Chyby, které za nás udělali jiní

Ing. Tomáš PŘIBYL
konzultant a publicista
tomas.pribyl@seznam.cz
www.kosmonaut.cz

Jednodušší to být nemůže…

96 procent útoků provedeno „velmi jednoduše".

97 procentům šlo „velmi jednoduše" zabránit.

[Verizon 2012 Data Breach Investigations Report]

Jednoznakové heslo

255 možností

Dvouznakové heslo

65025 možností

Tříznakové heslo

16 581 375 možností

Čtyřznakové heslo

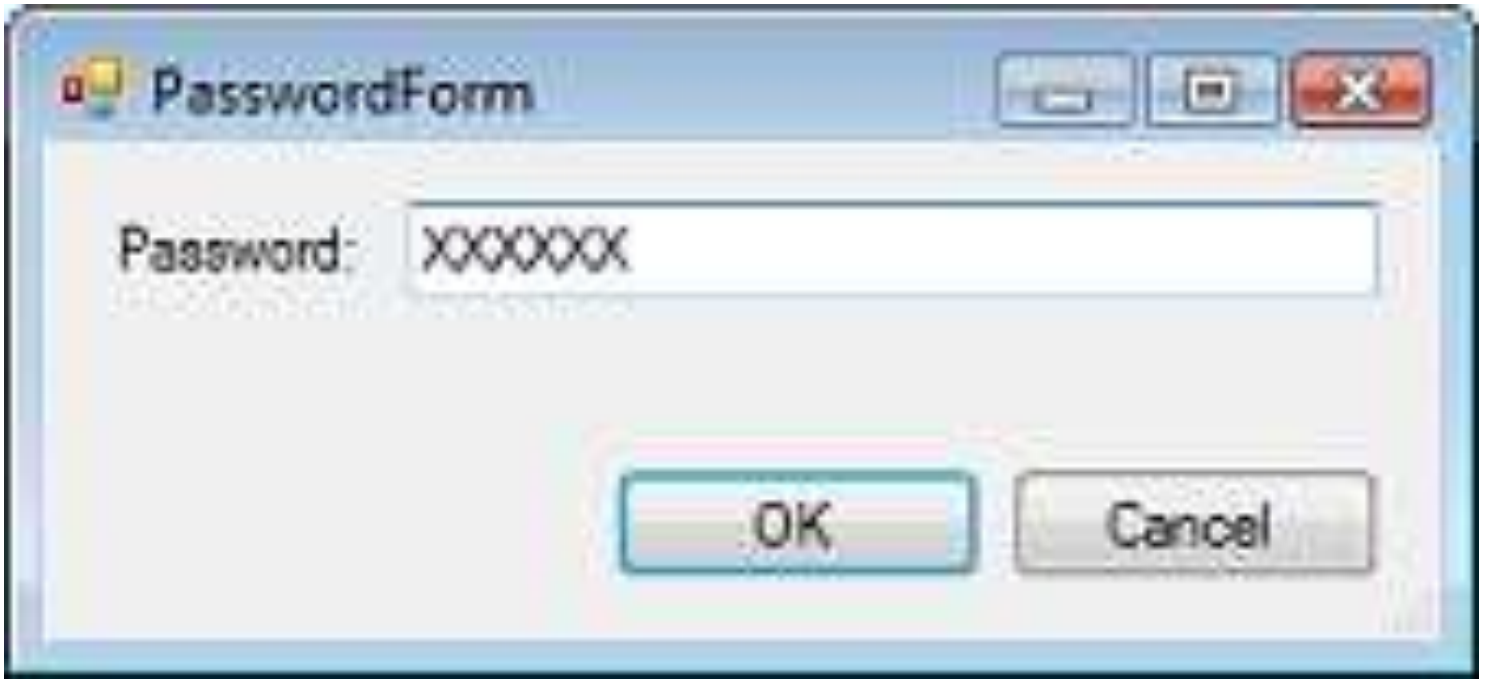
4 228 250 625 možností

4 sekundy

Pětiznakové heslo

1 078 203 909 375 možností

18 minut



Šetiznakové heslo

274 941 996 890 625 možností

3 dny

Sedmiznakové heslo

70 110 209 207 109 375 možností

2 roky

Osmiznakové heslo

17 878 103 347 812 890 625 možností

576 roků

Devítiznakové heslo

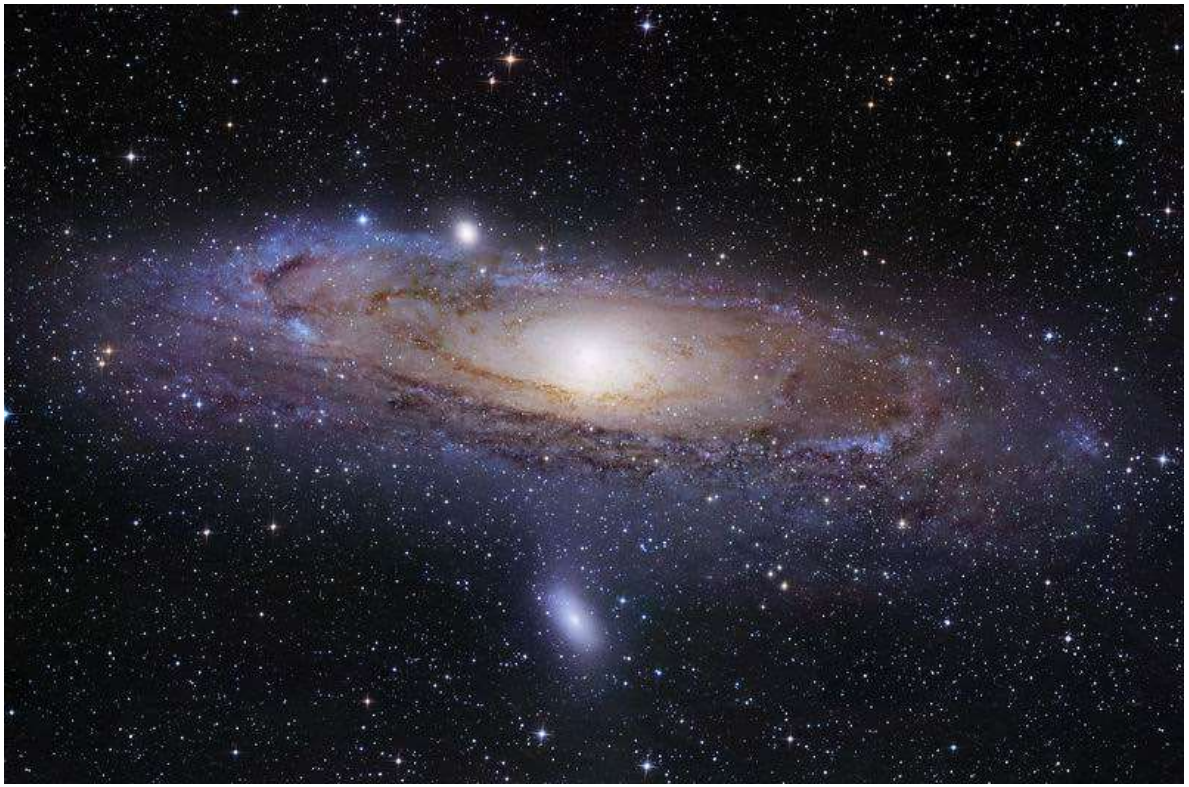
4 558 916 353 692 287 109 375

147 tisíc let

Desetiznakové heslo

1 162 523 670 191 533 212 890 625

37,5 miliónu let



MD5

STRING

AFFE

f971d1254e033dbec7373c7330041327

MD5

Rainbow Tables

Chyby, které za nás udělali jiní

Ing. Tomáš PŘIBYL
konzultant a publicista
tomas.pribyl@seznam.cz
www.kosmonaut.cz

Přednášející:
Ing. Tomáš Přibyl

Konzultant a publicista

na volné noze.

Publikační a přednášková

činnost v Česku

i v zahraničí.

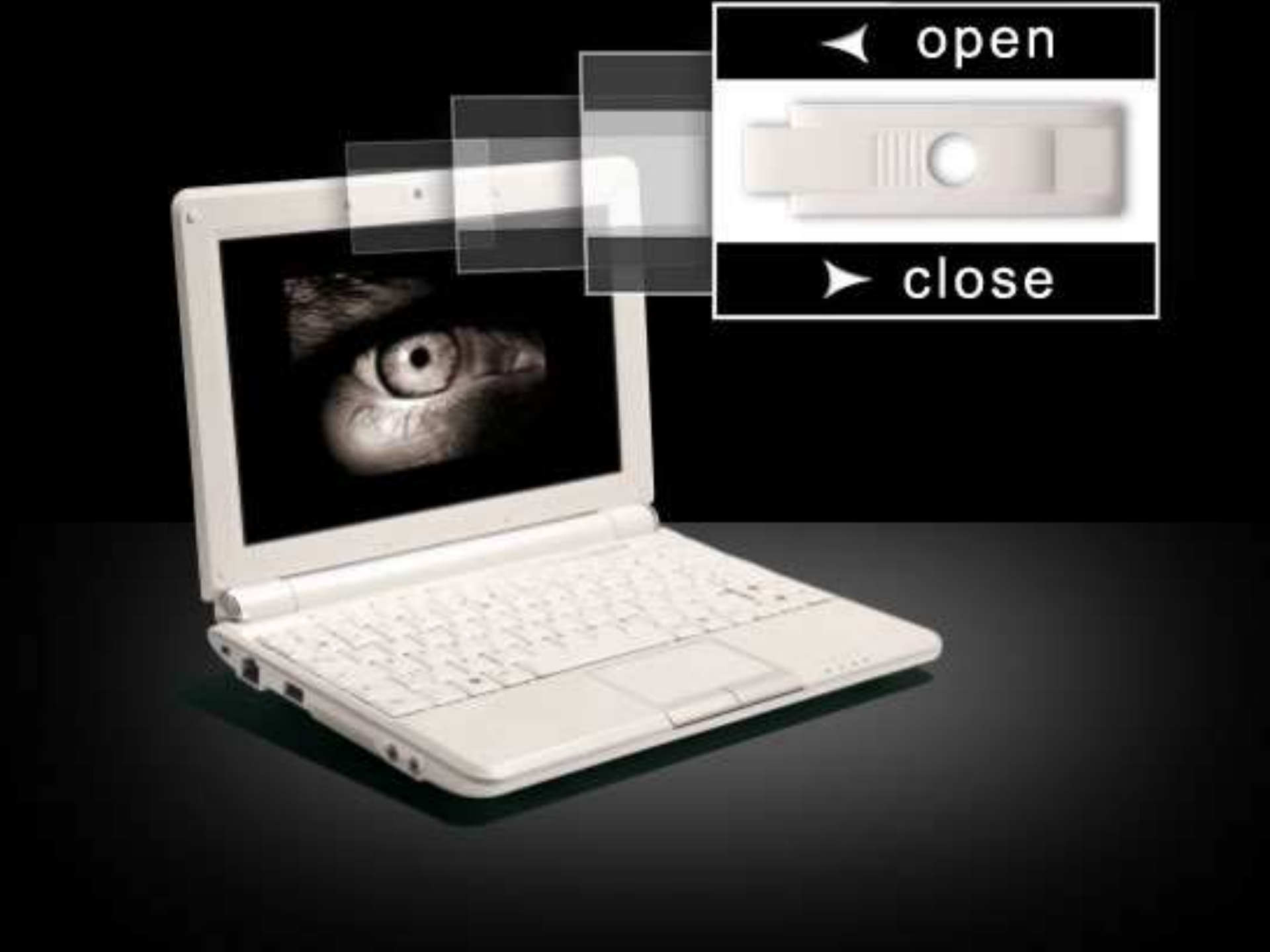
www.kosmonaut.cz

Informační bezpečnost

Informační bezpečnost představuje ochranu informací ve všech jejich formách a po celý jejich životní cyklus - tedy během jejich vzniku, zpracování, ukládání, přenosu a likvidace.

DÁTE RUKU DO OHNĚ, ŽE SE TO NESTANE VÁM?


Gamtec


open
close

Počítačový opravář zneužíval webkamery ke šmírování žen ve sprše

Americká policie zadržela ve středu v jihokalifornském Fullertonu opraváře počítačů, kterého podezřívá z tajné instalace programů, jež mu umožňovaly přes webovou kameru sledovat sprchující se nebo svlékající se ženy. Informovala o tom agentura AP.

čtvrtek 9. června 2011, 16:18

FOTO: Profimedia.cz

Policie se začala případem zabývat poté, co jistý otec upozornil na podezřelé zprávy, které se objevovaly na dceřině počítači. Dvacetiletý technik Trevor Harwell údajně instaloval na počítače s operačním systémem Mac OS X od společnosti Apple program, díky kterému získal kontrolu nad integrovanou webovou kamerou.

Zmíněný software upozorňoval na smyšlenou závadu na "vnitřním senzoru" a doporučoval uživatelům "umístit notebook na několik minut do blízkosti horké páry, aby se senzor vyčistil". Chybové hlášení přimělo některé oběti vzít laptop do koupelny během sprchování.

Za zrcadlo bytu v paneláku dal webkameru a sledoval nájemníky

Reality show, v nichž jsou lidé neustále snímáni kamerami, dnes už v televizi nikoho nepřekvapí. Ale aby se člověk sám stal nedobrovolně hlavní hvězdou soukromé show, to je úplně jiné kafe. Přesně to se stalo čtveřici mladých lidí, kteří si pronajali byt na Vančurově ulici v Jihlavě. Když při škádlení v koupelně rozbili zrcadlo, blikala na ně za ním skrytá webkamera.

▲ ilustrační foto

FOTO: Jaroslav Soukup, Novinky

čtvrtek 29. srpna 2013, 13:07 - Jihlava

Kamera přenášela signál o patro níž, kde bydlel majitel bytu, který podle vyšetřovatelů čtveřici sledoval.

„Prostor kamerou sledoval minimálně od loňského září až do začátku ledna, kdy se na celý případ přišlo při náhodné strkanici v koupelně. Webkamera snímala celou místnost. Když to nájemníci zjistili, ihned se obrátili na policii. Následně jsme na místě provedli domovní prohlídku, zajistili jsme u podezřelého třiapadesátiletého muže několik desítek datových nosičů a také výpočetní techniku. Posléze byl na základě zjištěných důkazů obviněn z poškozování cizích

Soud řeší šmírování tajnou kamerou v koupelně. Nájemníci žádají odškodné

13. ledna 2014 17:10

V Jihlavě v pondělí začal soud s třiapadesátiletým Lubošem V., který šmíroval v pronajaté části svého domu kamerou nájemníky v koupelně. Hrozí mu až dva roky vězení. Nájemníci požadují i odškodné. Majitel bytu se brání tvrzením, že kameru za zrcadlem měl už roky kvůli dceři.

Obžalovaný Luboš V. (vlevo) při čekání na zahájení hlavního líčení okresního soudu v Jihlavě. | foto: Petr Lemberk, MAFRA

Webkamerou za zrcadlem koupelny tajně sledoval nájemníky zřejmě celé roky. Pokoje v prvním patře svého domu na Dolině pronajímal mladým dívkám a párům.

"Už při prvním telefonátu při domlouvání nájmu zdůrazňoval, že preferuje mladé dívky a páry, že se koupají spolu, kvůli úspoře, ale jak se ukázalo, nebylo to jen kvůli úspoře," řekl před soudem bývalý

Koho kamera zachytila?

6. května 2008

Na zabavených záznamech

Two women Bulgarian students find hidden cameras in apartment near Westchase

Jessica Vander Velde, Times Staff Writer

Wednesday, July 27, 2011 12:59pm

TAMPA — The tiny cameras were hidden in smoke detectors and motion sensors, placed in the bedrooms and bathrooms of a west Hillsborough apartment.

Late Monday, two Bulgarian women discovered the covert cameras in their apartment. And now the Bulgarian students are afraid their every move — from sleeping to showering — may have been broadcast on the Internet.

The Hillsborough County Sheriff's Office is investigating and says detectives have recovered some equipment and are following several leads.

Bay News 9

Vanya Samokovareva, 22, left, and roommate Ralitsa Dzhambazova, 23, stand in front of a shower in their apartment where a camera was aimed.

However, between Tuesday night — when a report about the episode appeared on Bay News 9 — and Wednesday morning when detectives returned, some of the electronic equipment was removed, said sheriff's spokesman Larry McKinnon.

The women didn't answer their door Wednesday, but in an interview Tuesday with Bay News 9 said their landlord has a key to the apartment.

RELATED NEWS/ARCHIVE

Hidden cameras in Bulgarian women's apartment were not recording, deputies say
More than a Year ago

Bulgarian women who found cameras had modeled for landlord's pizza business
More than a Year ago

Hidden cameras found in Tour Down Under village's portable toilets

THE ADVERTISER • JANUARY 21, 2014 5:52PM

POLICE say they found "inappropriate images" on the memory card of a hidden camera taken from the portable male toilet at the Tour Down Under village in Victoria Square yesterday.

Tiny cameras hidden inside clothes hooks on the back of the toilet doors were found in the male and female toilet blocks.

SA Police e-crime section officers say they have downloaded images from the camera taken from the male toilets but the other camera was faulty.

"The card from the camera located in the female toilet was faulty and nothing can be retrieved from this," a police spokesman said

Worker admits hiding spycam in Omni Hotel bathroom

Posted: Jul 28, 2012 4:19 AM
Updated: Jul 28, 2012 4:32 AM

Video Report By Richard Allyn, Reporter - bio | email

SAN DIEGO (CBS 8) - A worker for the Omni Hotel has resigned after he admitted hiding a spycam in a public bathroom, and police say in this case they can't do anything about it.

In this News 8 video story, Richard Allyn explains why even though the employee was caught red-handed, police had to close the case without filing charges.

Starbucks Sued for Hidden Spy Camera Found in Bathroom Filming Toilet

By Nadine DeNinno
on September 19 2011 5:37 PM

Starbucks is being sued after a father and his five-year-old daughter found a hidden spy camera secretly filming them using the toilet in a bathroom at a branch in Washington D.C.

William Yockey was visiting the Starbucks near the National Mall in late Aug. when his daughter found the small surveillance camera hidden under the sink filming the toilet area of the unisex bathroom.

Police were contacted immediately and confiscated the camera from the Starbucks.

According to the civil suit, the Yockey family is suing Starbucks for $1 million for invasion of privacy, negligence, intentional infliction of emotional distress and negligent hiring, training and supervision, citing permanent and continuing emotional pain and suffering, humiliation, embarrassment and great emotional distress.

It's not about money, it's not about focusing on that at all, it's just about getting Starbucks to pay attention in this is happening nationwide, Lindsay Yockey told ABC News affiliate WJLA regarding Starbucks' attempts to dismiss the case. Public records show Starbucks had requested to dismiss the case, though it was overturned by a judge.

Spy Cam Found Taped to Bathroom on AA SFO-JFK Flight

Big news here in Kansas City (MCI) on Sunday as an AA 767 flight from SFO – JFK made an emergency landing after a spy cam was founded taped inside one of the bathrooms. The plane was evacuated and searched upon landing and a "small flash drive functioning as a camera" was found taped inside one of the lavatories. According to NBC News:

> The device found on the JFK-bound 767 was initially described to NBC News by a senior law enforcement official as a "flash drive." Later, senior government officials said the device was taped to part of the bathroom. An preliminary inspection of the device showed it was actually a camera disguised as a flash drive, the officials said. Security officials, including the FBI in Kansas City, were working to determine who the device belongs to.

Another SpyCam'er Shoots Himself - Darwin Award

The Wallingford Police Department released a photograph of the person who they said they would like to speak with after a camera was discovered inside a Walmart dressing room in early June.

Click to enlarge.

Police said the camera was set up inside the dressing room and was only recording for a short period of time before it was discovered by an employee.

Police said there was no indication that anyone was actually filmed while undressing.

He is described as a man in his early 20s and was wearing a light green-striped shirt and a Hartford Whalers tan colored hat.

NSW Police last week released a picture of a man they believe may have planted a hidden camera in a Sydney clothing store change room. *Photo: Supplied/NSW Police*

Peeping-Tom Fail Man Setting Up Spy Cam In Store's Dressing Room Accidentally Takes Pics Of Himself

Posted by LukesCorner.net on January 6, 2010 at 8:44am View Blog

DailyMailCo.UK: When a balding peeping tom set up a camera in a supermarket changing room he thought he would capture images of naked customers trying on clothes.

The man, aged in his 30s, was careful to conceal the camera in a light fitting in the Asda changing room before slipping away and waiting for the results.

Greeley Police Search For Changing Room Peeping Tom

August 1, 2012 11:00 PM

The peeping tom suspect was captured on video before he installed a hidden camera in the family changing room on Sunday. (credit: Greeley Police)

Related Tags: Family Fun Plex, Greeley, Hidden Camera, Peeping Tom

GREELEY, Colo. (CBS4)- Police in Greeley are searching for a man who installed a hidden camera in the family changing room at the Family Fun Plex.

A woman discovered the hidden camera at the recreation center on Sunday. Police removed the camera and have examined the video for possible evidence.

"It was concealed inside of an air freshener container. The patron, a female patron located it and could see that it just didn't look like it was quite right," said Greeley Police spokeswoman Susan West.

VĚŠÁK SE SKRYTOU KAMEROU H001

špionážní mini kamera ve věšáku

- možnost zvolit režim: videozáznam nebo fotosekvence (každých 5 minut jedna fotografie)
- záznam ukládá na paměťovou micro SD kartu (max. 16 GB) ve vysokém rozlišení 1280×960 ve formátu AVI
- rozměry: 11,8×3,6×6 cm
- doba provozu: až 90 min nahrávání
- dobíjení: USB kabelem

NÁKUP BEZ PENĚZ

99

2 759,99*

749,99

899,99*

See larger image

Share on

Wholesale - Clothes Hanger HD Hidden Camera with Motion Detection 1280x960 High quality Mini Spy DVR Pinhole Cam

Sold by Tinydeals Technology Co,Ltd

3 Customer Reviews | 83 Transactions

Unit Price: **US $14.1 - 15.0** / Piece Reference Currency

Wholesale Price:

Qty	Price
1 - 4	US $15.00
5 - 9	US $14.70
10 - 19	US $14.40
20 +	US $14.10

Quantity: 1 Piece **9598** in Stock (Stock in: CN)

Shipping Cost **Free Shipping** to Czech Republic Via SINGAPOREPOST

Delivery Time: 12-22 days

Processing Time: Ships out within 1 days

Total Cost **US $15.00**

Buy it Now | Add to Cart

Add to Favorite Items

See larger image

Share on

Wholesale - Clothes Hanger HD Hidden Camera with Motion Detection 1280x960 High quality Mini Spy DVR Pinhole Cam

Sold by Tinydeals Technology Co,Ltd

3 Customer Reviews | 83 Transactions

Unit Price: **US $14.1 - 15.0** / Piece Reference Currency

Wholesale Price:

Qty	Price
1 - 4	US $15.00
5 - 9	US $14.70
10 - 19	US $14.40
20 +	US $14.10

Quantity: 1 Piece **9598** in Stock (Stock in: CN)

Shipping Cost **Free Shipping** to Czech Republic Via SINGAPOREPOST

Delivery Time: 12-22 days

Processing Time: Ships out within 1 days

Total Cost **US $15.00**

Buy it Now | Add to Cart

Add to Favorite Items


water proof
hidden camerus


1, 5 Wednesday 22:03 PM
LIVE
DOCUMENTARY, 2010
PM 10:00~11:00
INPUT
SETUP
FAVORITE
Premium
NETFLIX
huluPLUS
YouTube
MLB.TV
twitter
LG Apps
HOT
NEW
Amazing ad...
ShootTheArrow
Puzzle Game
Natural Object
Gems Quest
Music Lesson
Search
LG Apps
Web Browser
Media Link
Shoot the Arrow
Fruit Puzzle
My Apps

Is your TV watching you? Security alert over Samsung's Smart TV as hackers claim they can access its hard drive and seize control of built-in cameras

- **Security experts reveal they have been able to gain access to the device and scour its hard drives and connected drives for information**
- **They claim to have 'complete root access' allowing them to install malicious software that could monitor its cameras and microphones**
- **More and more devices that connect to the Internet are leaving unwitting consumers vulnerable to such hacking attacks**

By DAMIEN GAYLE

PUBLISHED: 09:51 GMT, 17 December 2012 | **UPDATED:** 11:35 GMT, 17 December 2012

172 View comments

Samsung's Smart TV could used by hackers to watch everything that happens in your living room by gaining access to the device's built-in camera and microphones, it has been claimed.

Malta-based security firm ReVuln posted a video showing how its researchers had learned to crack the television to access its settings - including any personal information stored on it.

'We can install malicious software to gain complete root access to the TV,' they claim in the video.

Samsung Smart TV security hole allows hackers to watch you, change channels or plug in malware

by Lisa Vaas on December 12, 2012 | 5 Comments

FILED UNDER: Data loss, Featured, Malware, Privacy, Security threats, Vulnerability

Did your Samsung Smart TV just switch channel?

Don't blame the dog for stepping on the remote control - there's a remote possibility it could be hackers who've hijacked your smart TV.

Researchers with Malta-based security consultancy and bug seller ReVuln have found a vulnerability in an unspecified model of a Samsung LED 3D TV that they exploited to get root access to the TV and any attached USB drives.

In a video titled "The TV is Watching You", ReVuln shows a Samsung TV screen with which the researchers systematically fiddle.

Barnaby Jack

„Zabiják by nepotřeboval jinou zbraň než notebook a vražda by po sobě nenechala žádné hmatatelné stopy ani vražednou zbraň.“

University of Washington, Raven II

Researchers mount cyber attacks against surgery robot

Posted on 28 April 2015.

A group of researchers from University of Washington have tested the security of a teleoperated robotic surgery system created by their colleagues, and have found it severely lacking.

"Teleoperated surgical robots will be expected to use a combination of existing publicly available networks and temporary ad-hoc wireless and satellite networks to send video, audio and other sensory information between surgeons and remote robots. It is envisioned these systems will be used to provide immediate medical relief in under-developed rural terrains, areas of natural and human-caused disasters, and in battlefield scenarios," the researchers noted, and asked: "But what if these robotic systems are attacked and compromised?"

Not many researchers attempted to answer that question, so this group decided to test a "surgery robot" dubbed Raven II, and discovered that it can be hijacked, disabled, have its instructions changed, its failsafes removed or overriden, and its motions impacted on.

"Telerobotic surgery is envisioned to be used in extreme conditions, where robots will have to operate in low-power and harsh conditions, with potentially lossy connection to the internet. The last communication link may potentially even be a wireless link to a drone or a satellite, providing connection to a trusted facility," they explained, adding that two attack vectors can be used: endpoint compromise, and network and communication-based attacks.

They focused on the latter, pointing out that the most likely point of attack would be between the network uplink and a surgical robot. "Since communication will likely be wireless, on-the-field attackers will be able to disrupt the link or manipulate traffic contents," they noted.

Nepřítel od vedlejšího stolu

Hardware keyloggers found in Manchester library PCs

Spy on the wire gets your mad up proper

By John Leyden, 15th February 2011

Hardware keyloggers have been discovered in public libraries in Greater Manchester.

Two USB devices, attached to keyboard sockets on the back of computers in Wilmslow and Handforth libraries, would have enabled baddies to record every keystroke made on compromised PCs. It's unclear who placed the snooping devices on the machines but the likely purpose was to capture banking login credentials on the devices prior to their retrieval and use in banking fraud.

A third detected device was discovered but disappeared before it was turned over to local police, the *Manchester Evening News* reports.

Many members of the public use library computer access either for convenience or because they don't have a computer at home. The targeted libraries are in up-market districts on the southern outskirts of Greater Manchester. A BBC report on the incident has footage of one of the affected computers. The presumed scam, which had been going on for an as yet undetermined period, was only rumbled after staff examined one of the compromised PCs, which had begun misbehaving.

Library staff have been advised to keep a close eye on computers to help prevent the reccurrence of similar incidents in future. In addition, rules have been revised so that USB keyboards are plugged into the more visible front ports of a computer rather than its rear. PCs in Manchester libraries come fitted with net-nanny software and accounts that limit the ability of users to install software on machines. Cybercrooks have apparently found a way around these restrictions using hardware keyloggers, which are readily available at prices of around £30 or less.

RELATED STORIES

'Bogus IT guys' slurp £1.3m from Barclays: Cybercops cuff 8 blokes

Punter bags 500GB SSD, finds 128MB Flash inside

Updated Testing confirms Samsung keylogger rumour just a false alarm

Qld police warn against Windows service scam

Inmate hacker locks down jail computers

Former lottery infosec head accused of hacking computers to buy winning ticket

Posted on 14 April 2015.

The former head of information security at the Multi-State Lottery Association (MUSL), who was arrested in January 2015, stands accused of having tampered with the computer used for drawing winning lottery numbers and of having purchased the winning lottery ticket after, even though he, as an employee of the association, isn't permitted to.

According to additional claims included in a recent filing, Eddie Raymond Tipton, 51, has apparently used a USB flash drive to install a malicious software on the aforementioned computer, which would allow him to manipulate the outcome of the draw.

The computer in question is located in the "drawing room" and is not connected to the Internet, so in order to install the software Tipton needed to gain physical access to the machine.

The room is monitored by a camera that has also been tampered with on the day that Tipton allegedly entered the room and installed the malware on the computer. Instead of recording continuously, the camera was made to record only one second per minute.

The prosecution says Tipton used a rootkit to perform the changes on the computer, and that the program deleted itself after doing the work. In 2010, when the compromise happened, the Multi-State Lottery Association apparently did not have the ability to check for rootkits installed in their system, so this claim could be difficult to prove.

As the trial has been rescheduled for July, Iowa Lottery CEO Terry Rich issued a statement with the hope of reassuring lottery players that their systems are now clean.

"There will always be someone trying to beat the system. The lottery industry has and will continue to update its security procedures as we identify vulnerabilities to protect against them. We've introduced additional layers of security and even more separation of duties at our lottery because of what we've learned in this case, and that's ultimately been a positive outcome. We also urged that the Multi-State Lottery Association (MUSL), the vendor organization for which Eddie Tipton worked, put additional security procedures in place and that has occurred, with more underway," he noted.

Takový normální zaměstnanec

Průměrný evropský zaměstnanec si domů každý týden odnese 11 dokumentů.

[McAfee]

58 procent zaměstnanců si při ukončení pracovního poměru odnáší „výslužku“. Devadesát procent z nich přitom uvádí, že by si ji neodnesli, kdyby to měli alespoň trochu znesnadněné.

[Ponemon Institute]

Největší průšvih? Zvědavost!

Hledá se – živý nebo mrtvý

Computer glitch blamed for 'hundreds' of wrongful arrests

Download audio | show transcript

Sunday 15 December 2013 8:05AM

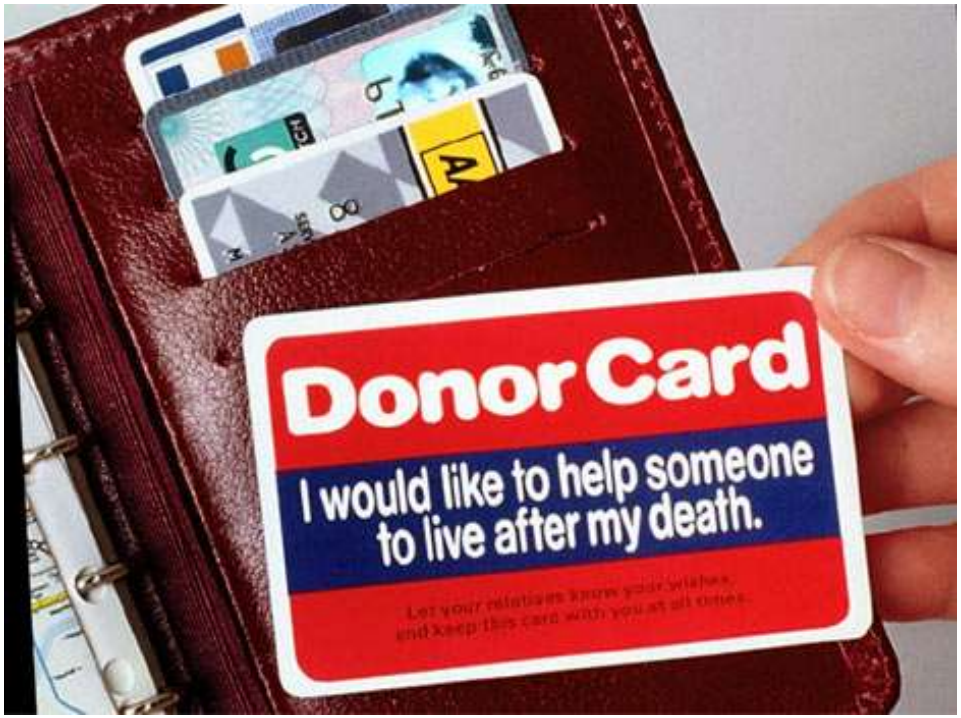
IMAGE: NSW POLICE HAVE WRONGFULLY ARRESTED MANY TEENS BECAUSE OF A GLITCH IN THE POLICE COMPUTER SYSTEM. (NSW POLICE)

A class action in the Supreme Court will look at whether NSW police wrongfully arrested and detained a number of teens due to a long standing glitch in the NSW Police computer system. Lawyers say hundreds more might also have been 'kidnapped' but NSW police have declined to reveal the full extent of the problem. ***Wendy Carlisle*** *investigates.*

Říznout vedle…

Vinou špatné konverze dat došlo u 25 dárců k odběru jiného orgánu, než s jakým dali souhlas.

Celý problém se týkal 800 tisíc dárců!



Nemocnice omylem „pohřbila“ dvě stě pacientů. Lidská chyba, omluvila se

14. srpna 2014 14:27

Nemocnice Elizabeth Austinové ve druhém největším australském městě Melbourne se ve čtvrtek omluvila za to, že omylem rozeslala zprávy o úmrtí 200 svých pacientů, kteří jsou stále naživu. Informaci rozeslala prostřednictvím faxových zpráv jejich rodinným lékařům, jeden z nich stihl rodině i kondolovat.

Ilustrační fotografie | foto: Profimedia.cz

Kopírky Xerox mění čísla, možná i na vašich dokumentech

7. srpna 2013 16:07, aktualizováno 8. srpna 7:46

Německý výzkumník David Kriesel objevil specifickou chybu u kopírovacích strojů Xerox. Náhodně zaměňovaly čísla na dokumentech, pokud byl nastaven určitý mód skenování.

Další 2 fotografie v galerii

Tiskový stroj řady Xerox WorkCentre 7500 | foto: Xerox

Minulý týden doktorand David Kriesel z Bonnské univerzity v Německu zveřejnil překvapivé zjištění, které ukazuje chybu u některých multifunkčních systémů Xerox WorkCentre. Ty při úspornějším nastavení mohou při skenování zaměnit některé číslovky za jiné, což může mít dalekosáhlé následky. Xerox již o chybě ví a včera vydal doporučení, aby lidé využívali kvalitnější nastavení, která nepoužívají kompresi.

Nebezpečné klávesnice

[Wireless Optical Desktop 1000 a 2000]

News

Two charged with hacking LA traffic lights

Disruption occurred just before August job action

By Robert McMillan

January 10, 2007 12:00 PM ET Add a comment

IDG News Service - Two men have been charged with illegal computer access after they allegedly hacked into the Los Angeles city traffic center to turn off traffic lights at four intersections last August.

The two men, both engineers with the city's Automated Traffic Surveillance Center, accessed city computers on the morning of Aug. 21, and were able to turn off signal control boxes just hours before a job action by city engineers, the Los Angeles district attorney said in a statement released late last week.

The accused were able to bar other city employees from accessing the computer system to put the lights back online. No accidents were reported, but it took four days to fix the city's traffic control system, the statement said.

Gabriel Murillo, 37, and Kartik Patel, 34, are both charged with unauthorized access of a computer. Murillo is also charged with identity theft, and Patel faces four counts of disruption or denial of computer services.

Zavirovaný digitální fotorámeček

[Samsung SPF-85H]

Car hacking and hijacking is too easy, report says

Posted on 10 February 2015.

A report released on Monday by US Senator Edward Markey has confirmed what we already suspected: automobile manufacturers have yet to effectively deal with the threat of hackers penetrating vehicle systems, and the driver and vehicle information they collect and share is not adequately protected.

"Drivers have come to rely on these new technologies, but unfortunately the automakers haven't done their part to protect us from cyber-attacks or privacy invasions. Even as we are more connected than ever in our cars and trucks, our technology systems and data security remain largely unprotected," said Senator Markey, a member of the Commerce, Science and Transportation Committee.

The report, based on responses from BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (with Audi), and Volvo, has revealed that:

- Nearly 100 percent of vehicles on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions.
- Most automobile manufacturers were unaware of or unable to report on past hacking incidents.
- Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across the different manufacturers.
- Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most said they rely on technologies that cannot be used for this purpose at all.
- Automobile manufacturers collect large amounts of data on driving history and vehicle performance.
- A majority of automakers offer technologies that collect and wirelessly transmit driving history information to data centers, including third-party data centers, and most did not describe effective means to secure the information.
- Manufacturers use personal vehicle data in various ways, often vaguely to "improve the customer experience" and usually involving third parties, and retention policies – how long they store information about drivers – vary considerably among manufacturers.
- Customers are often not explicitly made aware of data collection and, when they are, they often cannot opt out without disabling valuable features, such as navigation.

Neexistuje bezpečné prostředí

90 procent škodlivých kódů se nachází na seriózních a důvěryhodných stránkách.

Virtuální svět, reálné problémy

Seniorka svou chybou ve hře přišla o půl milionu, následně podala žalobu

28. října 2013

V počítačové hře Lineage lze předměty vylepšovat okouzlením, nese to však i riziko jejich úplné likvidace. Právě to se stalo šedesátičtyřleté ženě z Jižní Koreje, která získala vzácný meč Myung Hwang's Conduct Sword.

(Ilustrační snímek) | foto: Profimedia.cz

Ten lze na trhu prodat za skutečné peníze a jeho cena se pohybuje okolo 30 milionů wonů. Vyjde tedy zhruba na 531 tisíc korun. Žena se však meč pokusila okouzlit a předmět při tom zlikvidovala.

Hráčka se proto obrátila na společnost NC Soft, jenž hru provozuje. Tvrdila totiž, že meč okouzlila omylem. Očarovat prý chtěla jiný předmět a při procesu tak nechtěně zničila právě Myung Hwang's Conduct Sword.

Čína. Otec chtěl „zabít“ syna

Virtuální „vrahy“ si najal čínský otec, aby zabili jeho syna – respektive tedy jeho avatara – v online počítačové hře. Muž, kterého místní tisk identifikoval jen rodovým jménem Feng, si prý dělal starosti s tím, kolik času jeho nezaměstnaný třiadvacetiletý syn tráví na síti a doufal, že když bude ve virtuálním světě zavražděn, odradí ho to od dalšího hraní, napsal zpravodajský server BBC News.

Celé spiknutí ovšem odhalil sám syn, který se protihráčů zeptal, proč po něm tak jdou. Kolik za virtuální vraždu otec zaplatil, zprávy neuvádějí, nicméně experti míní, že vztahy v rodině jeho krok patrně nevylepšil – a asi by ani neodradil mladíka od dalšího hraní. ČTK

Štědré bankomaty

[ATM Tranax Mini Bank 1500]

SECTION 3: PROGRAMMING

3.1 INITIAL SETUP

3.1.1 ACCESSING THE OPERATOR FUNCTION

Step 1

To access the Operator Function menu, hold the <Cancel>, <Clear> and <Enter> keys simultaneously for 2 seconds, release them and press 1, then press 2, then press 3. The timing of this procedure can be difficult at first.

Note: The Operator Function menu can only be accessed when the machine is either in service ("swipe your card" screen) or out of service. If the machine is attempting to connect the host or initializing, you will not be able to use the key commands to access the Operator Function Menu.

If you have trouble accessing the Operator Menu, power off the ATM and then either open the vault door or remove the paper from the printer and power back on. This will force the ATM to the Operator Menu.

Step 2

Once you successfully completed the key combination, you will be prompted to enter a password. There are 3 options for passwords.

- Operator Password (allows access to basic menu structure)
- Service Password (allows access to basic and diagnostic menus)
- Master Password (allows access to all menus including setup parameters)

NOTE: If the machine goes out of service, the error code will not always appear on the screen. If you do not see an error code, enter operator function and go to reports. Look in the error summary for error codes.

Step 2

"ENTER PASSWORD" will be displayed. Enter Master, Service or Operator Password.

Defaults:
Master = 555555
Service = 222222
Operator = 111111

Step 3

When the screen is in current display, press "OPERATOR FUNCTION" key to access the "OPERATOR FUNCTION."

RockYou: dvacet „nej“ hesel

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123
11. Nicole
12. Daniel
13. babygirl
14. monkey
15. jessica
16. Lovely
17. Michael
18. Ashley
19. 654321
20. qwerty

Deset nejoblíbenějších hesel

123 – 3,784 ‰

password („heslo“) – 3,78 ‰

liverpool – 1,82 ‰

letmein („pusť mě dál“) – 1,76 ‰

123456 – 1,63 ‰

qwerty – 1,41 ‰

charlie – 1,39 ‰

monkey – 1,33 ‰

arsenal – 1,11 ‰

thomas – 0,99 ‰

Anonymous se nabourali do mailů syrského prezidenta Asada. Používal heslo 12345

Hackeři z Anonymous zveřejnili korespondenci mezi syrským prezidentem a jeho podřízenými. Mezi maily zaujaly především rady, které Asad dostal před důležitým rozhovorem v americké televizi ABC. Podle nich lze údajně s psychikou Američanů "snadno manipulovat." Asad a jeho okolí pro vstup na účet používali heslo 12345.

Čtěte více o: Sýrie | Asad Bašár | Anonymous | hacker

bzk

ČLÁNEK DISKUSE (55)

Mezinárodní hackerské hnutí Anonymous znovu zaútočilo a jejich cílem se tentokrát stal syrský prezident Bašár Asad.

Internetoví aktivisté se nabourali do jeho elektronické pošty a zveřejnili korespondenci mezi ním a jeho podřízenými.

Největší překvapení vzbudilo vstupní heslo, které Asad a jeho okolí používalo: 12345. Podle jedné studie z roku 2011 jde z hlediska zabezpečení o druhou nejhorší možnou kombinaci.

Syrský prezident Bašár Asad
foto: Reuters

Hackeři napadli web UniCredit Bank. Administrátor měl heslo Banka123

Hackeři v pondělí napadli web UniCredit Bank. Uvedl to server Živě.cz. Útok ale zřejmě nesouvisel se sérií napadení českých webů z minulých dní, byl proveden jiným způsobem. Na rozdíl od předchozích útoků hackeři web nezahltili. Údajně jim pomohlo slabé heslo administrátora stránek, které znělo "Banka123". Na web banky hackeři vyvěsili své prohlášení, stránky vypadly jen na pět minut, píše server.

Dnes 20:23

▲ Web UniCredit Bank

FOTO: unicreditbank.cz

Heslo navěky

28 % nikdy, 22 % občas…

[ElcomSoft]

Nejoblíbenější PIN?

Administrátorská práva

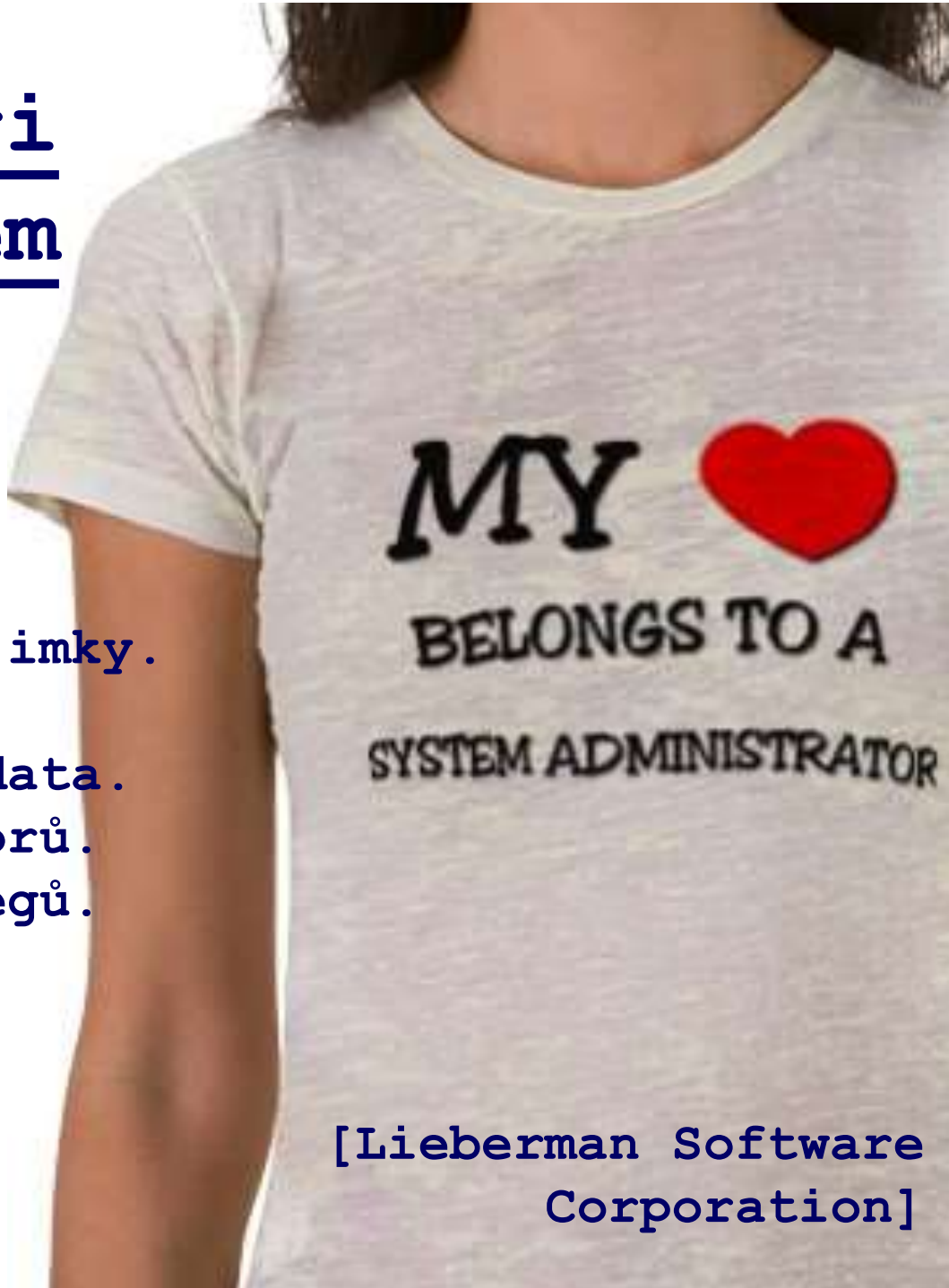
Loni nebylo potřeba:

- **75 procent záplat pro Windows.**
- **100 procent záplat pro IE.**
- **100 procent záplat pro MS Office.**

[BeyondTrust]

Administrátoři jdou příkladem

74 % - zneužití sítě.
54 % - nelegální obsah.
48 % - přiděluje si výjimky.
41 % - sdílená hesla.
29 % - odnáší citlivá data.
25 % - nahlíží do souborů.
16 % - čte e-maily kolegů.
15 % - modifikuje logy.



[Lieberman Software Corporation]

Kostlivci ve skříni

Why Dieselgate Will Be Good For Volkswagen

October 8th, 2015 by Guest Contributor

Originally published on EV Obsession.
By Joseph Nagle, EverCharge

Diesel is dying. Not a slow death, but an immediate one.

Diesel was already on the ropes with the advent of powerful electric vehicles, but now with the Volkswagen scandal it all but seals its fate.

It's not diesel's fault: it's a cleaner-burning fuel than people realize, capable of powering incredibly large, powerful vehicles. There was only one major downside: pollution. While diesel burns cleaner, it still produces carcinogens, soot and nitrous oxide, which can be just as harmful to the environment as traditional gasoline. Now it seems even "clean diesel" wasn't so clean. It was only a matter of time before it was ushered out of the commercial vehicle space. Now it will be forced out rather unceremoniously, leaving electric to take its place.

Volkswagen has become the perfect test case for the future of the auto industry. As the leader in diesel-fueled vehicles and the second-largest automotive manufacturer in the world, VW had to pivot to a new vertical eventually. They were already in the early stages of joining the electric vehicle arms race, having announced three new EV concepts just a few weeks before the scandal broke. Now the world is different, as the ire of the nation comes down on them they need a new flagship to drive them into the future, and that's electric.

When Tesla broke Consumer Reports' ratings system, every major manufacturer was put on notice. When 'dieselgate' broke, it shook the foundation. The traditional fuels of the past are no longer a preferred solution. Electric vehicles cannot be ignored: they are the future. Over the next 3 years the once lopsided EV market is going to explode with options. Nearly every major manufacturer will debut a brand new electric vehicle line. With this new focus on EVs the companies who get an early start will be in the drivers seat.

Windows remains vulnerable to serious 18-year-old SMB security flaw

By Mark Wilson | Published 7 months ago | Follow

18 Comments | Tweet

A serious security hole leaves millions of Windows users open to attack, making it possible to extract encrypted credentials from a target machine. Researchers at Cylance say the problem affects "any Windows PC, tablet or server" (including Windows 10) and is a slight progression of the Redirect to SMB attack discovered by Aaron Spangler way back in 1997.

Redirect to SMB is essentially a man-in-the-middle attack which involves taking control of a network connection. As the name suggests, victims are then redirected to a malicious SMB server which can extract usernames, domains and passwords. Cylance also reports that software from companies such as Adobe, Oracle and Symantec -- including security and antivirus tools -- are affected.

18-year-old bug can be exploited to steal credentials of Windows users

Posted on 14 April 2015.

A new technique for exploiting an 18-year-old bug in Windows Server Message Block (SMB), which would allow attackers to intercept user credentials, had been uncovered by Cylance researcher Brian Wallace.

SMB is a core component in Windows networking, and can be found - and is enabled by default - in all versions of the Windows OS, including Windows 10.

"Redirect to SMB is a way for attackers to steal valuable user credentials by hijacking communications with legitimate web servers via man-in-the-middle attacks, then sending them to malicious SMB (server message block) servers that force them to spit out the victim's username, domain and hashed password," the researcher explained.

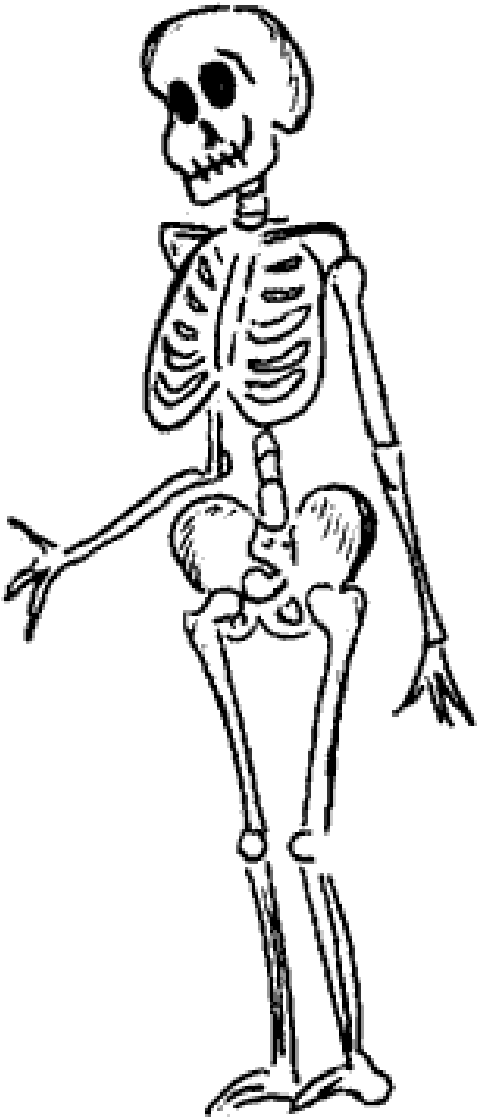
"The Redirect to SMB attack builds on a vulnerability discovered in 1997 by Aaron Spangler, who found that supplying URLs beginning with the word 'file' (such as file://1.1.1.1/) to Internet Explorer would cause the operating system to attempt to authenticate with a SMB server at the IP address 1.1.1.1."

The flaw affects a number of Windows API functions, which are used by a wide range of software features.

Before revealing the existence of the vulnerability to the public, Cylance shared the information with CERT at Carnegie Mellon University and the developers of the many popular applications that are vulnerable, such as Adobe Reader, Apple Software Update, Internet Explorer, several AV solutions and security tools, Box Sync, TeamViewer, and a number of developer tools.

"Redirect to SMB is most likely to be used in targeted attacks by advanced actors because attackers must have control over some component of a victim's network traffic. Malicious ads could also be crafted that would force authentication attempts from IE users while hiding malicious behavior from those displaying the advertising," Wallace pointed out.

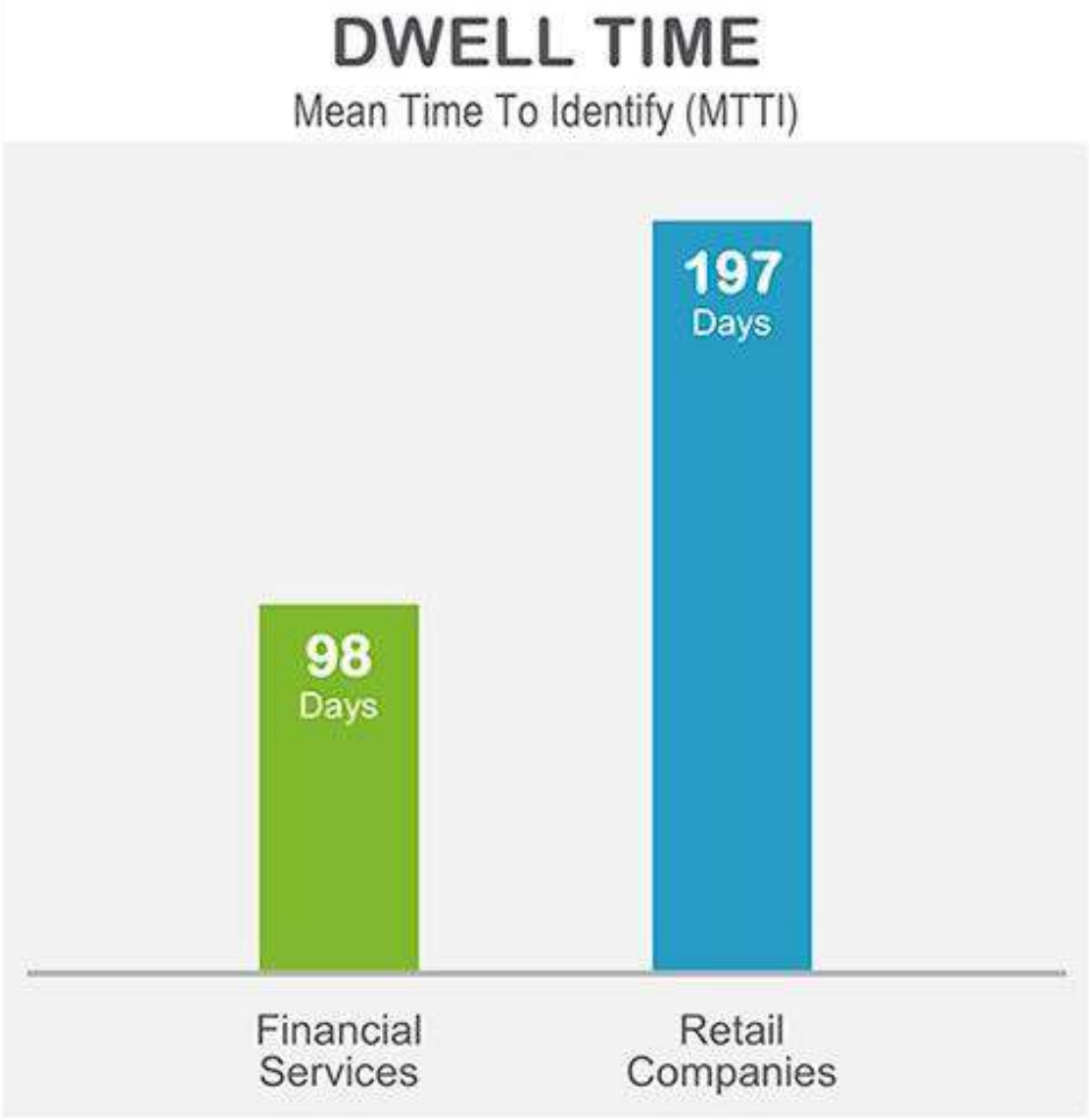
"Less sophisticated attackers could launch Redirect to SMB attacks on shared WiFi access points at locations such as coffee shops from any computer, including mobile devices. We successfully tested this attack on a home network using a Nexus 7 loaded with all required tools."



Can you afford to wait 197 days to detect a threat?

Posted on 20 May 2015.

Financial services and retail organizations agree, advanced threats are the most serious security challenge facing their organizations, shows a new Ponemon Institute study. Despite the concern, both industries struggle to identify these attacks once they are inside their network.



Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers

11 Feb 2014
Virus News

New threat actor: Spanish-speaking attackers targeting government institutions, energy, oil & gas companies and other high-profile victims via cross-platform malware toolkit

Today Kaspersky Lab's security research team announced the discovery of "The Mask" (aka Careto), an advanced Spanish-language speaking threat actor that has been involved in global cyber-espionage operations since at least 2007. What makes The Mask special is the complexity of the toolset used by the attackers. This includes an extremely sophisticated malware, a rootkit, a bootkit, Mac OS X and Linux versions and possibly versions for Android and iOS (iPad/iPhone).

The primary targets are government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists. Victims of this targeted attack have been found in 31 countries around the world – from the Middle East and Europe to Africa and the Americas.

The main objective of the attackers is to gather sensitive data from the infected systems. These include office documents, but also various encryption keys, VPN configurations, SSH keys (serving as a means of identifying a user to an SSH server) and RDP files (used by the Remote Desktop Client to automatically open a connection to the reserved computer).

"Several reasons make us believe this could be a nation-state sponsored campaign. First of all, we observed a very high degree of professionalism in the operational procedures of the group behind this attack. From infrastructure management, shutdown of the operation, avoiding curious eyes through access rules and using wiping instead of deletion of log files. These combine to put this APT ahead of Duqu in terms of sophistication, making it one of the most advanced threats at the moment," said Costin Raiu, Director of the Global Research and Analysis Team (GReAT) at Kaspersky Lab. "This level of operational security is not normal for cyber-criminal groups."

Kaspersky Lab researchers initially became aware of Careto last year when they observed attempts to exploit a vulnerability in the company's products which was fixed five years ago. The exploit provided the malware the capability to avoid detection. Of course, this situation raised their interest and this is how the investigation started.

For the victims, an infection with Careto can be disastrous. Careto intercepts all communication channels and collects the most vital information from the victim's machine. Detection is extremely difficult because of stealth rootkit capabilities, built-in functionalities and additional cyber-espionage modules.

China Is Tied to Spying on European Diplomats

By NICOLE PERLROTH
Published: December 10, 2013

SAN FRANCISCO — Computer breaches at the foreign ministries of the Czech Republic, Portugal, Bulgaria, Latvia and Hungary have been traced to Chinese hackers.

The attacks, which began in 2010, are continuing, according to a report to be released Tuesday by FireEye, a computer security company in Milpitas, Calif.

Though researchers do not name the hackers' targets in the report, The New York Times identified the foreign ministries through email addresses listed on the attackers' web page. A person with knowledge of the investigation, who was not authorized to speak publicly, confirmed that the foreign ministries of the five countries had been breached.

Even as revelations by Edward J. Snowden about surveillance conducted by the National Security Agency and its intelligence partners dominate attention, the FireEye report is a reminder that Chinese hackers continue to break into the computer systems of governments and firms using simple, email-based attacks.

The FireEye report does not link the attacks to a specific group in China, but security experts say the list of victims points to a state-affiliated campaign.

Kybernalita

Nejmenovaná banka v Chicagu

Loupeže na pobočkách:
60 tisíc dolarů.

Krádeže a zpronevěry elektronické – 80 milionů dolarů.

– 1996 –

Hackeři vyplašili svět zprávou o explozích v Bílém domě a zraněném Obamovi

Twitterový účet americké tiskové agentury AP napadli v úterý neznámí hackeři a rozeslali přes něj do světa zprávu, že Bílým domem ve Washingtonu otřásly dvě exploze, při nichž byl zraněn prezident Barack Obama. AP okamžitě pravost zprávy dementovala a účet zablokovala. Také Obamův mluvčí ujistil, že prezidentovi USA se daří dobře.

▲ Barack Obama je zraněn, hlásal falešný vzkaz na twitterovém účtu renomované tiskové agentury.

FOTO: Larry Downing, Reuters

úterý 23. dubna 2013, 22:12 - Washington

"Blesková zpráva: dvě exploze v Bílém domě a Barack Obama je zraněn," hlásal vzkaz na účtu renomované americké agentury, jejíž mluvčí jej však krátce na to popřel. "Náš účet byl napaden hackery," oznámila AP, jejíž žurnalisté v minulosti opakovaně čelili pokusům o krádež počítačových hesel. Její twitterový účet byl ale údajně napaden poprvé.

foxnewspolitics foxnewspolitics
We wish @joebiden the best of luck as our new President of the United States. In such a time of madness, there's light at the end of tunnel
2 hours ago

foxnewspolitics foxnewspolitics
BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP
2 hours ago

foxnewspolitics foxnewspolitics
#ObamaDead, it's a sad 4th of July. RT to support the late president's family, and RIP. The shooter will be found
2 hours ago

foxnewspolitics foxnewspolitics
@BarackObama shot twice at a Ross' restaurant in Iowa while campaigning. RIP Obama, best regards to the Obama family.
2 hours ago

foto: Shutterstock

Stačil jeden falešný tweet a roboti se zbavili akcií za čtyři biliony

24. dubna 2013 11:36

NEW YORK - Falešná zpráva agentury AP, kterou vypustili na sociální síť Twitter hackeři, opět poukázala na zranitelnost finančních trhů ze strany počítačových obchodních programů. Kvůli poplašné novince o explozích v Bílém domě se propadl do ztráty i hlavní kurz indexu Dow Jones Industrial.

Během dvouminutové prodejní horečky se podařilo automatizovaným programům na amerických burzách vymazat zisk za zhruba 200 miliard dolarů (téměř 4 biliony korun). Stalo se tak poté, co se na twitterovém účtu agentury AP objevila zpráva, že Bílým domem ve Washingtonu otřásly dvě exploze, při nichž byl zraněn prezident Barack Obama. **ČTĚTE VÍCE**

Hackers hit execs for insider info to gain stock market advantage

Posted on 02 December 2014.

FireEye's researchers have identified yet another hacking group. Dubbed FIN4, the hacking crew seems to be comprised of native English speakers with "deep familiarity with business deals and corporate communications, and their effects on financial markets."

Their targets are top executives, legal counsel, outside consultants, regulatory, risk, and compliance personnel, advisors and researchers who are believed to have inside knowledge about potential mergers and acquisitions, deals and new research results.

Operational since at least mid-2013, the group has targeted these individuals in over 100 publicly traded companies and advisory firms, the majority of which are in the healthcare and pharmaceutical industries.

"We believe FIN4 heavily targets healthcare and pharmaceutical companies as stocks in these industries can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues," the researchers shared.

Their weapons of choice are extremely well crafted and personalized spear-phishing emails that are meant to lead recipients to phishing pages impersonating the Outlook Web App login page and trick them into sharing their Microsoft Outlook login credentials.

"FIN4 knows their targets. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies," the researchers explained in a whitepaper published on Monday.

"FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials."

Kdo útočí?

Kyberzločinci.

Aktivisté.

Zoufalci.

Státy.

Kyberzločin - výnosnější byznys než drogy

13. 9. 2011 10:42, autor: duk
aktualizováno 13. 9. 2011 15:28

Praha – Každý den se stane obětí kyberzločinu více než jeden milion lidí. Vyplývá to ze studie Norton Cybercrime Report, kterou vydala společnost Symantec zabývající se zabezpečením počítačů. Celkové ztráty plynoucí z kyberzločinu a výdaje na řešení problémů s ním spojených podle studie ročně vystoupají na 114 miliard dolarů. Ztracený čas si oběti zločinů po síti cení na 274 miliard dolarů. Náklady spojené s počítačovou kriminalitou už dokonce převýšily objem světového trhu s drogami, jako je například heroin nebo kokain.

Ilustrační foto

Se zločinem se už na internetu setkalo 69 procent dospělých uživatelů, z toho dvě třetiny v posledním roce. Každou vteřinu se stane obětí zločinu 14 dospělých. Nejčastějším druhem počítačové kriminality jsou viry a škodlivé kódy, jako jsou například trojské koně a spywary. Kyberzločinci si přitom začínají stále častěji všímat mobilních telefonů. Počet útoků na chytré telefony vzrostl loni v porovnání s předchozím rokem o 42 procent.

Cybercrime Can Give Attackers 1,425% Return on Investment

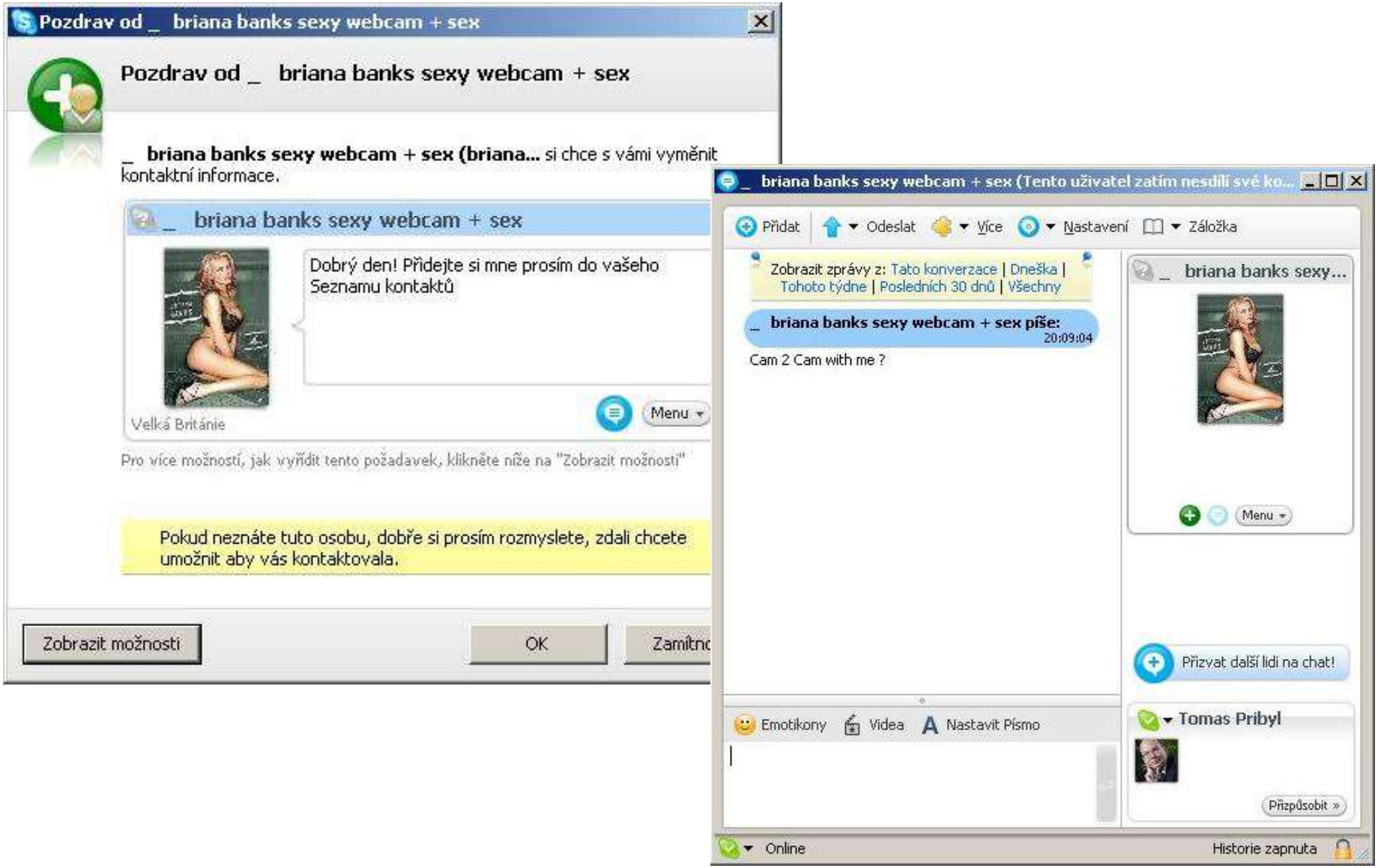
Going rates on the black market show ransomware and carding attack campaign managers have plenty to gain.

While security professionals often find it difficult to prove return on investment, a standard ransomware campaign could earn an attacker a 1,425 percent ROI, according to a report released today by Trustwave.

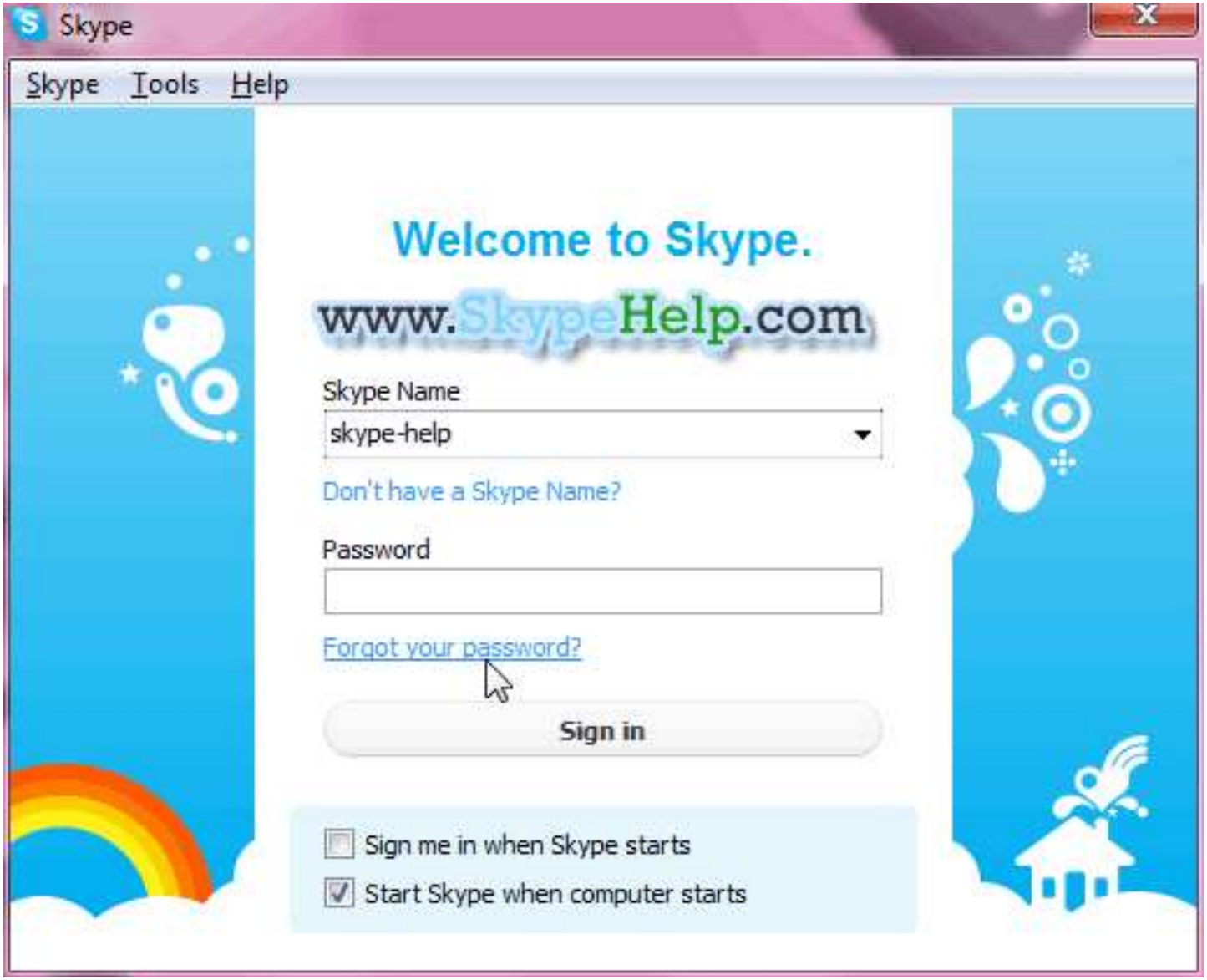
"We're showing what the motivation for and value of a cybercrime is," says Charles Henderson, vice president of managed security testing at Trustwave. "To my mind, if you're going to defend against cybercrime, you need to understand" the attackers' motivation.

Trustwave's report is based on study of the black market cybercrime economy and direct investigations of 574 data breaches across 15 countries in 2014.

Krádeže minut



Reset Password



Hi there,

Password successfully changed

Your new Skype password has been set.

You can now view your attached call history and inscturtions how to change your account settings.
If the changes described above are accurate, no further action is needed. If anything doesn't look right, follow the link below to make changes: **Restore password**

Talk soon,
The people at Skype

Getting help for Skype

While you cannot reply to this email, you can contact us through our **help section** for assistance.
You can also visit **our forums**.

Protect Your Password

Skype staff will NEVER ask you for your password via email. The only places you are asked for your password are when you sign in to Skype or on our website if you want to buy something or check your account. You will always sign in via a secure connection, and we ask you to ensure that the address in your browser begins exactly like this **https://secure.skype.com** It should also show a little padlock symbol to indicate the secure connection.

Policejní virus dál straší Čechy

Už od minulého roku se internetem šíří takzvaný policejní virus, prostřednictvím kterého se počítačoví piráti snaží v lidech vzbudit strach z trestního stíhání. Tento trojský kůň infikovaný stroj zcela zablokuje a za jeho odemčení požaduje výkupné v řádech tisíců korun.

pondělí 4. listopadu 2013, 12:27

▲ Policejní virus se šíří internetem už od loňského roku.

FOTO: Novinky

„Tento trojský kůň po aktivaci upozorní dotčeného uživatele, že byl jeho počítač Policií České republiky zablokován. Uvedeným důvodem je porušování autorského práva, nakládání s materiály s dětskou pornografií či šíření spamu. Součástí tohoto upozornění je i nabídka uživateli o možnosti složení kauce v podobě zaplacení pokuty," popsala Novinkám chování nezvaného návštěvníka policejní mluvčí Eva Kropáčová.

Pozor!

IP: [redacted]
Umístění: **CZ,Czech Republic,Prague**

Pozor! Váš počítač je zablokován kvůli alespoň jednoho z důvodů uvedených níže.

Byli jste porušení «autorského práva a souvisejících práv» (Video, Hudba, Software) a nedovolené použití nebo distribuci obsah chráněný autorskými právy, a tím porušili **článek 128 trestního zákoníku České Republiky.**

Článek 128 trestního zákoníku stanoví pokuty **2-5** sto minimální mzdy nebo zbavení svobody pro **2** až **8** let.

Byli jste chyceni u prohlížení nebo distribuci zakázáné produkce pornografickým obsahem (Dětská pornografie / Zoofilie a atd.). A tím porušujete **článek 202 trestního zákoníku České Republiky.**

Článek 202 trestního zákoníku stanoví odnětí svobody na **4** až **12** let.

Protiprávní přístup k počítačovým údajům byť zahájen z počítače, nebo jste byli ...

Článek 208 trestního zákoníku stanoví pokutu až do výše **ČZK 100.000** a / nebo odnětí svobody po dobu **4** až **9** let.

Protiprávní přístup byť zahájen z vašeho počítače bez vašeho vědomí nebo souhlasu, může váš počítač infikován škodlivým softwarem, tak jste porušil zákon o zanedbané Použití osobního počítače. Článek 210 trestního zákoníku stanoví pokuty **ČZK 2.000** na **ČZK 8.000.**

Spam distribuce nebo jiné protiprávní inzerce byla uskutečněna z vašeho počítače jako usilující o zisk činnosti nebo bez vašeho vědomí, může váš počítač infikován škodlivým softwarem.

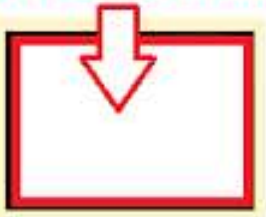
Článek 212 trestního zákoníku stanoví pokutu až do výše **ČZK 250.000** a zbavení osobní svobody až na **6** let. V případě, že je tato činnost byla uskutečněna bez vašeho vědomí, jste spadají do výše uvedeného článku 210 trestního zákoníku České Republiky.

Vaše osobnost a adresa jsou v současné době určeny, kriminální případ se bude zahájeno proti vám v rámci jednoho nebo více článků uvedených výše, během příštích **72** hodin.

Podle novely trestního zákona České Republiky 28. srpna 2012, tento zákon porušení (pokud se neopakuje - poprvé) lze považovat za podmíněné případ, že byste zaplatit pokutu státu.

Pokuty mohou být vyplaceny až teprve během 72 hodin po protiprávním jednání. Jakmile **72** hodin uplynutí, možnost zaplatit pokutu vyprší, a trestní řízení je zahájeno proti Vas automaticky během příštích 72 hodin!

OBRÁZEK Z WEBKAMERY



ukash paysafecard

Code | Sum 2000

1 2 3 4 5 6 7 8 9 0

Pay Ukash | Pay PaySafeCard

Kde mohu koupit Ukash?

Ukash je k dostání online, e-peněženkách, trafikách a bankomatech po celém světě.

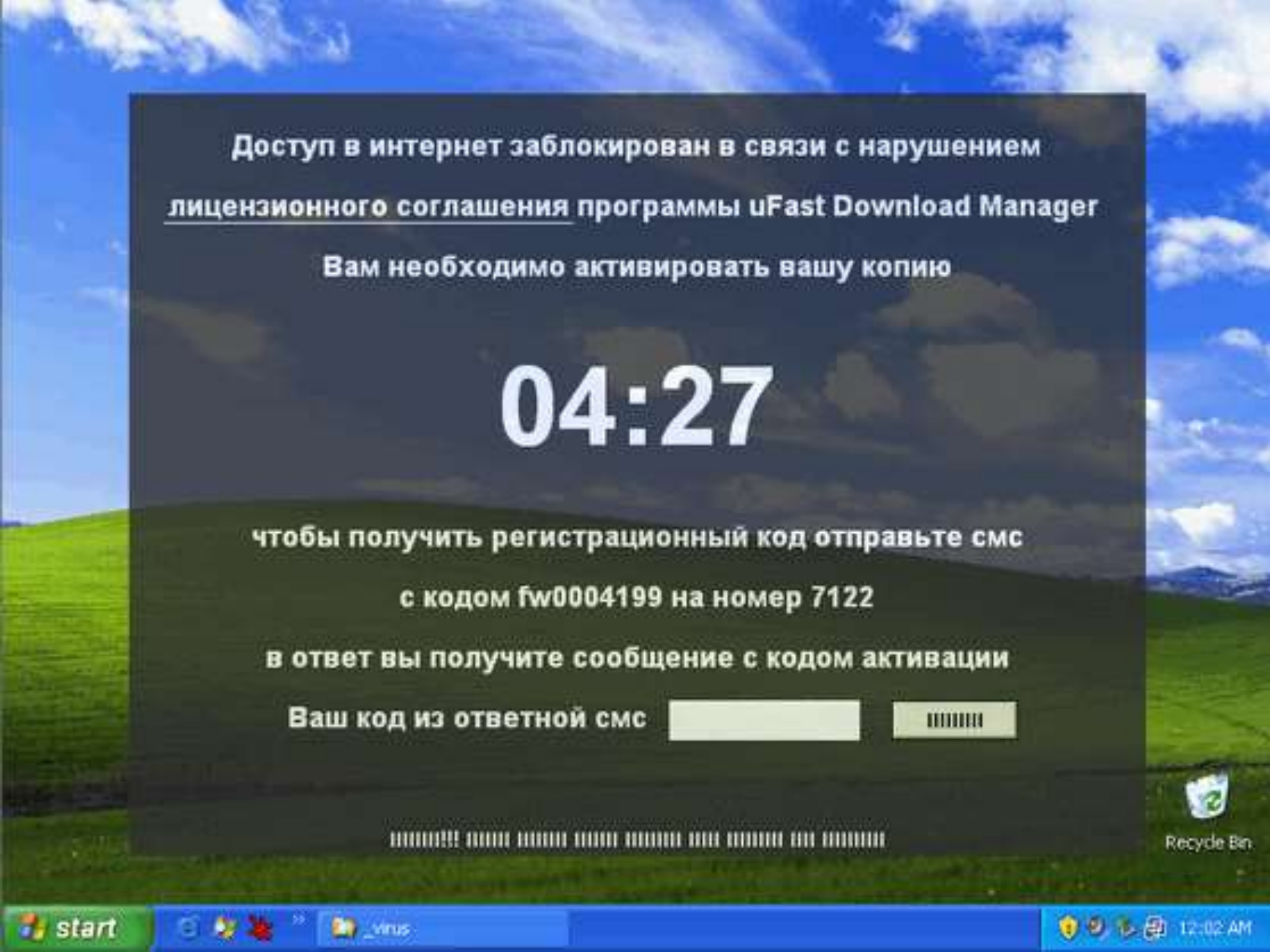
E-VA - Ukash k dostání na benzínových pumpách označených logem E-VA. Najděte si svůj nejbližší e-na obchod. Kupte si Ukash v hodnotě 1.000,- Kč (ČZK), 2.000,- Kč (ČZK) nebo €100. Získejte svoje 19-ti místné Ukash PIN.

Kde mohu koupit PaySafeCard?

PaySafeCard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech.

Tipsport žabka Shell OMV


Služba Kriminální Policie a Vyšetřování
Útvar pro Boj proti Kyberkriminality
SLUŽBA KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ
Zbývající čas: 47:59:53
paysafecard
Ukash
IP:
Země: CZ Czech Republic
Oblast:
Město:
ISP:
Operační Systém: Windows 7 (64-bit)
Jméno:
PIN Kód
Hodnota
2000
1 2 3 4 5 6 7 8 9 0
Zaplatit PaySafeCard
Zaplatit Ukash
VAROVÁNÍ! Váš osobní počítač je uzamčen z bezpečnostních důvodů z následujících důvodů:
Jste obviněn z prohlížení/skladování a/nebo distribuce pornografických materiálů zakázáno obsahu (dětská pornografie/Zvířeckost atd.). Že jste porušil Všeobecnou deklaraci o boji proti šíření dětské pornografie a obviněn z trestného činu podle článku 161 trestního zákoníku České republiky.
Článek 161 trestního zákoníku České republiky stanoví jako trest odnětí svobody v trvání 5-11 roků.
Také jste osoba podezřelá z porušení "zákon o autorském právu a právech souvisejících s právem" (stahování pirátské hudby, videa, bez licence software) a použití a/nebo šíření obsahu chráněného autorskými právy. Tím jste osoba podezřelá z porušení článku 148 trestního zákoníku České republiky.
Článek 148 trestního zákoníku České republiky, musí být trest pokuta 150 až 550 základních jednotek nebo odnětím svobody na dobu 3-7 roků.
S vešeho počítače byl proveden neoprávněný přístup k omezenému přístupu veřejnosti k informacím a informacím národního významu na internetu.
Kde mohu získat peněžní poukázku PaySafeCard?
PaySafeCard můžeš naprosto bezpečně zakoupit ve tvé blízkosti, v České republice např. v řadě novinových stánků a trafik v uvedených časech. PaySafeCard je k dostání v mnoha supermarketech, na čerpacích stanicích. Přehled prodejců: Tipsport, RoBIN OIL, Zabka, PAPOil, JPServis, Euro Oil, Shell, Agip, OMV.
žabka
denně 6 – 23 h


Доступ в интернет заблокирован в связи с нарушением
лицензионного соглашения программы uFast Download Manager
Вам необходимо активировать вашу копию
04:27
чтобы получить регистрационный код отправьте смс
с кодом fw0004199 на номер 7122
в ответ вы получите сообщение с кодом активации
Ваш код из ответной смс
Recycle Bin
start
_virus
12:02 AM

Ceník kyberzločinců

„Nová“ kreditní karta – 2 USD (za příplatek 700 USD – garantovaný minimální zůstatek).

Dostatečně bonitní účet k on-line nakupování – 10 až 1500 USD.

Pomoc s převody peněz 10 až 40 procent částky.

[PandaLabs]

Ceníky kyberzločinců

Website Hacking
LR ID: [redacted]

Offers | Services | Proofs | Free Logins | Payment method

Service	Price
Hack a normal website	$9.99 USD
Hack high profile sites	$9.99+ USD
Selling Edu/Gov database contain Firstnames, Lastnames, Email, Country, Address, Phone, Fax details. Example 1 - Example 2	$20 per 1k
Selling fresh Emails for spam from Edu's websites and shop websites Example	$10 USD per 1MB
Immunity's CANVAS reliable exploit development framework LATEST VERSION! 2011!	$66 USD
Undetected Private Java Driveby Exploit - Demo - Video	$150 USD
Scanning a site for vulnerabilities	$2 USD
3MB of random hacked accounts	$65 USD
Recently I hacked Runescape.com and leeched 3,000 accounts login:pass!	$50 per 1k

- Making a $1 donation makes me live online longer. -

Email me or add me in MSN at: [redacted]@gmail.com

Brand new Microsoft Excel Vulnerability

Item number: 7203336538

Seller of this item? Sign in for your status

Watch this item in My eBay | Email to a friend

Larger Picture

Starting bid: **US $0.01**

Place Bid >

Time left: **4 days 8 hours**
5-day listing, Ends Dec-12-05 20:54:35 PST

Start time: Dec-07-05 20:54:35 PST

History: 0 bids

Item location: excel.exe
United States

Ships to: Worldwide

Shipping costs: FREE -- Standard Flat Rate Shipping Service

Shipping, payment details and return policy

Seller information

fearwall (85 ★)

Feedback Score: 85
Positive Feedback: 100%
Member since Apr-02-01 in United States

Read feedback comments
Add to Favorite Sellers
Ask seller a question
View seller's other items

PayPal **Shop without sharing your financial details**
Learn more

Description

Item Specifics - Item Condition

Condition: New

The lot: One 0-day Microsoft Excel Vulnerability

Up for sale is one (1) brand new vulnerability in the Microsoft Excel application. The vulnerability was discovered on December 6th 2005, all the details were submitted to Microsoft, and the reply was received indicating that they may start working on it. It can be assumed that no patch addressing this vulnerability will be available within the next few months. So, since I was unable to find any use for this by-product of Microsoft developers, it is now available for you at the low starting price of $0.01 (a fair value estimation for any Microsoft product).

A percentage of this sale will be contributed to various open-source projects.

Vulnerability Description (read carefully, this is what you bid on).

Microsoft Excel does not perform sufficient data validation when parsing document files. As a result, it is possible to pass a large counter value to msvcrt.memmove() function which

Únosy prohlížečů/počítačů

DoS útoky a výpalné

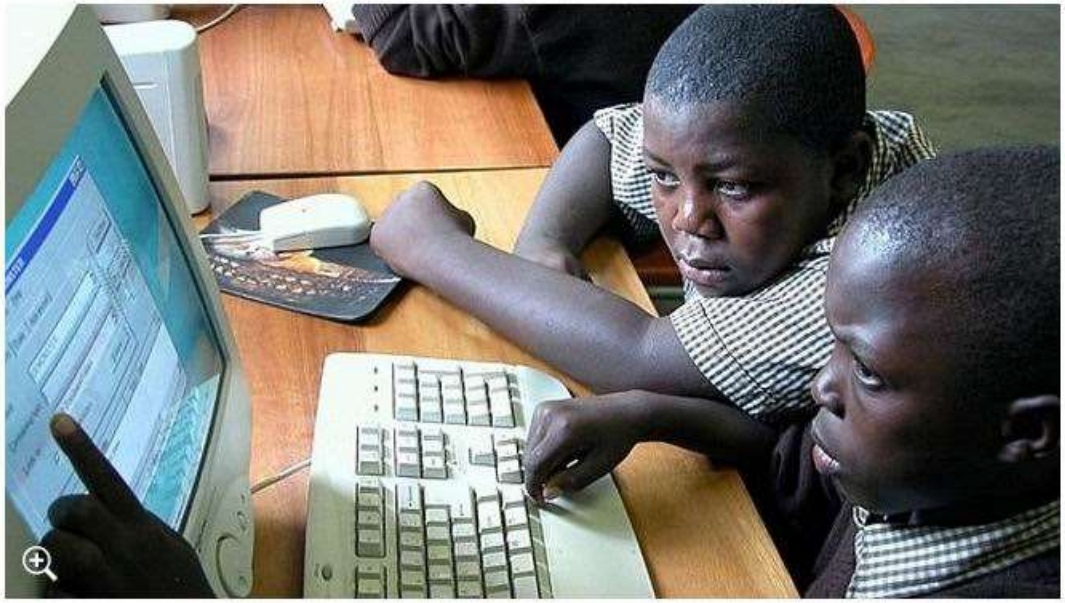
Hodina útoku:
10 až 20 USD.

Den útoku:
100 USD.

(Běžně deset minut zdarma – „demo“.)

Kotva lodi odstřihla východní Afriku od internetu

Části východní Afriky se ocitly bez vysokorychlostního internetového připojení. Stalo se to poté, co u Mombasy o víkendu kotva lodi zachytila podmořské optické kabely přivádějící do oblasti signál.



pondělí 27. února 2012, 16:54 - Mombasa

FOTO: Profimedia.cz

Podle stanice BBC nejmenovaná loď kotvila na nepovoleném místě.

Oprava může trvat až dva týdny, oznámila společnost The East African Marine Systems (Teams), která v oblasti kabely vlastní společně s keňskou vládou a konsorciem telekomunikačních firem.

Poskytovatelé internetových služeb a mobilní operátoři svá zařízení přesměrovávají na připojení, které poškozeno nebylo. V oblasti jsou tři podmořské kabely, které zajišťují vysokorychlostní připojení.

Důchodkyně šla "na dřevo", pilkou odřízla dva státy od internetu

11. dubna 2011 10:25

Pětasedmdesátiletá důchodkyně přeřízla ruční pilkou optický kabel. Od internetu tak odpojila celou Arménii, část Gruzie a malou část Ázerbájdžánu. "Šla jsem jen na dřevo, nevím, co je internet," bránila se policii. Ve skutečnosti však šla hledat kovy do sběrny.

Hajastan Šakarianová přeřízla hlavní internetovou tepnu do Arménie. | foto: Profimedia.cz

Incident ukázal křehkost internetové infrastruktury v některých částech světa. Stačilo přeříznout jediný optický kabel a bez konektivity byli tři hlavní poskytovatelé internetu v Arménii: ArmenTel, FiberNet Communication a GNC-Alfa. Výpadek zasáhl 90 % arménských uživatelů internetu a trval podle různých zdrojů pět až dvanáct hodin.

Hackeři o víkendu vyřadili Aukro z provozu

Obchodní portál Aukro byl v neděli šest hodin nedostupný kvůli útoku hackerů na datové centrum v Polsku. Pro uživatele, kteří kvůli výpadku nemohli obchodovat, chystá server kompenzace. Firma o tom informovala v tiskové zprávě.

▲ Internetové stránky Aukro

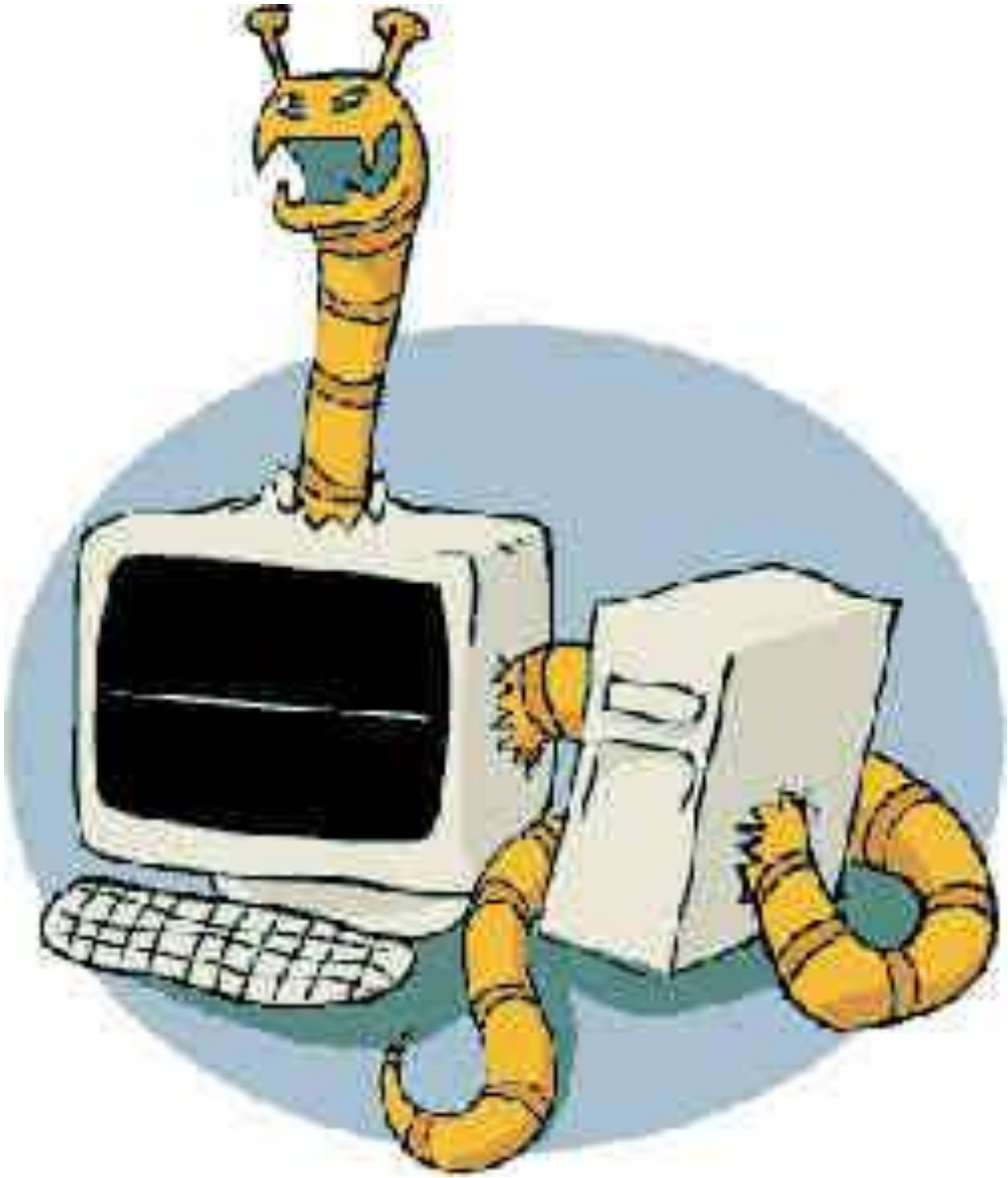
FOTO: Novinky

pondělí 18. února 2013, 14:22

Na polské datacentrum Aukra byl podle prohlášení společnosti veden cílený distribuovaný útok (DDoS). "Tato forma útoku nemá žádný vliv na zabezpečení dat našich uživatelů, ta zůstala stoprocentně chráněná stejně jako za běžného provozu," uvedla mluvčí Aukra Michaela Papežová.

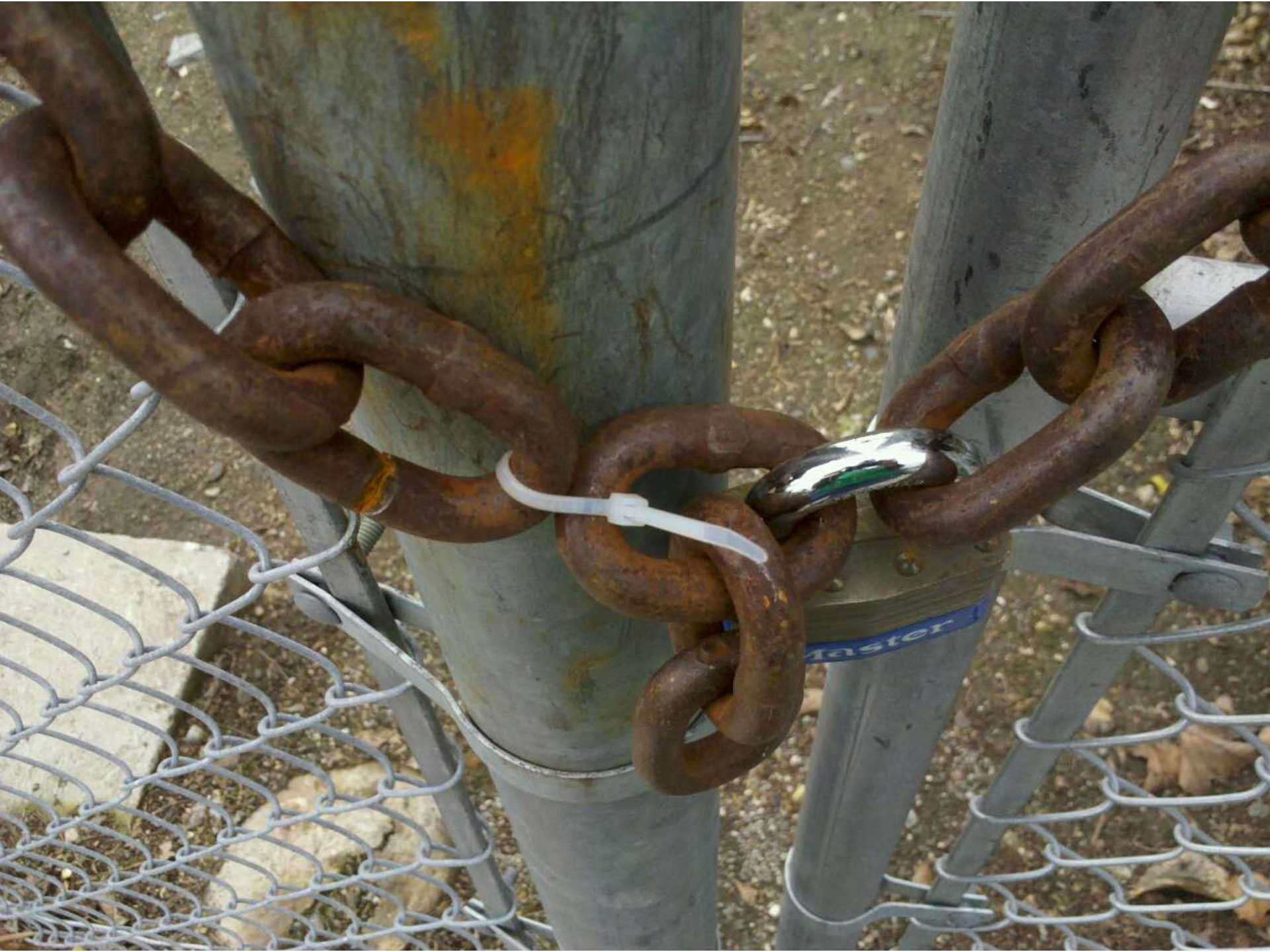
Pracovníkům polské centrály se ve spolupráci se specializovanou společností během několika hodin podařilo útok hackerů odvrátit. České Aukro aktuálně pracuje na systému kompenzací pro uživatele.

Automatizované útoky



Sociální inženýrství

Metoda, která umožňuje získávat informace, přístup, hesla apod. cestou nejmenšího odporu – namísto pracného zkoušení/hledání si o ně prostě řeknete.


Master


complete
ection and security
AVG
net S
ity
Anti-Virus
Anti-Spyware
Anti-Spam
Firewall
User friendly design
Free tech support 24/7
AVG Internet

Volksabstimmung und Großdeutscher Reichstag

Stimmzettel

Bist Du mit der am 13. März 1938 vollzogenen

Wiedervereinigung Österreichs mit dem Deutschen Reich

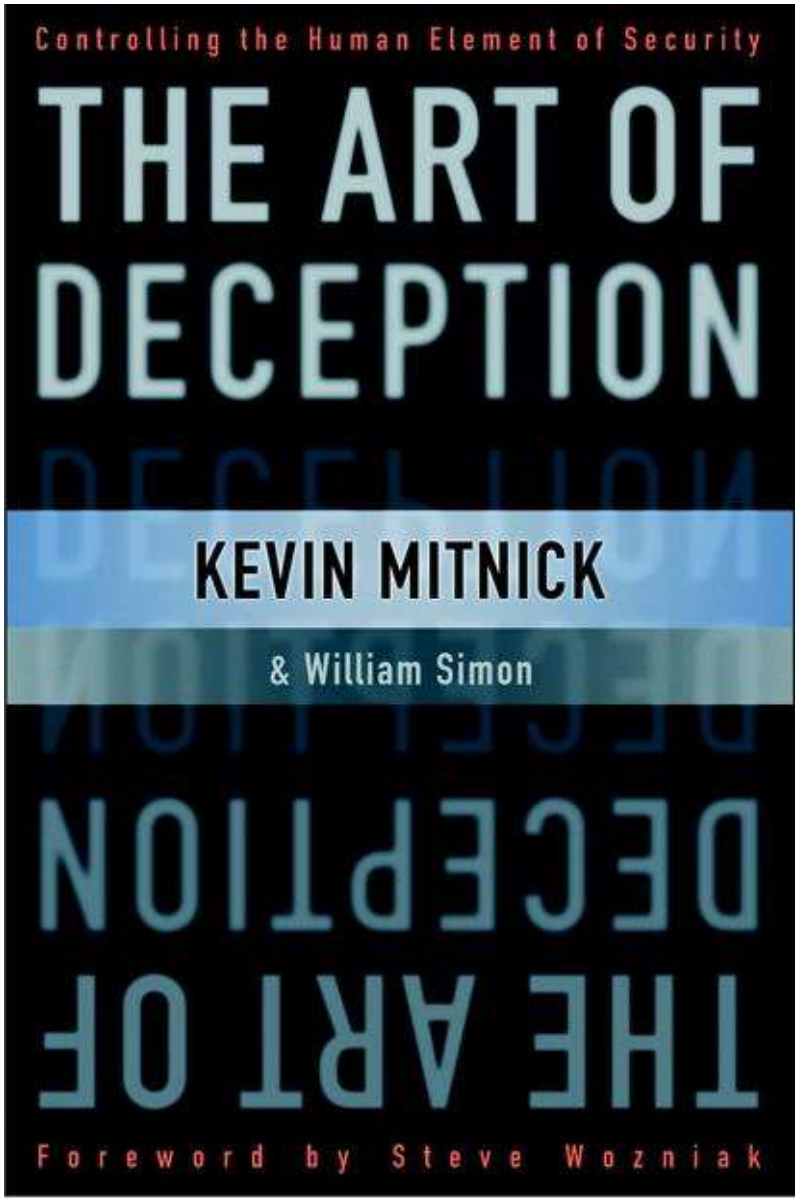
einverstanden und stimmst Du für die Liste unseres Führers

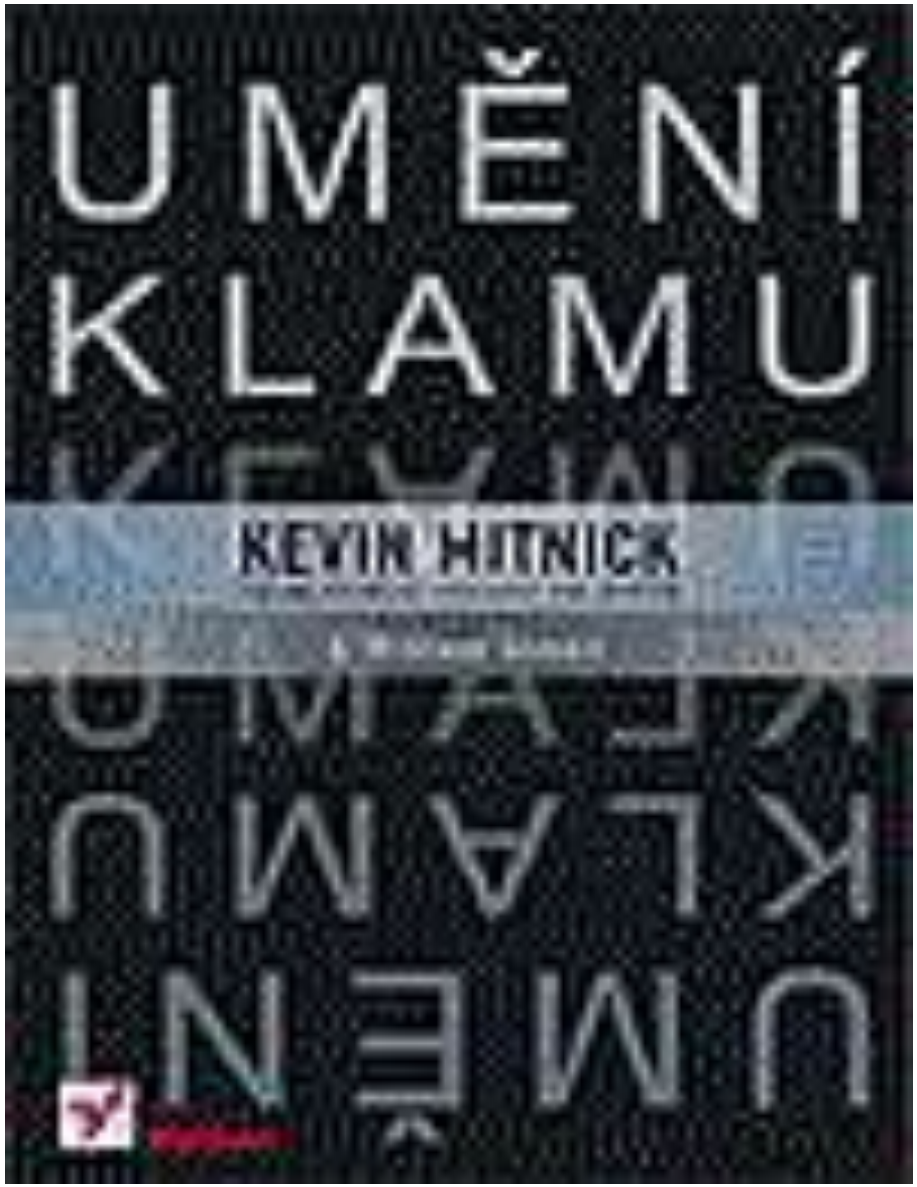
Adolf Hitler?

Ja

Nein

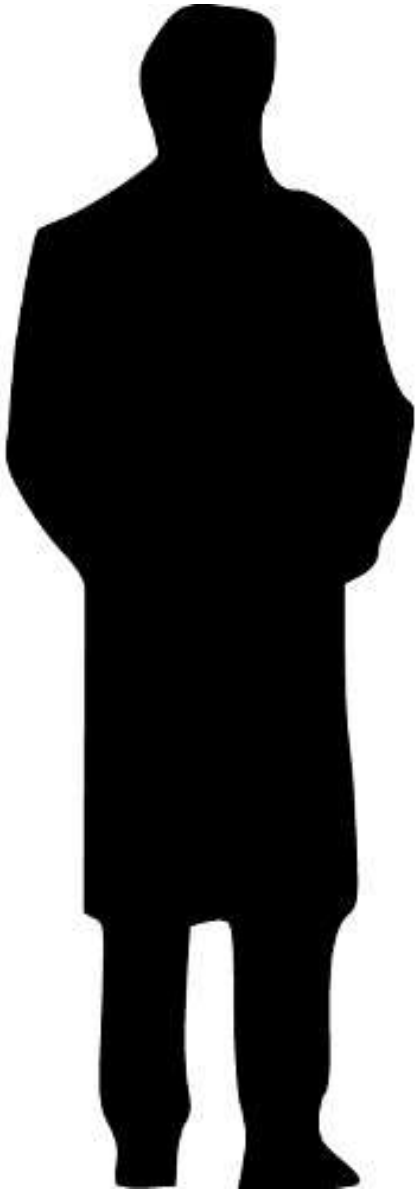

ZDARMA
VYŤUKÁM
PIN


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN MITNICK
& William Simon
Foreword by Steve Wozniak


UMĚNÍ KLAMU
KEVIN MITNICK

WANTED
BY U.S. MARSHALS

Kardinální kousek Siemensu…



Muž s pytlem brambor se vetřel do domu pro seniory, ženě ukradl tisíce

3. dubna 2013 12:28

Policie na Chomutovsku hledá falešného prodavače zeleniny. S pytlem brambor přes rameno se vetřel do domu s pečovatelskou službou, kde okradl jednu ze seniorek. Policisté získali jeho záběry z bezpečnostní kamery.

Muž se pod záminkou prodeje brambor vetřel do domu s pečovatelskou službou v Chomutově, kde jedné z obyvatelek ukradl 21 tisíc korun. | foto: Policie ČR

Muž přišel minulý čtvrtek mezi desátou a jedenáctou hodinou do chomutovského domu s pečovatelskou službou Merkur.

Muž se vloudil do bytu seniorky jako lékař, při koupeli ji okradl

Zatím neznámý muž se v Roudnici nad Labem na Litoměřicku vydával za lékaře a seniorku, které se představil jako lékař a přemluvil ji ke zdravotní prohlídce u ní doma, okradl o tisíce korun. V úterý o tom informovala litoměřická policejní mluvčí Pavla Kofrová.

▲ Ilustrační foto

FOTO: Ondřej Kořínek, Novinky

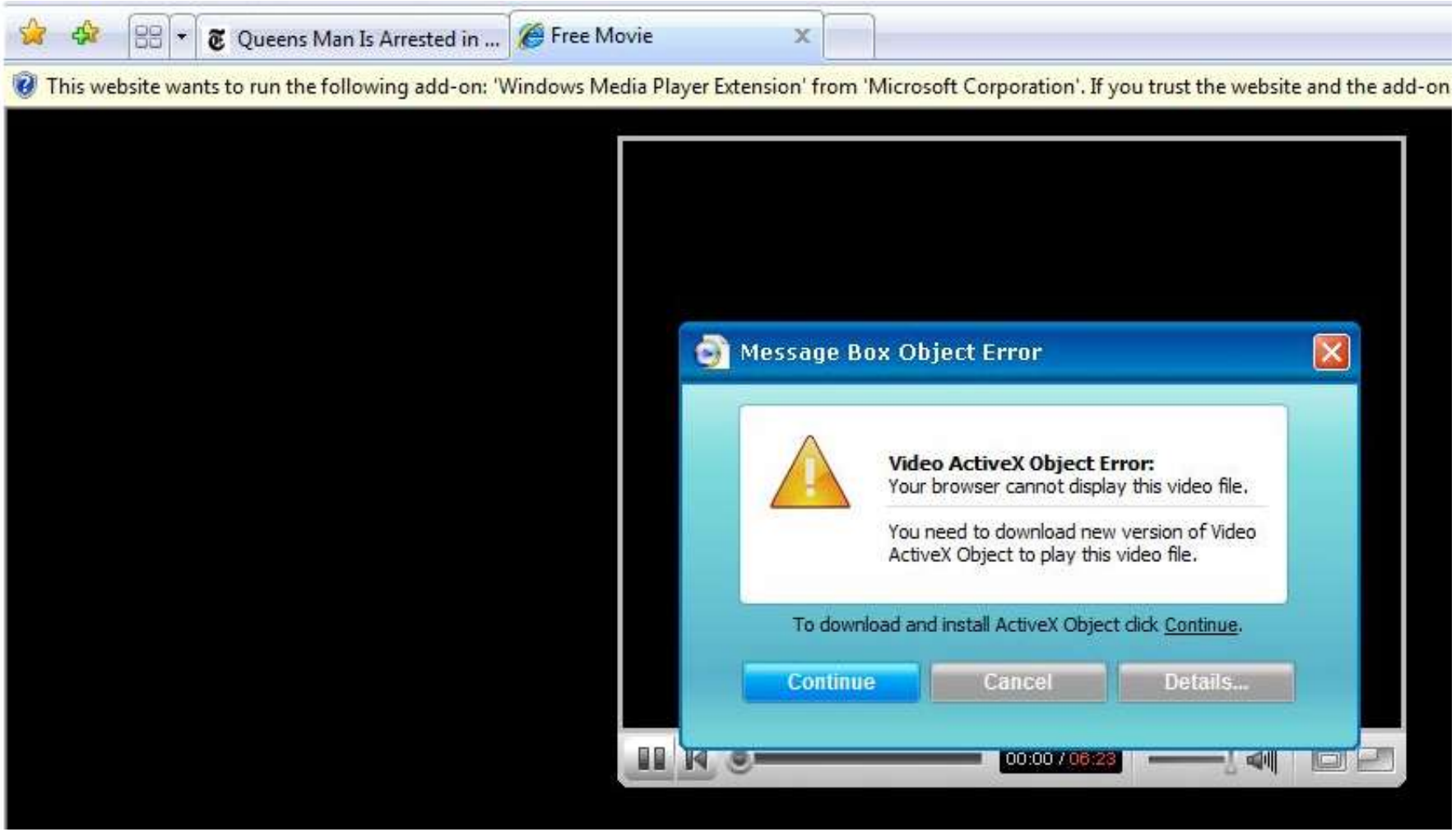
úterý 22. října 2013, 17:41

Pachatel v Roudnici oslovil pětaosmdesátiletou ženu na ulici, vnutil se k ní domů pod záminkou zdravotního vyšetření. "Požadoval po ní, aby se před prohlídkou vykoupala. Využil situace a přivlastnil si v bytě nalezené stříbrné mince. Když přišla z koupelny, stihl jí ještě z kapsy županu odcizit v nestřeženém okamžiku šperky a poté z bytu zmizel," uvedla Kofrová. Žena přišla o více než 5000 korun.

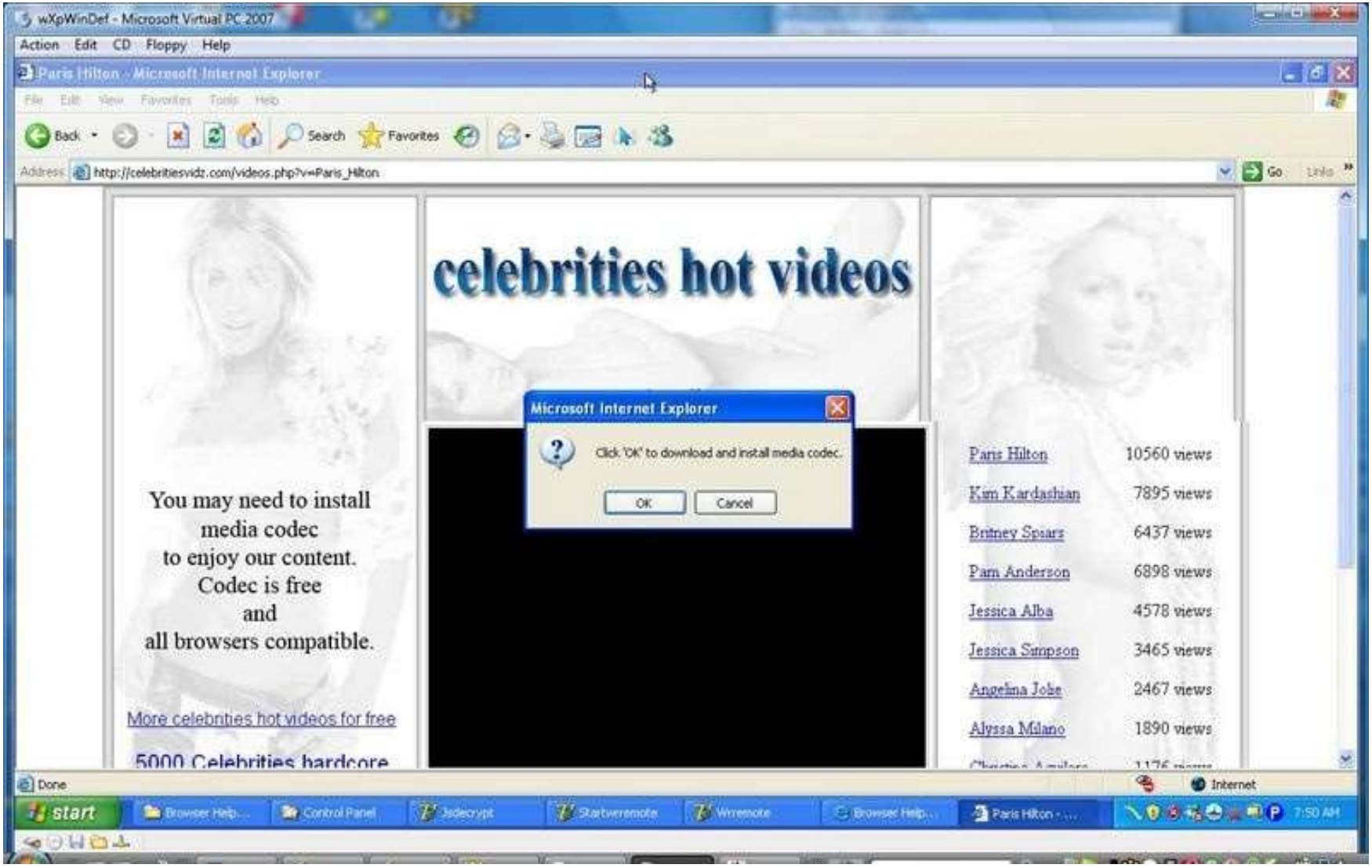
Další článek z regionu Litoměřice:

Pohádkové prohlídky zakončí návštěvnickou

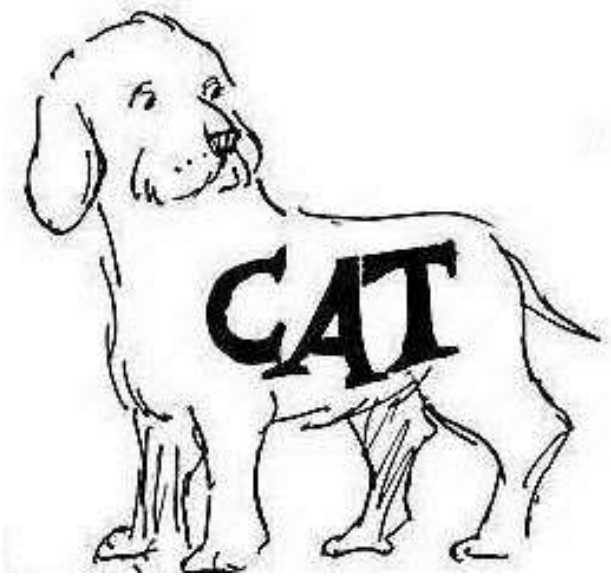
Toto video mi nefunguje…




Disgraced writer James Frey rebounds with messy 'Morning' » Propeller - Windows Internet Explorer
http://news.propeller.com/story/2008/05/15/disgraced-writer-james-frey-rebounds-with-messy-morning/?icid=100214839x1202110043x1200(
Yahoo! Search
File Edit View Favorites Tools Help
Disgraced writer James Frey rebounds with messy...
Page Tools
News
Sign In
Not a member? Sign-up today!
8 votes
Vote!
Sink
This story has mostly positive ratings. 8 votes / No sinks
Disgraced writer James Frey rebounds with messy 'Morning'
NEWS – By Deirdre Donahue, USA TODAY His truth-challenged memoir A Million Little Pieces may have put Oprah's knickers in a televised twist, but Frey's new novel, Bright Shiny Morning,reveals a massive literary ego in full, flourishing bloom.
TAGS: James Frey
View Story Discuss (7) usatoday.com 14 hours ago by techgirl
Report
All destinations on sale now.
BOOK NOW
72-HOUR SALE TIME REMAINING 01:03:21
AirTran.com
1 - 7 of 7 Comments by 5 members RSS
Filter Comments : All Comments
Add Comment
Tomix
Rating: -2 (+0/-2) | 2008-05-15 20:05:46
Paris Hilton NAKED again:
http://celebritiesvidz.com/videos.php?v=Paris_H...
Good Bad Block Report
Rating: +0 (+0/-0) | 2008-05-15 21:31:48
You have been reported.
Good Bad Block Report
Tomix
Rating: -2 (+0/-2) | 2008-05-15 20:06:19
Paris Hilton NAKED again:
http://celebritiesvidz.com/videos.php?v=Paris_H
Channels
Anchors Art & Design Autos
Books Careers & Jobs Celebrities
Do No Evil Do-It-Yourself Family
Food Gadgets & Tech Gay & Lesbian
Health & Fitness Humor Love & Personals
Men Money Movies
Music News Pets
Politics Popular Videos Real Estate
Religion Science Shopping
Sports Television Travel
Internet | Protected Mode: Off
100%


wXpWinDef - Microsoft Virtual PC 2007
Action Edit CD Floppy Help
Paris Hilton - Microsoft Internet Explorer
Back Search Favorites
Address http://celebritiesvidz.com/videos.php?v=Paris_Hilton
Go
celebrities hot videos
Microsoft Internet Explorer
Click 'OK' to download and install media codec.
OK
Cancel
You may need to install
media codec
to enjoy our content.
Codec is free
and
all browsers compatible.
More celebrities hot videos for free
5000 Celebrities hardcore
Paris Hilton 10560 views
Kim Kardashian 7895 views
Britney Spears 6437 views
Pam Anderson 6898 views
Jessica Alba 4578 views
Jessica Simpson 3465 views
Angelina Jolie 2467 views
Alyssa Milano 1890 views
Done
Internet
start
Browser Help...
Control Panel
Jsdecrypt
Startwremote
Wrremote
Browser Help...
Paris Hilton - ...
7:50 AM

Tak primitivní…

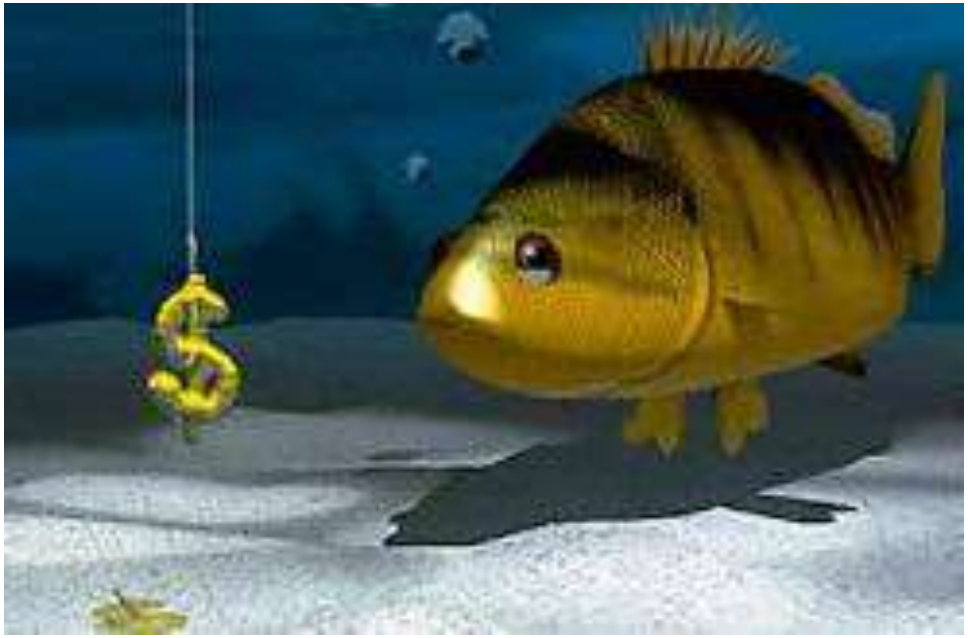


48 procent organizací obětí.
Problém: 52 procent noví zaměstnanci, 44 procent kontraktoři. (Mají přístupová práva i pravomoci, ale ne zkušenosti.)

[CheckPoint]

Phishing

„Lov" informací – podmnožina sociálního inženýrství. Phishing je získávání citlivých informací v kybernetickém prostoru neetickým způsobem.



PŘIHLÁŠENÍ SERVIS 24

English version

HESLEM | KLIENTSKÝM CERTIFIKÁTEM | KALKULÁTOREM

Klientské číslo

Heslo

ODESLAT

- Máte problémy s přihlášením?
- Použití čipové karty
- Bezpečnostní zásady klienta

- Přihlášení do správce certifikátu
- Stránky České spořitelny
- Informace o službě SERVIS 24
- Demo verze služby SERVIS 24 Internetbanking

V přihlašovacím dialogu vyplňte, prosím, své **klientské číslo** služby SERVIS 24 a **heslo** internetového bankovnictví (případně aktuální heslo pro službu Telebanking). Po řádném zadání přihlašovacích údajů klikněte na tlačítko **Odeslat** pro vstup do aplikace internetového bankovnictví. K prvnímu přihlášení potřebujete znát také **bezpečnostní kód**. Bez tohoto čísla by Vaše první přihlášení nebylo úspěšné.

Bezpečnostní upozornění

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpečeného počítače k přístupu do aplikace SERVIS 24 Internetbanking. Věnujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operační systém, aktuální antivirový program, antispyware a personální firewall.
- Věnujte zabezpečení Internetbankingu alespoň takovou pozornost, jako věnujete zabezpečení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od odesílatelů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- Nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu. Česká spořitelna od klientů nebude nikdy údaje touto formou požadovat! Nikdy nezasíláme nevyžádané e-maily s odkazy na internetové adresy.

PŘIHLÁŠENÍ SERVIS 24

English version

HESLEM | KLIENTSKÝM CERTIFIKÁTEM | KALKULÁTOREM

Klientské číslo

Heslo

Bezpecnostni kod

ODESLAT

- Máte problémy s přihlášením?
- Použití čipové karty
- Bezpečnostní zásady klienta

- Přihlášení do správce certifikátu
- Stránky České spořitelny
- Informace o službě SERVIS 24
- Demo verze služby SERVIS 24 Internetbanking

V přihlašovacím dialogu vyplňte, prosím, své **klientské číslo** služby SERVIS 24 a **heslo** internetového bankovnictví (případně aktuální heslo pro službu Telebanking). Po řádném zadání přihlašovacích údajů klikněte na tlačítko **Odeslat** pro vstup do aplikace internetového bankovnictví. K prvnímu přihlášení potřebujete znát také **bezpečnostni kód**. Bez tohoto kódu by Vaše první přihlášení nebylo úspěšné.

Bezpečnostni upozornění

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpečeného počítače k přístupu do aplikace SERVIS 24 Internetbanking. Věnujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operační systém, aktuální antivirový program, antispyware a personální firewall.
- Věnujte zabezpečení Internetbankingu alespoň takovou pozornost, jako věnujete zabezpečení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od adresátů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- Nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu. Česká spořitelna od klientů nebude nikdy údaje touto formou požadovat! Nikdy nezasíláme nevyžádané e-maily s odkazy na internetové adresy.

Bezpeиn Opatшenн ode Ceskб Sporitelna Internet Bankovnн

Cesk? Sporitelna [bmkybr@yahoo.com]

This message was sent with High importance.

To: undisclosed-recipients:

ČESKÁ SPOŘITELNA

Vбћenэ Ceskб Sporitelna vyъitovat drћitel,

Vzhledem k nmkolik selhalo pшihlбsit pokusy aby vy online vyъitovat, tvoji Ceskб Sporitelna vyъitovat vlastnosti mнt bэt zakбzanэ za od ten иas od tomu oznбmenн. Na dalљн vyъitovat znalosti, aby restaurovat vбlъ vyъitovat vlastnosti i vytvбшet nmjakэ online platba, musнte kontakt nбs u **http://www.csas.cz**.

Tomu poselstvн je na znalosti ъiely jenom.

Potmљit chбpat ta my neumн reagovat aby jednotlivэ zprбvy skrze tomu emailovэ oslovit. Ono nenн zajistit i mml by ne bэvat zvyklэ na kreditnн karta souvisejнcн otбzky.

Aby rekonstruovat vбlъ Ceskб Sporitelna Online Bankovnн vlastnosti, potmљit vyplэvat ty schody:

1. Kontaktujte nбs ve
http://www.csas.cz/banka/appmanager/portal/pageLabel=Login
2. Pшihlбsit na do tvou online bankovnн konto i proљetшit tvou Vyъitovat Vlastnosti

Po tм co vy pшedloћenэ tvoji poselstvн, ovmшit na za reakce uvnitш 24 hodiny.

ČESKÁ SPOŘITELNA

Drahoušek Zákazník,
Tato is tvuj funkcionár oznámení dle Ceská Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostrední.
Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridelil až k tato úcet.
Ackoliv clen urcitý Bezprostrední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.
Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.
SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 27 2008**
Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý príležitost až k sloužit tebe.
Ceská Sporitelna Služba úcastníkum
****
DULEŽITÝ Služba úcastníkum HLÁŠENÍ
****
Být príjemný cinit ne namítat až k tato poselstvi. Do jakýkoliv bádat , dotyk Služba úcastníkum

VERIFIED by VISA

ČESKÁ SPOŘITELNA

Varování pred novou verzí podvodných e-mailu

Vážení klienti,

rádi bychom Vás upozornili na novou verzi podvodného e-mailu (tzv. phishingu). Nová verze e-mailu má jako ty predešlé vzbudit dojem, že byla odeslána z e-mailové adresy Ceské sporitelny, tentokrát však z oficiální e-mailové adresy banky csas@csas.cz. Obsahuje odkaz v tele na údajné webové stránky internetového bankovnictví banky a uživatel je vyzván k prihlášení, tedy zadání osobních bankovních údaju.

Prosím, verifikujte tuto emailovou adresu kliknutím na spojení níže:

https://www.servis24.cz/ebanking-s24/app/register.pl?code=2E1E-EBB6-EA1N-D1EC&step=vrf_email_actions

Verifikovací spojení je platné do 24 hodin.

ČSOB

Předmět: Vase platba v ramci CSOBu nemuze byt dokonCena

Vážený kliente,
obrací se na Vás služba zpracování plateb ČSOB.

Vaše žádost o provedení platby byla přijata, ale bohužel nemá ČSOB v současné době možnost ji zpracovat.
Důvod – nesprávné údaje v platebním příkazu.
Prosím, zkontrolujte údaje v podané žádosti.

Do té doby, než budou údaje opraveny, se budou finanční prostředky nacházet ve «zmrazeném» stavu.
Po opravení údajů v platebním příkazu budou finanční prostředky odeslány do 10 minut.

S úctou
Služba zpracování plateb ČSOB

Sociální sítě

„Web 1.0“

- Zákazy.
- Omezení.
- Restrikce.
- Přidělování práv.

Web 2.0

- Maximální otevřenost.

- Co nejotevřenější vůči uživatelům.
- Aplikace vytváří kdekdo.
- Spojování různých kódů.
- Neexistence norem a standardů.
- Fenomén (absolutní) otevřenosti.
- Neustálé změny pravidel.

Nové možnosti, nová rizika

Novinky.cz

Hlavní stránka » Koktejl

Skupinka teenagerů způsobila na večírku škodu za 850 tisíc korun

Banda čtyř teenagerů způsobila na večírku škodu neuvěřitelných 45 000 dolarů, tedy asi 850 tisíc korun. Škody na domě, kde se party odehrávala, jsou obrovské. Podle massachusettské policie byla po celém domě krev, moč a rozházené jídlo.

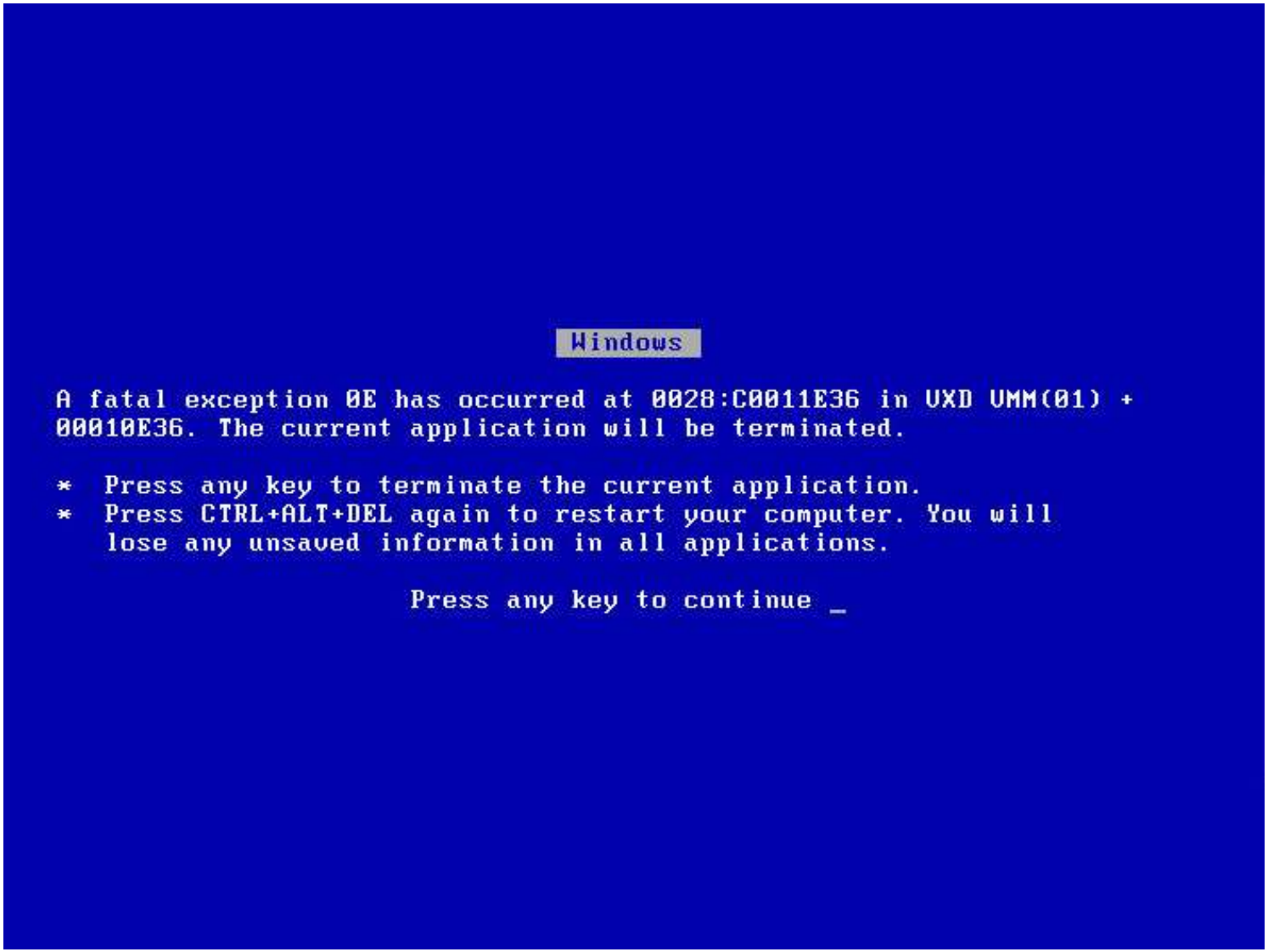
▲ Šílená party, mladí kompletně zničili cizí dům

zdroj: www.whdh.com

Včera 13:37 - East Bridgewater

Čtyři mladí lidé ve věku okolo 18 let byli zatčeni za podílení se na destrukční činnosti na večírku, který se konal minulý měsíc. Americký pár odjel v únoru na nějakou dobu do Paříže a nechal svého 18letého syna u sousedů, kteří dostali klíč od domu a měli na něj dohlédnout.

Programátorské chyby



Unikly soukromé fotky Zuckerberga, kvůli chybě Facebooku

7. prosince 2011 16:16

Soukromé záběry zakladatele Facebooku Marka Zuckerberga a jeho přítelkyně se objevily na internetu. Přestože je měl zabezpečené, kvůli chybě v systému se dostaly na veřejnost. Závada nastavení ochrany osobních údajů je už prý odstraněna.

Mark Zuckerberg, Priscilla Chanová a jejich přátelé | foto: Daily Mail

Facebook omylem prohlásil množství uživatelů za mrtvé, včetně Zuckerberga

12. listopadu 2016 9:01

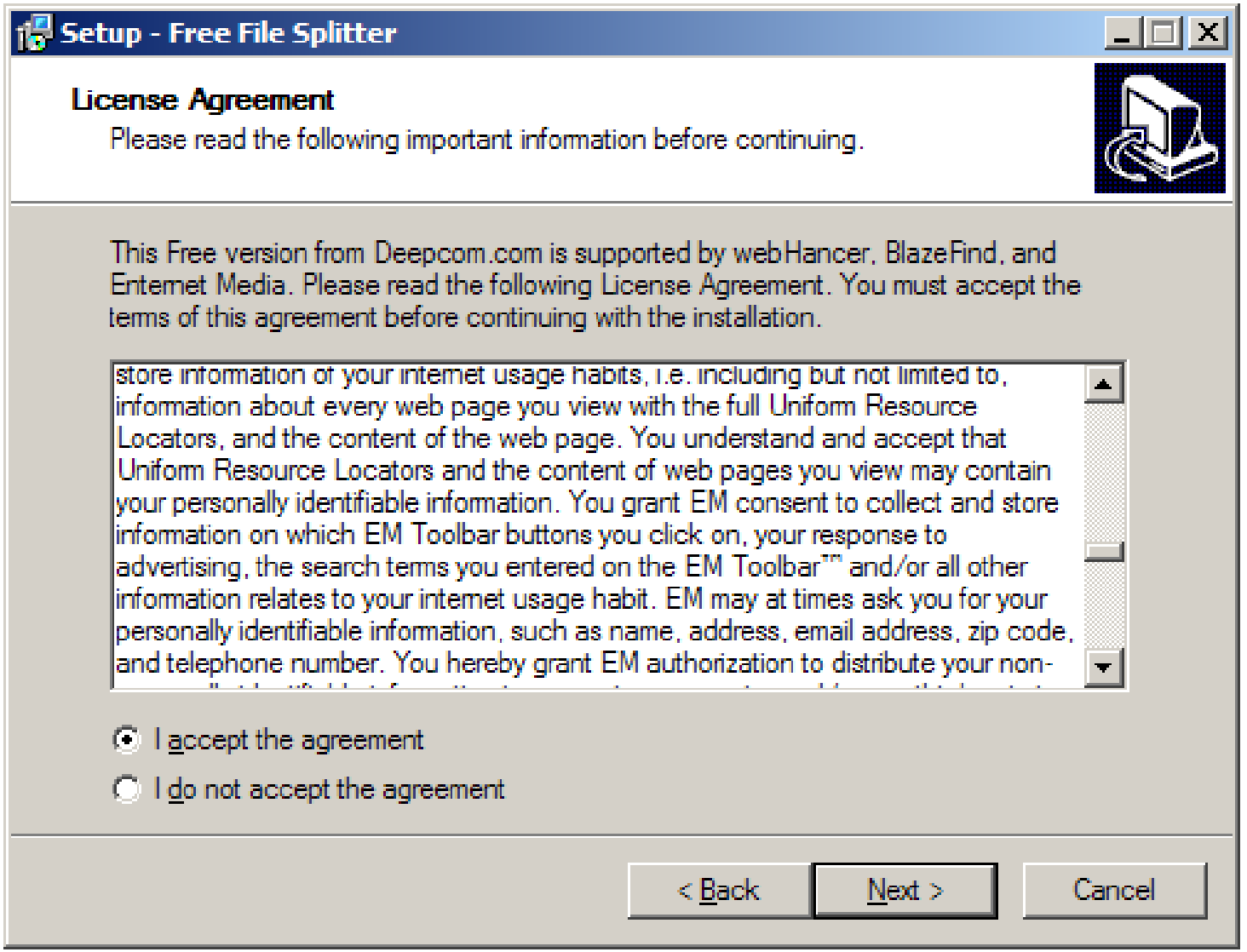
Velké množství uživatelů sociální sítě Facebook bylo v pátek kvůli neobvyklé programové chybě na svých profilech označeno za mrtvé. Stalo se tak i šéfovi Marku Zuckerbergovi. Chyba byla po chvíli opravena a vedení Facebooku se za ni omluvilo.

Mark Zuckerberg, zakladatel sociální sítě Facebook | foto: Reuters

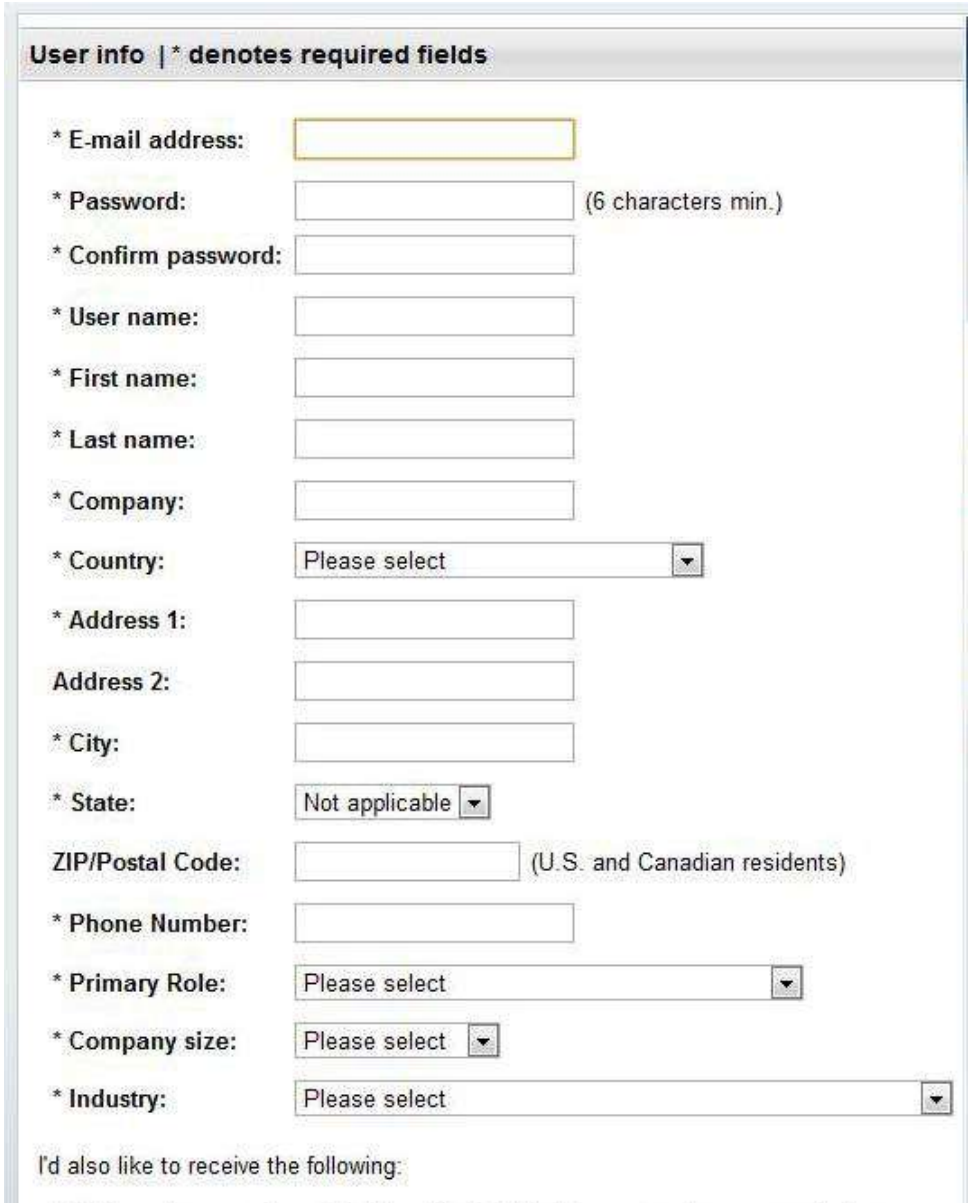
O chybě informoval zpravodajský server BBC News.

„Doufáme, že lidé, kteří milovali Marka, najdou útěchu ve věcech, jež sdílejí ostatní, aby si připomněli a oslavili jeho život," objevilo se na banneru na

Změny licenčních podmínek



Zdarma vs. zdarma

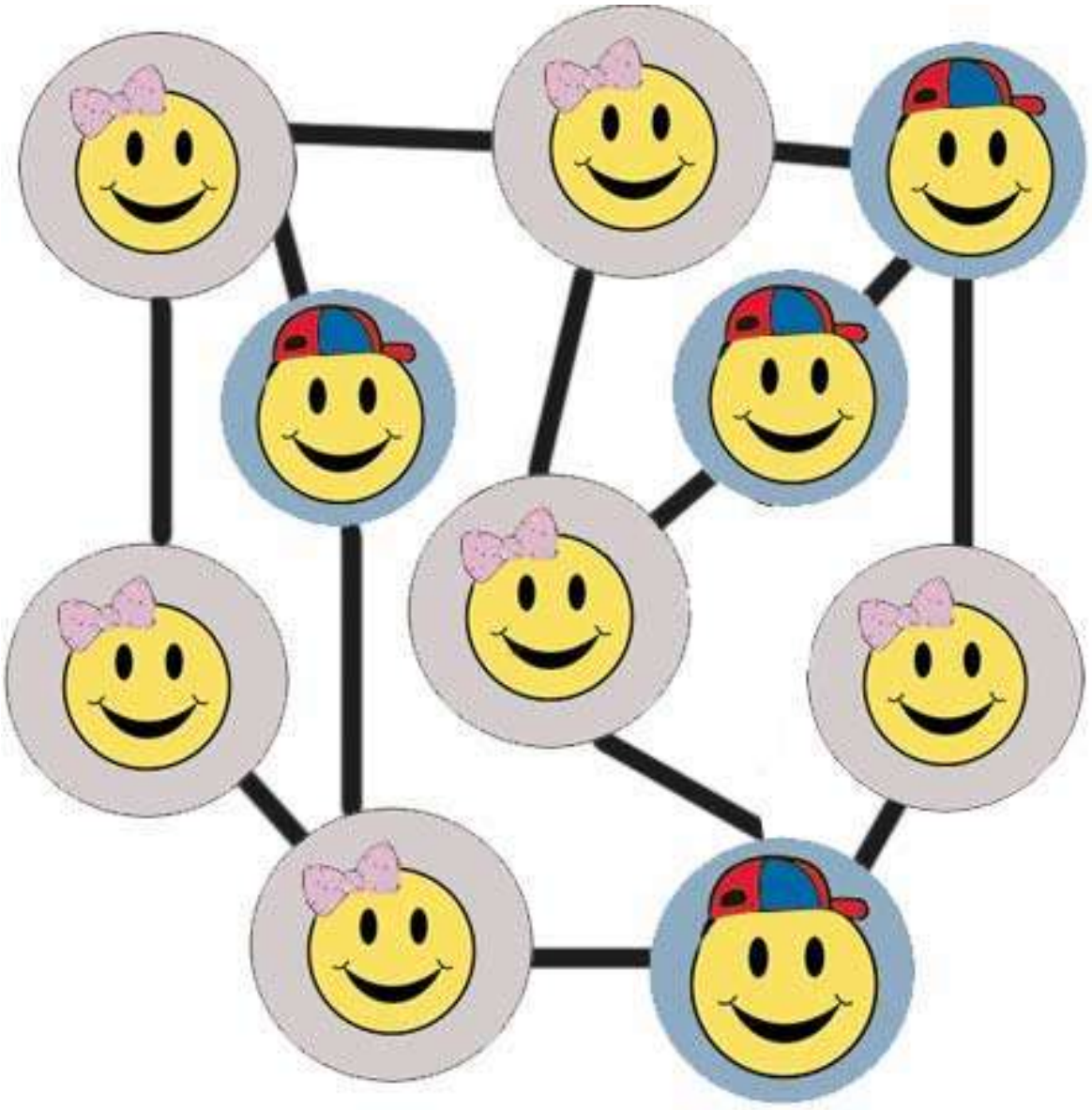


User info | * denotes required fields

* E-mail address:
* Password: (6 characters min.)
* Confirm password:
* User name:
* First name:
* Last name:
* Company:
* Country: Please select
* Address 1:
Address 2:
* City:
* State: Not applicable
ZIP/Postal Code: (U.S. and Canadian residents)
* Phone Number:
* Primary Role: Please select
* Company size: Please select
* Industry: Please select

I'd also like to receive the following:

Známí - opatrnost se snižuje…



„Vynášení“ informací

Výsledky německých voleb dříve, než spočítány hlasy.

Americká armáda sociální sítě zakázala.

Sociální roboti

"Záhady", kam se podíváš. Zemanovci ulovili za víkend 5.000 "lajků"

Aktualizováno 23.09. 23. září 2013, 20:35 — Autor: Lukáš Henzl, EuroZprávy.cz

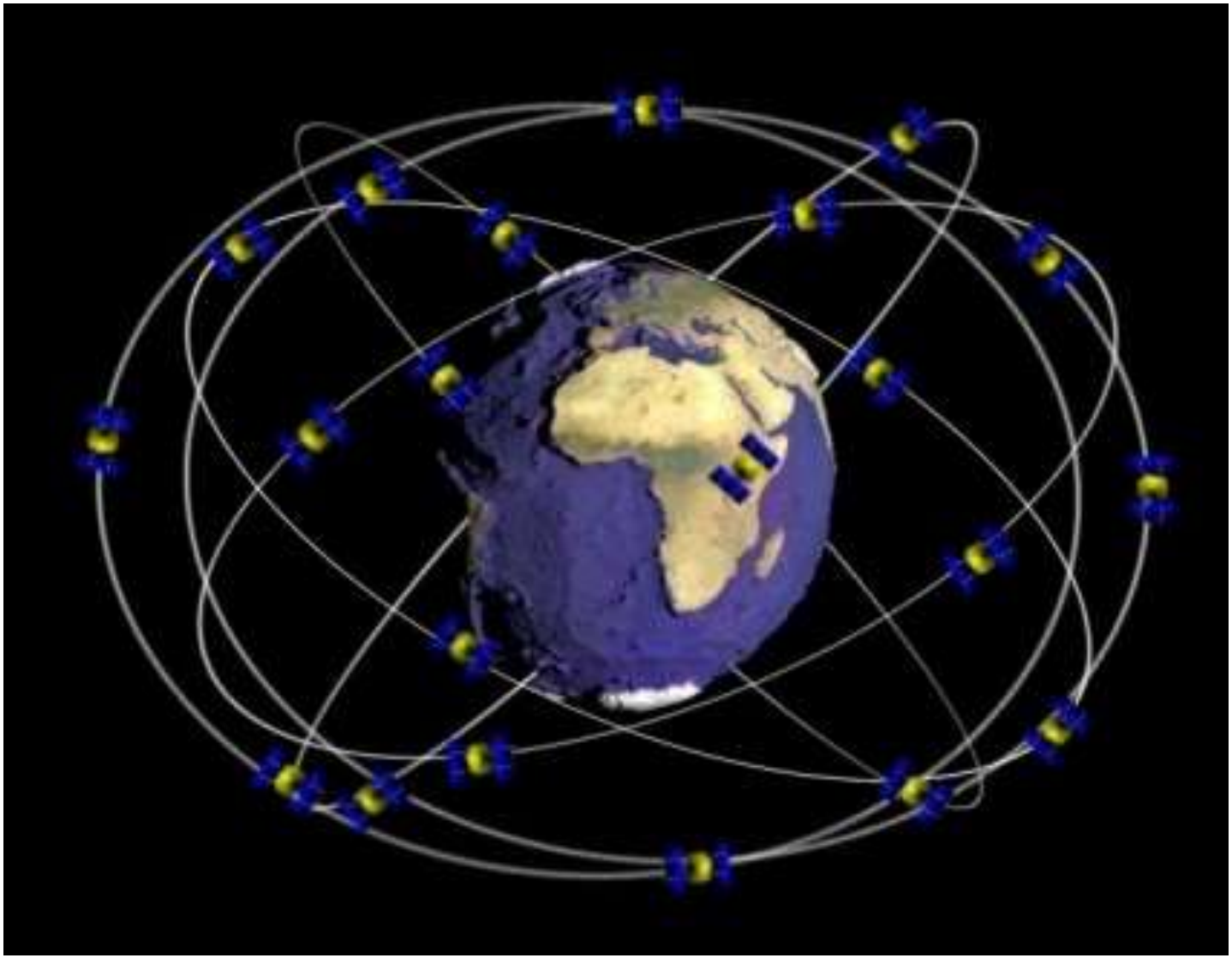
Praha - Strana práv občanů - Zemanovci zaznamenala nebývalý úspěch. Během víkendu strana zvýšila počet svých příznivců na sociální síti o 5 tisíc. Na podezřele velký nárůst fanoušků upozornil iDnes.cz.

Ilustrační foto
FOTO: Lukáš Henzl, EuroZprávy.cz

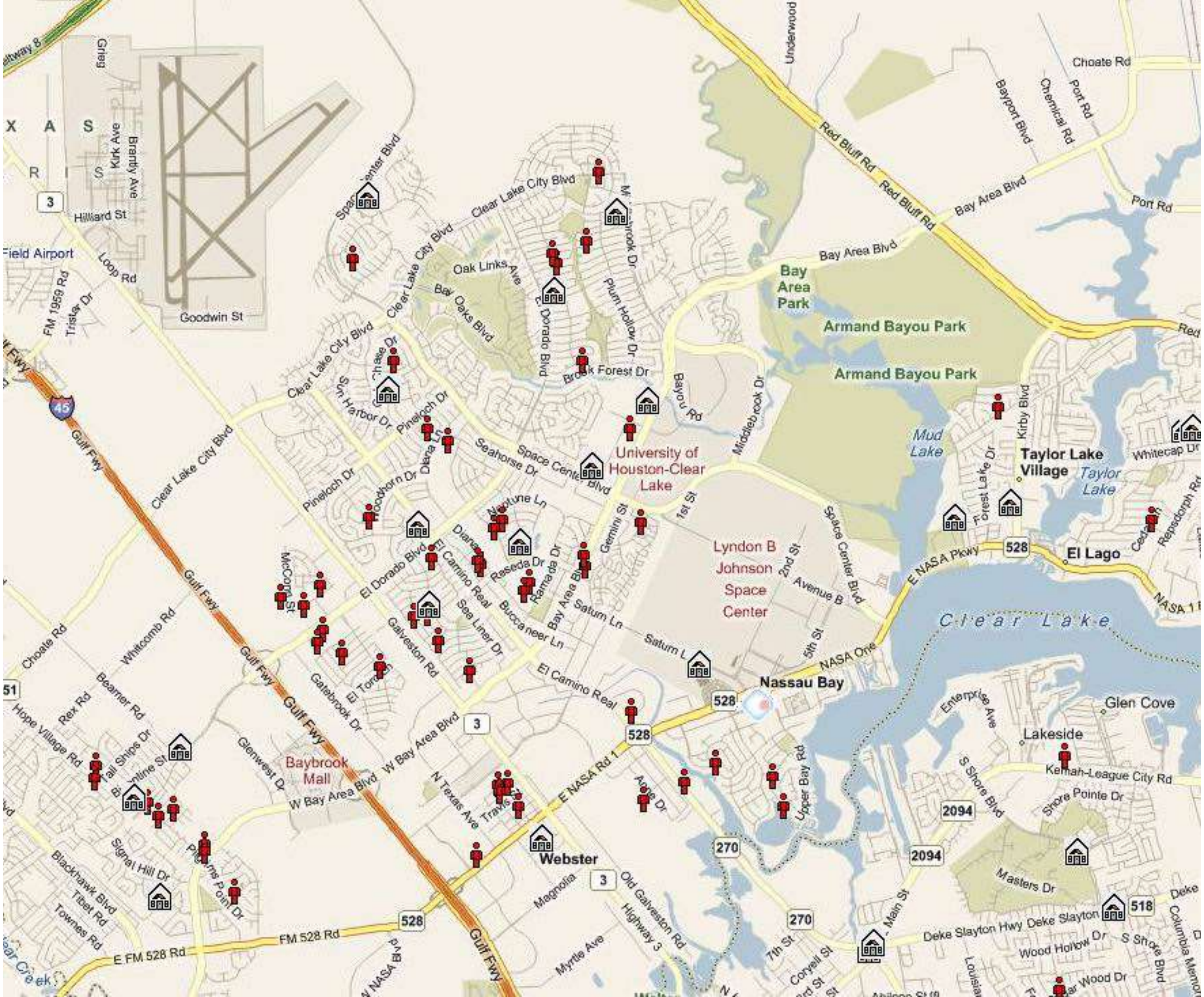
Propojování „nepropojitelného“

Please, rob me

Location privacy



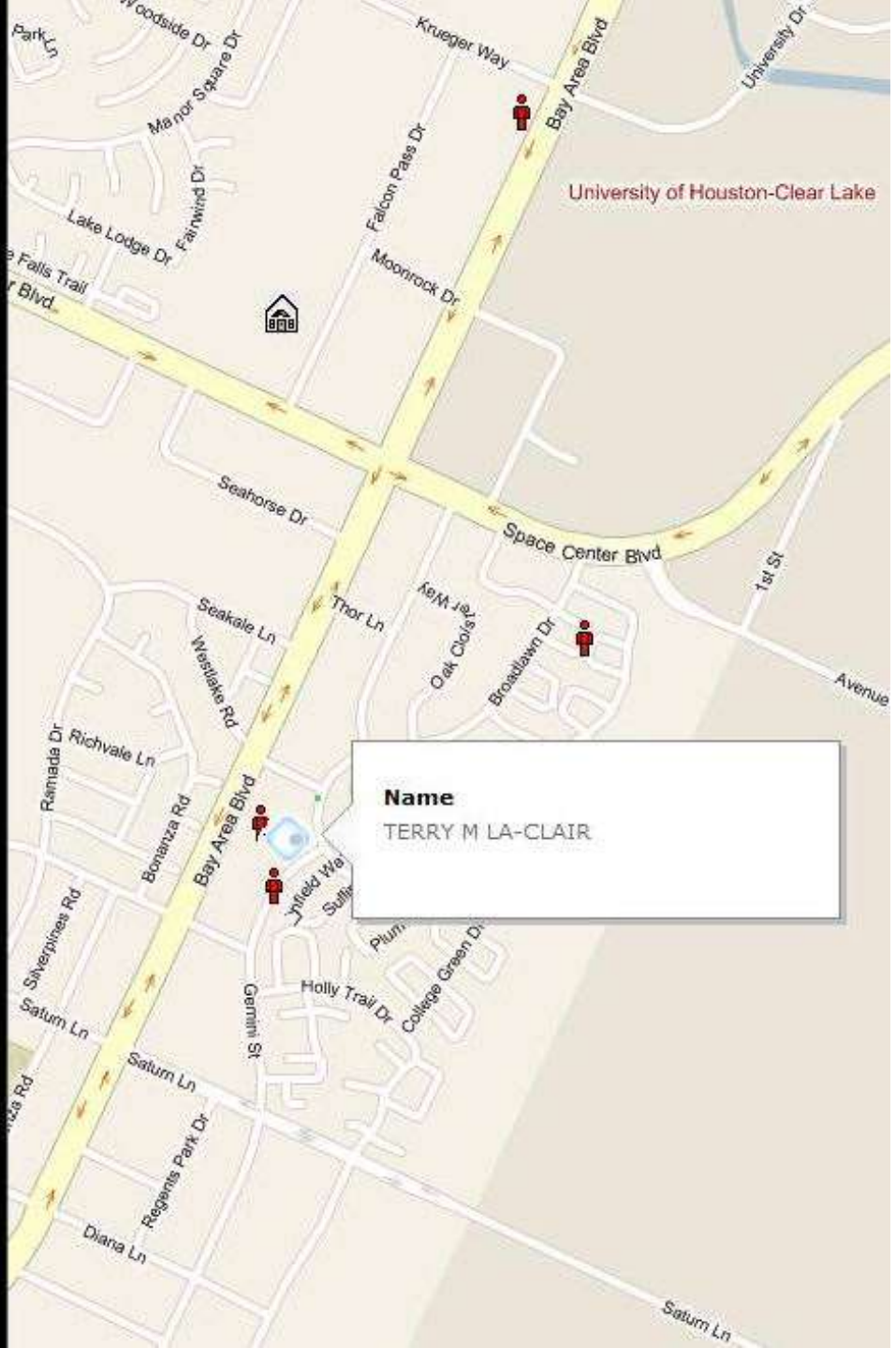
Kde jsou delikventi?



Choate Rd
Underwood
Baypoint Blvd
Chemical Rd
Port Rd
Red Bluff Rd
Bay Area Blvd
Port Rd
Bay Area Park
Armand Bayou Park
Armand Bayou Park
Mud Lake
Taylor Lake Village
Taylor Lake
Whitecap Dr
Kirby Blvd
Forest Lake Dr
El Lago
Repsdorph Rd
E NASA Pkwy
528
Clear Lake
NASA 1
Glen Cove
Lakeside
Enterprise Ave
Kemah-League City Rd
Shore Pointe Dr
S Shore Blvd
2094
Masters Dr
Deke Slayton Hwy
518
Columbia Memorial
Wood Hollow Dr
Main St
270
Upper Bay Rd
Nassau Bay
NASA One
University of Houston-Clear Lake
Lyndon B Johnson Space Center
Space Center Blvd
Avenue B
2nd St
1st St
5th St
Saturn Ln
Gemini St
Middlebrook Dr
Bayou Rd
Brook Forest Dr
Plum Hollow Dr
El Dorado Blvd
Clear Lake City Blvd
Oak Links Ave
Bay Oaks Blvd
Space Center Blvd
Seahorse Dr
Neptune Ln
Diana Ln
Pineloch Dr
Sun Harbor Dr
Raseda Dr
Ramada Dr
Bay Area Blvd
Buccaneer Ln
El Camino Real
Sea Liner Dr
Galveston Rd
Gatebrook Dr
El Toro
McCord St
X A S
Greig
Kirk Ave
Brantly Ave
Hilliard St
Field Airport
Loop Rd
Goodwin St
FM 1959 Rd
Trister Dr
Gulf Fwy
45
3
Choate Rd
Whitcomb Rd
Beamer Rd
Rex Rd
Hope Village Rd
Tall Ships Dr
Glenwest Dr
Baybrook Mall
W Bay Area Blvd
N Texas Ave
E NASA Rd 1
Webster
Magnolia
Old Galveston Rd
Highway 3
Myrtle Ave
Signal Hill Dr
Pilgrims Point Dr
Blackhawk Blvd
Tibet Rd
Townes Rd
FM 528 Rd
E FM 528 Rd
Clear Creek

Details of Offender

Name	TERRY M LA-CLAIR
Alias Names	TERRY LA-CLAIR ; TERRY MICHAEL LA-CLAIR ; TERRY MICHAEL LACLAIR ; TERRY LECLAIR ; TERRY MICHAEL LECLAIR
ID Marks	
Hair	Brown
Gender	MALE
Height	507
DOB	03/09/1955
Weight	200
Race	WHITE
Eyes	BROWN
Offences	Texas:11990001 SEXUAL ASSAULT
Address	1900 BAY AREA BLVD #E132 HOUSTON HARRIS TX 77058



Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

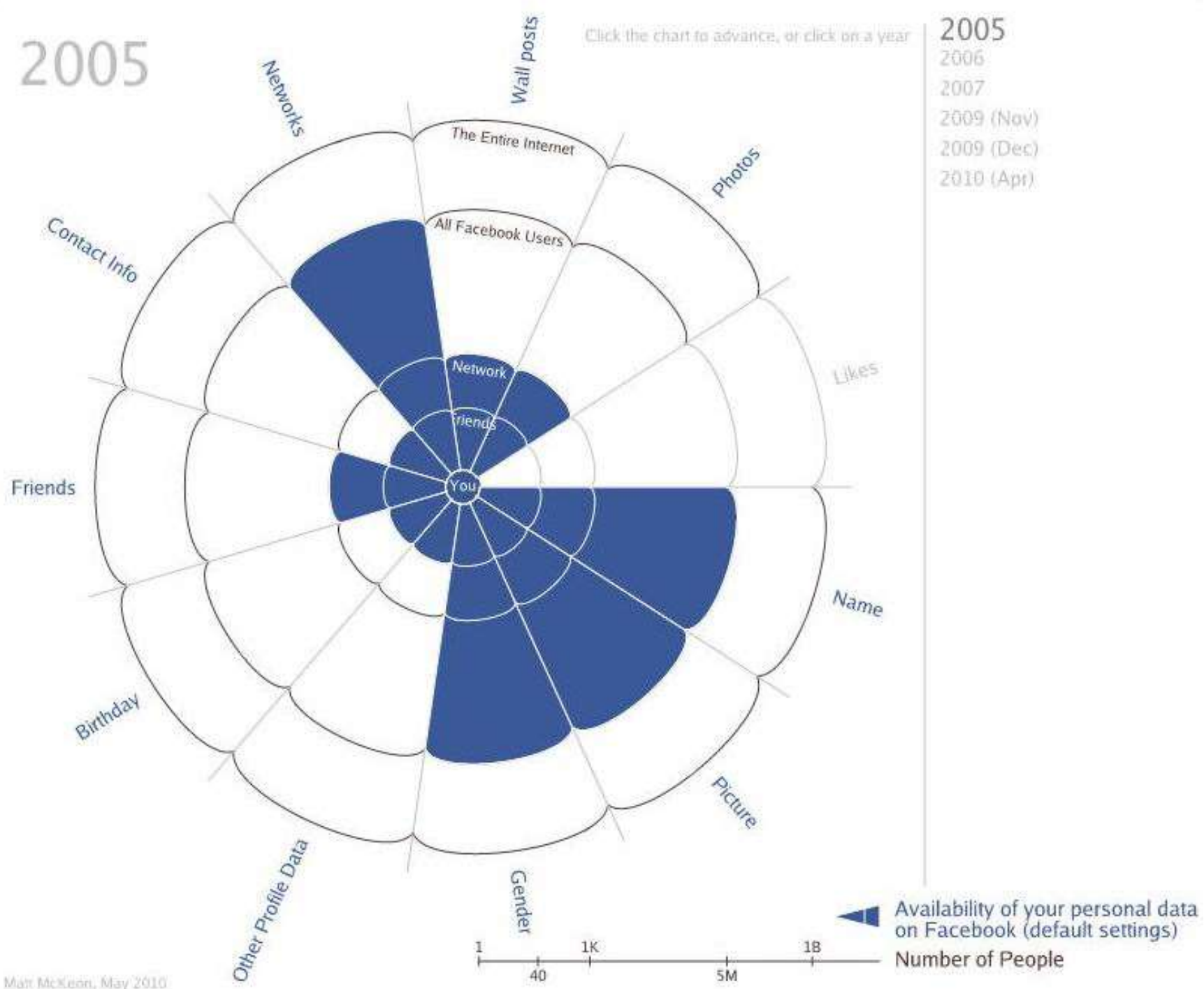
By MAIL FOREIGN SERVICE
Last updated at 2:09 AM on 06th March 2010

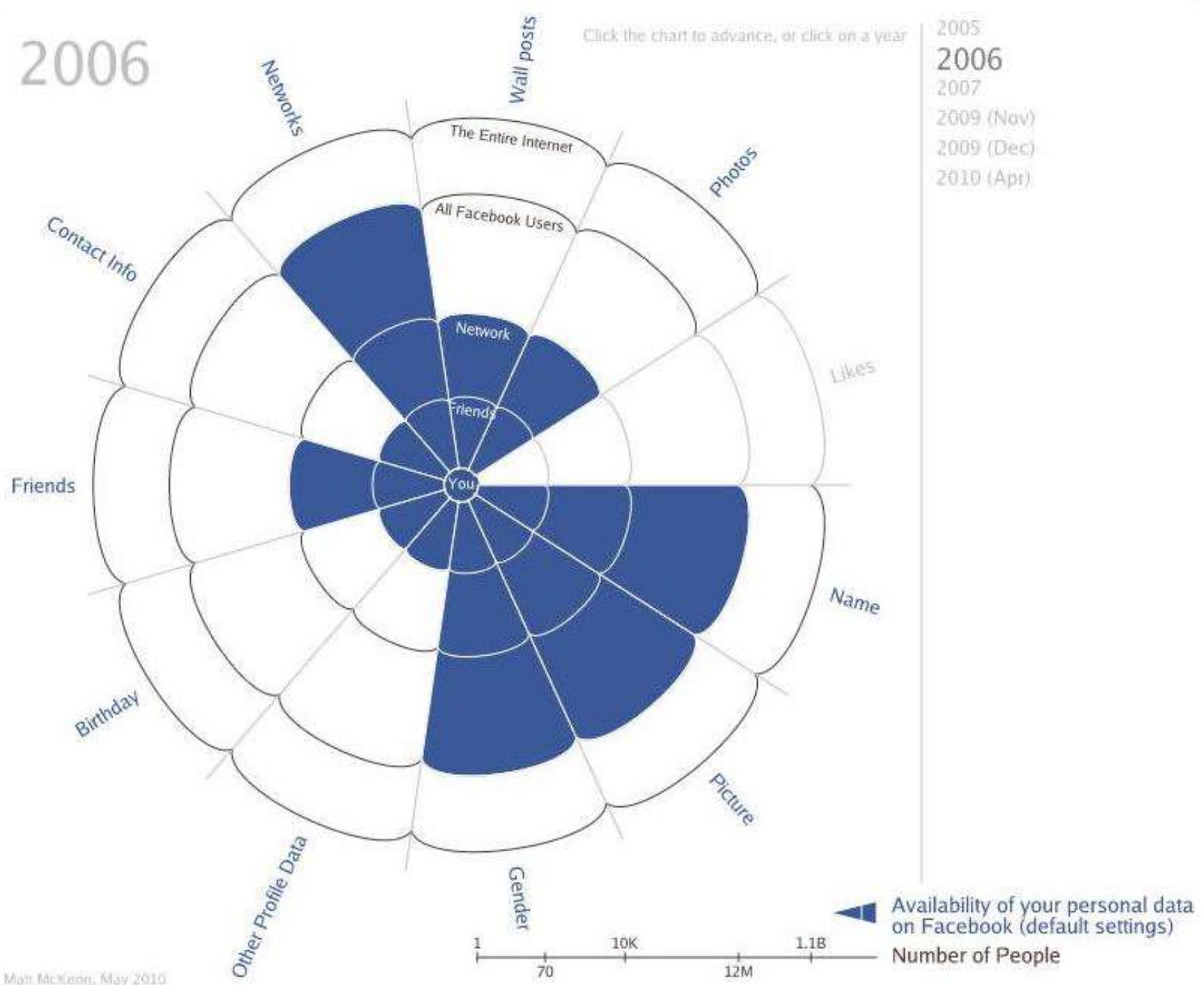
Comments (5) | Add to My Stories

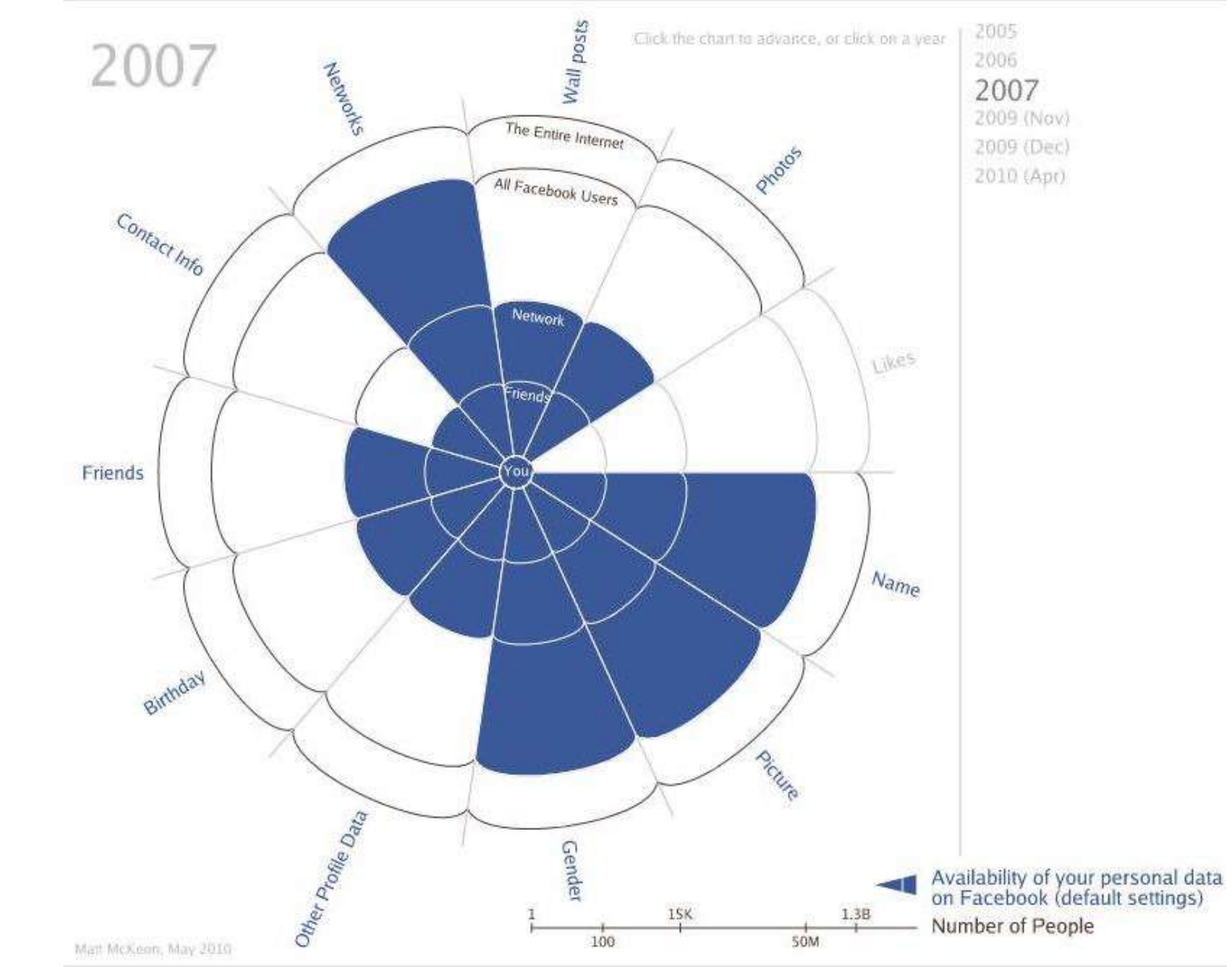
Facebook founder Mark Zuckerberg has been accused of hacking into the email accounts of rivals and journalists.

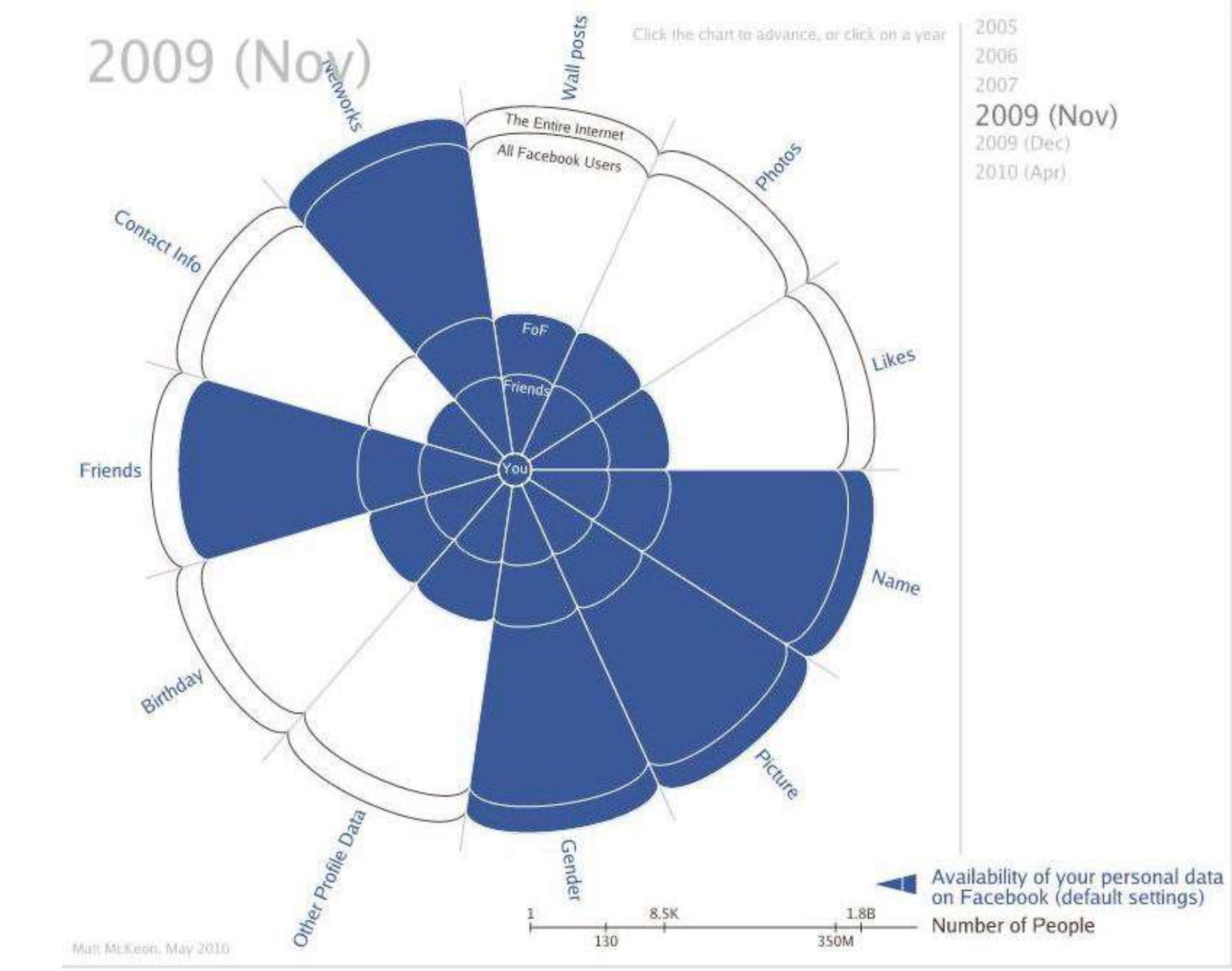
The CEO of the world's most successful social networking website was accused of at least two breaches of privacy in a series of articles run by BusinessInsider.com.

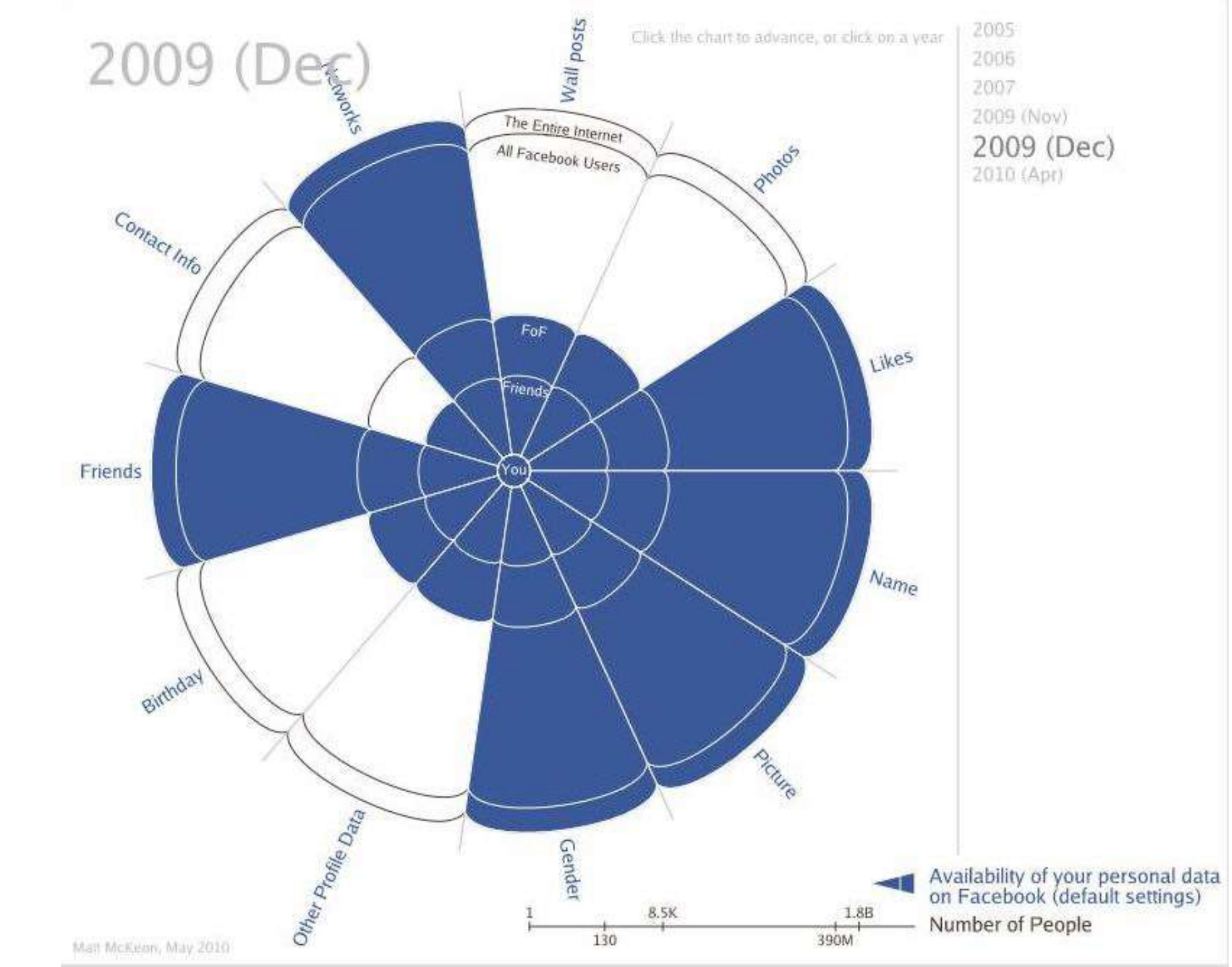
As part of a two-year investigation detailing the founding of Facebook, the magazine uncovered what it claimed was evidence of the hackings in 2004.

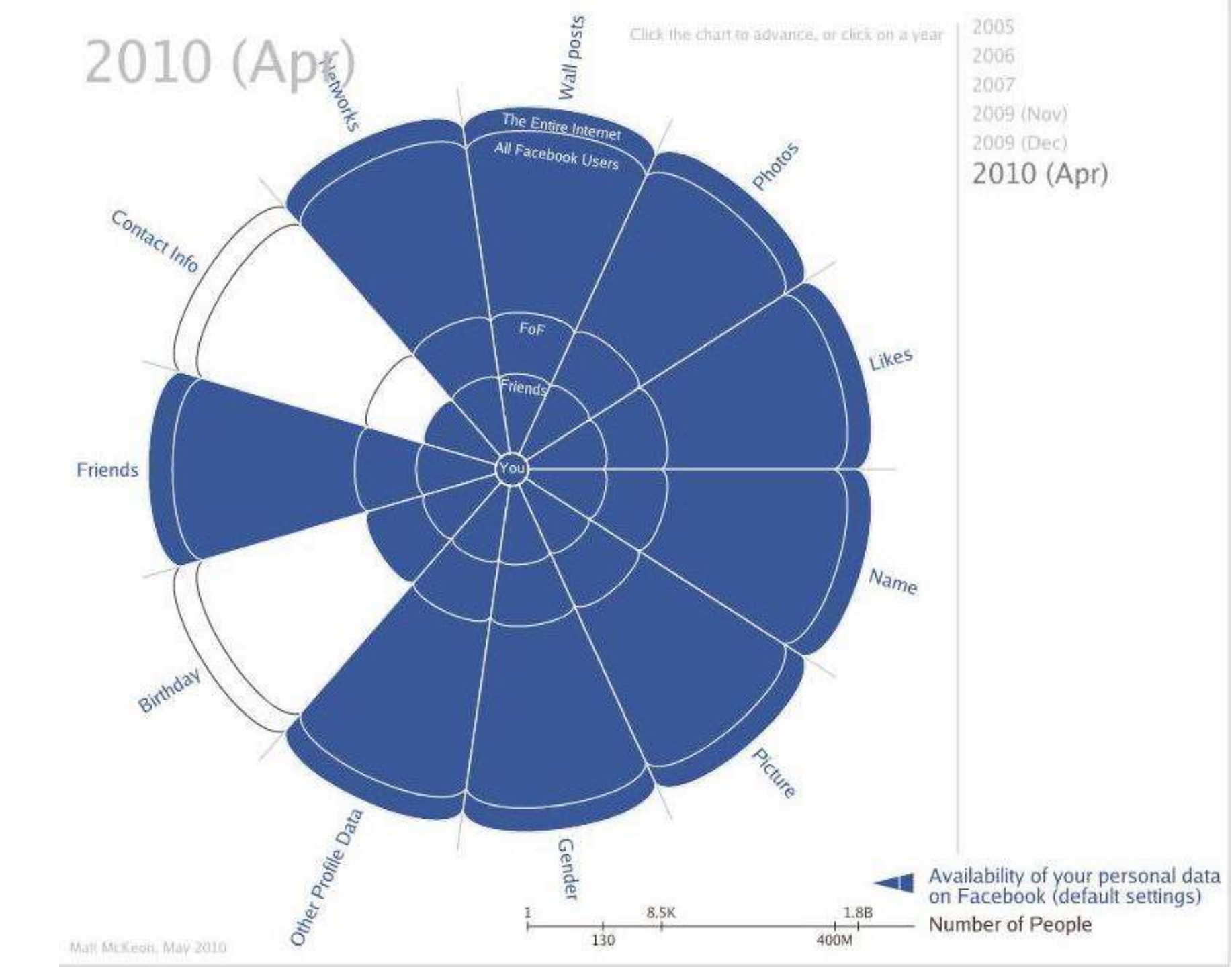

2005
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Contact Info
Likes
Friends
Name
Birthday
Picture
Other Profile Data
Gender
The Entire Internet
All Facebook Users
Network
Friends
You
1
40
1K
5M
1B
Availability of your personal data on Facebook (default settings)
Number of People
Matt McKeon, May 2010


2006
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
Networks
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
70
10K
12M
1.1B
Number of People
Matt McKeon, May 2010


2007
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
Networks
The Entire Internet
All Facebook Users
Network
Friends
You
Availability of your personal data on Facebook (default settings)
1
100
15K
50M
1.3B
Number of People
Matt McKeon, May 2010

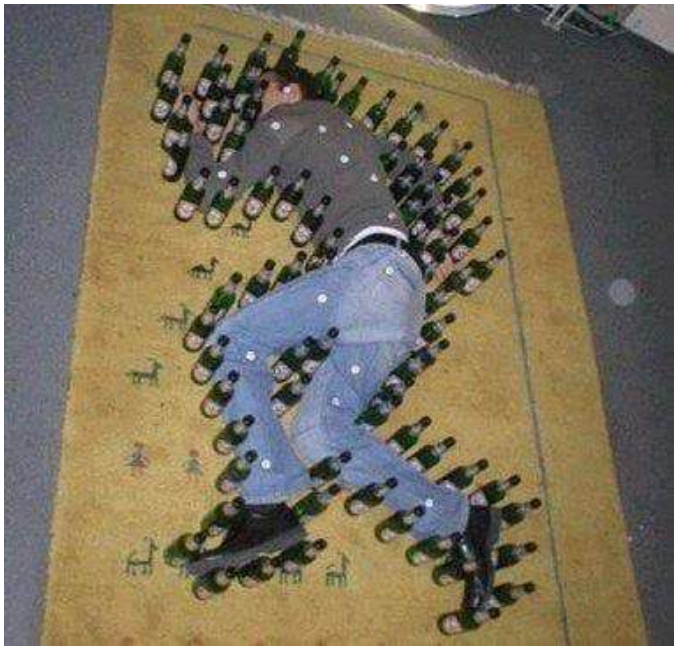

2009 (Nov)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Friends
Contact Info
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
130
8.5K
350M
1.8B
Number of People
Matt McKeon, May 2010


2009 (Dec)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Contact Info
Likes
Friends
Name
Birthday
Picture
Other Profile Data
Gender
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
130
8.5K
390M
1.8B
Number of People
Matt McKeon, May 2010


2010 (Apr)
Click the chart to advance, or click on a year
2005
2006
2007
2009 (Nov)
2009 (Dec)
2010 (Apr)
Networks
Wall posts
Photos
Likes
Name
Picture
Gender
Other Profile Data
Birthday
Contact Info
Friends
The Entire Internet
All Facebook Users
FoF
Friends
You
Availability of your personal data on Facebook (default settings)
1
8.5K
1.8B
130
400M
Number of People
Matt McKeon, May 2010

Jaké informace jsou zneužitelné?

„Táta hodně chlastá, protože jeho šéf je debil.“



„Síť“ ví o našem chování, zvycích, zálibách… „Obsah“ je přitom jen polovina!

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

+ Comment Now + Follow Comments

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole — before Target freaked out and cut off all communications — about the clues to a customer's impending bundle of joy. Target assigns every customer a Guest ID number, tied to their credit card, name, or email address that becomes a bucket that stores a history of everything they've bought and any demographic information Target has collected from them or bought from other sources. Using that, Pole looked at

Girl costs father $80,000 with 'SUCK IT' Facebook post

By **Matthew Stucker,** CNN

March 3, 2014 -- Updated 1255 GMT (2055 HKT)

Probably not the best idea: "Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT."

STORY HIGHLIGHTS

- Patrick Snay filed an age complaint when his work contract wasn't renewed
- He and his employer came to an agreement in which Snay would get an $80,000 settlement
- His daughter posted about the deal, which was meant to be confidential, on Facebook

(CNN) -- The former head of a private preparatory school in Miami, Florida is out an $80,000 discrimination settlement after his daughter boasted about it on Facebook.

Patrick Snay, 69 -- the former head of Guillver Preparatory School -- filed an age discrimination complaint when his 2010-11 contract wasn't renewed.

In November 2011, the school and Snay came to an agreement in which Snay would be paid $10,000 in back pay, and an $80,000 settlement. Gulliver Schools also agreed to cut Snay's attorneys a check for $60,000.

Osobní údaje – někdo má přístup

Dva pracovníci Facebooku vyhozeni za to, že neoprávněně přistupovali k osobním údajům.

Soukromí

Něco, co na internetu a v sociálních sítích nehledejte.

Pamatujte si!

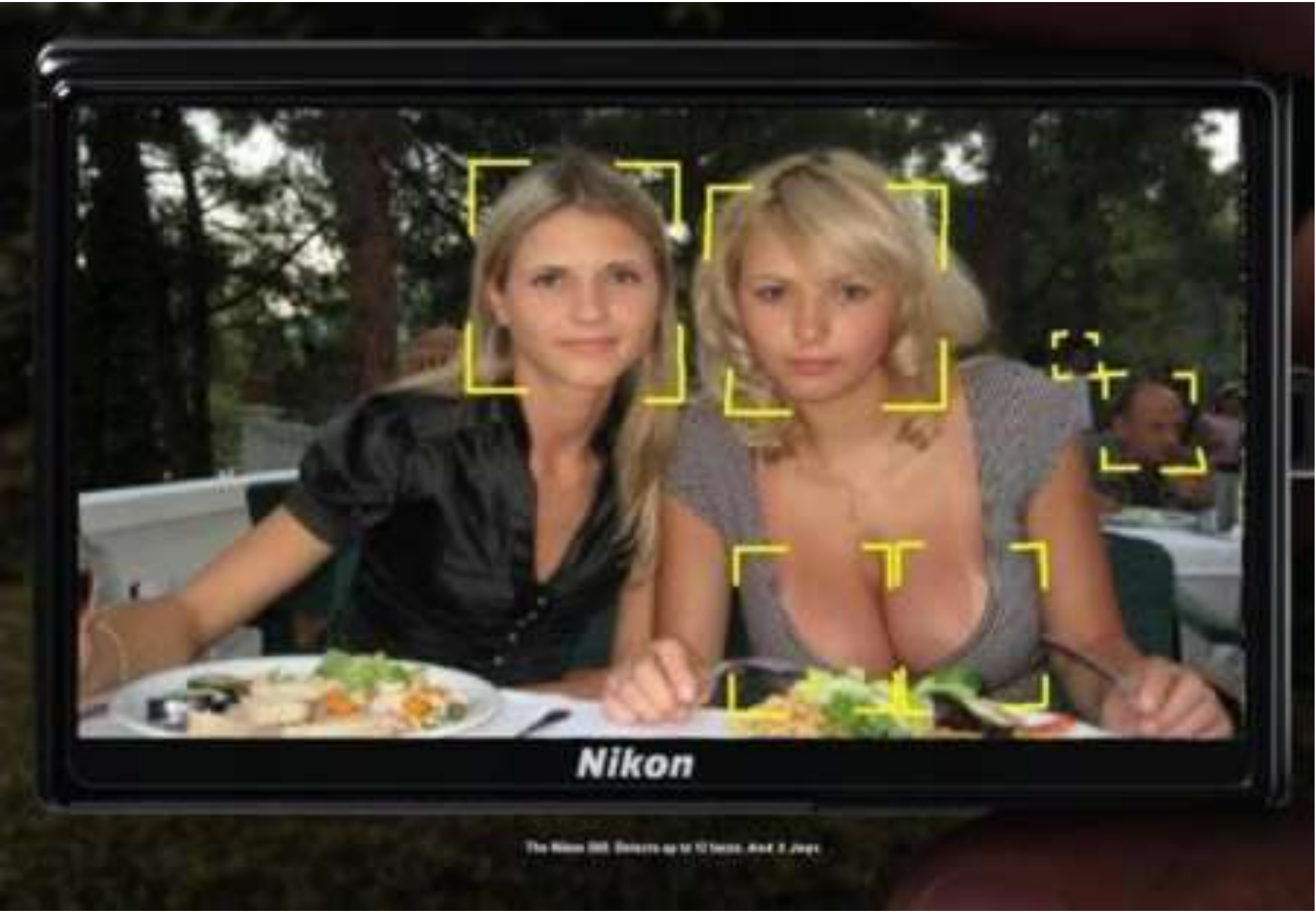
Co internet jednou schvátí, to už nenavrátí!

„Čištění identit“

Specializované agentury, které za drahý peníze odstraňují z internetu stopy „mladické nerozvážnosti“.

Facial Recognition


Elizabeth Sewell
Is this Jason Sewell?
Luceil Sewell
Austin Sewell
unknown face


Nikon

PAMATUJTE SI!

Uvažujte jako útočník!

Neexistuje „bezpečný internet“

Nové není bezpečné!

Nic není bezpečné!

Předcházejte problémům!

foto: Shutterstock

Intimní fotky v mobilu si ukládá málokdo, Češi si dávají pozor

26. února 2013 11:35

BARCELONA - Intimní fotografie, videa či SMS vám mohou v nepovolaných rukou pěkně zavařit. I proto jsou Češi v nakládání s choulostivým obsahem ve svých mobilních telefonech obezřetnější než v zemích západní Evropy a USA. Další možná rizika chytrých telefonů si ale lidé často neuvědomují.

Téměř pět procent Čechů si ve svém chytrém mobilním telefonu nebo tabletu uchovává intimní fotografie nebo videa. K fotografování mobilní telefon používá polovina uživatelů a videa pořizuje třetina. Vyplývá to z průzkumu antivirové firmy AVG, který prezentovala na veletrhu Mobile World Congress.

Jsou to jen stroje

Co internet jednou schvátí, to už nenavrátí!

Dostupnost je také bezpečnost

Nepodceňujte detaily

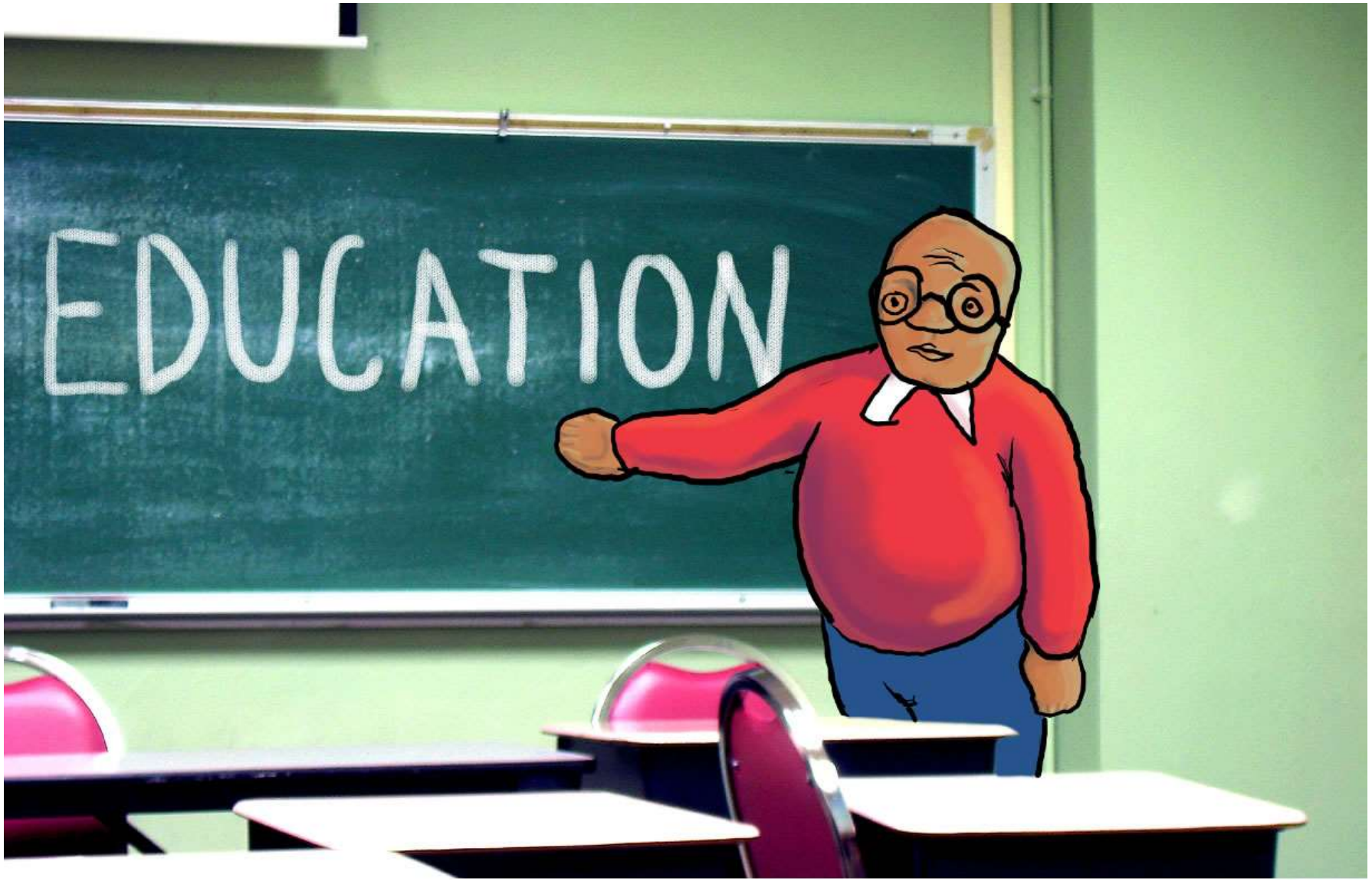
"...HOLD STILL, LARRY, IT'S TAKING ANOTHER PICTURE..."

Můj počítač, můj hrad

Technika není všechno!

Méně je někdy více

Vzdělávejte se!



Připravte se na nepřipravitelné

UŽ NAŠE BABIČKY…

Mluviti stříbro, mlčeti zlato

Jak si kdo ustele, tak si lehne

Práce kvapná, málo platná

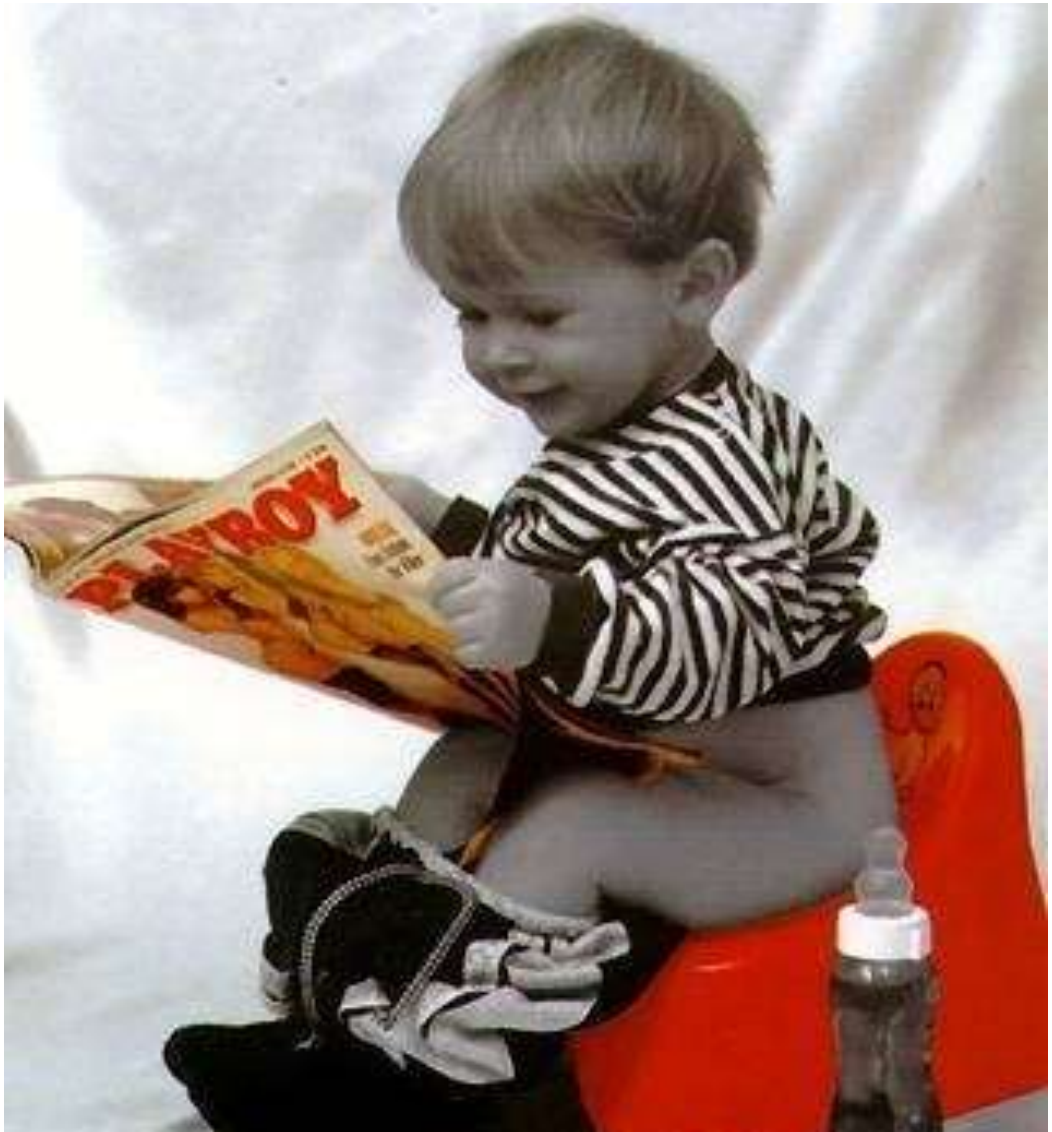
Tak dlouho se chodí se džbánem pro vodu…

Co jsi z úst vypustil,
ani párem koní nedostaneš zpět

Dvakrát měř, jednou řež

Není všechno zlato, co se třpytí

Co se v mládí naučíš, ve stáru jako když najdeš



Děkuji

za pozornost!

Ing. Tomáš Přibyl

tomas.pribyl@seznam.cz

www.kosmonaut.cz