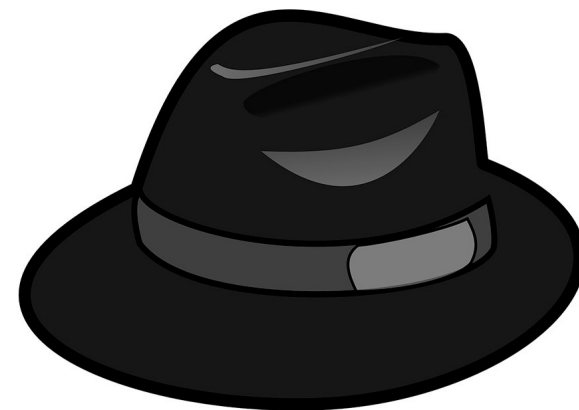


# Kiberkriminal

---



Magija, radovednost, zabava, posel in imunski sistem interneta

Matej Kovačič  
(CC) 2016

Tožilski izobraževalni dnevi | Portorož, 10. junij 2016

Kiberkriminal in  
kiberkriminalci

# Kiberkriminal

Kiberkriminal ni zgolj samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kiberkriminala v tem, da ta kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takem obsegu.

Kiberkriminal se od navadnega kriminala razlikuje še po treh pomembnih značilnostih:

- lahko je izveden na daljavo;
- identiteto osebe, ki kaznivo dejanje izvede je mogoče razmeroma enostavno zakriti ali ponarediti;
- sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kiberprostor, ni vedno mogoče, saj napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov, kar onemogoči ali vsaj oteži sledenje.

# »Hekanje«

Izraz hekanje se večinoma uporablja za *”kompleksno mešanico legalnih in nelegalnih aktivnosti, od legitimnega kreativnega programiranja, do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov”* (Taylor).

Najbolj pogosto se ga dojema kot sofisticirano ilegalno dejavnost.

Levy pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas.

- Prva generacija: izvira iz MIT, je v 50-tih in 60-tih letih prejšnjega stoletja razvila prve programske tehnike.
- Druga generacija: posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop računalniške tehnologije širšim množicam.
- Tretja generacija: vodilni razvijalci računalniških iger.
- Četrta generacija: osebe, ki na nedovoljene načine vstopajo v tuje računalnike.

Prvotni hekerji so bili predvsem ustvarjalni, zadnja generacija hekerjev pa naj bi bila že v večji ali manjši meri destruktivna.

# »Heker«

---

Izraz "heker" (ang. hacker) je prvi uporabil Joseph Weizenbaum leta 1976.

Popularno izraz danes opisuje posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme, kar hekerje uvršča v polje računalniške kriminalitete.

Po samodefiniciji se hekerji v hekerskem slovarju (Jargonfile) opisujejo kot *"osebe, ki uživajo v raziskovanju računalniških sistemov in iskanju novih načinov njihove uporabe; osebe, ki navdušeno (celo obsedeno) programirajo ... osebe, ki uživajo v intelektualnih izzivih v aktivnem premagovanju in zaobhajanju omejitev"*.

# »Heker«

---

Eden izmed slovenskih hekerjev, je v pogovoru povedal: *“Ne razumem zakaj ljudje izraz hekanje vedno povezujejo z vdiranjem in asocialnimi tipi. Ta termin ne pomeni nič drugega kot da si zelo dober v neki stvari, pa naj si bo to računalništvo ali kaj drugega. sem menja da je to bolj način razmišljanja, želja po znanju, izziv...”*.

Bruce Schneier hekanje razume kot **stanje duha**, pri čemer način razmišljanja povsem ločuje od namena uporabe le-tega: *“Heker je nekdo, ki razmišlja izven okvirov. Je nekdo, ki opusti običajno modrost in namesto tega naredi nekaj drugega. Je nekdo, ki gleda na rob in se sprašuje kaj je na oni strani. Je nekdo, ki vidi niz pravil in se sprašuje, kaj se zgodi, če jim ne slediš. Heker je nekdo, ki eksperimentira z omejitvami sistema zaradi intelektualne radovednosti. ...”*

# »Heker«

---

*“Računalniki so odlično igrišče za hekerje. Računalniki in računalniška omrežja so ogromni zakladi skrivnega znanja. Internet je brezmejna pokrajina neodkritih informacij. Več kot veš, več lahko storiš. ... To je varnostno hekanje: vdiranje v sisteme s pomočjo razmišljanja na drug način. ‘Heker’ je stanje duha in nabor veščin; kako to uporabiš, pa je drugo vprašanje.” (Bruce Schneier).*

Richard Pryce, »Datastream Cowboy«, ki je leta 1994 v starosti 16 let vdrl v več visoko zaupnih ameriških vojaških sistemov: *“Nekateri so gledali televizijo po šest ur na dan, jaz pa sem hekal računalnike.”*

# Vrste »hekerjev«

**Beli hekerji** ali **etični hekerji** svoje znanje uporabljajo za zakonito preverjanje varnosti sistemov.

**Črni hekerji** hekersko znanje zlorablajo za slabe namene, predvsem nezakonito vdiranje v računalnike s pridobitnimi nameni ter za povzročanje škode.

**Krekerji** (ang. *cracker*) so posamezniki, ki se ukvarjajo s tim. reverznim inženiringom programske opreme, predvsem z namenom razbijanja zaščite programov prek kopiranjem.

**Skriptarji** (ang. *script kiddies*) so osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi. Motivi so večinoma samodokazovanje, zabava ali vandalizem.

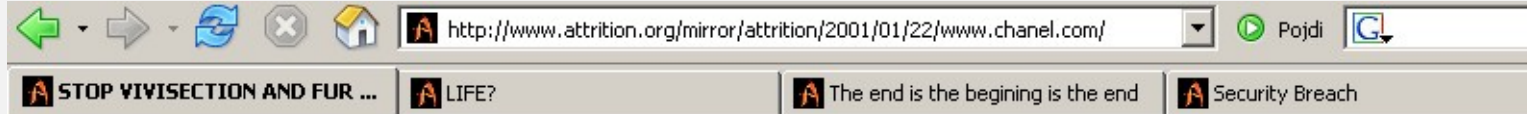


# Haktivizem

Obstajata dve definiciji "haktivizma":

- nudenje informacijske (tehnične) podpore političnim aktivistom (praviloma povsem zakonito);
- nelegalno politično delovanje na internetu. Denningova ga definira kot povezavo med aktivizmom (pri katerem gre za uporabo interneta v namene širjenja informacij, debatiranje, načrtovanje in koordinacijo političnih in družbeno angažiranih aktivnosti, itd., skratka legitimno uporabo, ki ni dekstruktivna) in hekanjem. Po njeni definiciji je haktivizem sicer v osnovi **dejavnost povzročanja motenj**, ne pa tudi resni škodi.

# Haktivizem



## Pain for Profit

**The fur ads we see in magazines and commercials portray fur coats as a symbol of elegance. But these ads fail to show how the original owners of these coats met their gruesome deaths.**

**Approximately 3.5 million furbearing animals - raccoons, coyotes, bobcats, lynxes, opossums, nutria, beavers, muskrats, otters, and others - are killed each year by trappers in the United States. Another 2.7 million animals are raised on fur "farms." Despite the fur industry's attempts to downplay the role of trapping in fur "production," it is estimated that more than half of all fur garments come from trapped animals.**



## Jaws and Paws



# Kibekriminal in država

---

## **Informacijsko-obveščevalni napadi:**

- ZDA (NSA, industrijska špijonaža);
- Stuxnet (napad na iranski jedrski program);
- Severna Koreja (Mirrim College);
- Kitajska (sile kibernetike varnosti, APT napadi na zahodne države, napadi na politične aktiviste).

## **Kiberterorizem:**

- uporaba hekerskih tehnik v aktivistične a destruktivne namene (povzročanje ekonomske škode ali ogrožanje življenja ljudi).
- 911 worm, računalniški virus, ki je po uspešni okužbi skušal z modemom klicati na številko za klic v sili;
- napad na pristaniške v Houstonu leta 2003;
- pogojno: napad SQL Slammerja na jedrsko elektrarno v Ohio leta 2003.

# Kibekriminal in država

---

## **Kibervojna:**

- DDoS napadi na Gruzijske strežnike julija 2008 s strani Rusije;
- v Ukrajini so leta 2014 ruske sile za nekaj časa prevzele nadzor nad več središči s telekomunikacijsko opremo - s tem naj bi preprečili uporabo mobilnih telefonov članov parlamenta in drugim pomembnim posameznikom;
- decembra 2015 je 80.000 gospodinjstev na zahodu Ukrajine ostalo brez električne energije, saj so napadalci izključili razdelilne transformatorske postaje.

Magija

# Kiberkriminal kot magija



# Kiberkriminal kot magija





# Kiberkriminal kot magija



Radovednost in zabava

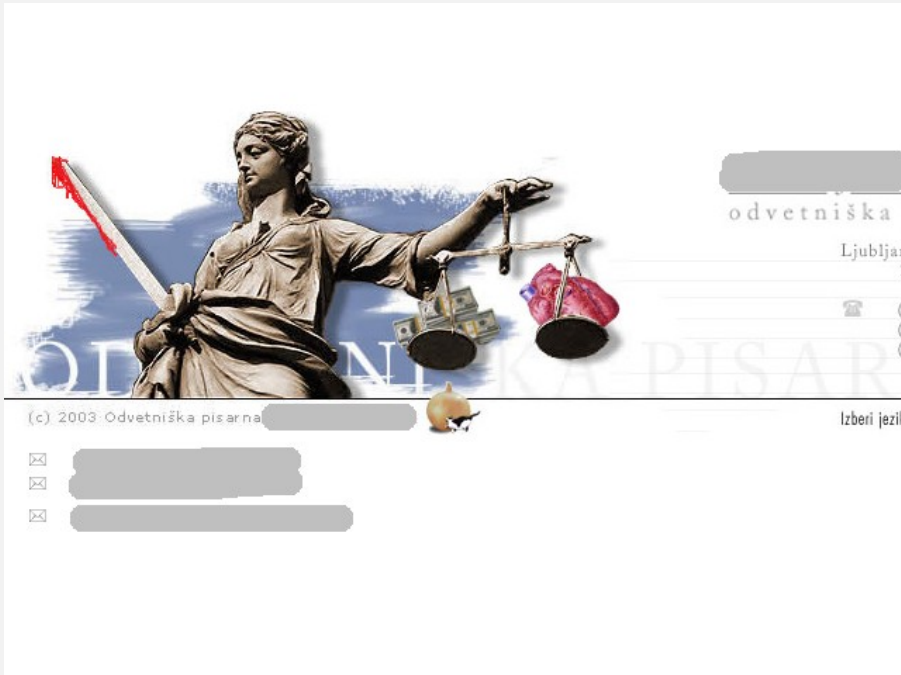
# Kiberkriminal kot zabava

---



Hekerski napad na tiskalnik.

# Kiberkriminal kot zabava



Razobličena spletna stran  
odvetniške pisarne.

Slovensko satanistično gibanje

Pavlihove domače strani na internetu: [Prva stran](#) | [Aktualno](#) | [Povezave](#)

## Slovensko satanistično gibanje se predstavi

### NAMEN

- *Slovensko biblično gibanje* si prizadeva po besedah 2. vatikanskega cerkvenega zbora v dogmatični konstituciji *O Božjem razodetju* (22), da bi bil "na široko odprt dostop do Svetega pisma".
- Zato hočemo *Sveto pismo* vsem ljudem predstaviti, ponuditi, posebej vernim pa pomagati, da ga bodo mogli zavestno sprejemati kot Božjo besedo znotraj živga izročila celotne Cerkve.

### NALOGE

- povezovati svetopisemske ali biblične skupine,
- spodbujati nastajanje novih in jim pomagati pri delu
- prirejati biblične tečaje, razstave, predavanja

Razobličenje spletne strani  
rimokatoliške cerkve.


# Kiberkriminal kot zabava



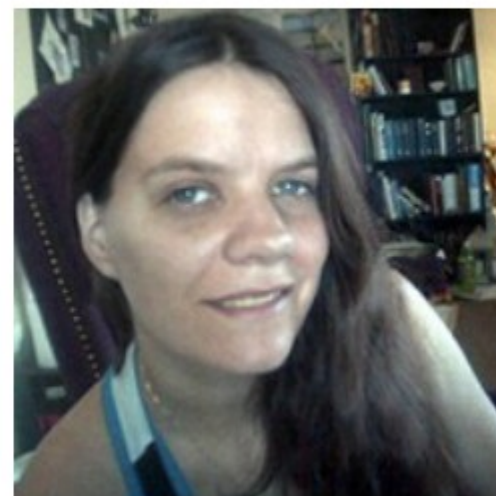
Hekerski napad na prometne znake.

# Kiberkriminal kot zabava

## Hackers embed flashing animations on epilepsy support forum

By Darren Murph  posted March 29th 2008 8:50PM

Shortly after hearing a [sad tale](#) of a 7-year old cancer patient having his medication and PSP stolen whilst en route to treatment comes yet another story of the world's meanest [preying](#) on the innocent. This go 'round, a group of griefers (which appear to be members of Anonymous) managed to invade a support forum established by the nonprofit Epilepsy Foundation and use JavaScript code and messages littered with flashing animations to effectively assault dozens of visitors who suffer from the disorder. The Foundation managed to catch wind of the problem within 12 hours of the attack, and while the boards were closed down temporarily to purge it of offending messages, many readers (such as RyAnne Fultz, pictured) experienced headaches and seizures before rescue arrived. Let's just say we sincerely hope the culprits get what's comin' to 'em.



Hekerski napad na bolnike z epilepsijo.

# Kiberkriminal kot zabava

Si.mobil d.d. - Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

http://www.simobil.si/sl/search.cp2?q=<h3>Dimitrij+Rupel+postal+svetovalec+ unauthenticated

Si.mobil Vodafone live! Orto Prodajna mesta Vprašajte nas Registrirajte se English


zasebni uporabnik predplačnik poslovni uporabnik

<h3>Dimitrij Rupel postal IŠČI

TELEFONI IN NAPRAVE PAKETI STORITVE AKCIJE TUJINA POMOČ IN INFORMACIJE VODAFONE LIVE! SI.MOST

Iskali ste:

**Dimitrij Rupel postal svetovalec uprave Simobila**



Z današnjim dnem dr. Dimitrij Rupel postaja svetovalec Simobila za področje zunanje naročniške politike.

:-)

Število vseh rezultatov: 3  
Prikazani rezultati: 1 - 3  
Stran: 1

**Rezultati iskanja**

**IT specialist v CRM skupini, zadolžen za DMS področje (m/ž)**

Želite razvijati svojo profesionalno pot pri enem najuglednejših in najboljših slovenskih zaposlovalcev? Podjetje Si.mobil d.d. je zaupanja vredno podjetje, kjer so ljudje na prvem mestu. Zaposleni v Si.mobilu so visoko usposobljeni profesionalci, ki so zaljubljeni v svoje delo in v komunikacijo. Prek vpetosti v globalne povezave pa zaposleni lahko pridobivajo tudi mednarodno znanje in bogate izkušnje.

**Novi direktor prodaje**

Novi direktor prodaje v družbi Si.mobil je s 3. januarjem 2007 postal Gregor Banič.

**Nastavitve zunanjega odjemalca**

Končano Apache 1337 Anonimizacija izključena

Programi Mesta Sistem [Pr... Si.... [Se... TO... \*go... SVN pet 16. jan, 10:28

Prvi april.

# Kiberkriminal kot radovednost

prevzem.php5 (Predmet application/pdf) - Mozilla Firefox

Datoteka Urjanje Pogled Pojdi Zaznamki Orodja Pomoč

http://lgl.esiti.com/si/prevzem.php?id=24400

Firefox Help Firefox Support Plug-in FAQ

LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA prevzem.php5 (Predmet application...

163%

LGL - LUTKOVNO GLEDALIŠČE LJUBLJANA

potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu / potrdilo o nakupu

Lutkovno gledališče Ljubljana

**VILA MALINA, izven**  
**LGL-Veliki oder, 11. januar 2007 ob 17:00**

segment	vrsta	Številka	količina	cena
Veliki oder	6	7b	1	3,24 EUR
Veliki oder	6	7a	1	3,24 EUR
Veliki oder	6	6b	1	3,24 EUR
Veliki oder	6	6a	1	3,24 EUR
<b>skupaj</b>				<b>12,96 EUR</b> <b>3.105,73 SIT</b>

**številka potrdila o nakupu**  
010-000-107-788-454-883-142760

Vaše potrdilo o nakupu zamenjajte za vstopnice na blagajni dvorane.

V primeru, da prireditev odpade, lahko potrdilo o nakupu zamenjate na blagajni organizatorja za drugo prireditev ali pa vam organizator vrne denar, ki ga morate prevzeti v enem mesecu na njegovi blagajni. Za vse dodatne informacije nam pišite na elektronski naslov info@lgl.si.

Končano Anonimizacija izključena

Start prevze... The GIMP Layers, ... Untitled... LGL - LU... http://l... 10:19

»Igranje« z URL naslovi...



# Kiberkriminal kot radovednost

The screenshot shows a Mozilla Firefox browser window displaying the Sparkasse website. The main window shows the user's account information, including the user name, contact number (01/583 6666), and the Sparkasse logo. A smaller window is overlaid on top, showing the details of a MasterCard credit card account. The URL in the address bar of the smaller window is highlighted with a yellow circle, showing a series of blacked-out parameters: `https://netstik.sparkasse.si/eb/kartica.asp?x= [redacted] &y= [redacted] &z= [redacted] &q= [redacted] &k= [redacted] &s= [redacted]`. The card details include the user name, card type (primary card on credit account), card number (5209 [redacted]), validity date ([redacted]-12), card name ([redacted]), issue date ([redacted] 2006), and monthly limits for purchases and cash withdrawals.

MasterCard kartični račun: [redacted]	
Uporabnik:	[redacted] n
Vrsta kartice:	primarna kartica na kartičnem računu
Številka kartice:	5209 [redacted]
Veljavnost do:	[redacted]-12
Naziv na kartici:	[redacted]
Datum otvoritve kartice:	[redacted] 2006
Datum blokacije:	/
Mesečni limit (nakup):	[redacted] EUR
Mesečni limit (dvig gotovine):	[redacted] EUR

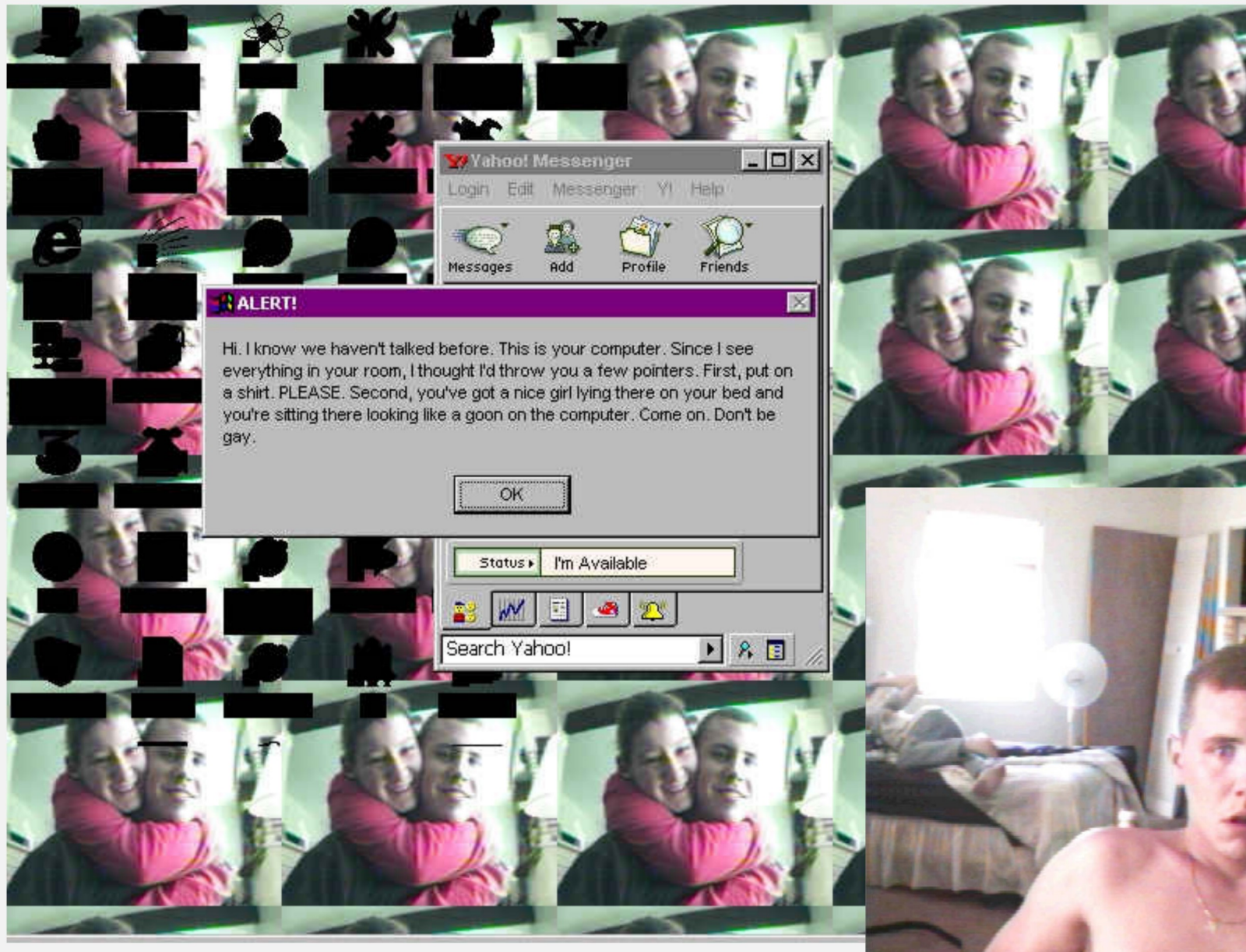
**Za preklic kartice, prosimo, pokličite 01/583 41 83.**

© 2002-2009, BANKA SPARKASSE d.d. Pravica do napak in sprememb pridržana.

»Igranje« z URL naslovi v spletni banki.

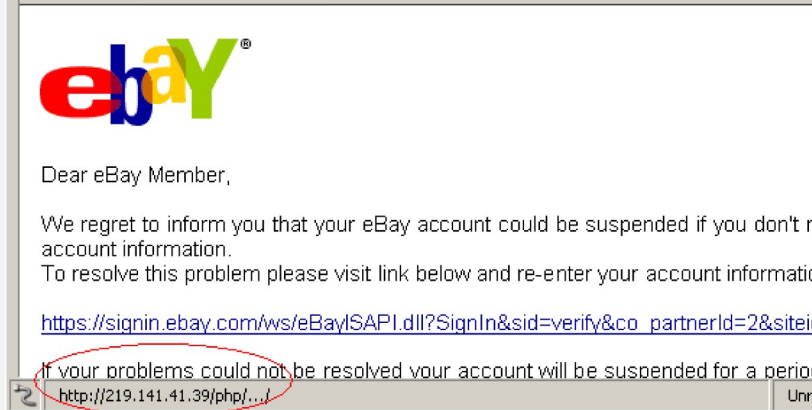
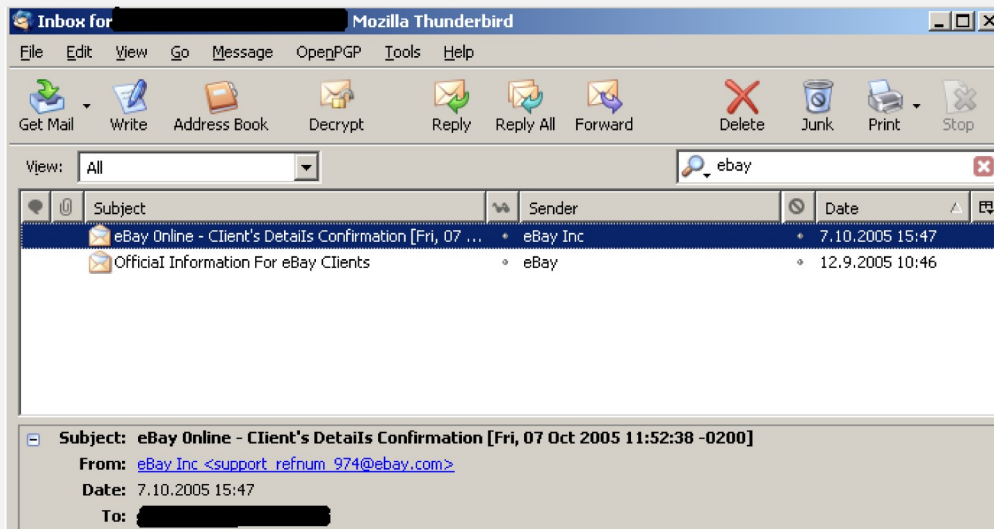
Pose1

# Kiberkriminal kot posel



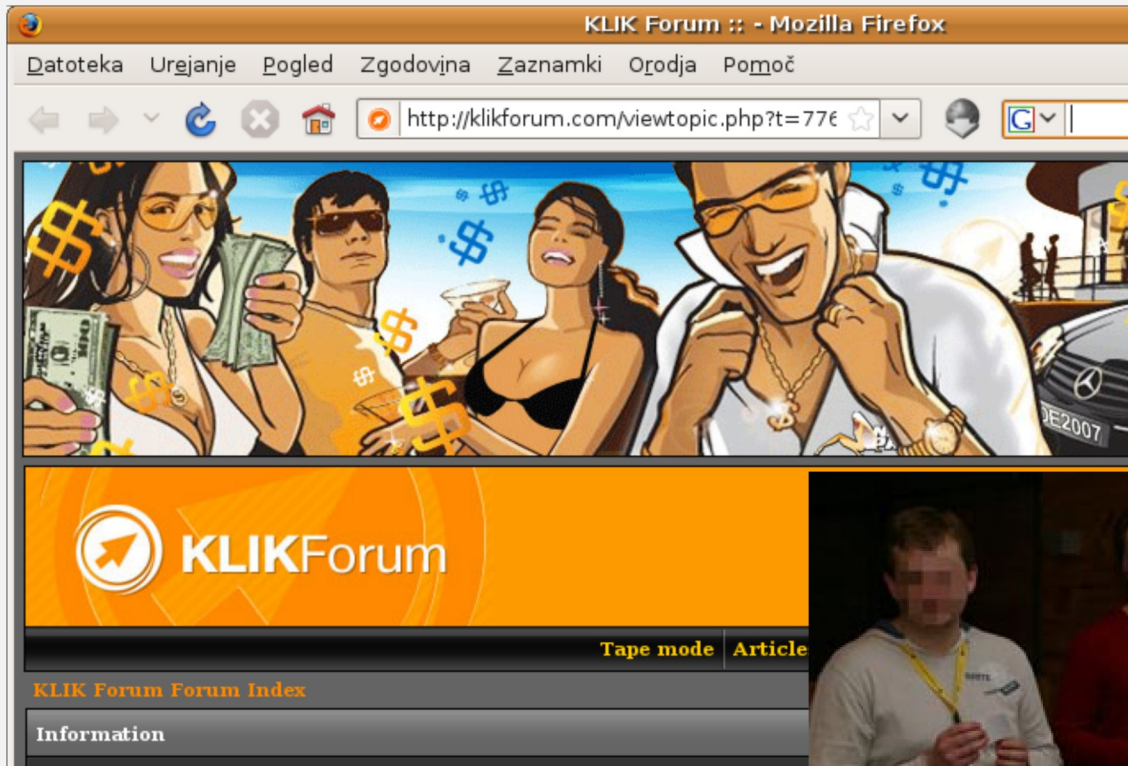
Izsiljevanje...

# Kiberkriminal kot posel



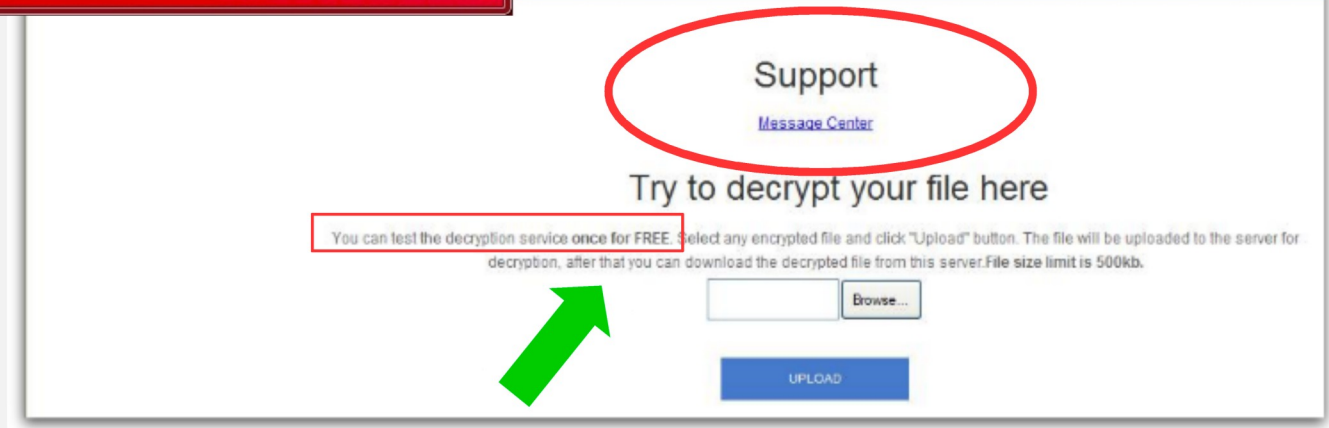
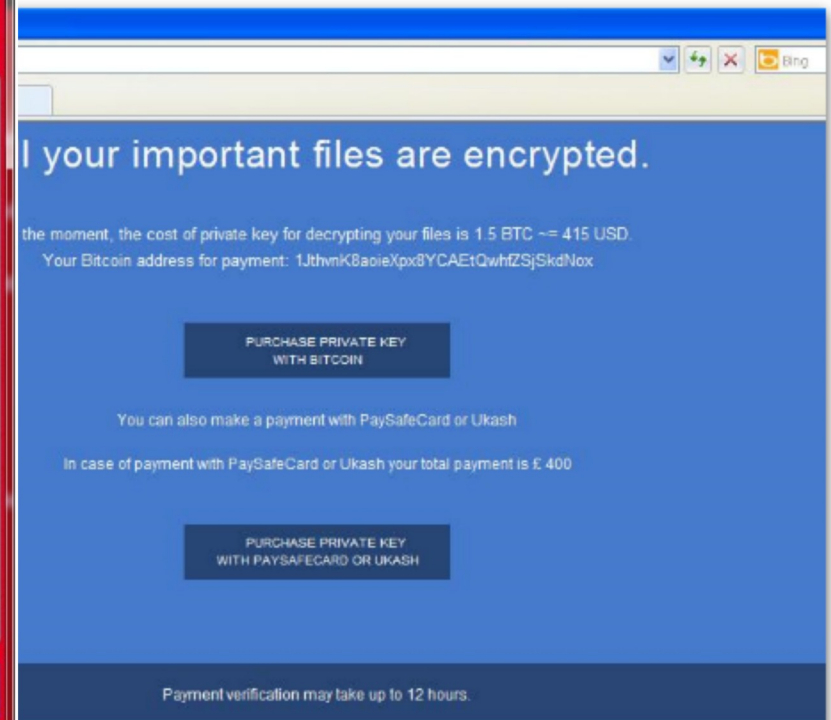
Ribarjenje (phishing), »pump-and-dump«.

# Kiberkriminal kot posel



»Podjetje« KlikTeam, s 95 zaposlenimi.

# Kiberkriminal kot posel



Izsiljevalski virusi.

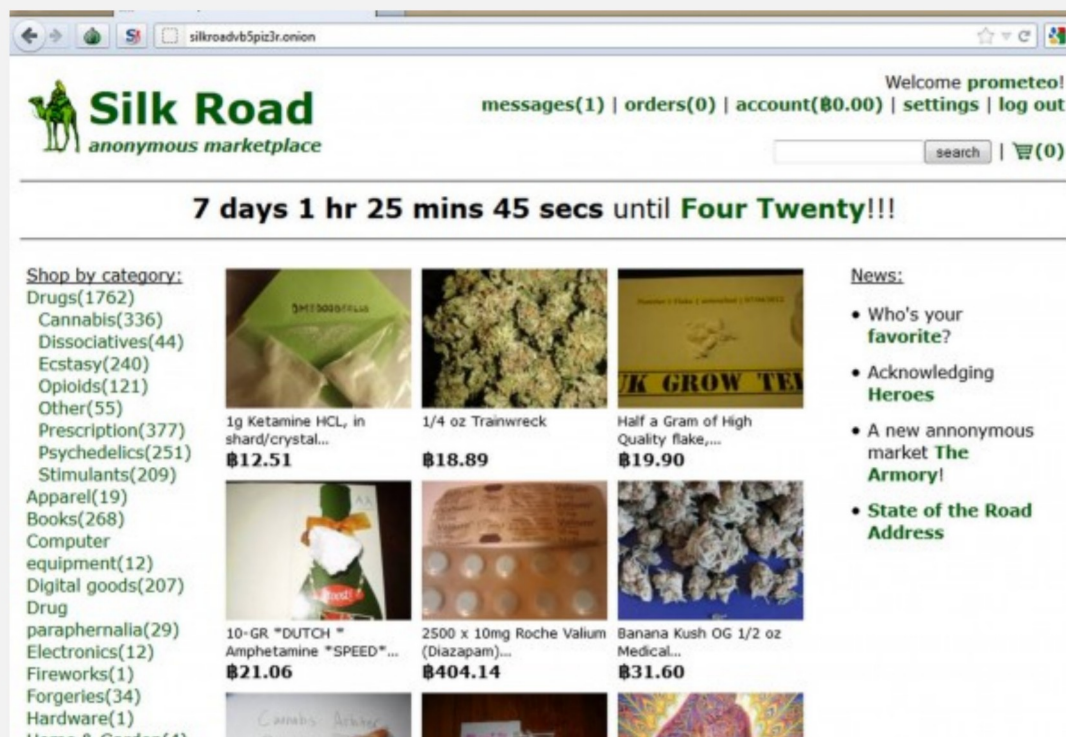
# Kiberkriminal kot posel

- Leta 2009 je Wikileaks objavil anonimno pismo osebe, ki je 10 let delala v poslu z otroško pornografijo. Oseba je v pismu razkrila nekaj podatkov o tej »industriji«:
  - **Mesečni promet** enega izmed »podjetij«: **1,8 milijona USD** (na letni ravni okrog 21,6 milijona USD) - neobdavčeno.
  - Po odbitju vseh stroškov (za fotografе, iskalce gradiva po forumih, modele, spamerje, hekerje, itd.) **lastniku ostane okrog pol milijona USD - mesečno.**
  - **Problem marketinga**: odkrito oglaševanje ni mogoče. Marketing se zato izvaja s pomočjo spama (in preko vdorov na pornografske in druge spletne strani). Po navedbah anonimnega avtorja naj bi spamerji pobrali okrog 20 odstotkov vsega dobička.
  - **Skrivanje vsebine**: večina vsebin naj bi se nahajala na nemških strežnikih na šifriranih diskih. Strežniki niso neposredno dostopni, pač pa so dostopni preko posebnih posredniških strežnikov (tim. *proxy*), le-ti pa preko Fast Flux domen.
  - Ruske kriminalne združbe so namesto spletnih vsebin začele ponujati **virtualne stroje** s prednaloženo ilegalno vsebino ter celo **RDP dostop do strežnikov.**

Vir: [https://wikileaks.org/wiki/My\\_life\\_in\\_child\\_porn](https://wikileaks.org/wiki/My_life_in_child_porn)

# Kiberkriminal kot posel

- Spletišče *Silk Road* je od 6. februarja 2011 do 23. julija 2013 ustvarilo 1,2 milijarde USD prometa in 79,8 milijonov USD (neobdavčenega!) dobička.



- Silk Road je omogočal ocenjevanje prodajalcev, skrbel za anonimnost prodajalcev in kupcev, omogočal anonimno plačevanje z BitCoini, izvajali so tudi teste čistosti drog...



# Kiberkriminal kot posel

- Po zaprtju Silk Road s strani FBI se je pojavilo še več podobnih strani. *Atlantis* in *Project Black Flag* sta kmalu po ustanovitvi ugasnila ter izginila z denarjem svojih strank.



Atlantis je ubral precej inovativen način oglaševanja  
[[https://youtu.be/uD1y0kK\\_aH8](https://youtu.be/uD1y0kK_aH8)]

Imunski sistem

# Kiberkriminal kot imunski sistem

---

Na računalniška omrežja bi morda morali gledati kot na nekakšne organizme z imunskimi sistemi, za katere je značilno, da jih napadi bolezniki krepijo.

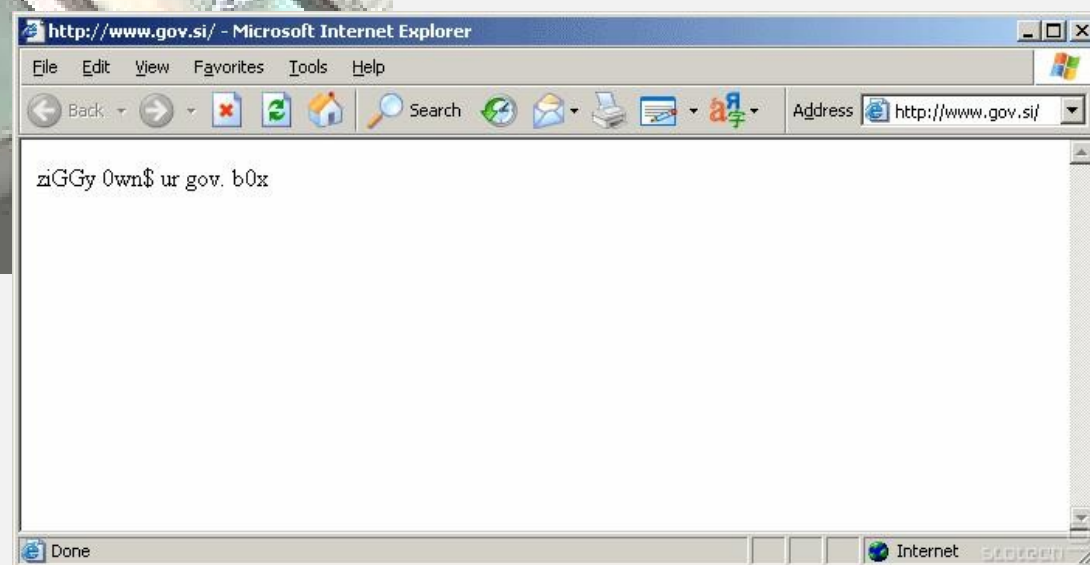
Odkrite in izrabljene varnostne ranljivosti imajo za posledico reakcijo - odpravo teh ranljivosti s strani proizvajalcev ter povišano varnostno kulturo uporabnikov.

To na nek način krepil "imunski sistem" interneta in zmanjšuje verjetnost, da bi nekoč prišlo do katastrofalnega napada, ki bi lahko ogrozil nacionalno ali celo globalno varnost.

Kiberkriminal tako na nek način prinaša tudi koristi.

(Harvard Law Review, 2006: 2442)

# »Kiberkriminalal« kot imunski sistem





# »Kiberkriminal« kot imunski sistem

The image shows a Mozilla Firefox browser window with a security warning for the website **erisk.sigov.si**. The warning message reads: "Uporabnik: **Matej Kovačič** / **KOMISIJA ZA PREPREČEVANJE KORUPCIJE** Četrtek, 10. marec, 2011 / [redacted] O aplikaciji | Omogoči | Odiava". A red box highlights the text "e-RISK DUNZ" in the top left corner of the browser's address bar area.

Below the main browser window, there are several overlapping windows and dialog boxes:

- A "Podatki o strani" (Page Info) window for **https://erisk.sigov.si/erisk/index.faces** showing security icons for Splošno, Večpredstavnost, Dovoljenja, and Varnost.
- A "Piškoti" (Cookies) dialog box for **sigov.si** showing a list of cookies for **erisk.sigov.si** with names **JSESSIONID**, **LtpaToken**, and **LtpaToken2**. The details for **JSESSIONID** are visible: Ime: JSESSIONID, Vsebina: 0000IXLMzITJWUZUQTVL\_er6b:C075CB88E4DE844900001B00, Gostitelj: erisk.sigov.si, Pot: /, Poslan za: Vse povezave, Preteče: na koncu seje. A red arrow points to the "Zapri" (Close) button.
- A "Podatki o strani" window for **https://erisk.sigov.si/erisk/logoff** showing a security warning: "Ta spletna stran ne vsebuje podatkov o lastništvu. state-institutions". A red arrow points to the "Preglej digitalno potrdilo" (View digital certificate) button.
- A second "Piškoti" dialog box for **sigov.si** is also visible, identical to the one above, with a red arrow pointing to the "Zapri" button.

# »Kiberkriminal« kot imunski sistem

## GSM modul za odpiranje garažnih ali vhodnih vrat

**Ponujamo vam uporabno napravo, ki z enostavnim telefonskim klicem odpre ali zapre avtomatizirana garažna ali vhodna vrata.**

GSM modul je naprava, katero lahko avtorizirani uporabnik pokliče z namenom, da s hitrim klicem odpre ali zapre avtomatizirana vrata. Naprava prepozna največ pet določenih telefonskih števil, iz katerih se lahko na GSM modul pokliče in se s takim klicem sproži odprtje ali zaprtje vrat.

IKU d.o.o. vam nudi:

- o dobavo paketa z navodili za uporabo,
- o montažo na dogovorjena mesta (pokličite nas in poslali vam bomo ponudbo).

Uporaba GSM modula za odpiranje vrat:

na avtomatizirana garažna, vhodna ali druga vrata se namesti GSM modul, v katerega se zapiše do pet telefonskih (mobilnih) števil, s katerimi je možno s hitrim telefonskim klicem omenjena vrata odpreti ali zapreti. S tem načinom odpade uporaba daljinskih upravljalnikov oziroma dodatnih naprav in aparatov, ker predpostavljamo, da je mobilni telefon že »obvezna oprema« vseh ljudi.



# »Kiberkriminal« kot imunski sistem





# »Kiberkriminalal« kot imunski sistem



RTSP/1.0 200 OK  
CSeq: 1  
Server: Hipcam RealServer/V1.0  
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, SET\_PARAMETER, GET\_PARAMETER



Vprašanja?

<https://pravokator.si>