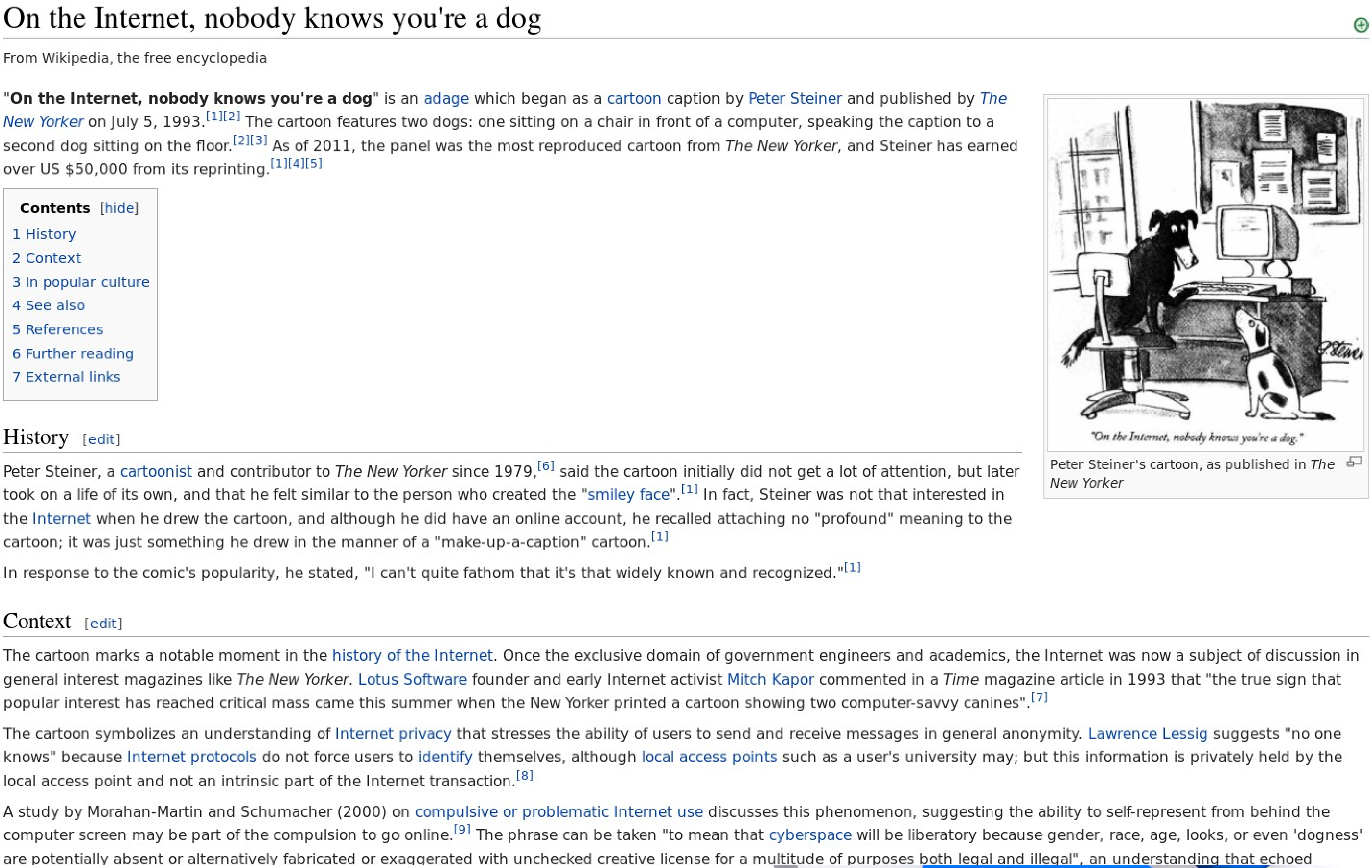
Primjena elektroničkih računala

Sigurnost na internetu

Izv. prof. dr. sc. Hrvoje Kalinić

Sigurnost na internetu

"On the Internet, nobody knows you're a dog."



On the Internet, nobody knows you're a dog

From Wikipedia, the free encyclopedia

"**On the Internet, nobody knows you're a dog**" is an adage which began as a cartoon caption by Peter Steiner and published by *The New Yorker* on July 5, 1993.[1][2] The cartoon features two dogs: one sitting on a chair in front of a computer, speaking the caption to a second dog sitting on the floor.[2][3] As of 2011, the panel was the most reproduced cartoon from *The New Yorker*, and Steiner has earned over US $50,000 from its reprinting.[1][4][5]

Peter Steiner's cartoon, as published in *The New Yorker*

Contents [hide]

History [edit]

Peter Steiner, a cartoonist and contributor to *The New Yorker* since 1979,[6] said the cartoon initially did not get a lot of attention, but later took on a life of its own, and that he felt similar to the person who created the "smiley face".[1] In fact, Steiner was not that interested in the Internet when he drew the cartoon, and although he did have an online account, he recalled attaching no "profound" meaning to the cartoon; it was just something he drew in the manner of a "make-up-a-caption" cartoon.[1]

In response to the comic's popularity, he stated, "I can't quite fathom that it's that widely known and recognized."[1]

Context [edit]

The cartoon marks a notable moment in the history of the Internet. Once the exclusive domain of government engineers and academics, the Internet was now a subject of discussion in general interest magazines like *The New Yorker*. Lotus Software founder and early Internet activist Mitch Kapor commented in a *Time* magazine article in 1993 that "the true sign that popular interest has reached critical mass came this summer when the New Yorker printed a cartoon showing two computer-savvy canines".[7]

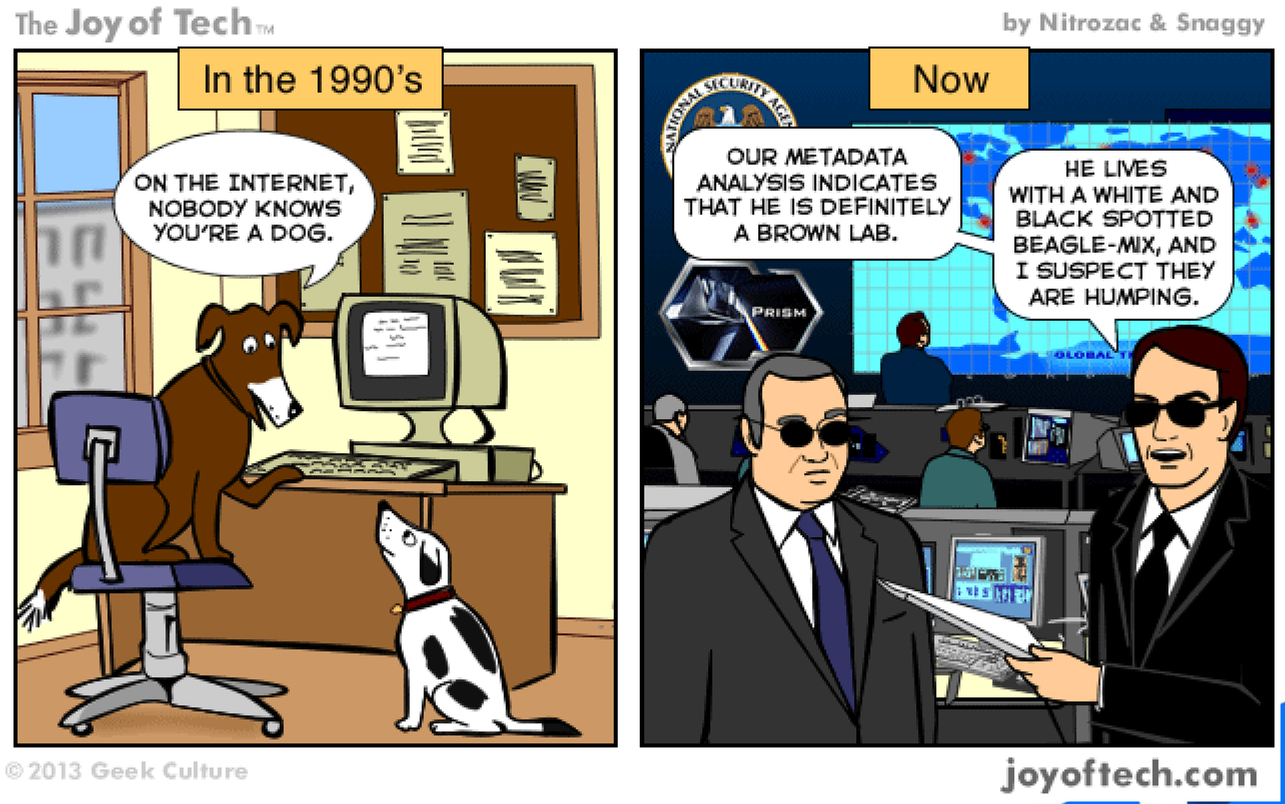
The cartoon symbolizes an understanding of Internet privacy that stresses the ability of users to send and receive messages in general anonymity. Lawrence Lessig suggests "no one knows" because Internet protocols do not force users to identify themselves, although local access points such as a user's university may; but this information is privately held by the local access point and not an intrinsic part of the Internet transaction.[8]

A study by Morahan-Martin and Schumacher (2000) on compulsive or problematic Internet use discusses this phenomenon, suggesting the ability to self-represent from behind the computer screen may be part of the compulsion to go online.[9] The phrase can be taken "to mean that cyberspace will be liberatory because gender, race, age, looks, or even 'dogness' are potentially absent or alternatively fabricated or exaggerated with unchecked creative license for a multitude of purposes both legal and illegal", an understanding that echoed

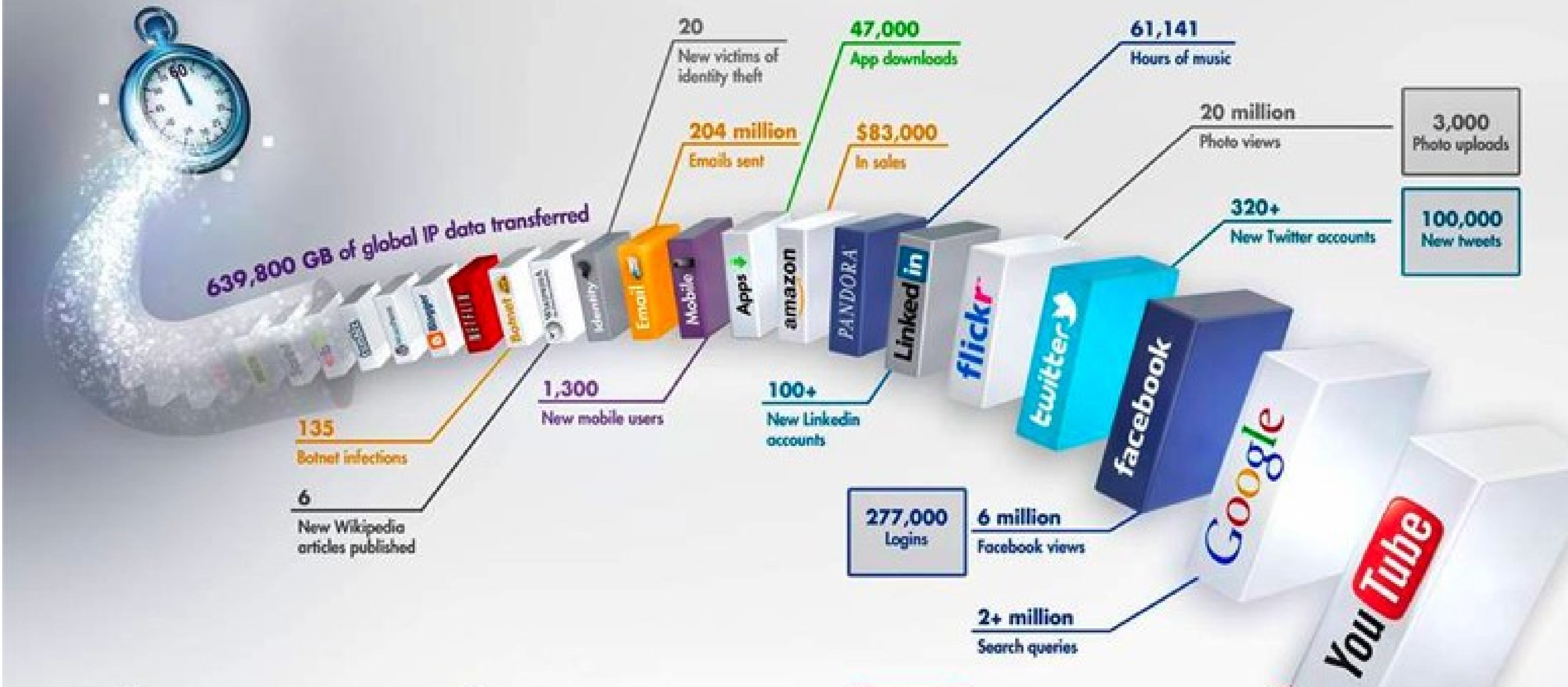
Sigurnost na internetu

- Adresa elektroničke pošte
  - ime.prezime@yahoo.com
  - ccorax83@yahoo.com

Sigurnost na internetu


The Joy of Tech™
by Nitrozac & Snaggy
In the 1990's
ON THE INTERNET, NOBODY KNOWS YOU'RE A DOG.
Now
NATIONAL SECURITY AGENCY
OUR METADATA ANALYSIS INDICATES THAT HE IS DEFINITELY A BROWN LAB.
PRISM
HE LIVES WITH A WHITE AND BLACK SPOTTED BEAGLE-MIX, AND I SUSPECT THEY ARE HUMPING.
GLOBAL
© 2013 Geek Culture
joyoftech.com

What Happens in an **Internet Minute?**



639,800 GB of global IP data transferred

20
New victims of identity theft

204 million
Emails sent

47,000
App downloads

$83,000
In sales

61,141
Hours of music

20 million
Photo views

3,000
Photo uploads

320+
New Twitter accounts

100,000
New tweets

135
Botnet infections

6
New Wikipedia articles published

1,300
New mobile users

100+
New Linkedin accounts

277,000
Logins

6 million
Facebook views

2+ million
Search queries

30
Hours of video uploaded

1.3 million
Video views

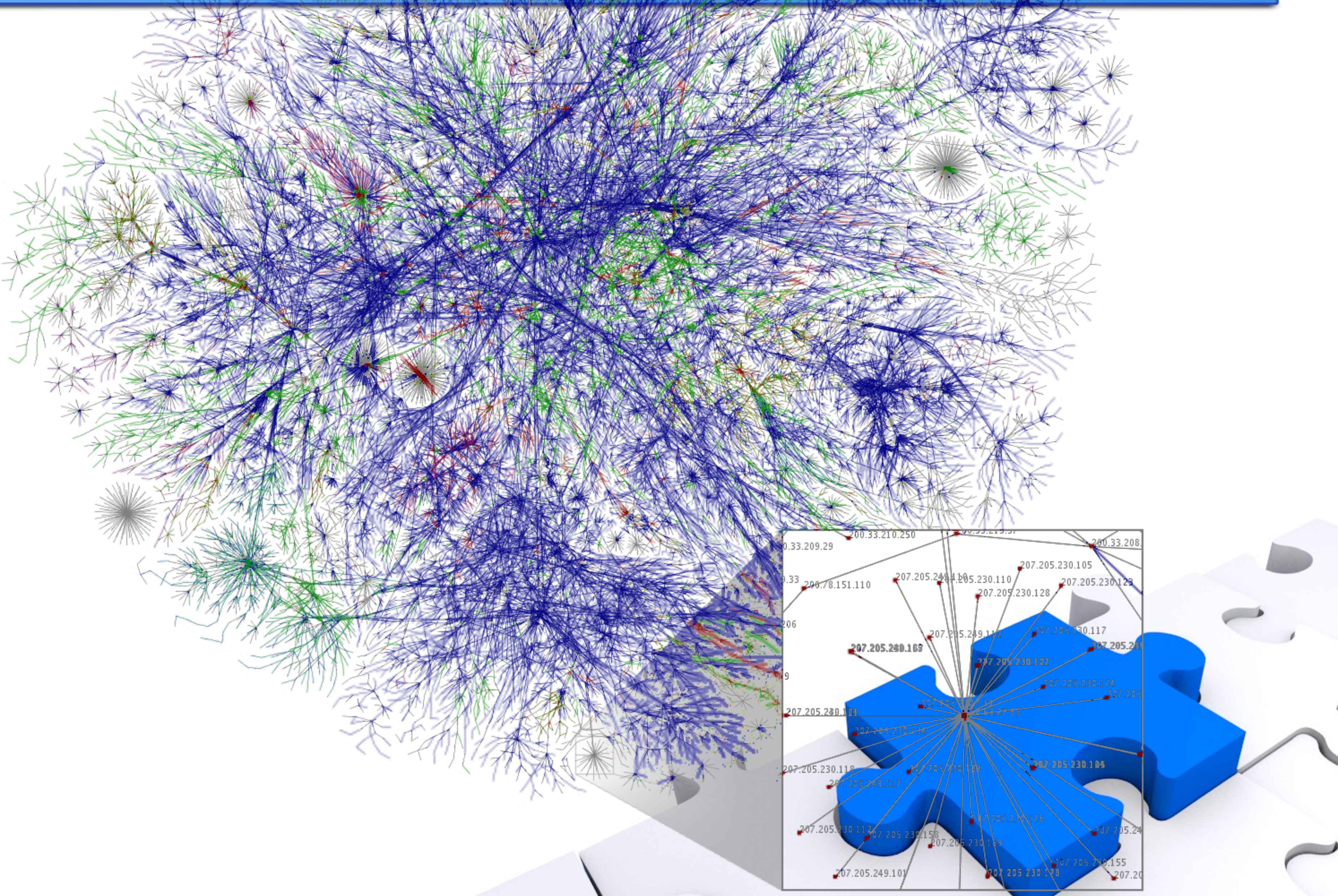
And **Future Growth** is **Staggering**

Today, the number of networked devices = the global population

By **2015**, the number of networked devices = 2x the global population

In **2015**, it would take you **5 years** to view all video crossing IP networks each **second**

Sigurnost na internetu



Sigurnost na internetu

- Moć interneta
  - Stotine milijuna korisnika na udaljenosti od par klikova i par sekundi
- Opasnost interneta
  - Postoje korisnici s lošim namjerama

Sigurnost na internetu

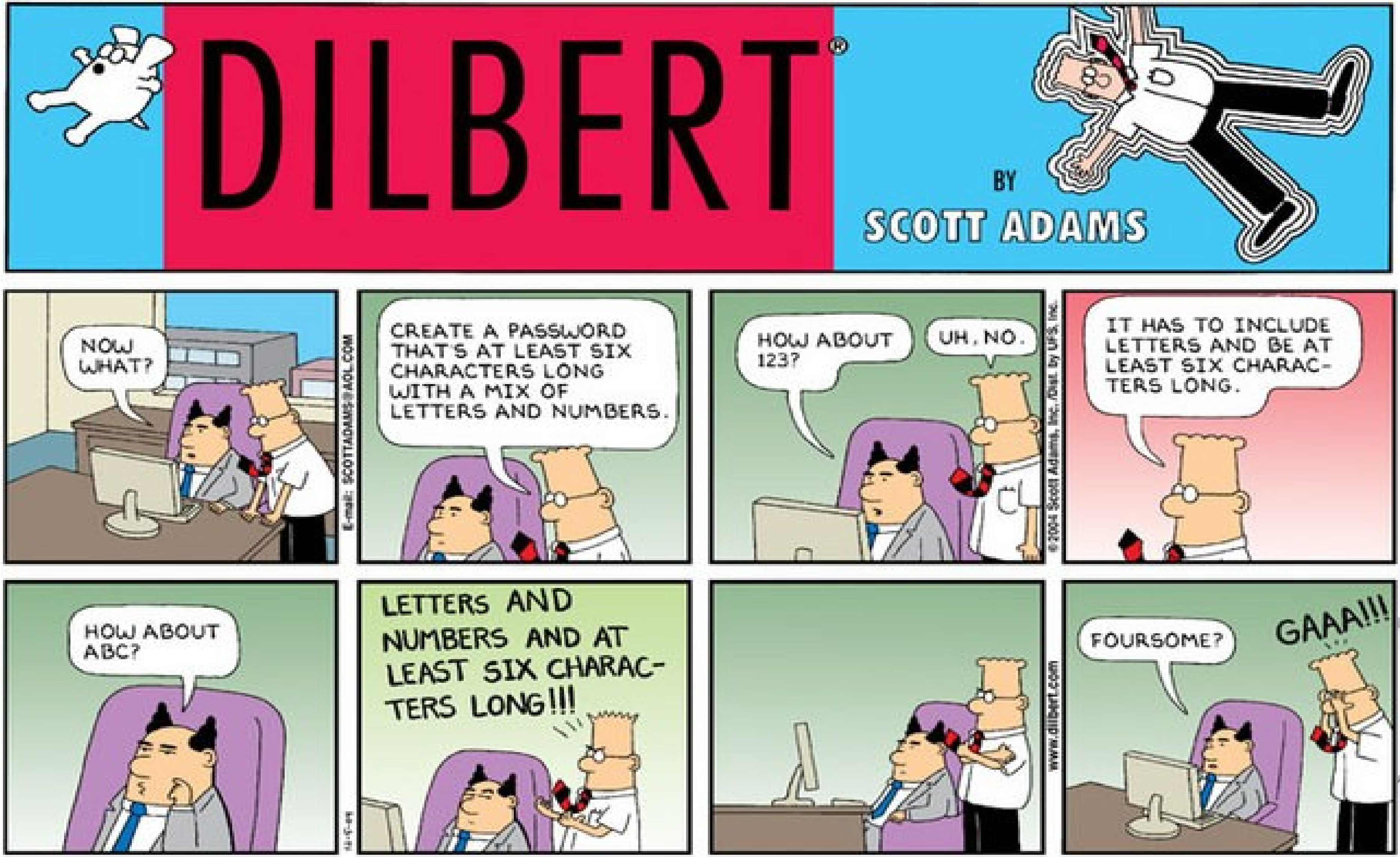
Sigurnost na internetu

- Identificiranje
  - Onim tko sam
  - Onim što znam
  - Onim što imam

Sigurnost na internetu

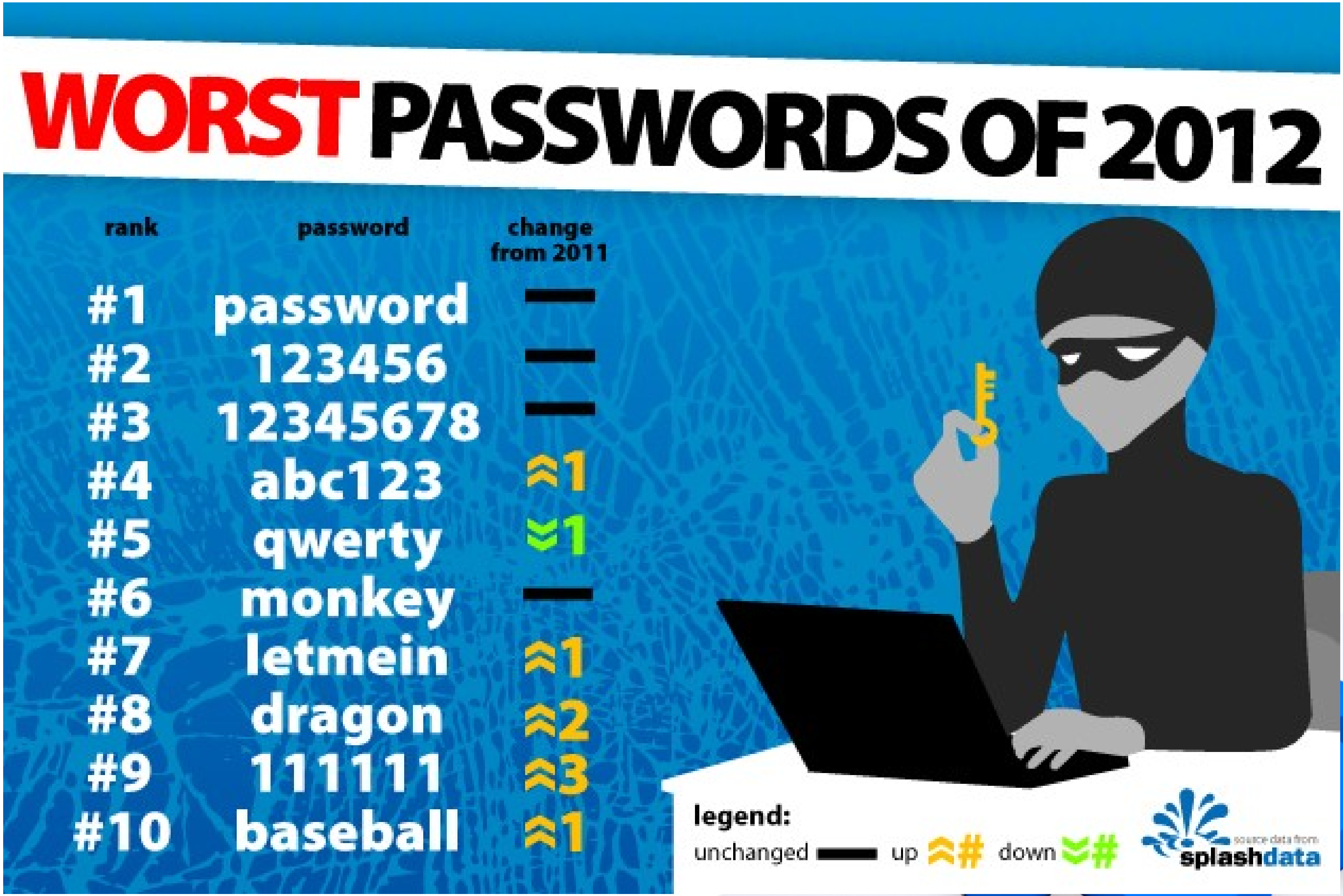
- Metafora ključa kao sredstvo identificiranja
  - Softwareski ključ – pin, zaporka...
- Preporuke
  - Koristiti jake lozinke za najvažnije servise:
    - Facebook, PayPal, Gmail...
    - Kumunikacija, društvene mreže, servise za elektroničku poštu, plaćanje...
  - TU lozinku ne koristiti na bilo forumima ili drugim manje provjerenim servisima
  - Odvagati sigurnost nasuprot praktičnosti

Sigurnost na internetu


DILBERT®
BY SCOTT ADAMS
NOW WHAT?
CREATE A PASSWORD THAT'S AT LEAST SIX CHARACTERS LONG WITH A MIX OF LETTERS AND NUMBERS.
HOW ABOUT 123?
UH, NO.
IT HAS TO INCLUDE LETTERS AND BE AT LEAST SIX CHARACTERS LONG.
HOW ABOUT ABC?
LETTERS AND NUMBERS AND AT LEAST SIX CHARACTERS LONG!!!
FOURSOME?
GAAA!!!
E-mail: SCOTTADAMS@AOL.COM
© 2004 Scott Adams, Inc. /Dist. by UFS, Inc.
www.dilbert.com

© UFS, Inc.

Sigurnost na internetu



WORST PASSWORDS OF 2012

rank	password	change from 2011
#1	password	—
#2	123456	—
#3	12345678	—
#4	abc123	↑1
#5	qwerty	↓1
#6	monkey	—
#7	letmein	↑1
#8	dragon	↑2
#9	111111	↑3
#10	baseball	↑1

legend:
unchanged — up ↑# down ↓#

source data from splashdata

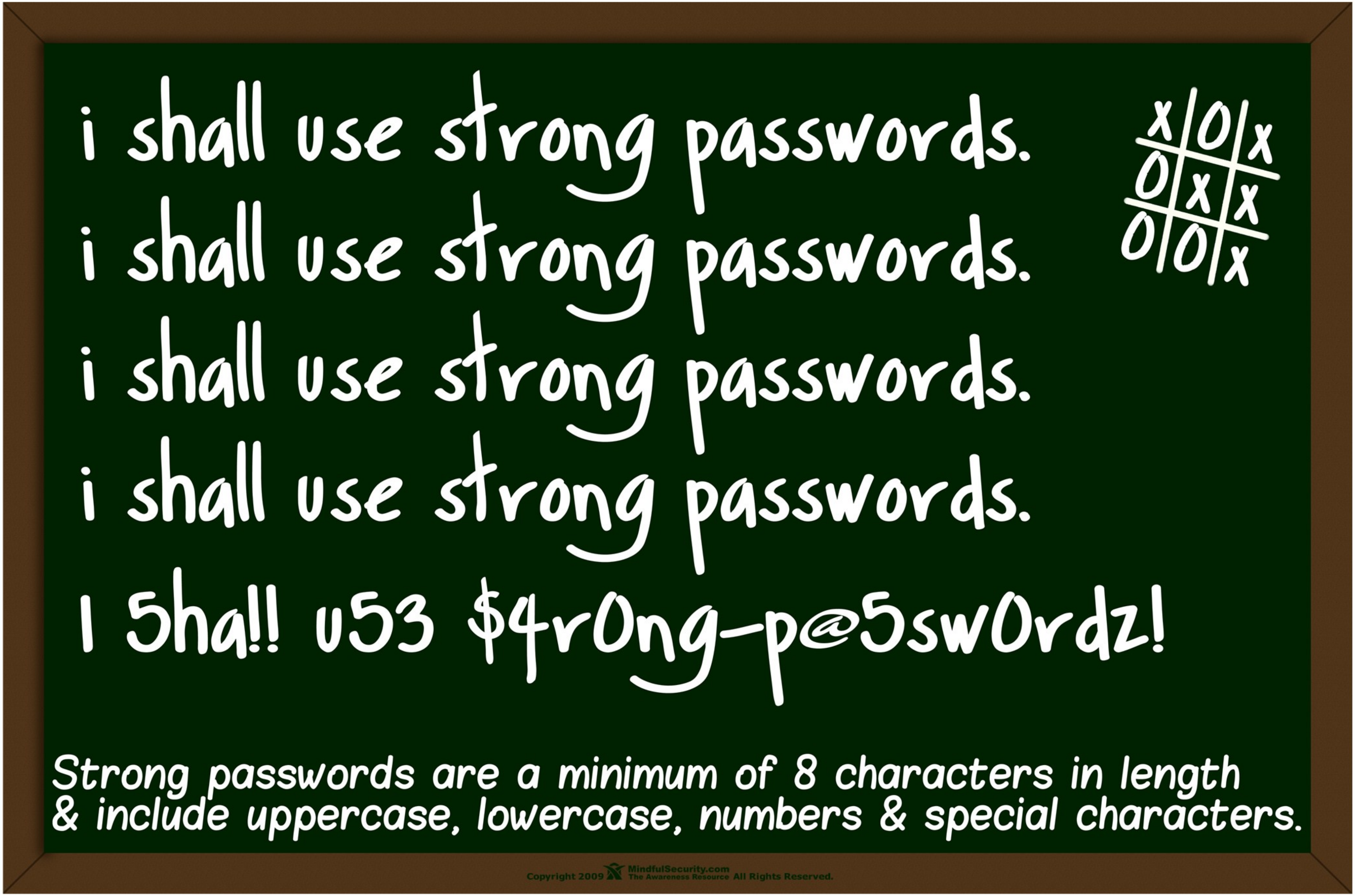
Sigurnost na internetu

- Moja draga voli filmove s Jamesom Bondom
  - MdvfsJB
  - Mdvf5J8#

* s, S = 5

b, B = 8

_ (ili neki drugi znak) na kraj



i shall use strong passwords.

i shall use strong passwords.

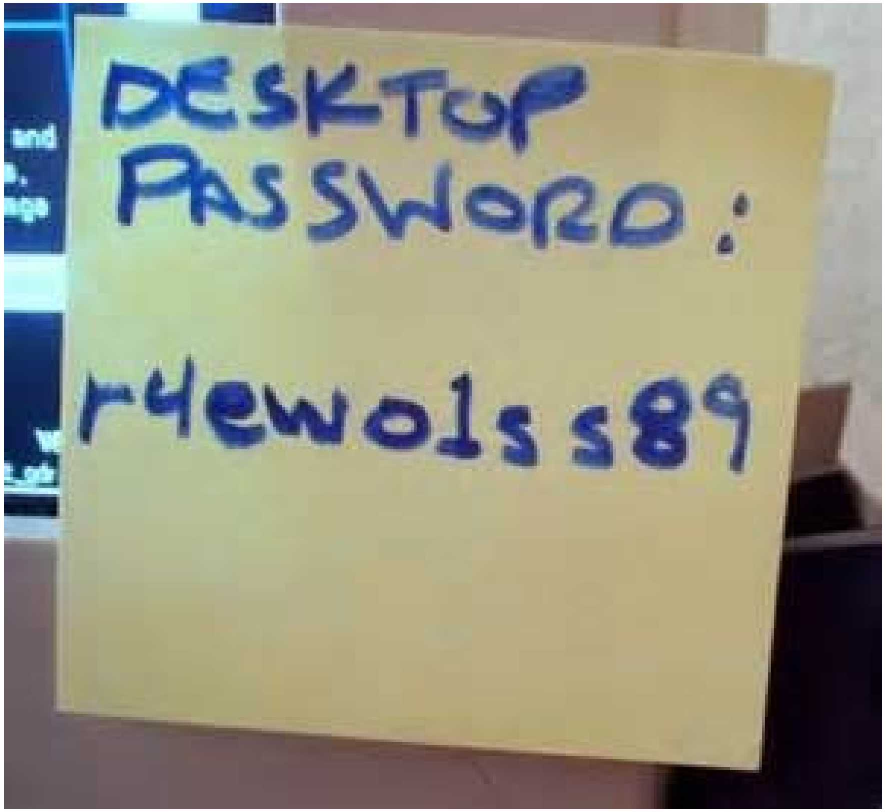
i shall use strong passwords.

i shall use strong passwords.

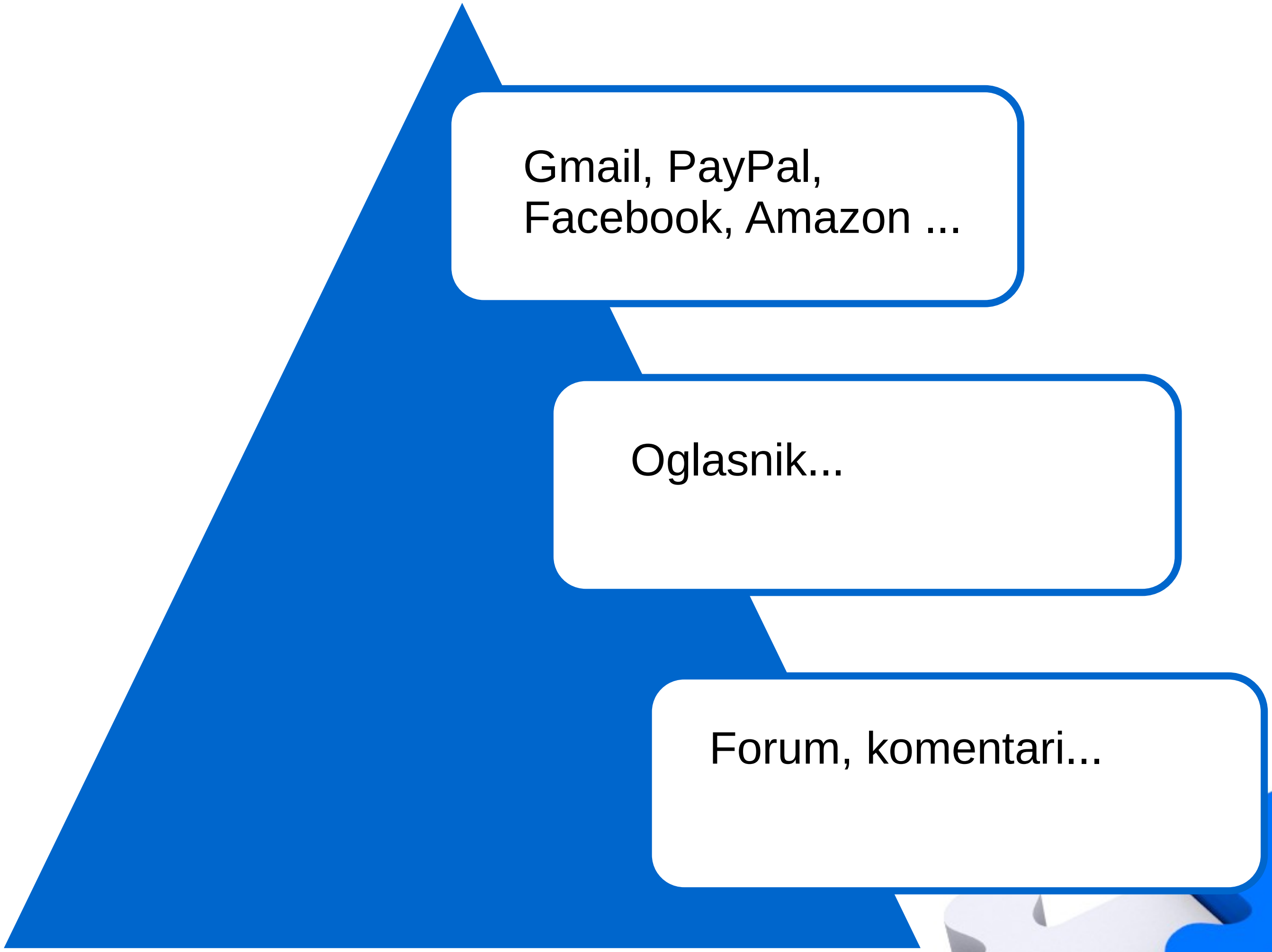
I 5ha!! u53 $4r0ng-p@5sw0rdz!

Strong passwords are a minimum of 8 characters in length & include uppercase, lowercase, numbers & special characters.

Sigurnost na internetu



Sigurnost na internetu

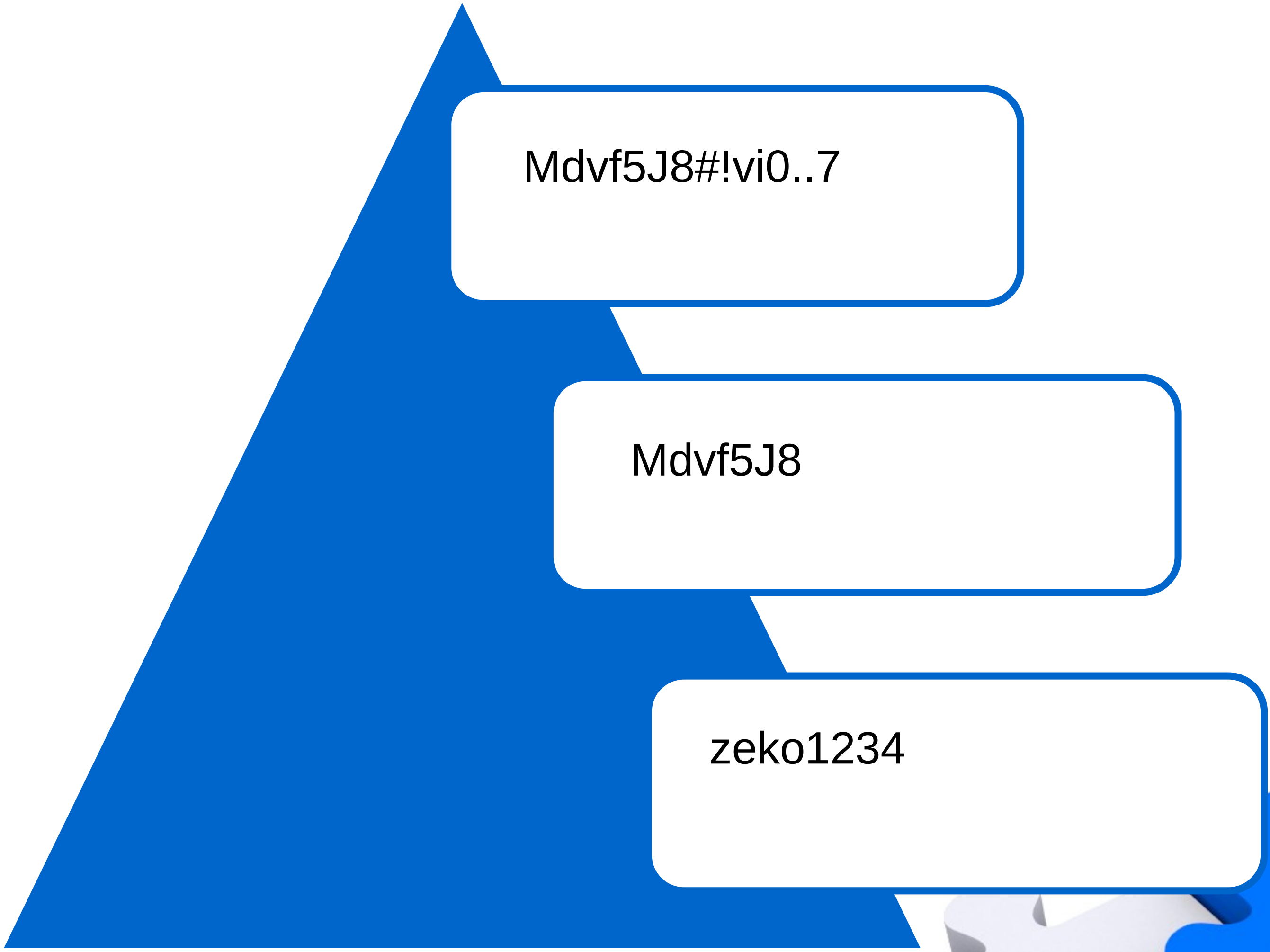


Gmail, PayPal, Facebook, Amazon ...

Oglasnik...

Forum, komentari...

Sigurnost na internetu



Mdvf5J8#!vi0..7

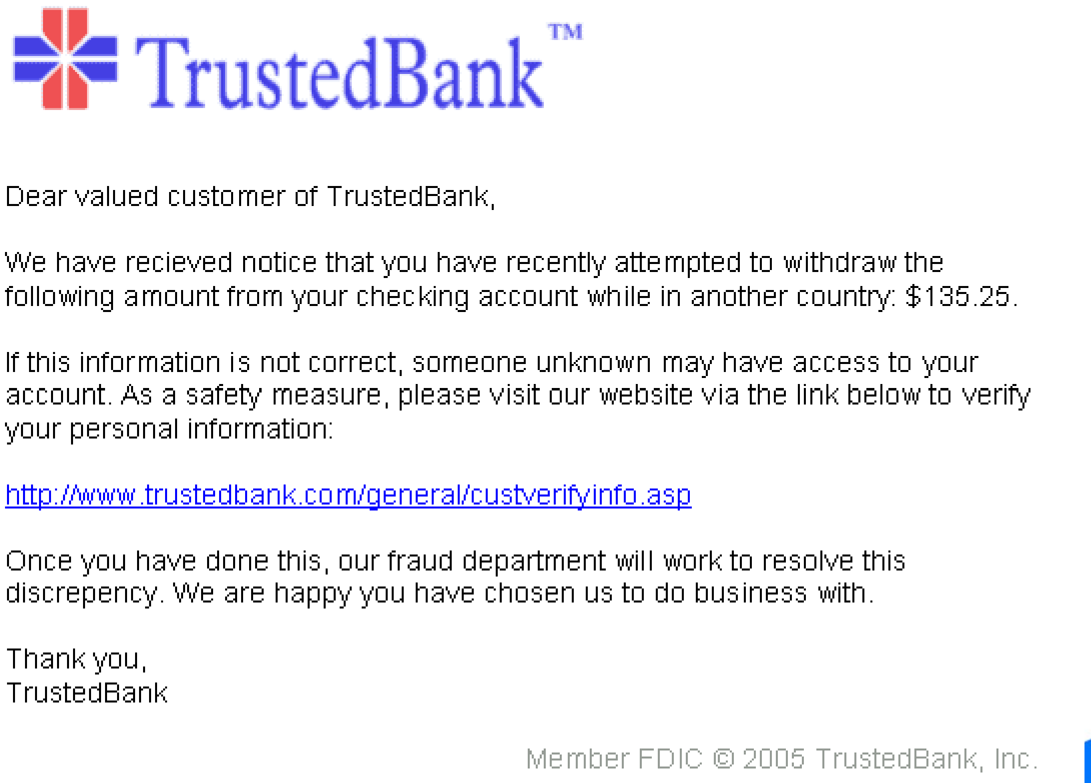
Mdvf5J8

zeko1234

Sigurnost na internetu

- Zašto?
  - napadač može otvoriti lažni forum s ciljem prikupljanja lozinki (phishing)

Sigurnost na internetu



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

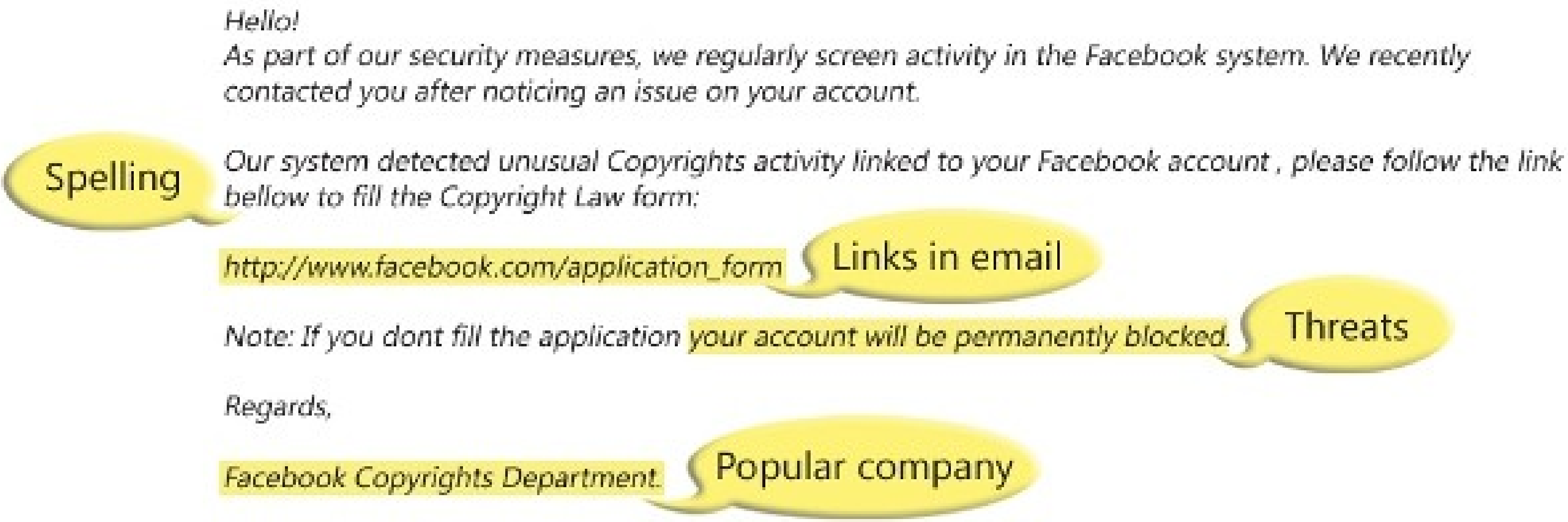
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Sigurnost na internetu



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

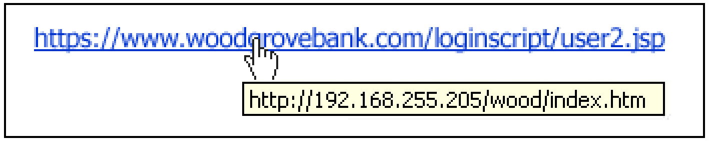
Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

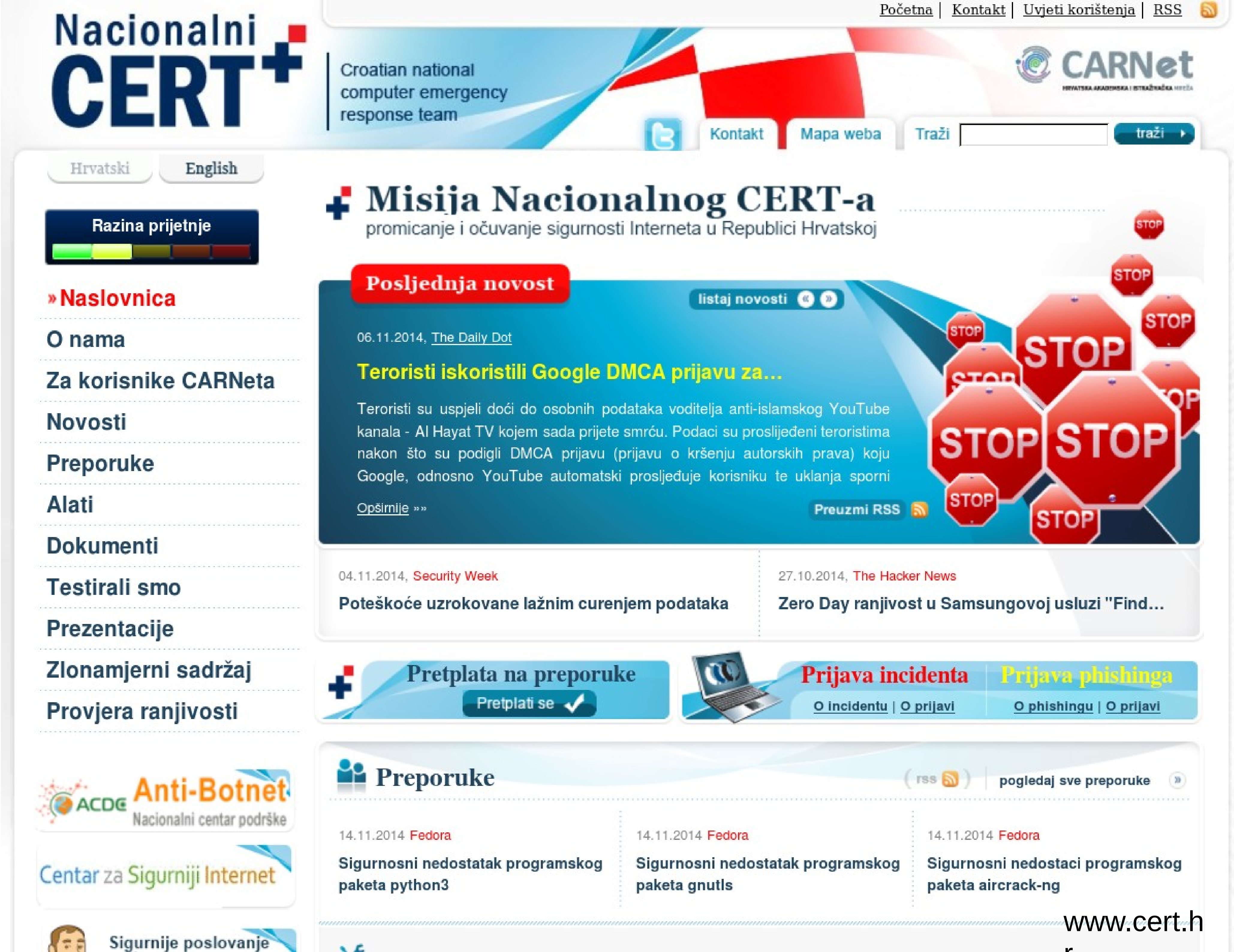
Regards,

Facebook Copyrights Department.



https://www.woodgrovebank.com/loginscript/user2.jsp

http://192.168.255.205/wood/index.htm



Početna | Kontakt | Uvjeti korištenja | RSS

Nacionalni CERT

Croatian national computer emergency response team

CARNet

Kontakt | Mapa weba | Traži | traži

Hrvatski | English

Razina prijetnje

» Naslovnica

O nama

Za korisnike CARNeta

Novosti

Preporuke

Alati

Dokumenti

Testirali smo

Prezentacije

Zlonamjerni sadržaj

Provjera ranjivosti

Anti-Botnet Nacionalni centar podrške

Centar za Sigurniji Internet

Sigurnije poslovanje

Misija Nacionalnog CERT-a

promicanje i očuvanje sigurnosti Interneta u Republici Hrvatskoj

Posljednja novost

listaj novosti

06.11.2014, The Daily Dot

Teroristi iskoristili Google DMCA prijavu za...

Teroristi su uspjeli doći do osobnih podataka voditelja anti-islamskog YouTube kanala - Al Hayat TV kojem sada prijete smrću. Podaci su proslijeđeni teroristima nakon što su podigli DMCA prijavu (prijavu o kršenju autorskih prava) koju Google, odnosno YouTube automatski prosljeđuje korisniku te uklanja sporni

Opširnije »»

Preuzmi RSS

04.11.2014, Security Week

Poteškoće uzrokovane lažnim curenjem podataka

27.10.2014, The Hacker News

Zero Day ranjivost u Samsungovoj usluzi "Find...

Pretplata na preporuke

Pretplati se

Prijava incidenta

O incidentu | O prijavi

Prijava phishinga

O phishingu | O prijavi

Preporuke

(rss) | pogledaj sve preporuke

14.11.2014 Fedora

Sigurnosni nedostatak programskog paketa python3

14.11.2014 Fedora

Sigurnosni nedostatak programskog paketa gnutls

14.11.2014 Fedora

Sigurnosni nedostaci programskog paketa aircrack-ng

www.cert.hr

Sigurnost na internetu

- Zaštita osobnih podataka
  - Na internetu
  - Na osobnom računalu

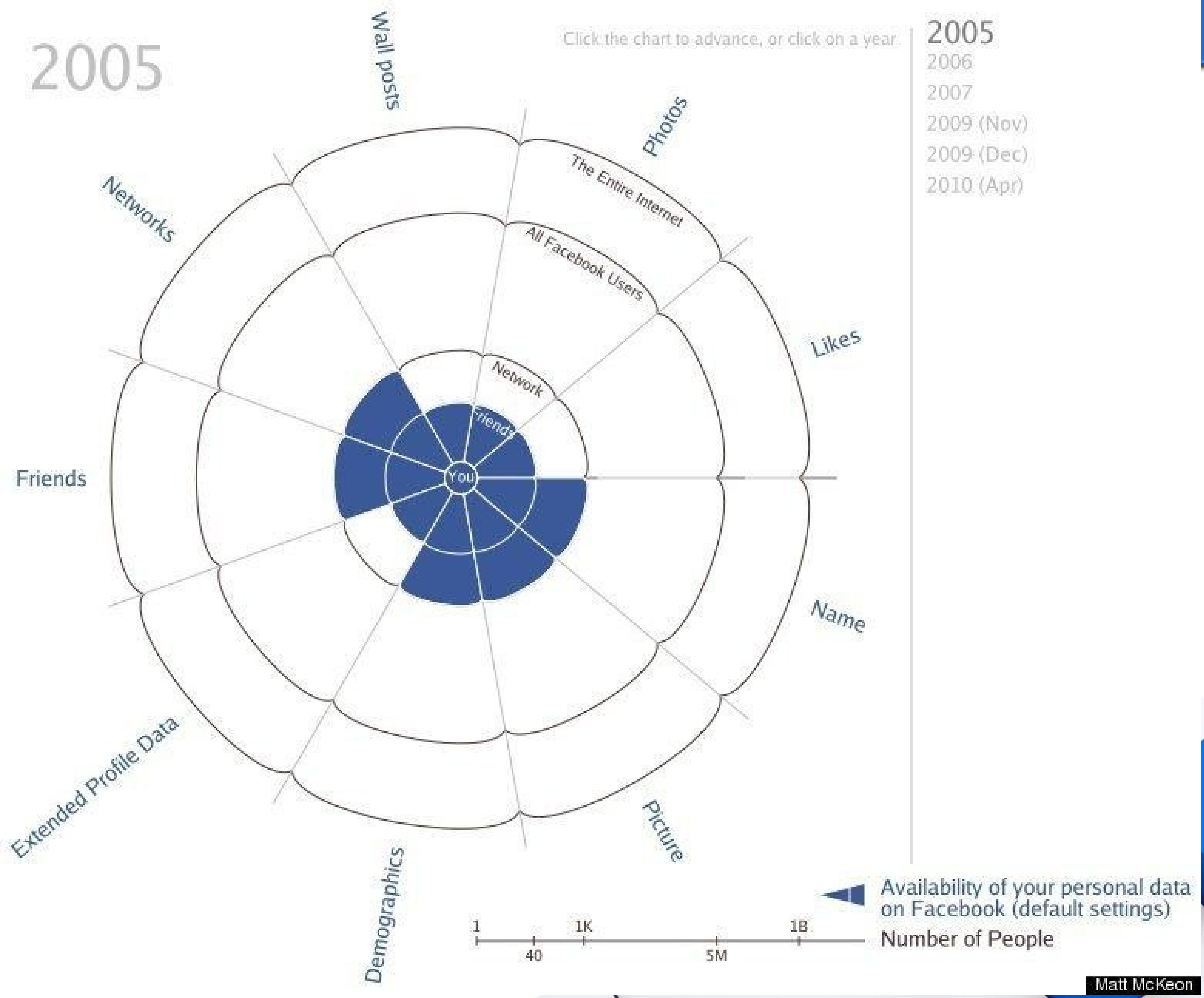
Sigurnost na internetu

CERT analiza
CarNet webinar

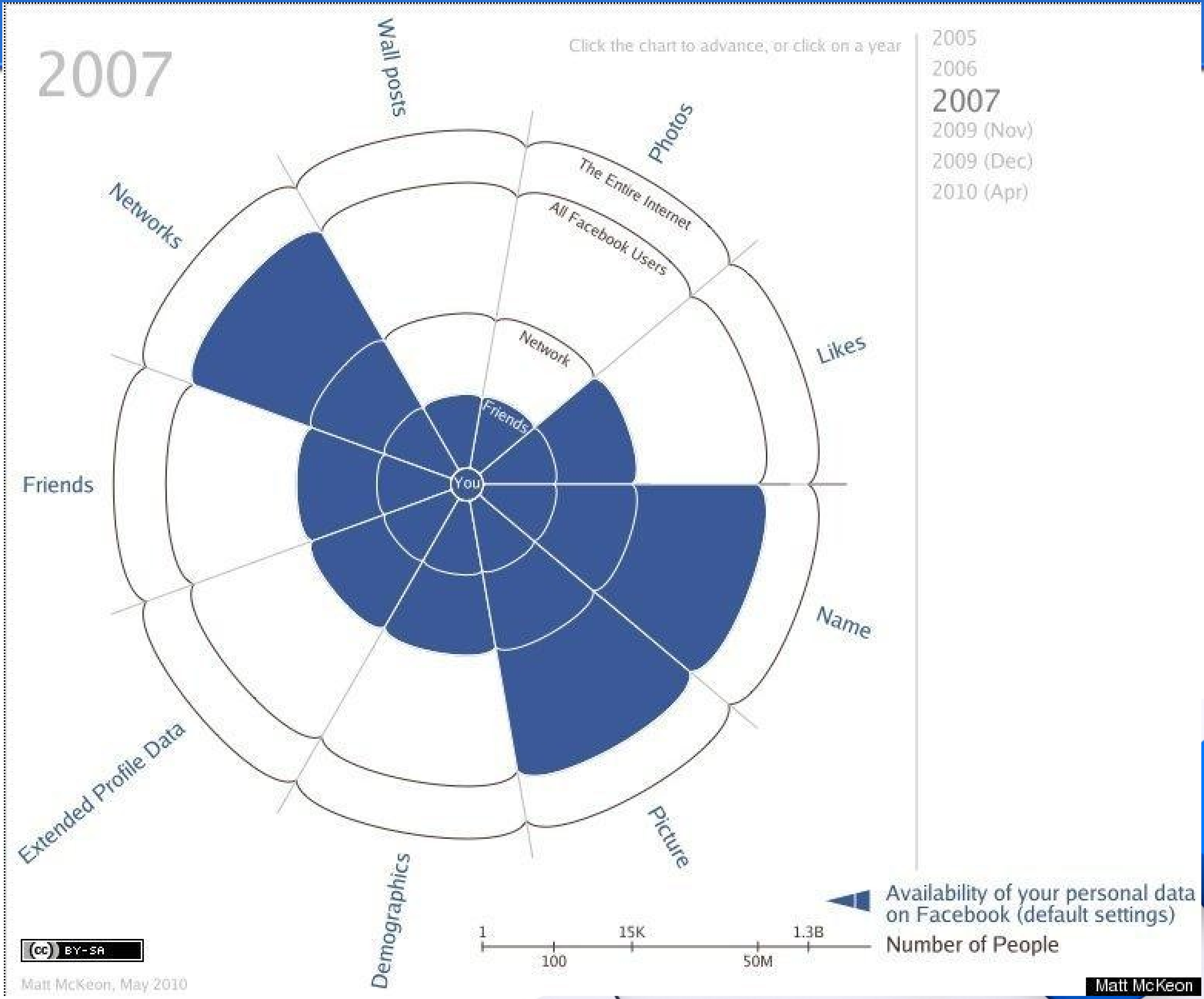
Sigurnost na internetu

- Registracija
  - Prihvaćanje pravila igre
- Vlasništvo, hijerarhija organizacije
  - Tvrtka
  - Upravljanja profitom
- "If you don't pay for the product – you are the product"

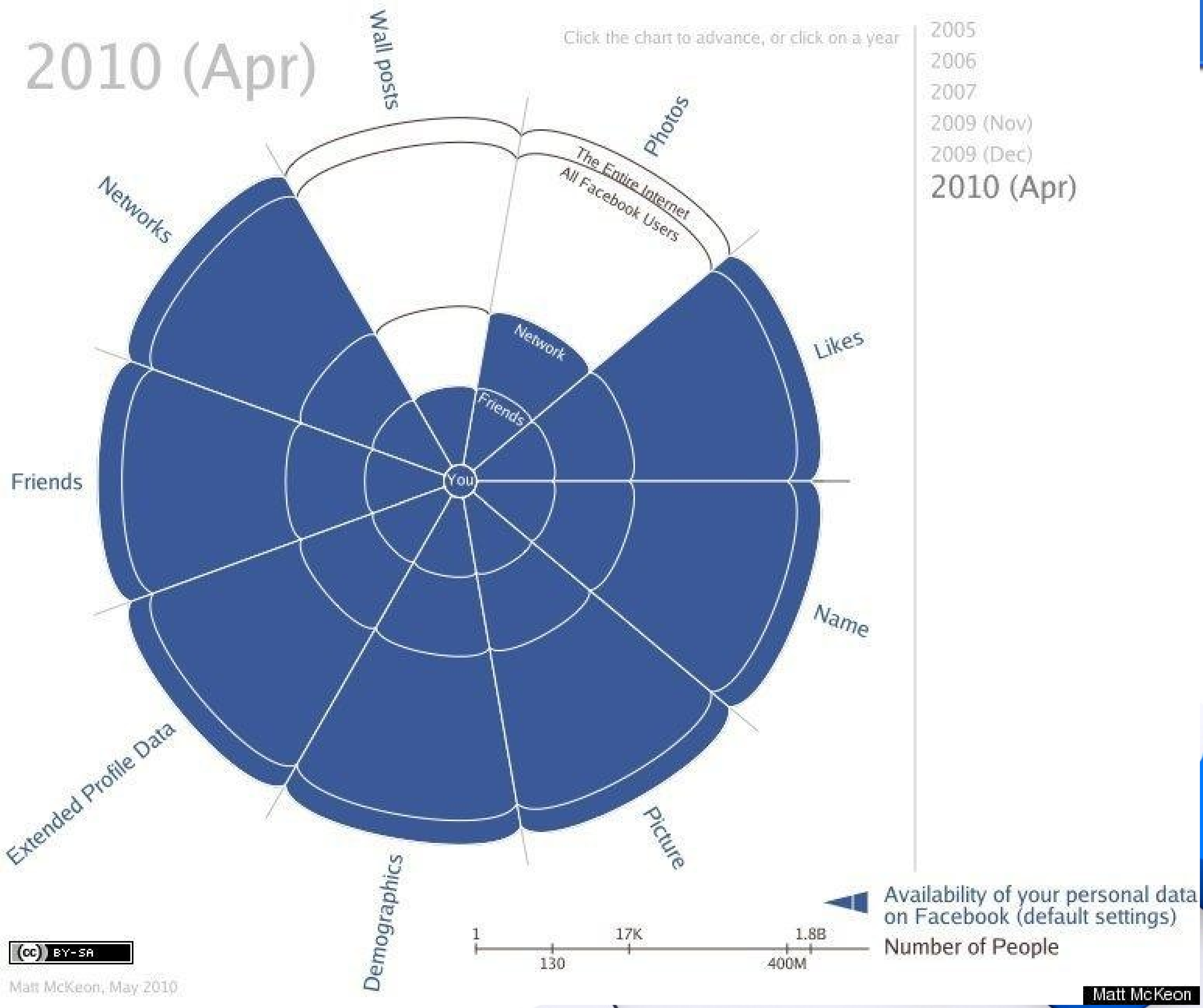
Sigurnost na internetu



Sigurnost na internetu



Sigurnost na internetu



Sigurnost na internetu

- Dostupnost FB podataka
  - U srpnju 2010., kanadski sigurnosni istraživač Ron Bowes, postavio je na javni P2P servis BitTorrent, bazu koja se sastoji od podataka iz čak 170 milijuna korisničkih računa sa Facebooka

Sigurnost na internetu

- Dostupnost FB podataka
  - http://www.facebook.com/policy.php
    - Politika privatnosti
  - http://www.facebook.com/terms.php
    - Uvjeti korištenja, 9. paragraf, točka 2 definira način na koji treće strane upravljaju našim podacima
    - kome će bit dostupni podatci koje ostavljamo na profilima drugih, ovisi o **njihovim postavkama** !

Sigurnost na internetu

- Koje osobne podatke držati privatnima (posebno zaštićenima)
  - bilo kakve kontakt informacije (e-mail adresa, telefonski broj itd.), adresa
  - datum rođenja
  - bilo koji osobni podaci koje su poznati jedino nama ili užem krugu (obitelji)

Sigurnost na internetu

- "Risk vs. Gain"
  - korist i zadovoljstvo u usporedbi s rizicima
- Koja je svrha društvene mreže
  - društvenost != prijateljstvo
  - Pravilo krda

Sigurnost na internetu

Sigurnost na internetu

- Štetni programi (malware)
  - Računalni programi kojima je glavni cilj kompromitacija računala
  - Virusi, crvi, trojanci, rootkiti...

Sigurnost na internetu

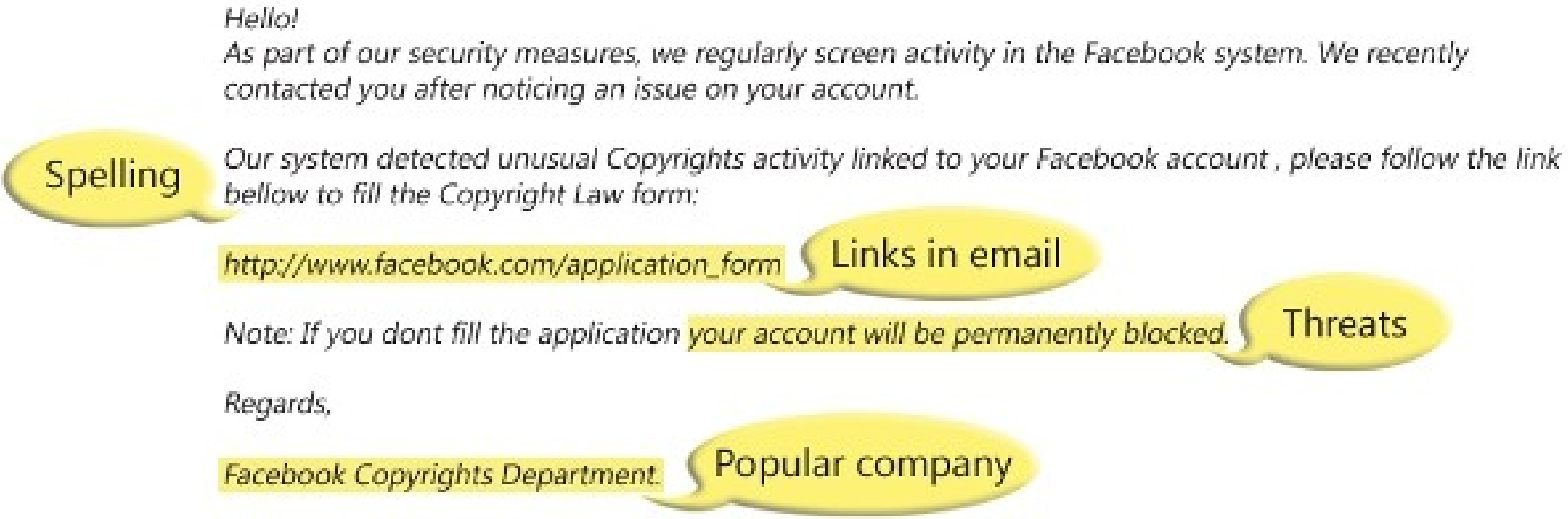
- Štetni programi (malware)
  - Računalni programi kojima je glavni cilj kompromitacija računala
  - Virusi, crvi, trojanci, rootkiti...
  - Posjeduju mogućnost samostalnog širenja
    - Elektronička pošta
    - Mrežne stranice
    - Prijenosni diskovi (USB)

Sigurnost na internetu

- Zaštita
  - Ne posjećivati sumnjive mrežne stranice
    - Kockanje
    - Piratski software
    - XXX

Sigurnost na internetu

- Zaštita
  - Ne otvarati sumnjivu poštu



Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Our system detected unusual Copyrights activity linked to your Facebook account , please follow the link bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you dont fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.

Sigurnost na internetu

- Zaštita
  - Ne otvarati sumnjivu poštu
    - Pošta od nepoznatih pošiljatelja
    - Preuzimati datoteke samo s provjerenjih mrežnih stranica
    - Ne preuzimati podatke od nepoznatih osoba (u "chat/messaging" programima)

Sigurnost na internetu

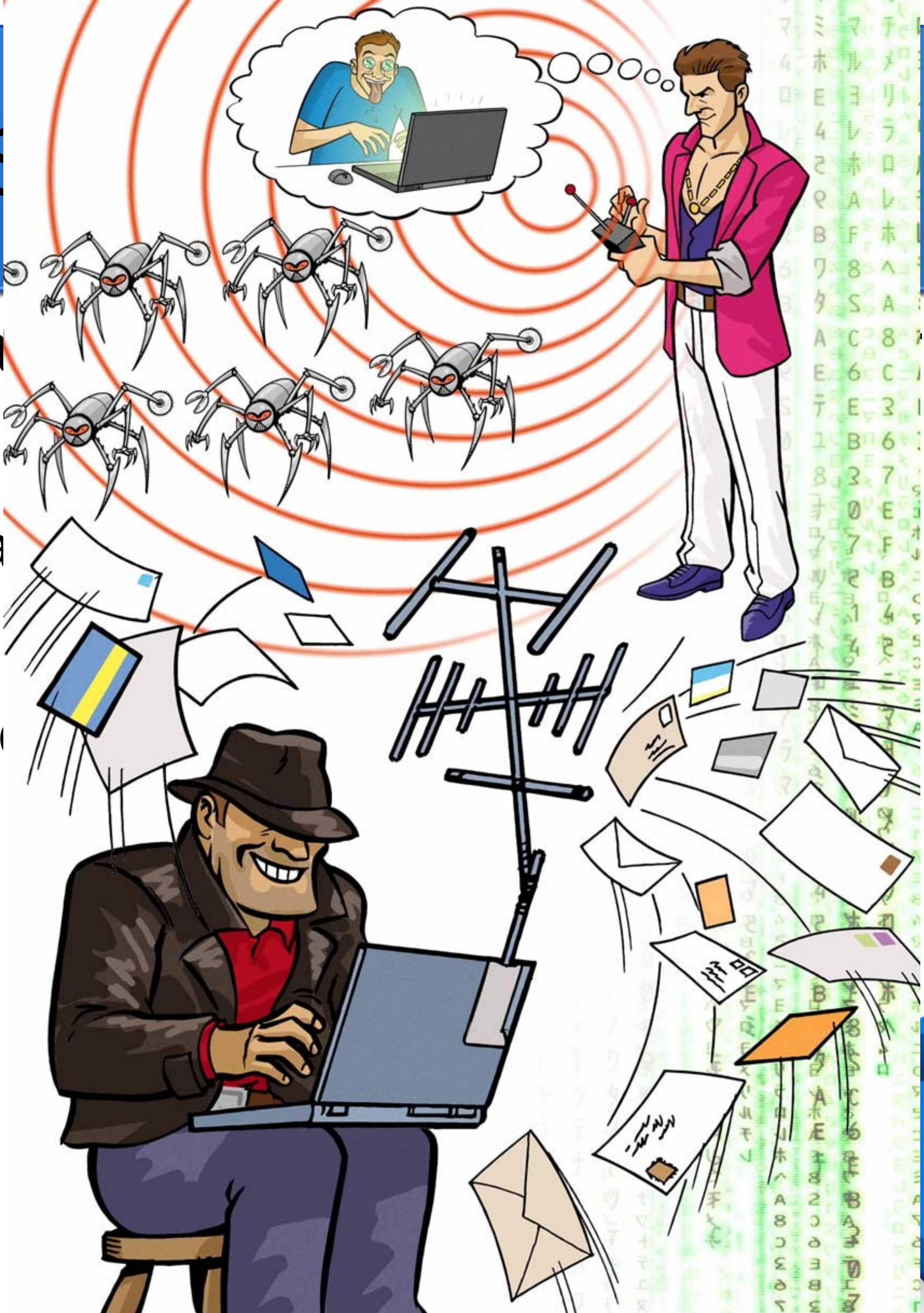
- Zaštita
  - Vatrozid
  - Antivirusni programi
    - ClamAV
    - Avast
    - AVG
    - BitDefender
  - Redovito održavanje softwarea

Sigurnost na internetu

- Uporaba tuđih računala za vlastitu korist
  - Spam
  - Oglašavanje
  - Bitcoin rudarenje
  - Napade
  - ...

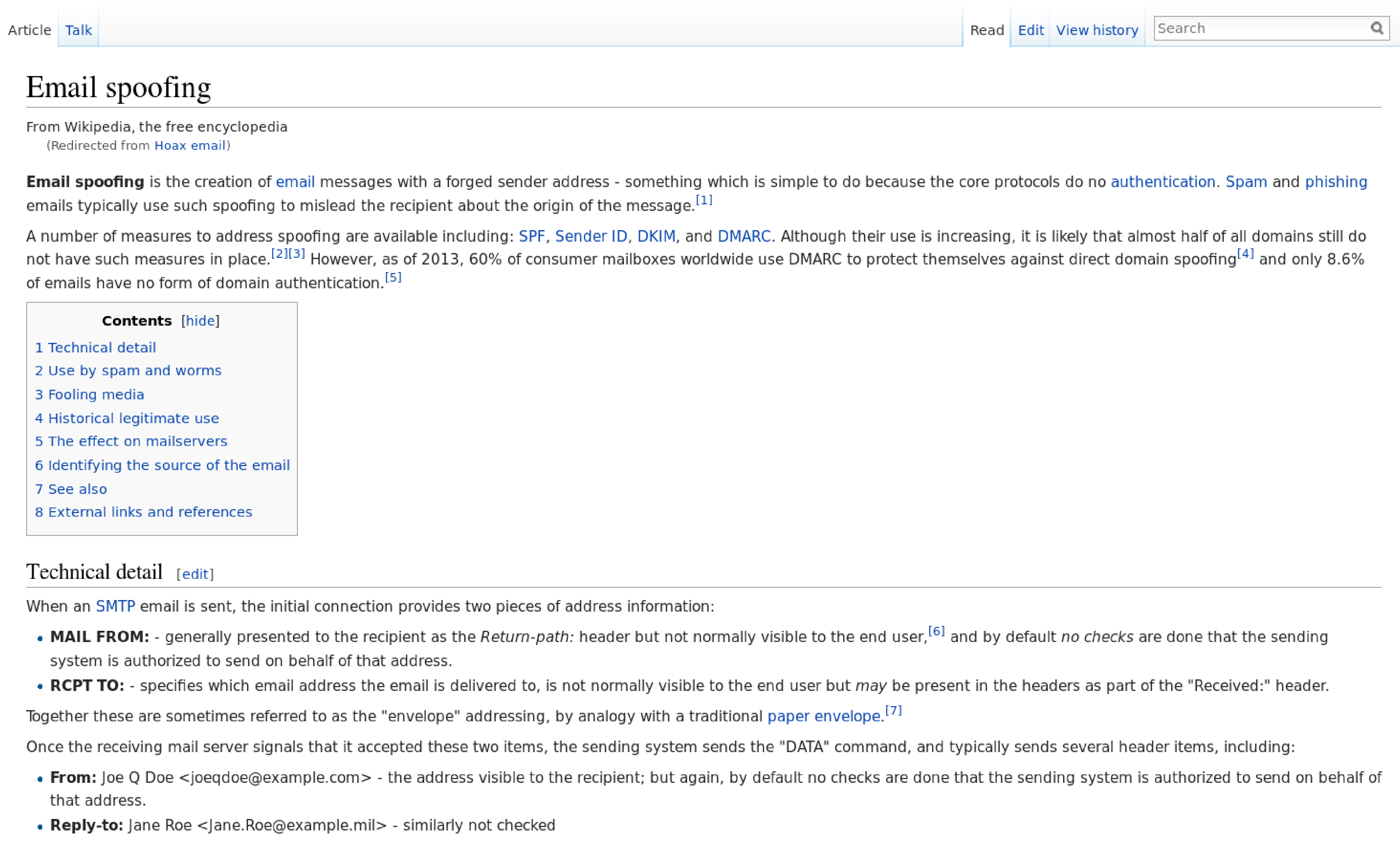
S

- Uporaba ist
  - Spam
  - Oglaša
  - Bitcoin
  - Napad
  - ...



Sigurnost na internetu

- Socijalni inženjering kao sredstvo dobivanja ovlasti
  - Lažiranje identiteta
  - Krađa identiteta
  - Krađa podataka
  - Zarada



Email spoofing

From Wikipedia, the free encyclopedia
(Redirected from Hoax email)

Email spoofing is the creation of email messages with a forged sender address - something which is simple to do because the core protocols do no authentication. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message.[1]

A number of measures to address spoofing are available including: SPF, Sender ID, DKIM, and DMARC. Although their use is increasing, it is likely that almost half of all domains still do not have such measures in place.[2][3] However, as of 2013, 60% of consumer mailboxes worldwide use DMARC to protect themselves against direct domain spoofing[4] and only 8.6% of emails have no form of domain authentication.[5]

Contents [hide]

Technical detail [edit]

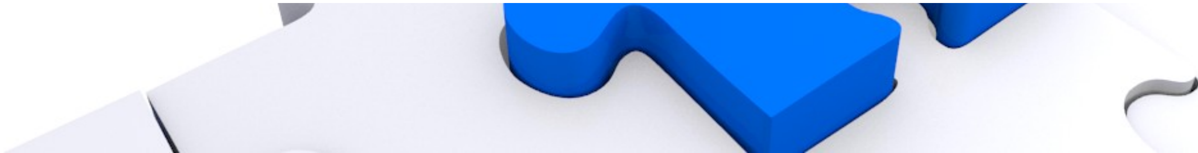
When an SMTP email is sent, the initial connection provides two pieces of address information:

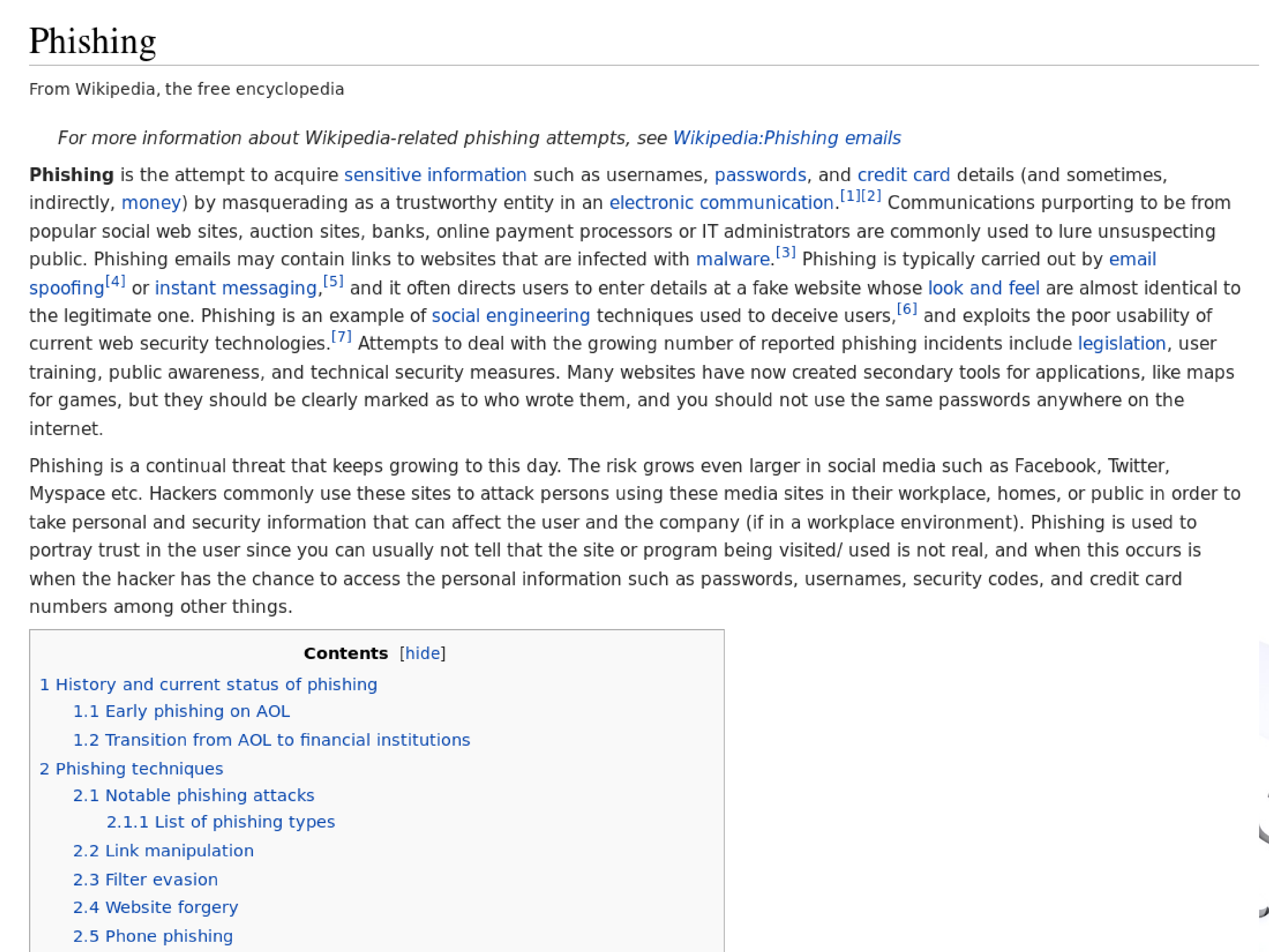
- **MAIL FROM:** - generally presented to the recipient as the *Return-path:* header but not normally visible to the end user,[6] and by default *no checks* are done that the sending system is authorized to send on behalf of that address.
- **RCPT TO:** - specifies which email address the email is delivered to, is not normally visible to the end user but *may* be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope.[7]

Once the receiving mail server signals that it accepted these two items, the sending system sends the "DATA" command, and typically sends several header items, including:

- **From:** Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.
- **Reply-to:** Jane Roe <Jane.Roe@example.mil> - similarly not checked





Phishing

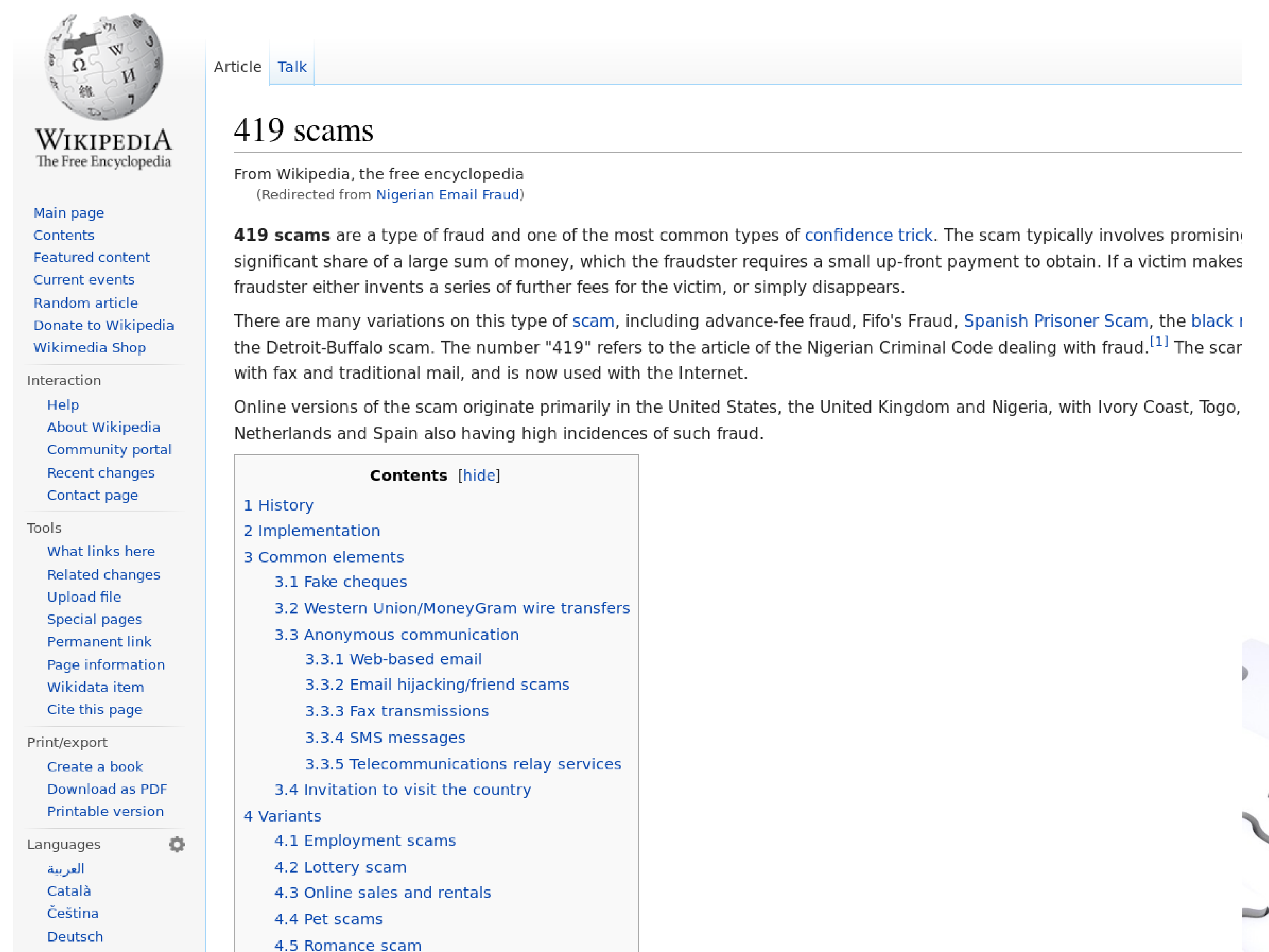
From Wikipedia, the free encyclopedia

For more information about Wikipedia-related phishing attempts, see Wikipedia:Phishing emails

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.[1][2] Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware.[3] Phishing is typically carried out by email spoofing[4] or instant messaging,[5] and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users,[6] and exploits the poor usability of current web security technologies.[7] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and you should not use the same passwords anywhere on the internet.

Phishing is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing is used to portray trust in the user since you can usually not tell that the site or program being visited/ used is not real, and when this occurs is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

Contents [hide]



Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
العربية
Català
Čeština
Deutsch

419 scams

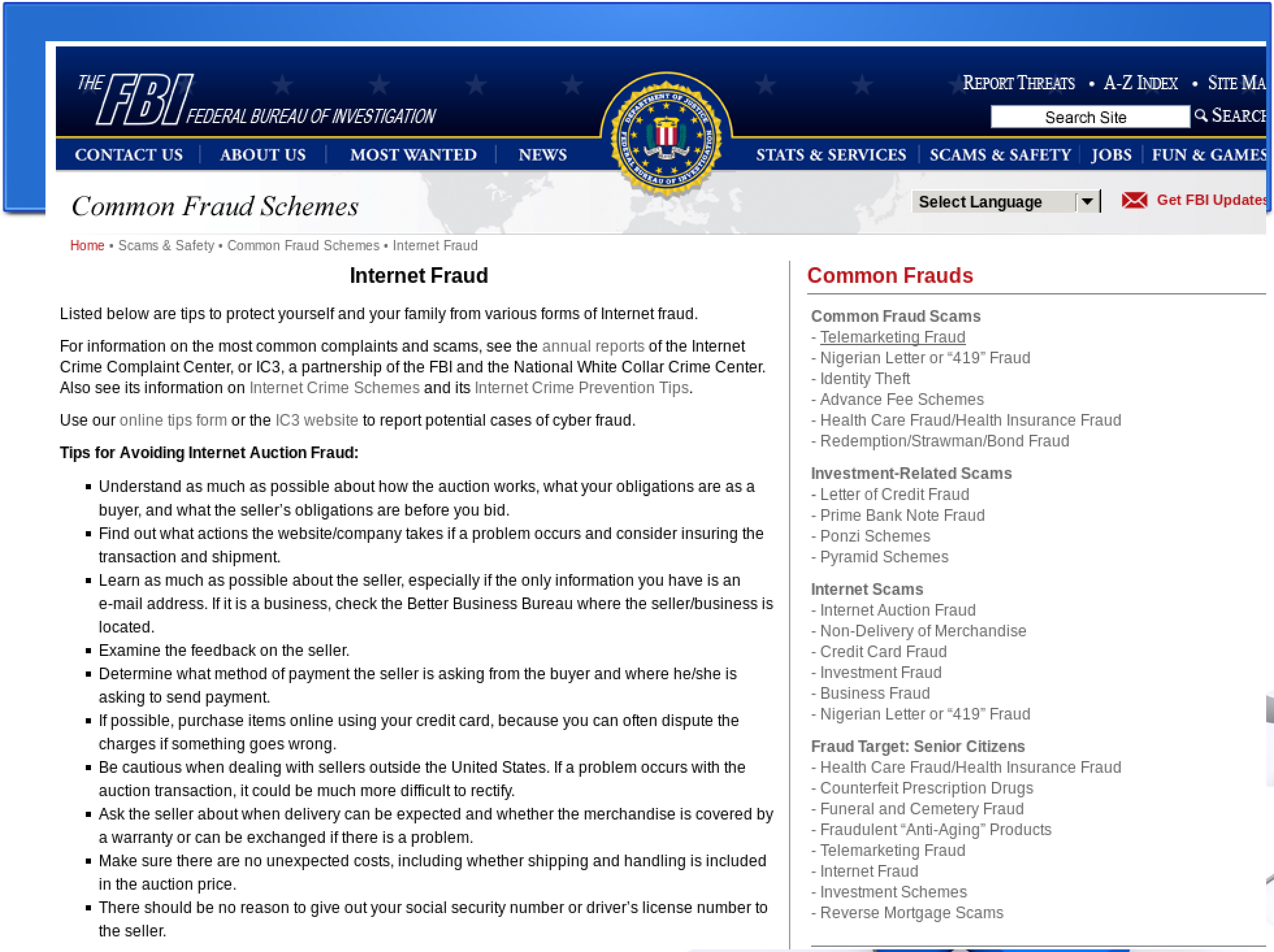
From Wikipedia, the free encyclopedia
(Redirected from Nigerian Email Fraud)

419 scams are a type of fraud and one of the most common types of confidence trick. The scam typically involves promisin
significant share of a large sum of money, which the fraudster requires a small up-front payment to obtain. If a victim makes
fraudster either invents a series of further fees for the victim, or simply disappears.

There are many variations on this type of scam, including advance-fee fraud, Fifo's Fraud, Spanish Prisoner Scam, the black r
the Detroit-Buffalo scam. The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.[1] The scar
with fax and traditional mail, and is now used with the Internet.

Online versions of the scam originate primarily in the United States, the United Kingdom and Nigeria, with Ivory Coast, Togo,
Netherlands and Spain also having high incidences of such fraud.

Contents [hide]



Common Fraud Schemes

Home • Scams & Safety • Common Fraud Schemes • Internet Fraud

Internet Fraud

Listed below are tips to protect yourself and your family from various forms of Internet fraud.

For information on the most common complaints and scams, see the annual reports of the Internet Crime Complaint Center, or IC3, a partnership of the FBI and the National White Collar Crime Center. Also see its information on Internet Crime Schemes and its Internet Crime Prevention Tips.

Use our online tips form or the IC3 website to report potential cases of cyber fraud.

Tips for Avoiding Internet Auction Fraud:

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website/company takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller.
- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Be cautious when dealing with sellers outside the United States. If a problem occurs with the auction transaction, it could be much more difficult to rectify.
- Ask the seller about when delivery can be expected and whether the merchandise is covered by a warranty or can be exchanged if there is a problem.
- Make sure there are no unexpected costs, including whether shipping and handling is included in the auction price.
- There should be no reason to give out your social security number or driver's license number to the seller.

Common Frauds

Common Fraud Scams
- Telemarketing Fraud
- Nigerian Letter or "419" Fraud
- Identity Theft
- Advance Fee Schemes
- Health Care Fraud/Health Insurance Fraud
- Redemption/Strawman/Bond Fraud

Investment-Related Scams
- Letter of Credit Fraud
- Prime Bank Note Fraud
- Ponzi Schemes
- Pyramid Schemes

Internet Scams
- Internet Auction Fraud
- Non-Delivery of Merchandise
- Credit Card Fraud
- Investment Fraud
- Business Fraud
- Nigerian Letter or "419" Fraud

Fraud Target: Senior Citizens
- Health Care Fraud/Health Insurance Fraud
- Counterfeit Prescription Drugs
- Funeral and Cemetery Fraud
- Fraudulent "Anti-Aging" Products
- Telemarketing Fraud
- Internet Fraud
- Investment Schemes
- Reverse Mortgage Scams

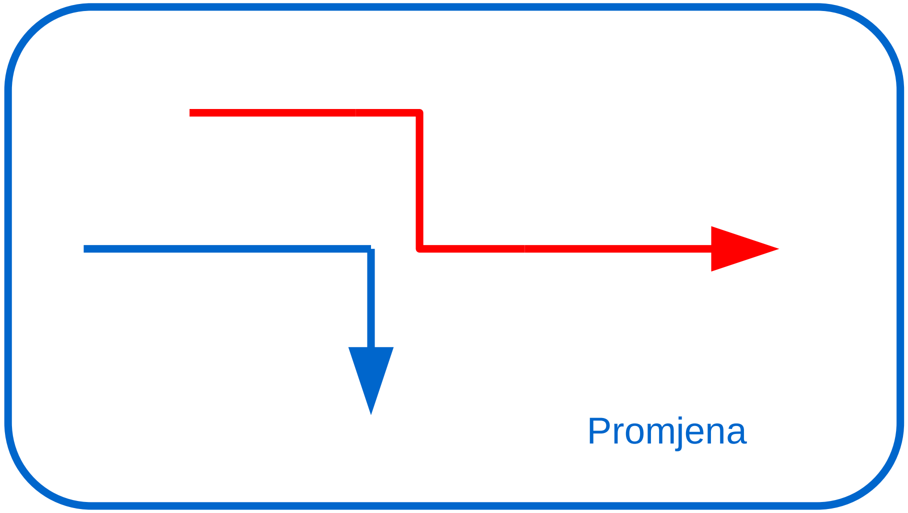
http://www.fbi.gov/scams-safety/fraud/internet_fraud

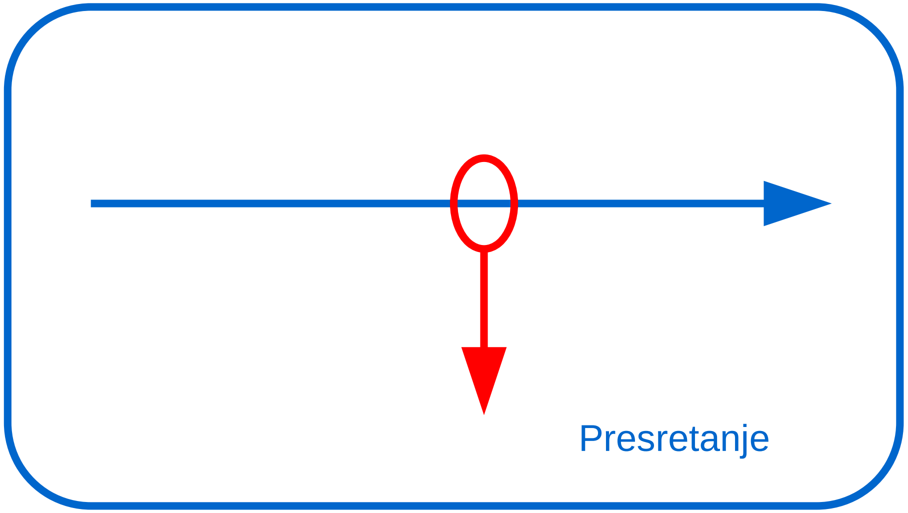
Sigurnost na internetu

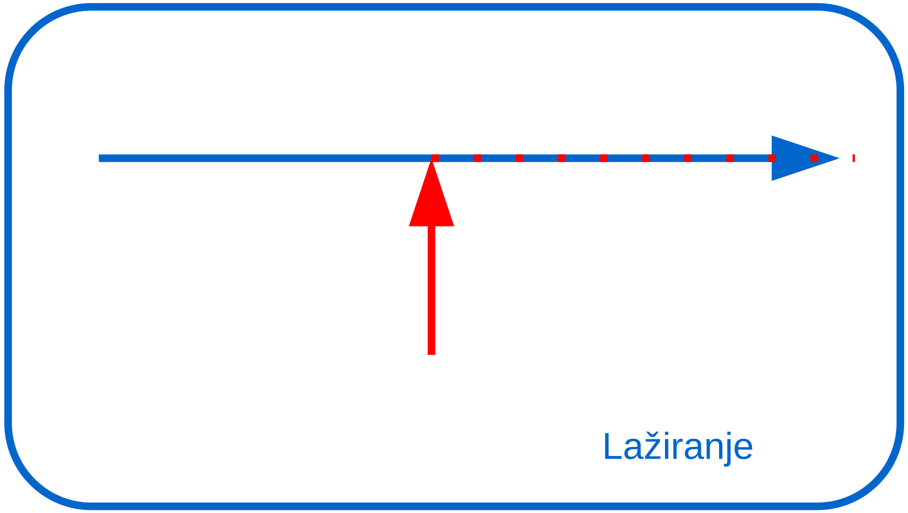
Sigurnost na internetu

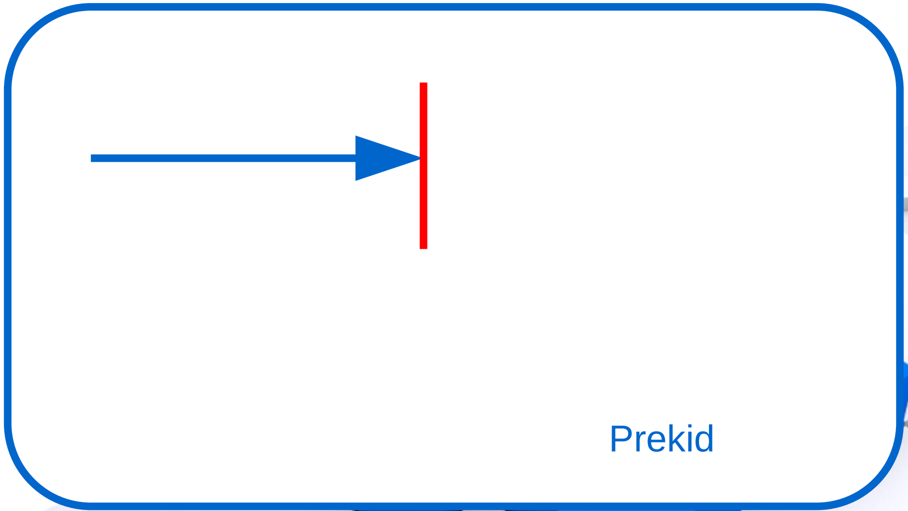
- Mogući napadi
  - Promjena
  - Lažiranje informacije
  - Presretanje
  - Prekid

Sigurnost na internetu


Promjena

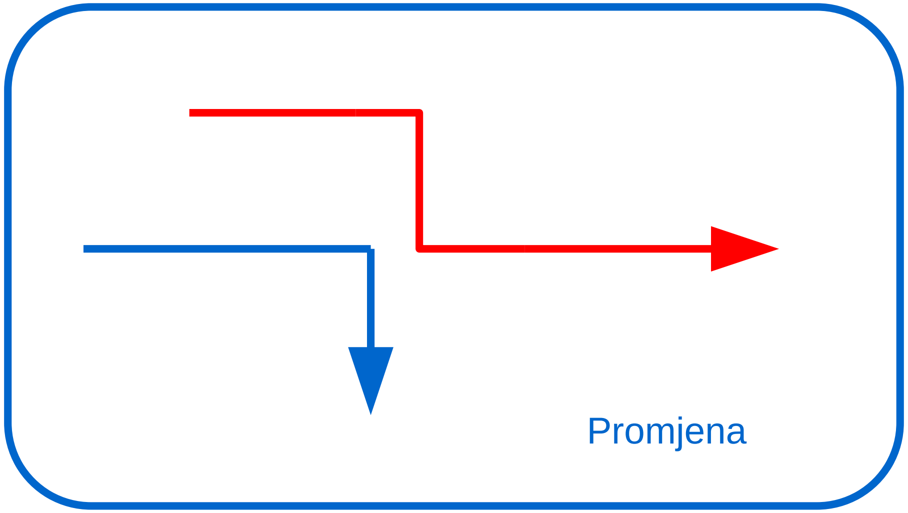

Presretanje


Lažiranje


Prekid

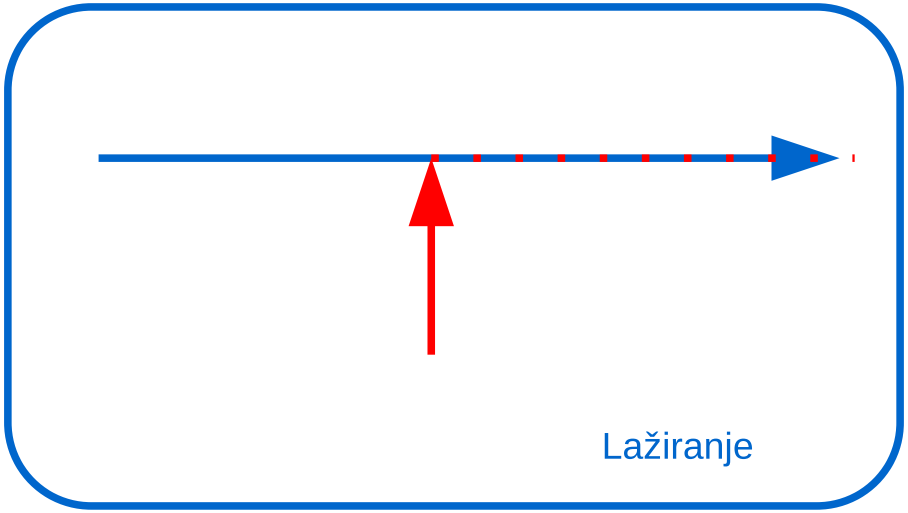
Sigurnost na internetu

- Promjena
  - Promjena podataka u bazi
  - Kompromitiranje sustava
  - Uskakanje u zastoj u komunikaciji
  - Promjena pogonivača sklopovlja



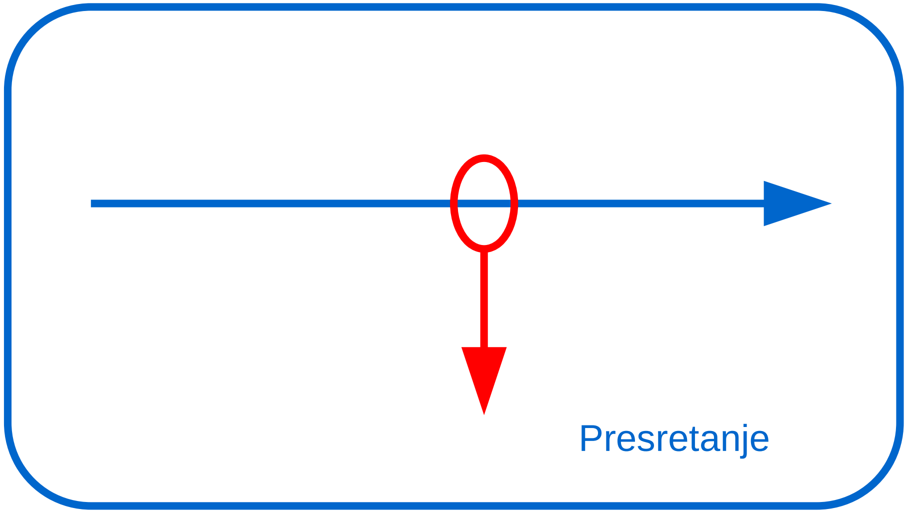
Sigurnost na internetu

- Lažiranje informacije
  - Lažne elektroničke poruke
  - Lažna mrežna sjedišta
  - Ubacivanje lažnih podataka u bazu
  - IP spoofing
  - DNS spoofing



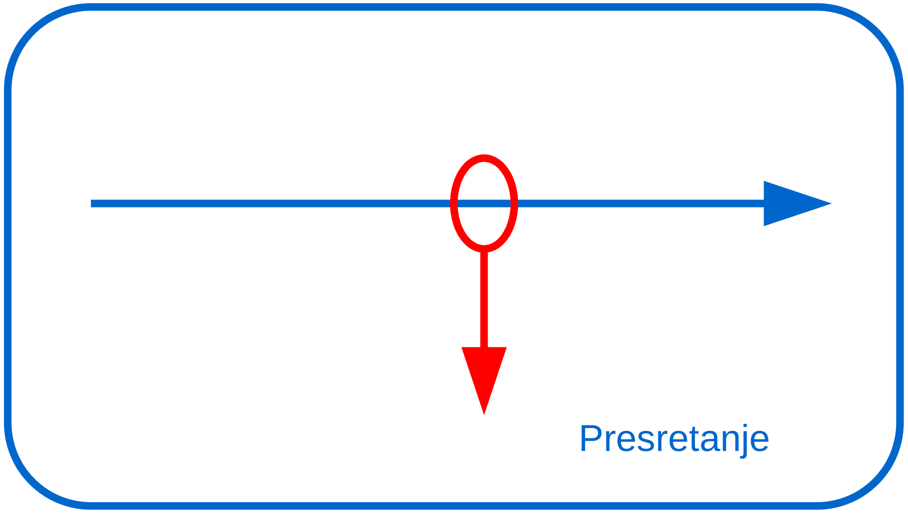
Sigurnost na internetu

- Presretanje
  - prisluškivanje (eavesdropping)
  - nadzor mrežne komunikacije (link monitoring)
  - snimanje mrežnog prometa (packet capturing)
  - kompromitacija sustava (system compromisation)



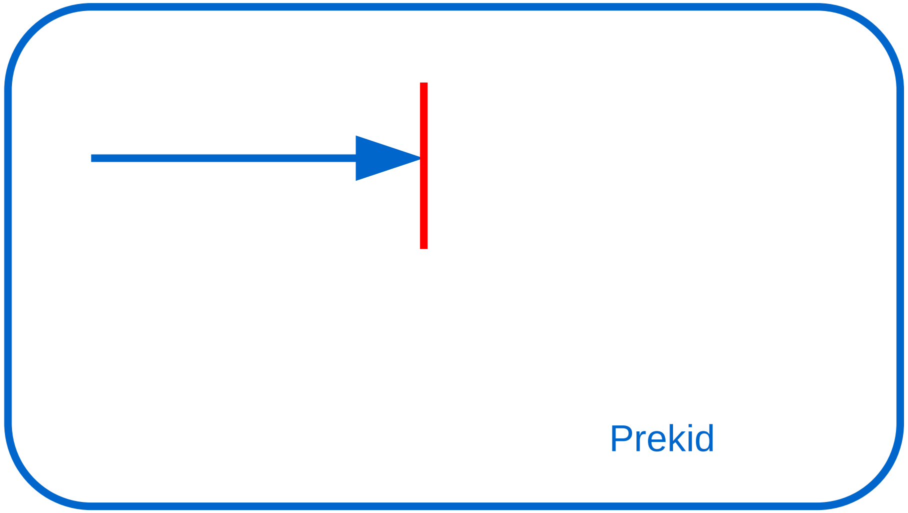
Sigurnost na internetu

- Presretanje
  - Neovlaštena osoba ima pristup informacijama
  - Rizik raste kod:
    - Bežične komunikacije
    - Grupne komunikacije



Sigurnost na internetu

- Prekid
  - uništavanje sklopovlja
  - fizičko uništavanje komunikacijskih medija
  - ometanje komunikacije (šum)
  - narušavanje tablica usmjeravanja
  - brisanje programa ili datoteka
  - uskraćivanje usluge



Sigurnost na internetu

ime.prezime@pmfst.hr