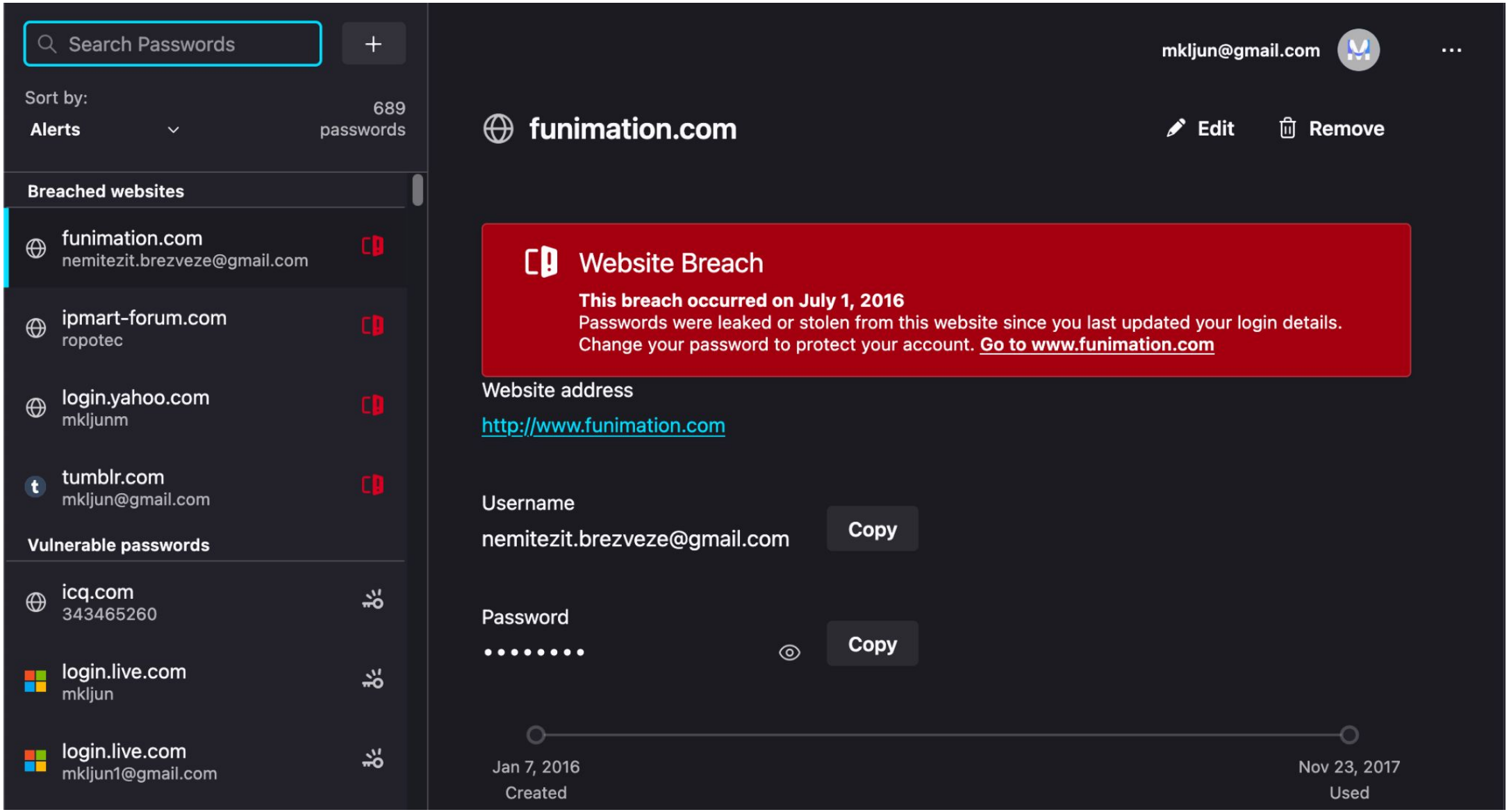


https://www.youtube.com/watch?v=1OVTmrXGHyU

Napotki / Guidance

- Raje kot javne WiFi uporabljamo telefon za dostop do interneta.
- Za prijavo v neznane storitve (prijava v Wifi, spletne strani, ipd.) uporabljamo e-naslove, ki se jih lahko zavrže.
- Uporabljamo VPN.
- Ne obiščemo strani, ki so občutljive narave, če smo na javnem Wifi
- Zamenjamo glavna gesla pred in po potovanju.
- Izklopimo samodejno priklapljanje na “prosta” ali neznana wi-fi omrežja.
- Ko obiščemo spletno stran se prepričamo, da uporablja HTTPS.
  - Enako pri e-pošti

- Use your phone as a hotspot to access internet.
- Use email addresses that can be discarded to log in unknown services (including free wifi, web services, etc.).
- Use a VPN
- Do not visit sites of a sensitive nature if on public Wifi.
- Change main passwords before and after travel.
- Turn off automatic connection to "free" or unknown wi-fi networks.
- When visiting a website make sure it uses HTTPS.
  - Same for email.


Search Passwords
Sort by:
Alerts
689 passwords
Breached websites
funimation.com
nemitezit.brezveze@gmail.com
ipmart-forum.com
ropotec
login.yahoo.com
mkljunm
tumblr.com
mkljun@gmail.com
Vulnerable passwords
icq.com
343465260
login.live.com
mkljun
login.live.com
mkljun1@gmail.com
mkljun@gmail.com
funimation.com
Edit
Remove
Website Breach
This breach occurred on July 1, 2016
Passwords were leaked or stolen from this website since you last updated your login details.
Change your password to protect your account. Go to www.funimation.com
Website address
http://www.funimation.com
Username
nemitezit.brezveze@gmail.com
Copy
Password
••••••••
Copy
Jan 7, 2016
Created
Nov 23, 2017
Used

Upravljalniki gesel

2fa, mfa, Passkey

Preverjanje znanja / Knowledge assessment

Napišite dokument o tem

- katere podatke in kam (zunanji medi, oblak) arhivirate na:
  - računalniku (datoteke, slike, e-pošta …),
  - telefonu (kontakti, slike …)
- kako upravljate z gesli,
  - na računalniku in telefonu
- koliko neznanih/neuporabljanih dodatkov imate v brskalniku,
- koliko neznanih/neuporabljanih aplikacij na računalniku in telefonu,
- ali v e-pošti samodejno dovolite, da se vam nalagajo slike,
- katerim aplikacijam na telefonu dovolite uporabljati GPS, kontakte, slike …?

- Imate druge naprave povezane v internet? Kako je z njihovo varnostjo?

- Razmislite in napišite kako boste določene stvari popravili. Kako skrbite za varnost in kje so še možnosti izboljšav.

Write a document about

- what information and where (external media, cloud) you are archiving or synchronising to:
  - your computer (files, images, emails ...),
  - phone (contacts, pictures ...),
- how do you manage passwords
  - on your computer and phone,
- how many unknown/unused add-ons you have on your browser,
- how many unknown/unused apps on your computer and phone,
- do you allow images to be uploaded in your emails automatically,
- which apps on your phone do you allow to use GPS, contacts, pictures, etc.,

- Do you have other devices connected to the internet? What about their security?

- Think and write how you will fix certain things. How do you take care of security and where are there room for improvement.

Hvala za pozornost / Thank you for your attention

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Vprašanja?

Matjaž Kljun
matjaz.kljun@upr.si
@_mkljun_

Questions?

Password managers

- Kakšno geslo je varno
- Kako lahko napademo gesla – en video od nekoga ki hacka gesla od ene baze ki so jo pobrali hackerji.
- Poglej kako FF opozarja katero stran so haknili ko imamo uporabniški račun na neki strani

- Vendor lock in – Prva zadeva, ki se je moramo zavedati pri uporabi vsake programske opreme

- Uvod v informacijsko varnost
- Gesla in dostopi
- Nevarnosti e-pošte in spleta
- Socialni inženiring in phishing
- Mobilna izpostavljenost
- Varnost podatkov in naprav
  - Koliko podatkov puščamo za sabo - > addons ki nas varujejo