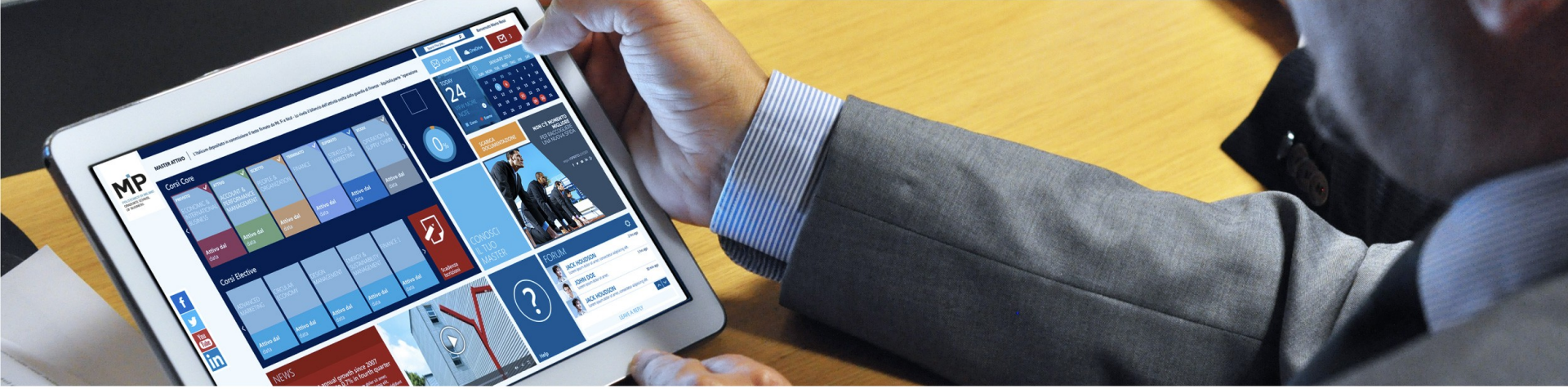


CORPORATE EDUCATION

Smartworking & Cybersecurity

Quali sono i rischi cyber dell'utilizzo dello smartworking? Consigli per lavorare "in sicurezza"?

Igor Falcomatà
CEO, Enforcer

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

FT Executive Education Ranking 2019 · FT European Business Schools Ranking 2018 · Bloomberg Businessweek 2018 Best B-Schools · EFMD EQUIS Accredited · Association AMBA Accredited · EFMD Global Network EOCCS Certified

Il relatore

- attività professionale:
  - analisi delle vulnerabilità
  - simulazioni di attacco
  - consulenza
  - formazione
- altro:
  - fondatore sikurezza.org
  - attivo in vari Linux User Group

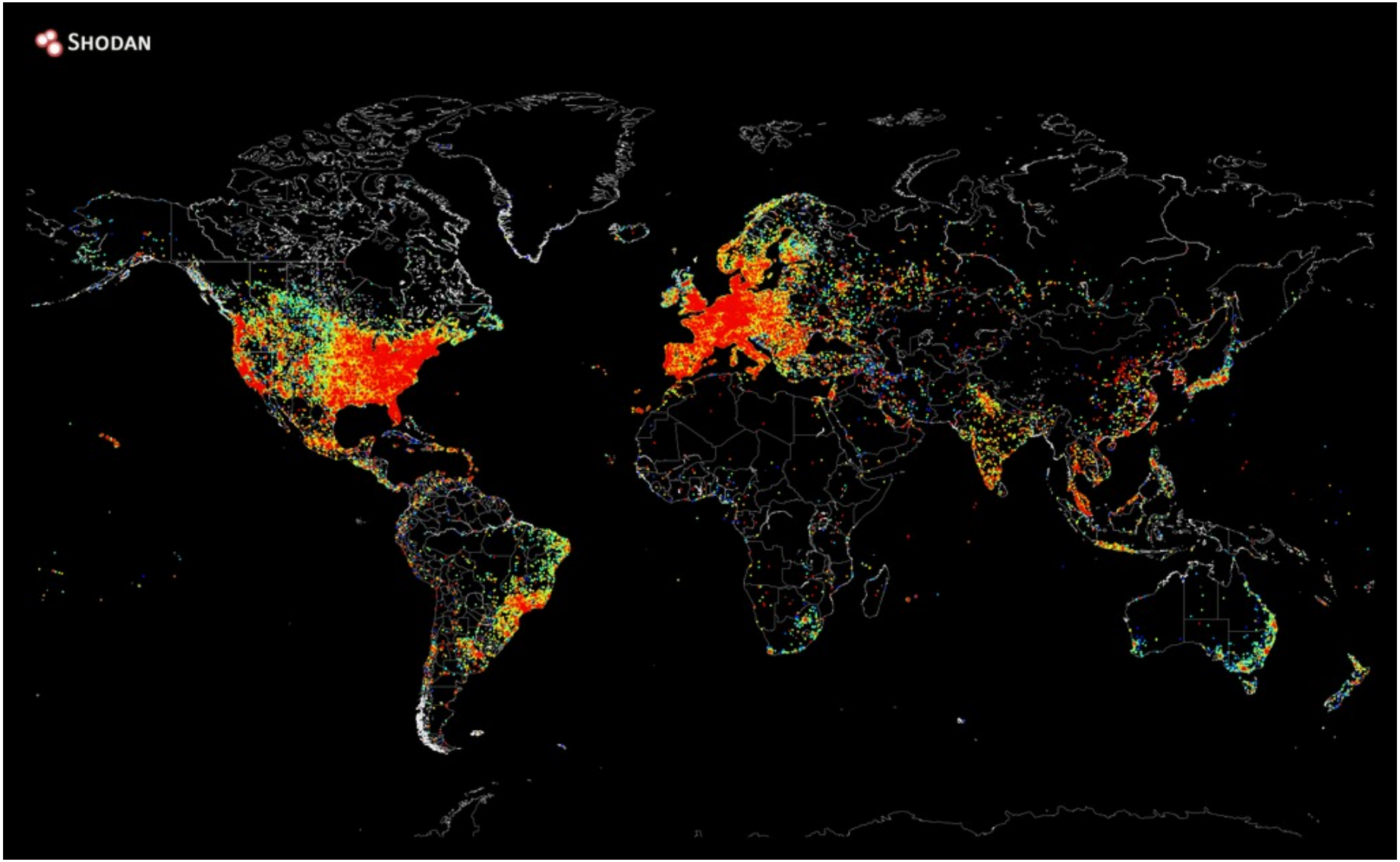
Igor Falcomatà
CEO, Enforcer
ifalcomata@enforcer.it

Agenda

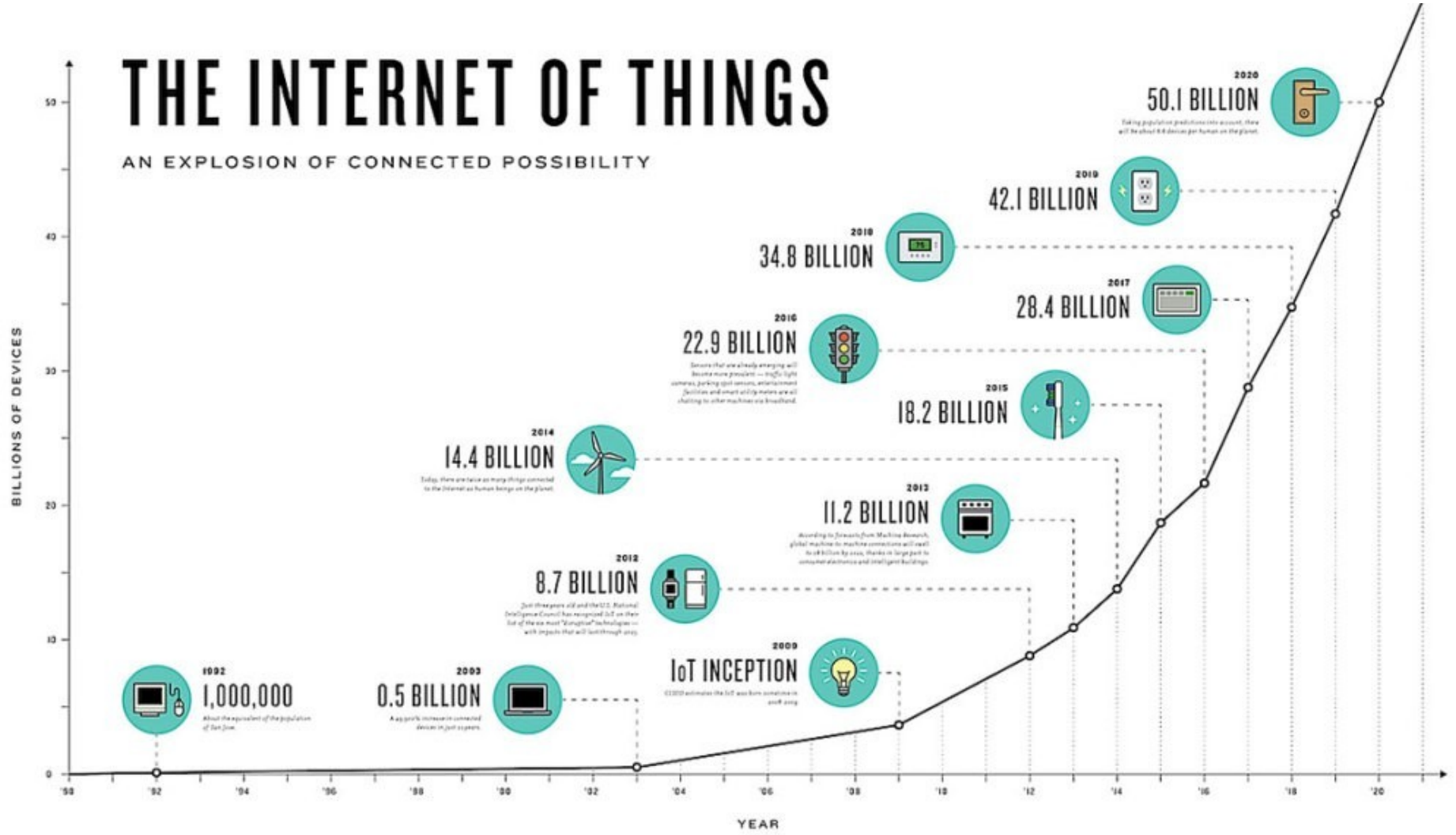
- Il contesto
- Smartworking
- Password
- Email
- Domande & Risposte

Il contesto

E’ un mondo interconnesso..

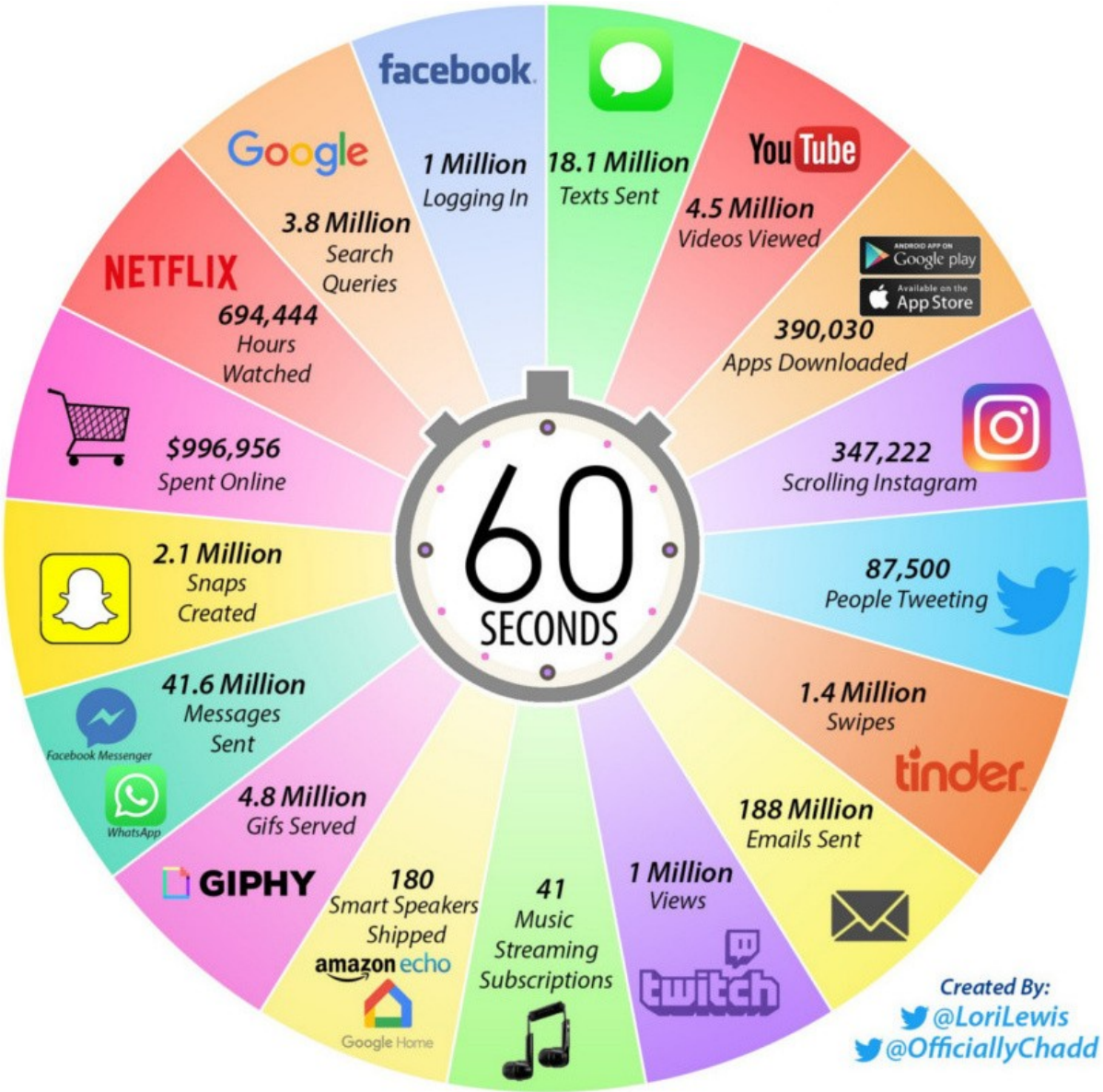


E in crescita..



https://hackernoon.com/internet-of-everything-the-iot-market-is-projected-to-expand-12x-from-2017-2023-175f845c2bcf

The Internet minute



Il contesto (generale)

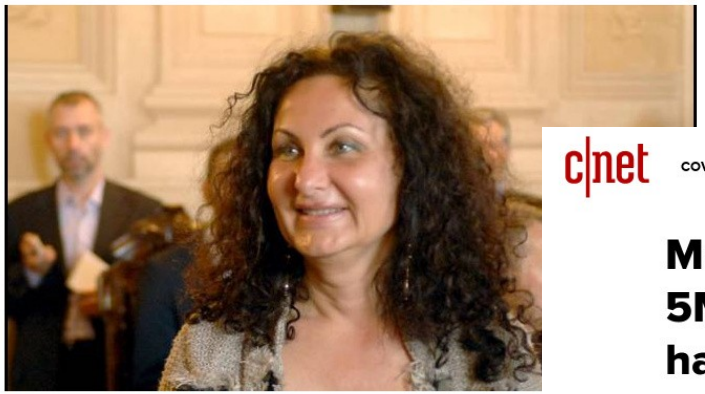
Attacco hacker alla Bonfiglioli. "Chiesto riscatto milioni"

L'azienda decide di non pagare: "Abbiamo scelto di non assoggettarci al ricatto e non alimentare un criminale"

Ultimo aggiornamento il 2 luglio 2019 alle 19:37

49 voti

Condividi Tweet



Attacco hacker alla Bonfiglioli, Sonia: "Non abbiamo ceduto al ricatto" (Foto Serra)

Bologna, 2 luglio 2019 – Un **attacco hacker** accompagnato dalla r **riscatto milionario**. Vittima dei pirati informatici, la **Bonfiglioli Rid** poche ore ha visto l'attività di vari stabilimenti compromessa; con produzione si è fermata per un giorno intero. Ma non ha ceduto a

Forbes

Billionaires Innovation Leadership Money Business Small Business Lifestyle

Aug 16, 2017, 11:47am EDT

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Senior Contributor

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

This article is more than 2 years old.

In June, the NotPetya ransomware hit companies in the U.S. and hardest hit was Copenhagen-Maersk, which moves about one- ions at Maersk terminals in four , causing delays and disruption

c|net

COVID-19 BEST PRODUCTS REVIEWS NEWS HOW TO FINANCE SMART HOME CARS

Marriott data breach exposes over 5M people: Latest major security hack

The hotel chain's most recent security breach is just one of dozens of attacks on various businesses that've revealed people's personal details.

Shelby Brown March 31, 2020 11:15 a.m. PT

Il contesto (particolare)

CORONAVIRUS DATA CENTRE SOFTWARE **SECURITY** DEVOPS BUSINESS PERSONAL TECH

{* SECURITY *}

At least someone's making out like a bandit: Scammers have pocketed $13m in Coronavirus fraud from the US this year

FTC tallies the cost of pandemic rip-offs

By Shaun Nichols in San Francisco 15 Apr 2020 at 02:26 3 SHARE

Fraud related to the coronavirus has cost Americans $13m and so far counting, according to the US government.

The US Federal Trade Commission has tallied up the accumulated cost of scams related to the deadly pandemic from January 1 through the current week.

MENU CERCA Il Messaggero.it

› CORONAVIRUS

Coronavirus, attacco hacker allo Spallanzani e sabotaggio al laboratorio del San Camillo, indaga la Procura

ROMA > NEWS

Mercoledì 1 Aprile 2020

Hanno provato ad attaccare il sistema informatico dell'ospedale **Spallanzani**, centro di eccellenza romano specializzato nella lotta al **coronavirus**, ma non ce l'hanno fatta. Mentre è purtroppo riuscito il raid di vandali o sabatori al **San Camillo**.

CISA CYBER+INFRASTRUCTURE

About Us Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity Landing > Defending Against COVID-19 Cyber Scams

Defending Against COVID-19 Cyber Scams

Original release date: March 06, 2020 | Last revised: April 15, 2020

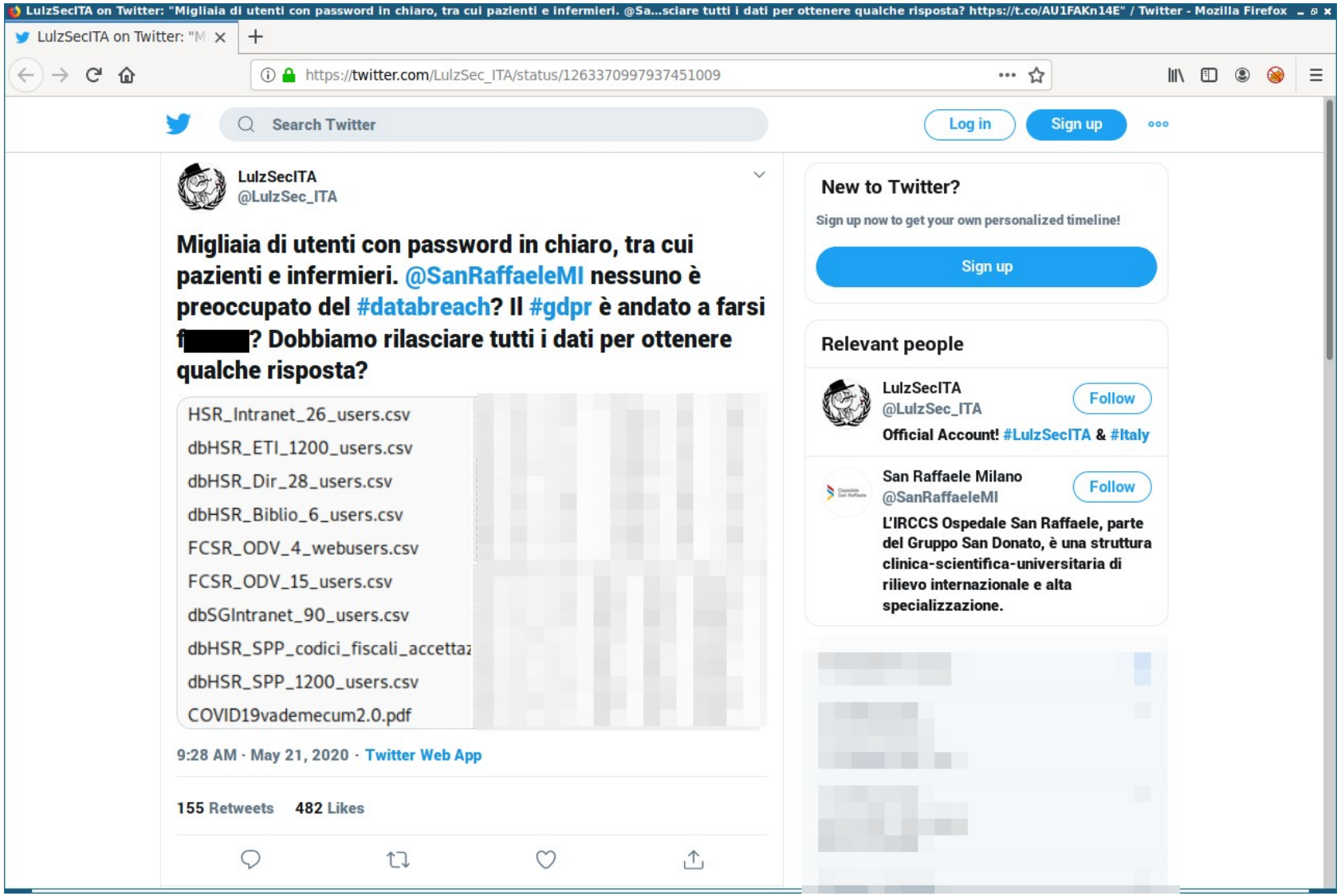
Print Tweet Send Share

The Cybersecurity and Infrastructure Security Agency (CISA) warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

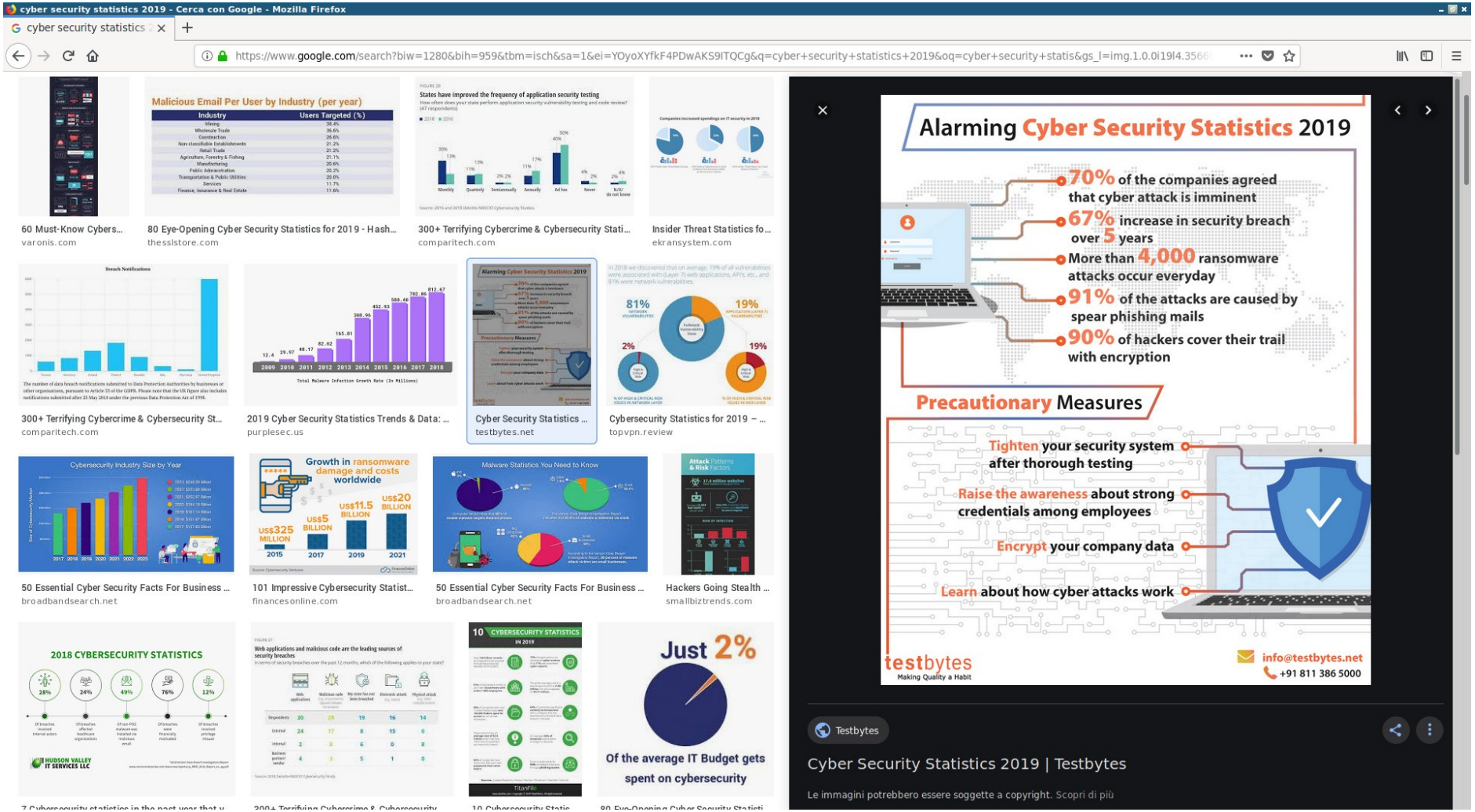
CISA encourages individuals to remain vigilant and take the following precautions.

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.

.. e peggiora..


LulzSecITA on Twitter: "Migliaia di utenti con password in chiaro, tra cui pazienti e infermieri. @Sa...sciare tutti i dati per ottenere qualche risposta? https://t.co/AU1FAKn14E" / Twitter - Mozilla Firefox
LulzSecITA on Twitter: "M
https://twitter.com/LulzSec_ITA/status/1263370997937451009
Search Twitter
Log in
Sign up
LulzSecITA
@LulzSec_ITA
Migliaia di utenti con password in chiaro, tra cui pazienti e infermieri. @SanRaffaeleMI nessuno è preoccupato del #databreach? Il #gdpr è andato a farsi f[redacted]? Dobbiamo rilasciare tutti i dati per ottenere qualche risposta?
HSR_Intranet_26_users.csv
dbHSR_ETI_1200_users.csv
dbHSR_Dir_28_users.csv
dbHSR_Biblio_6_users.csv
FCSR_ODV_4_webusers.csv
FCSR_ODV_15_users.csv
dbSGIntranet_90_users.csv
dbHSR_SPP_codici_fiscali_accettaz
dbHSR_SPP_1200_users.csv
COVID19vademecum2.0.pdf
9:28 AM · May 21, 2020 · Twitter Web App
155 Retweets
482 Likes
New to Twitter?
Sign up now to get your own personalized timeline!
Sign up
Relevant people
LulzSecITA
@LulzSec_ITA
Follow
Official Account! #LulzSecITA & #Italy
San Raffaele Milano
@SanRaffaeleMI
Follow
L'IRCCS Ospedale San Raffaele, parte del Gruppo San Donato, è una struttura clinica-scientifica-universitaria di rilievo internazionale e alta specializzazione.

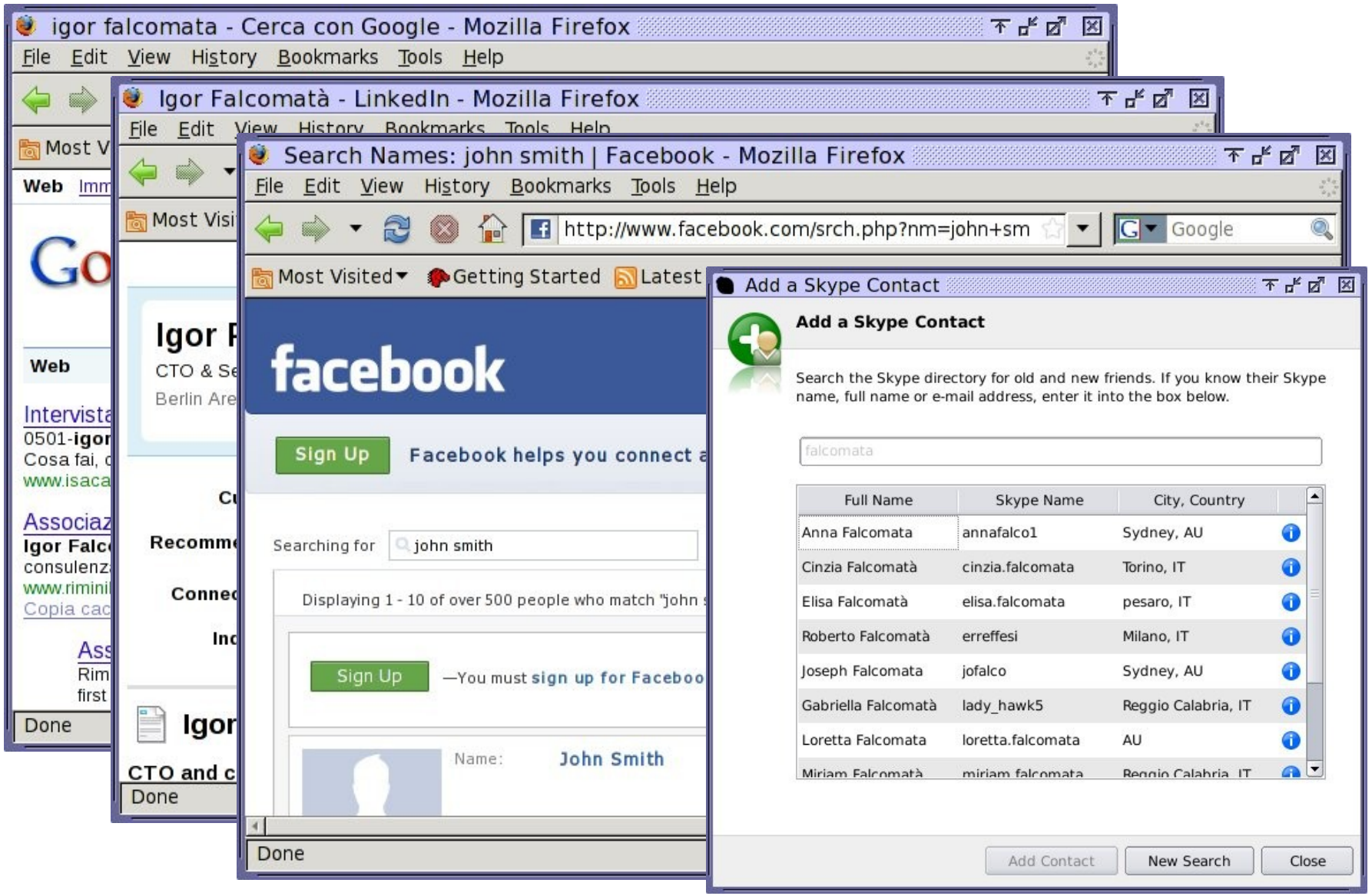
Prima dello smartworking..



Attacchi.. automatizzati

Immagine tratta da: https://limacharlienews.com/cyber/2016-mirai-botnet-hackers-plead-guilty/

Attacchi.. mirati



Competenze tecniche necessarie.. nessuna!

'Tox' Offers Free build-your-own Ransomware Malware Toolkit - Mozilla Firefox

'Tox' Offers Free build-yo

https://thehackernews.com/2015/05/ransomware-creator.html

120%

'Tox' Offers Free build-your-own Ransomware Malware Toolkit

May 29, 2015 Swati Khandelwal

SHARE

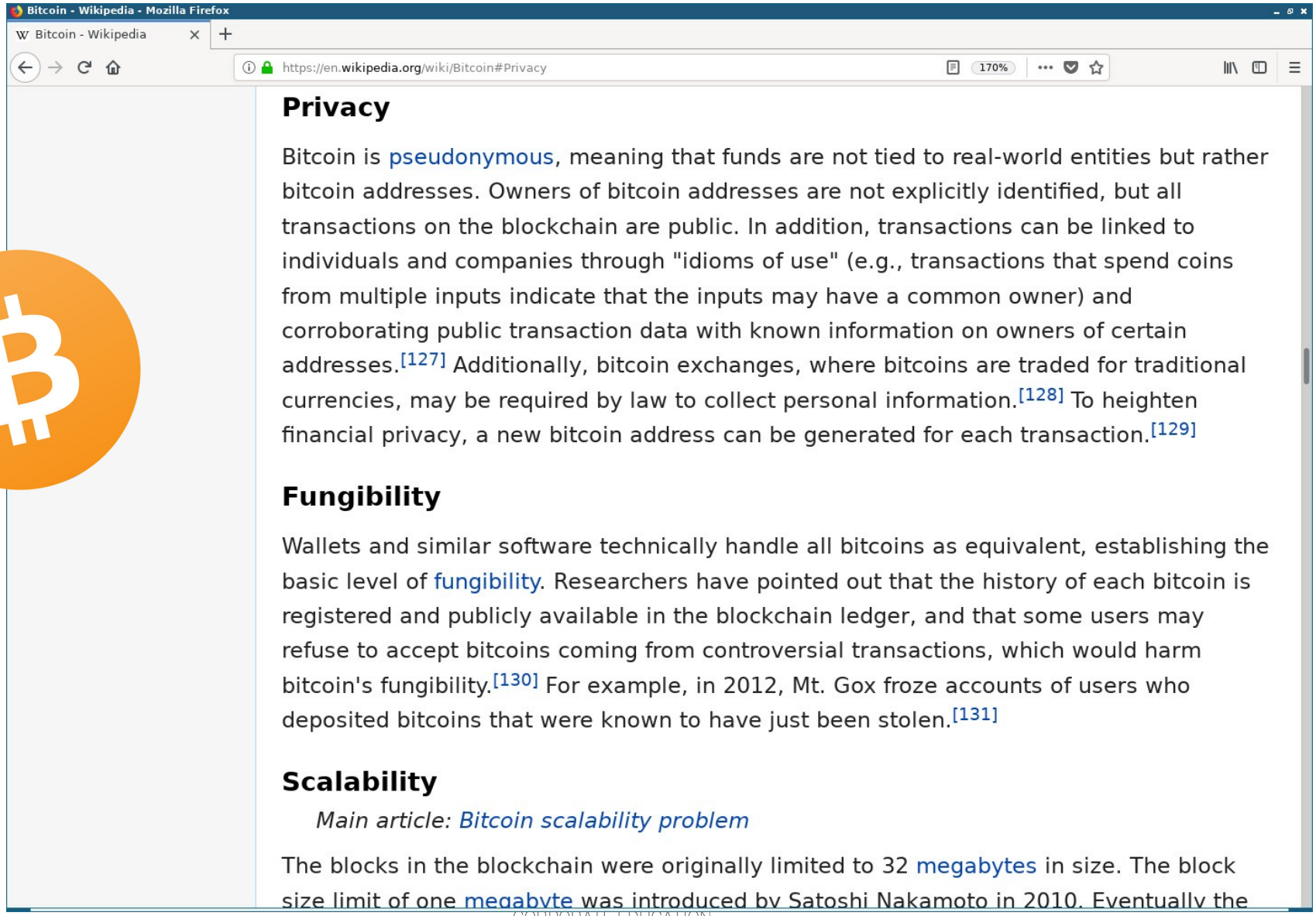
"**Ransomware**" threat is on the rise, but the bad news is that Ransomware campaigns are easier to run, and now a Ransomware kit is being offered by hackers for free for anyone to download and distribute the threat.

Ransomware is a type of computer virus that infects a target computer, encrypts their sensitive documents and files, and locks the out until the victim pays a ransom amount, most often in Bitcoins.

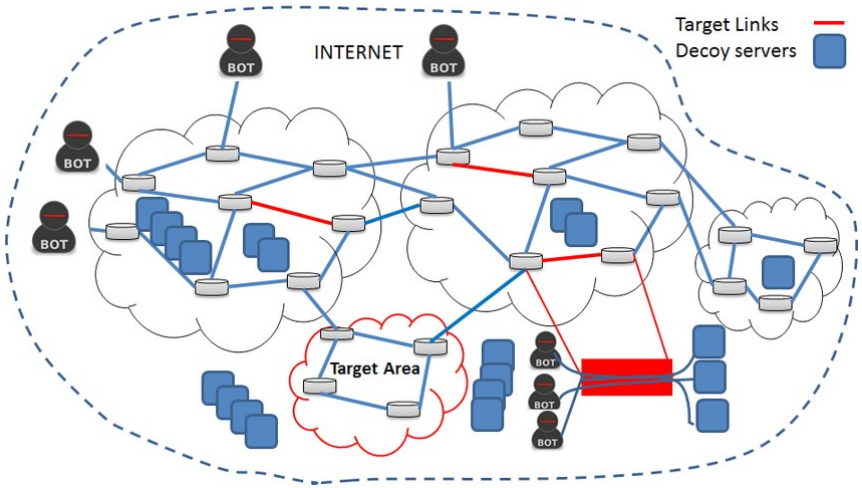
Sometimes even the best security experts aren't able to unlock them and end up paying off ransom to

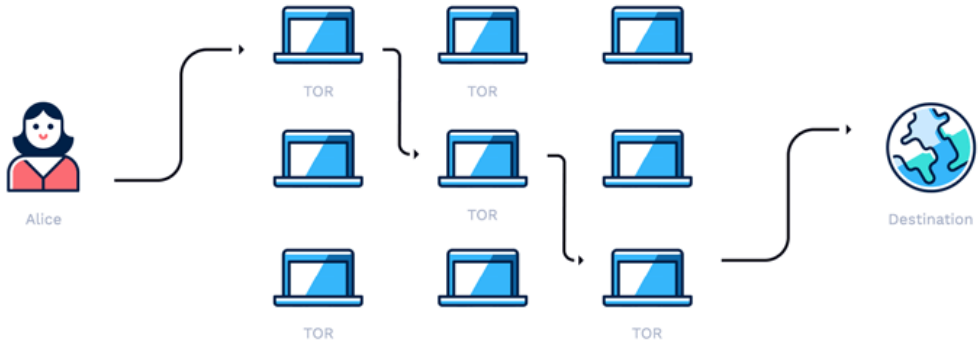
Popular This Week

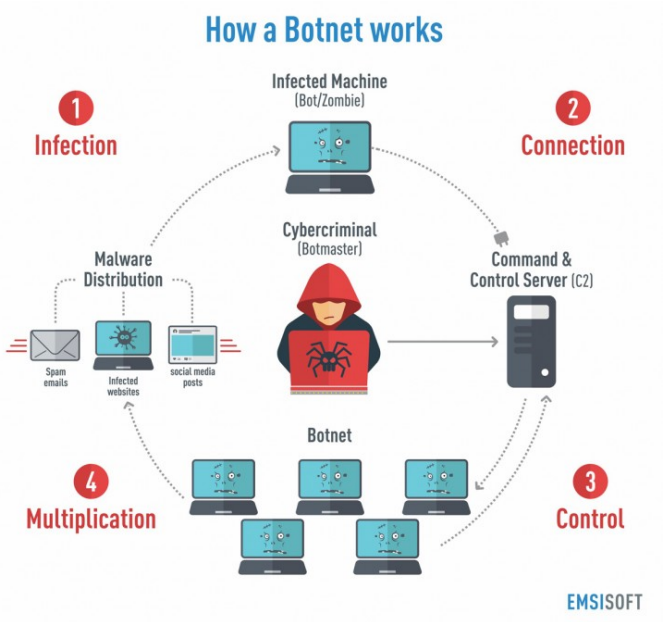
Monetizzabile!



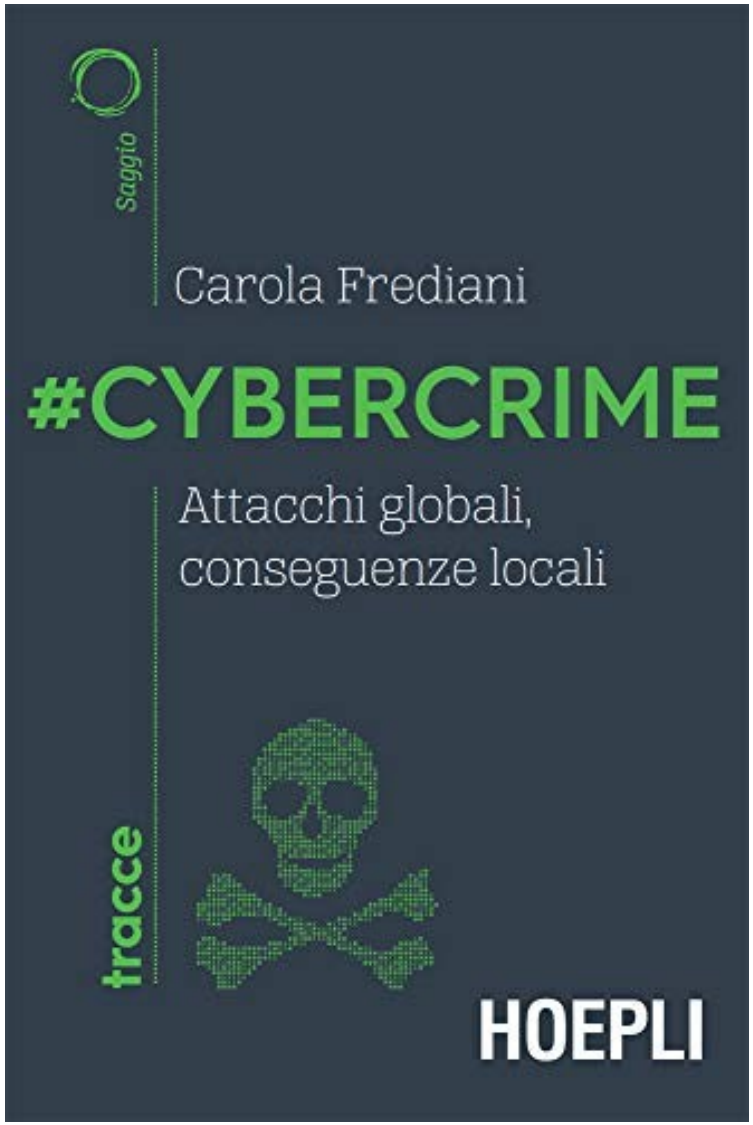
Facile rendersi anonimi..

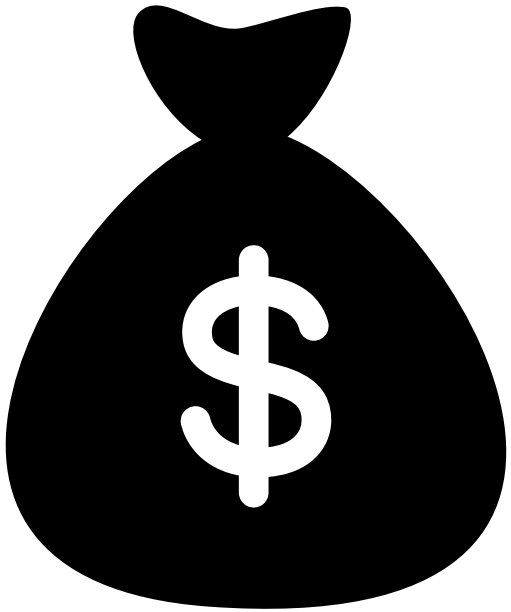




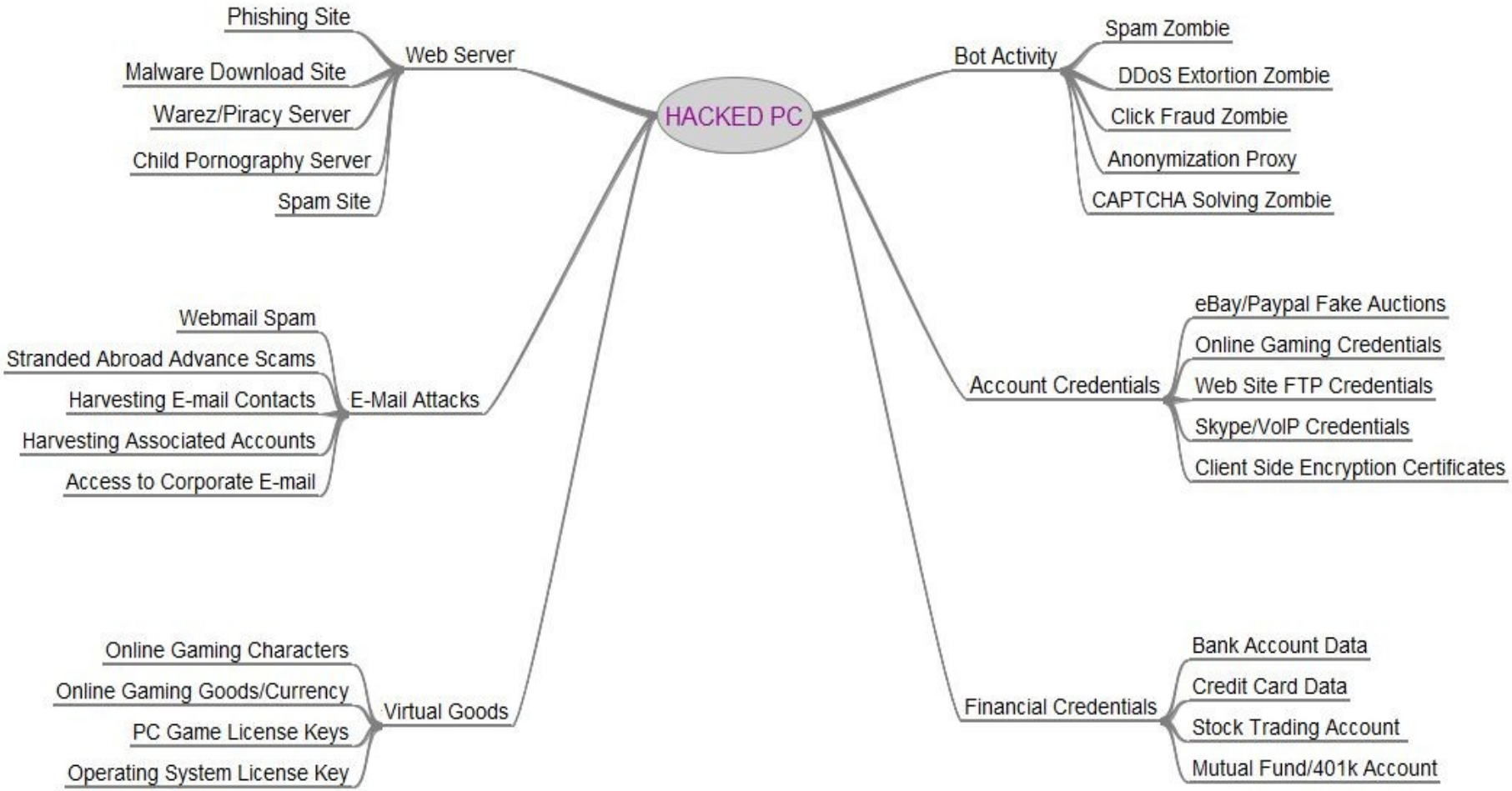


Follow the money!





Dispositivo compromesso → $$



Smartworking

Emergenza..

- Mettiamo tutti in smartworking..
- Un laptop.. il mio regno per un laptop!!
- Dispositivi separati per uso professionale dall'uso privato?
- Chi fa cosa? Utenti? Staff IT?
- E per l'accesso remoto? (VPN, VDI, remote desktop.., teamviewer o simile, ..)
- E per la gestione? (aggiornamenti

Cosa cambia ?

- “Non c’è più il perimetro”
  - (almeno siamo “alla moda”)
- Dispositivi personali ?
  - maggiormente vulnerabili (uso promiscuo, ..)
- Dispositivi aziendali..
  - meno controllabili (aggiornamenti, antivirus, firewall, ..)
- Utilizzo massiccio di “messaging” e “videoconferenza”
  - Dati riservati via email, cloud, ..
- Minore (ehm nessun) contatto diretto con colleghi & co.
  - Maggiore facilità di truffe, social engineering, BEC, ..

Consigli utili

Fonte AgID e CERT-PA
https://www.cert-pa.it/notizie/smart-working-il-vademecum-per-lavorare-online-in-sicurezza/

TECNOLOGIE D'IMPRESA Srl
www.tecnoimp.it

Consigli utili

Fonte AgID e CERT-PA
https://www.cert-pa.it/notizie/smart-working-il-vademecum-per-lavorare-online-in-sicurezza/

Non installare software proveniente da fonti/repository non ufficiali.

Utilizza i sistemi operativi per i quali attualmente è **garantito il supporto.**

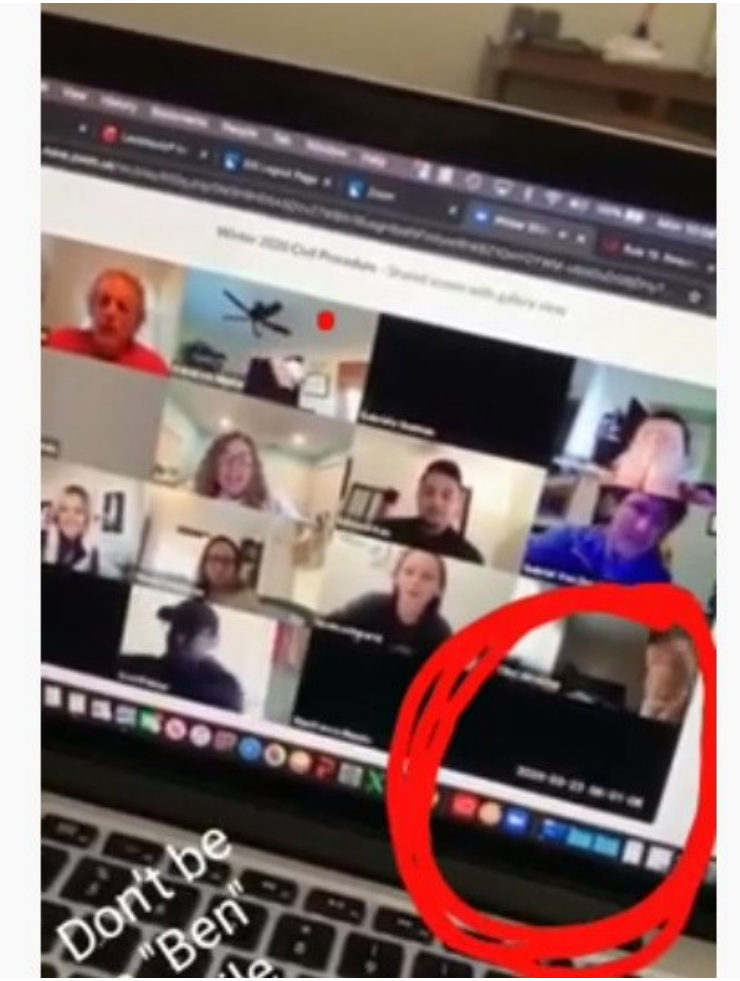
Effettua costantemente gli **aggiornamenti di sicurezza** del tuo sistema operativo.

Assicurati che i **software di protezione** del tuo sistema operativo siano abilitati e **costantemente aggiornati.**

Assicurati che gli **accessi al sistema operativo siano protetti da una password sicura** e **conforme** alle policy dalla tua azienda.

TECNOLOGIE D'IMPRESA Srl
www.tecnoimp.it

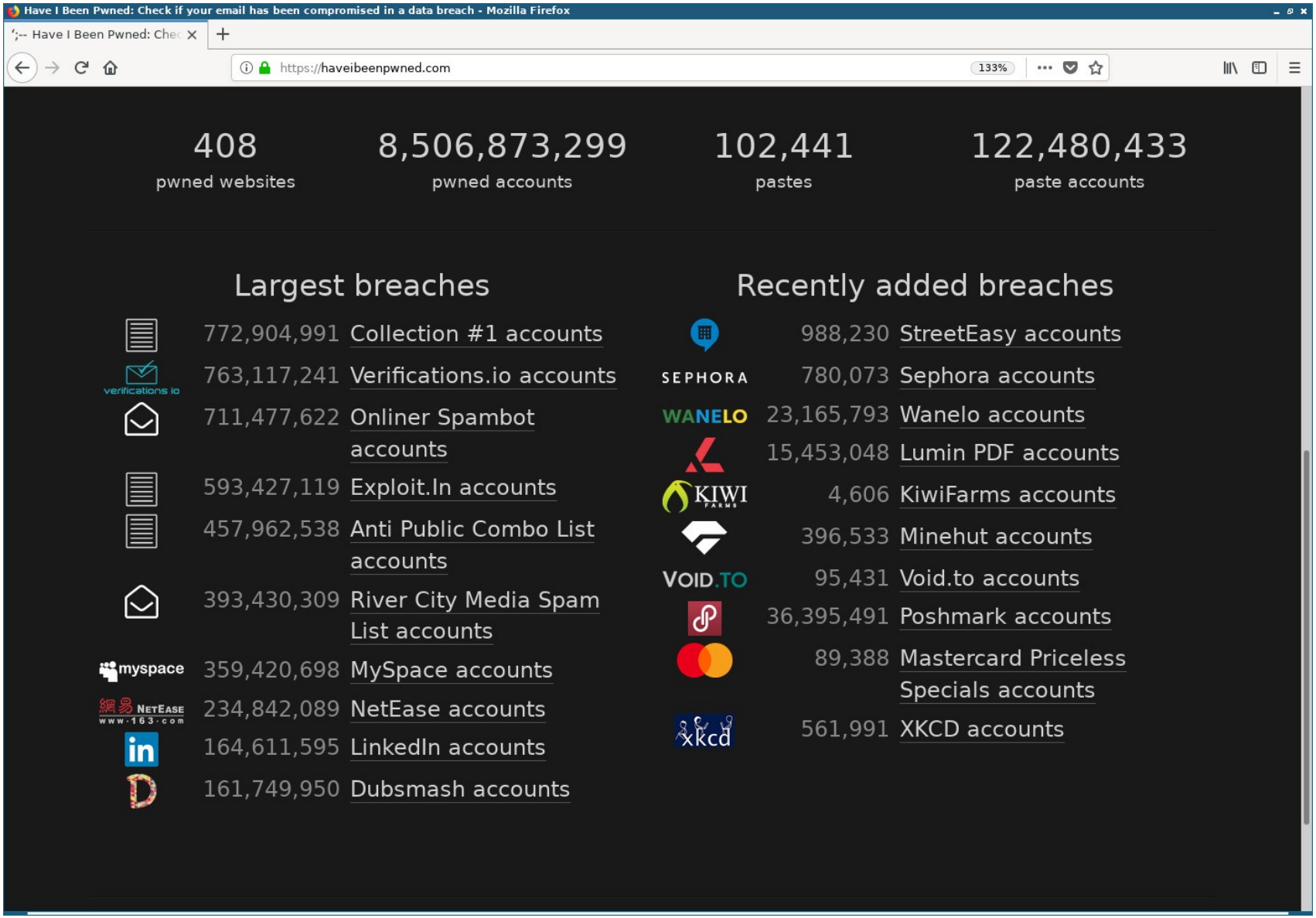
Videoconferenze..



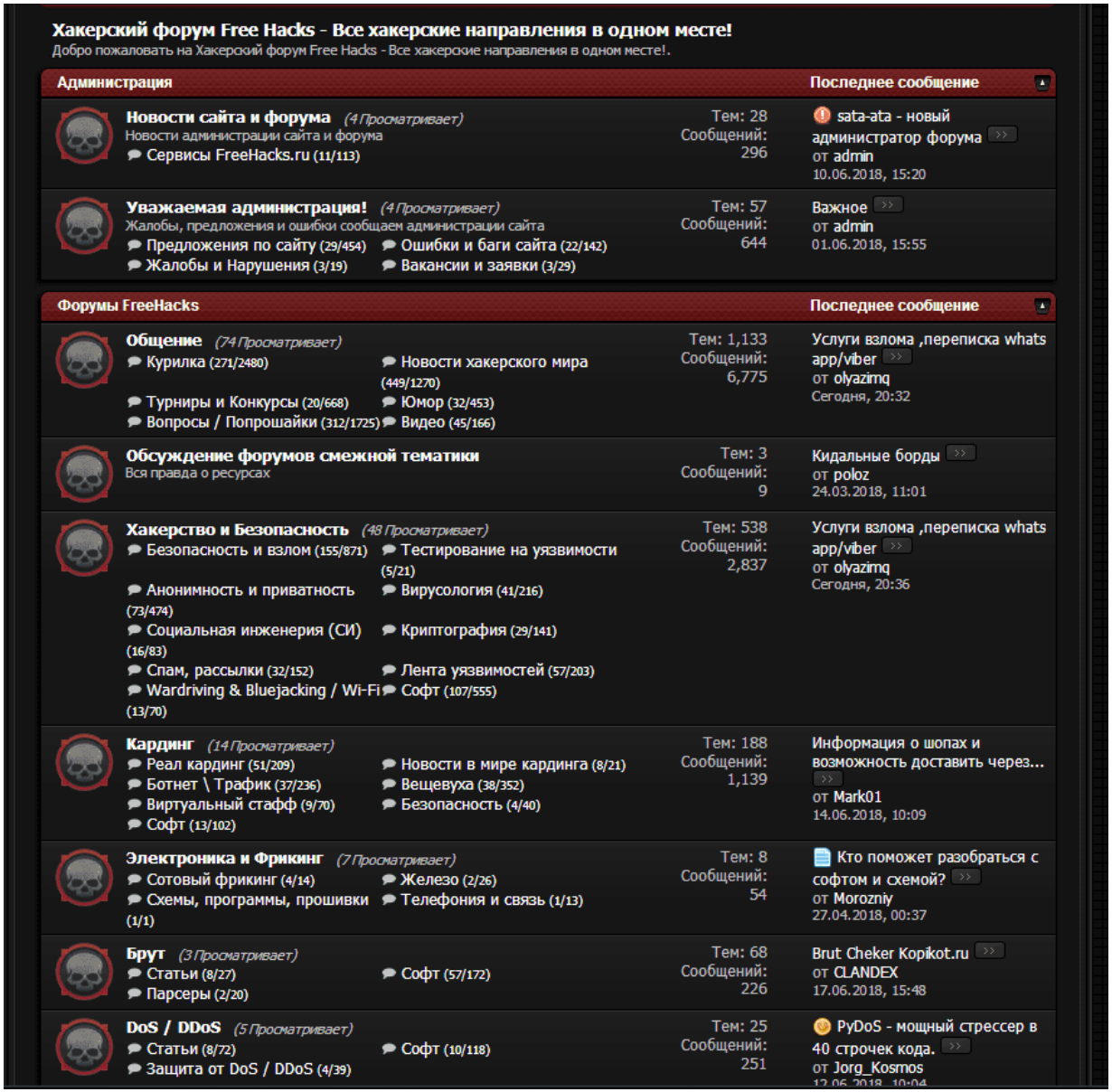
- **Siete in video/audio..**
- **Condivisione desktop..**
- **Controllo accessi**
- **Cifratura end-to-end**
- **Client-less (browser)**
- **Piattaforma “affidabile”**
- **Dispositivo dedicato ?**

Password

Have i been PWNED ?



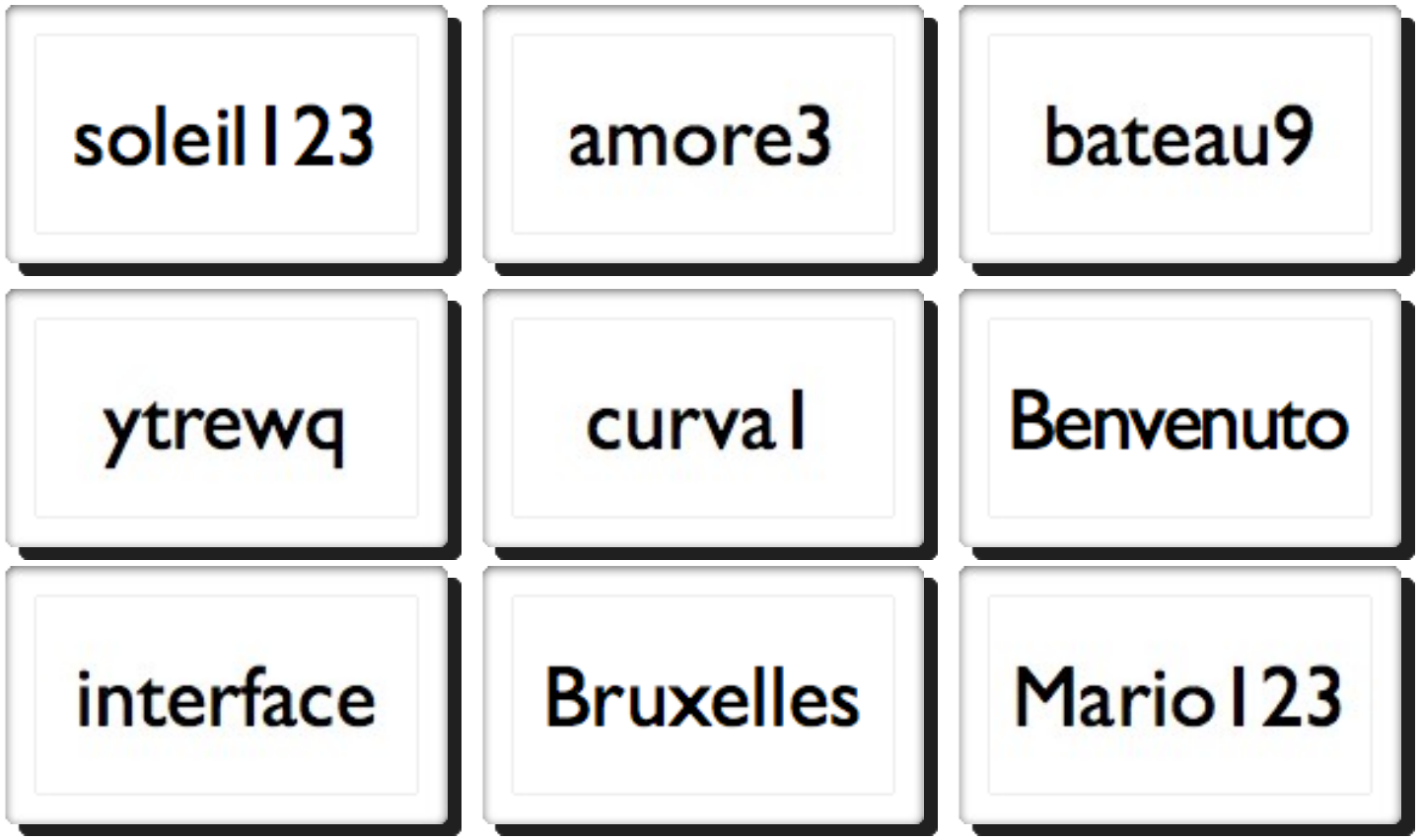
Maybe I don’t saccio!



Password..

Password..

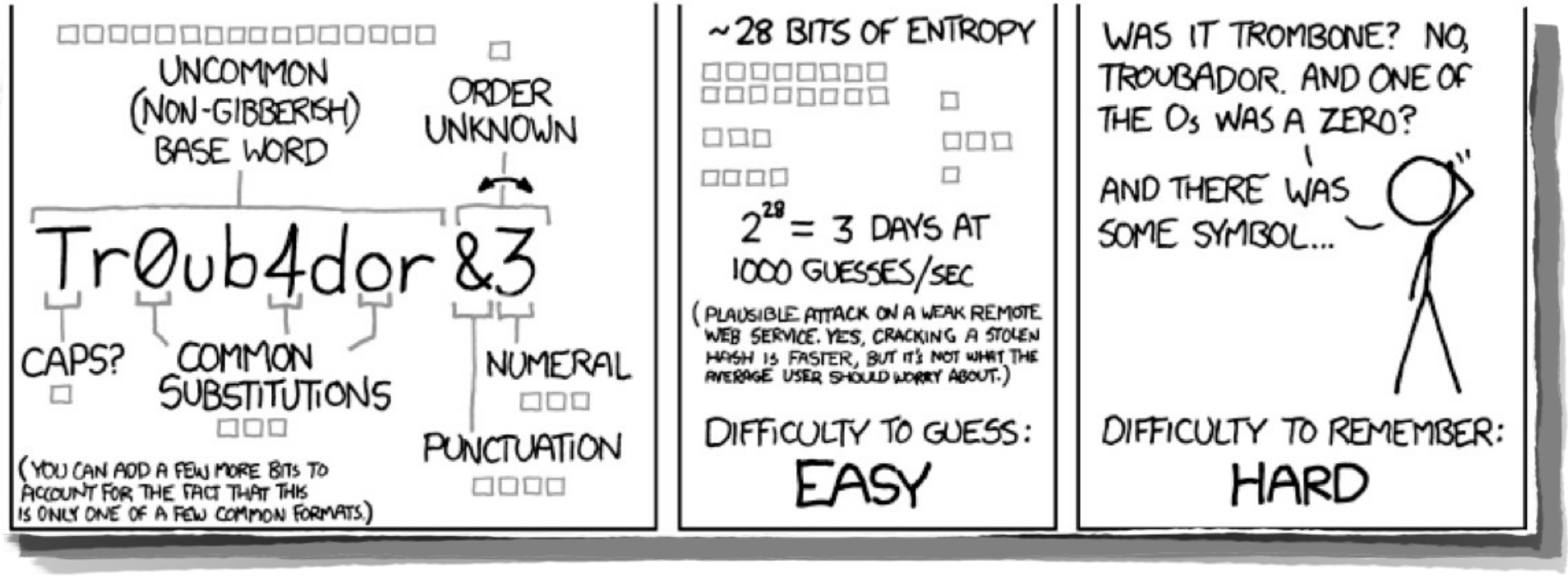
Password..


soleil123
amore3
bateau9
ytrewq
curval
Benvenuto
interface
Bruxelles
Mario123

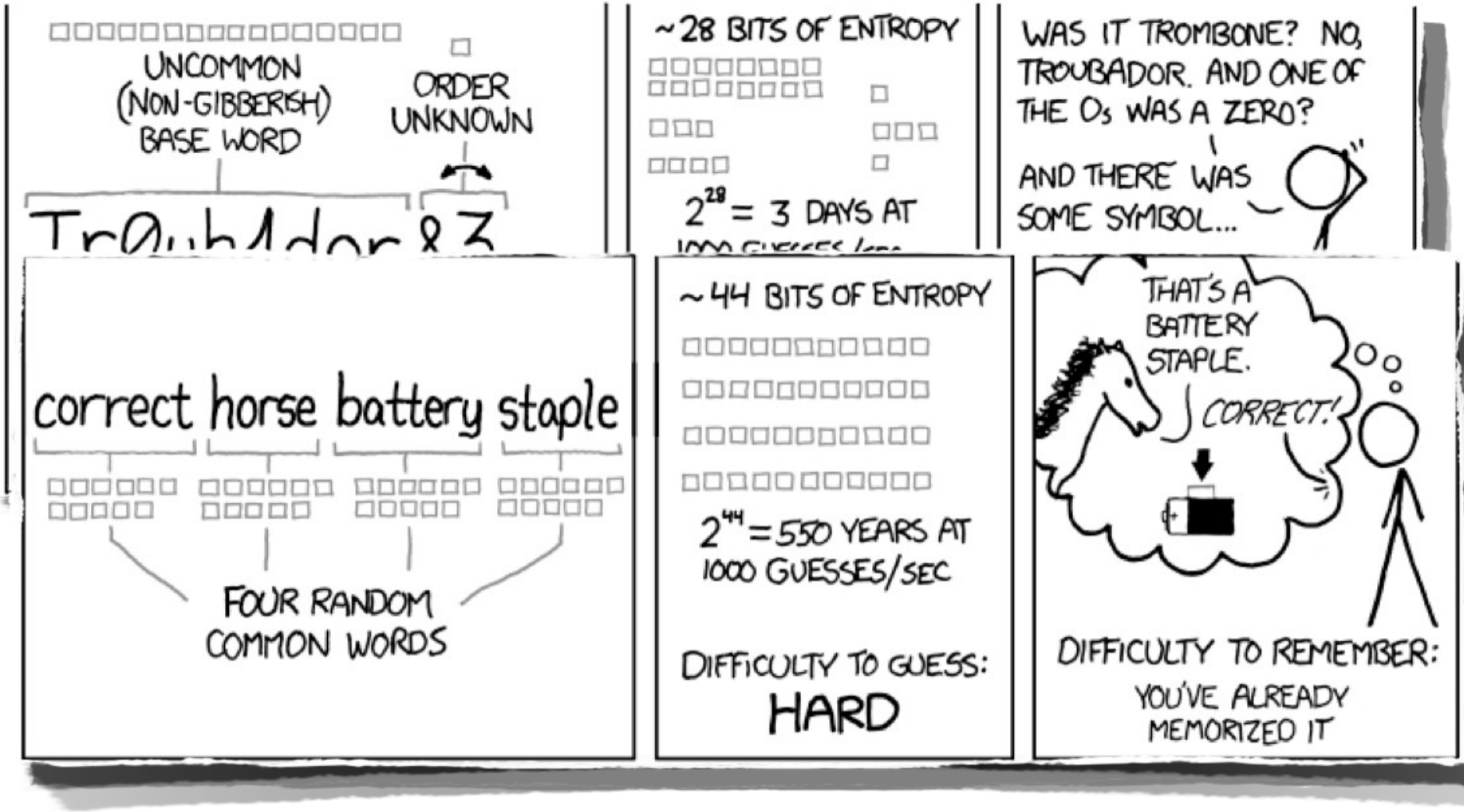
Password..


PASSWORDS ARE LIKE
UNDERPANTS
Change them often, keep them private and never share them with anyone.

Password..


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD

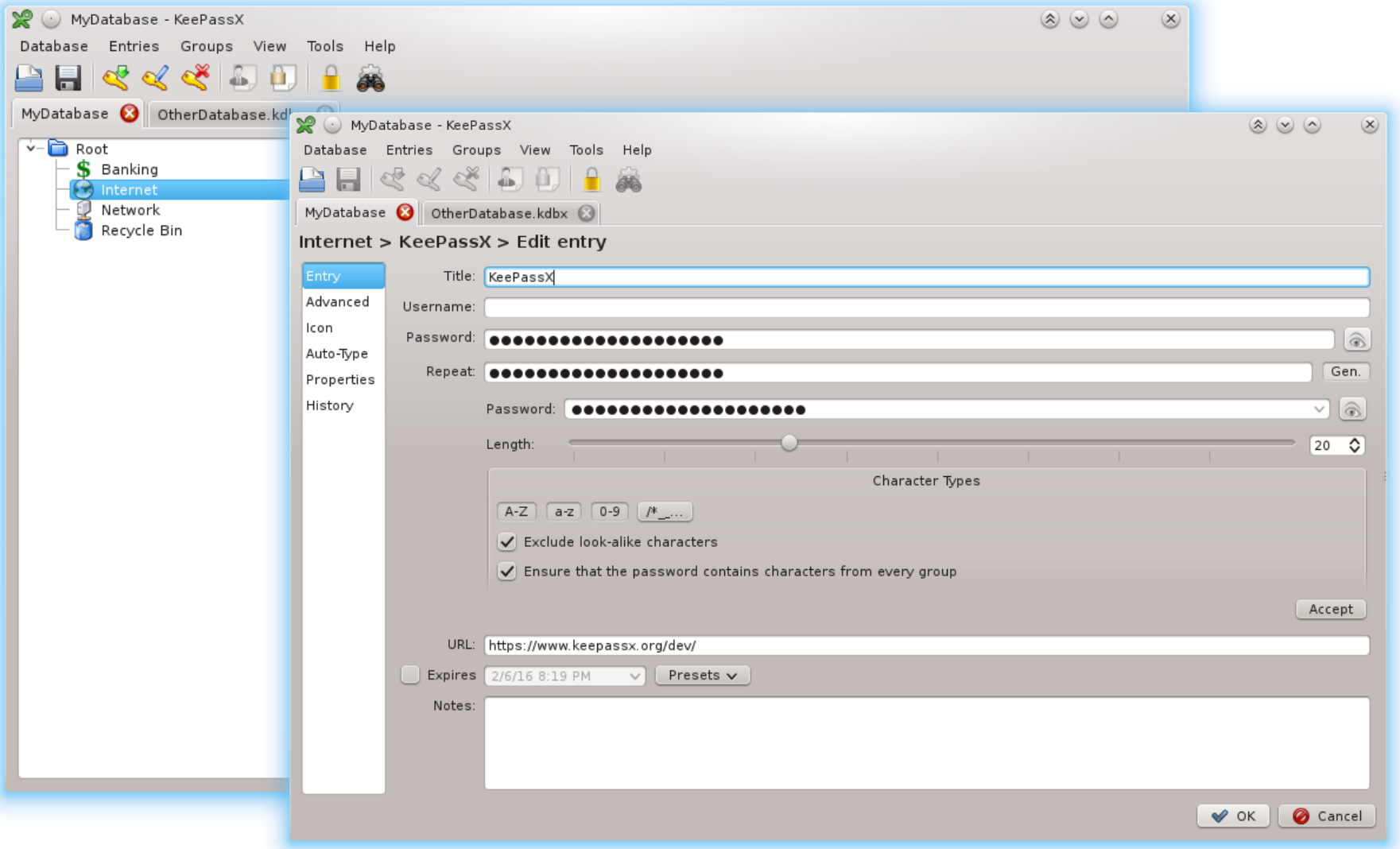
Password..


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

Password robuste

- **Almeno 10 caratteri**
- **Maiuscole, minuscole, numeri**
- **Usare i caratteri “speciali”**
- **Non riutilizzare le password**
- **Usare una frase (passphrase)**

Password manager



2FA, MFA, ..

token

app

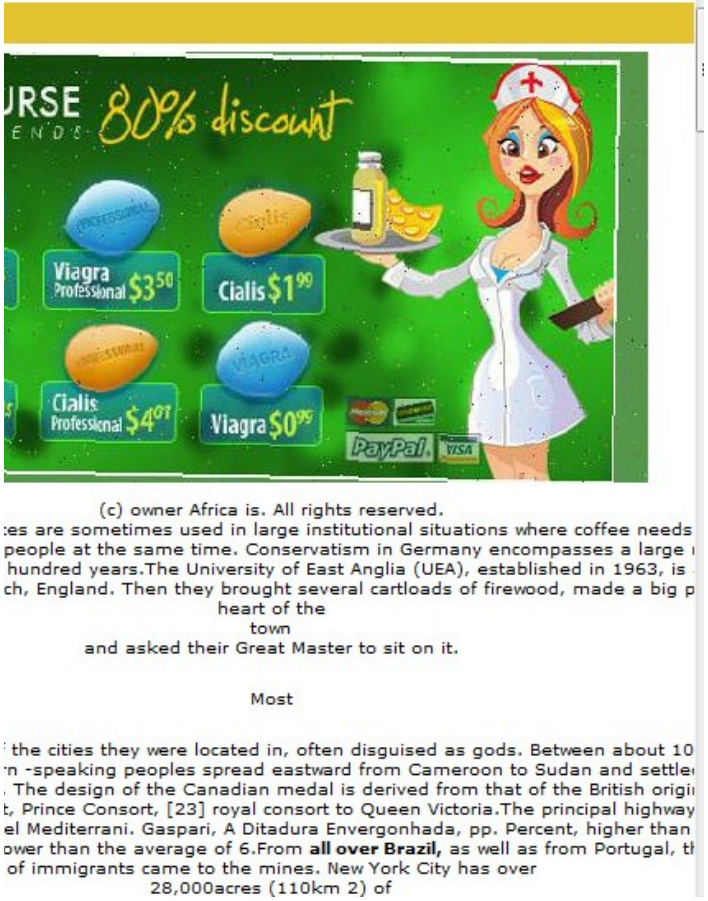

Dite amici,
mostrare il bastone
di Gandalf,
ed entrate!

Email

SPAM


SULLA POLIZZA A
RISPARM
FINO AL
40
Dettaglio s
FAI IL PREVEN
IN PIÙ, CON
Risparmiare tempo
Fai tutto online, via telefono, email o fax. 24 ore su 24.
Avere tutta la sicurezza


Important Information on your Life Insurance
PLANS FOR LESS THAN
$1
per day
Life Insurance Simplified.
Get up to $1,000,000 in Life Insurance coverage.
No physical medical exam.
Get insured in 20 minutes.
Get a FREE quote in 2 minutes.
CLICK TO START
100% Guaranteed Acceptance policies available for ages 18-79.
30-Day Money Back Guarantee. Tax-Free Protection for your Family!
Accidental Death & Dismemberment
Low cost coverage. If you're 25-44, accidental death is your life's single biggest risk.
Level Term Life Insurance
The best, most affordable way to protect your family's future.
Final Expense & Burial Insurance
Simple coverage to remove the burden of funerals and other final expenses.

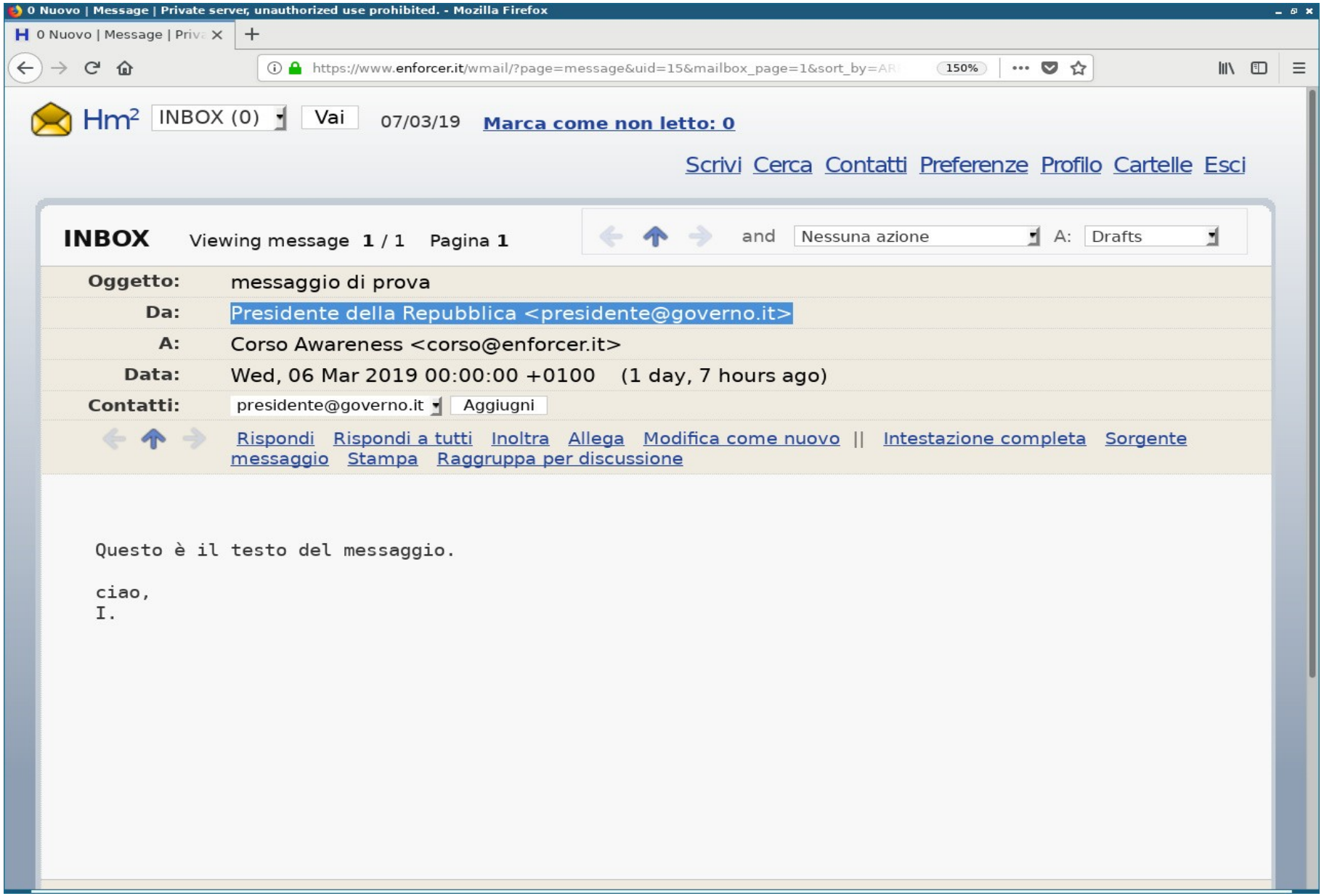

URSE
80% discount
Viagra Professional $3.50
Cialis $1.99
Cialis Professional $4.07
Viagra $0.99
PayPal
VISA
(c) owner Africa is. All rights reserved.
es are sometimes used in large institutional situations where coffee needs
people at the same time. Conservatism in Germany encompasses a large
hundred years.The University of East Anglia (UEA), established in 1963, is
ch, England. Then they brought several cartloads of firewood, made a big p
heart of the
town
and asked their Great Master to sit on it.
Most
the cities they were located in, often disguised as gods. Between about 10
n -speaking peoples spread eastward from Cameroon to Sudan and settle
The design of the Canadian medal is derived from that of the British origi
t, Prince Consort, [23] royal consort to Queen Victoria.The principal highway
el Mediterrani. Gaspari, A Ditadura Envergonhada, pp. Percent, higher than
ower than the average of 6.From all over Brazil, as well as from Portugal, th
of immigrants came to the mines. New York City has over
28,000acres (110km 2) of

Difendersi dallo SPAM

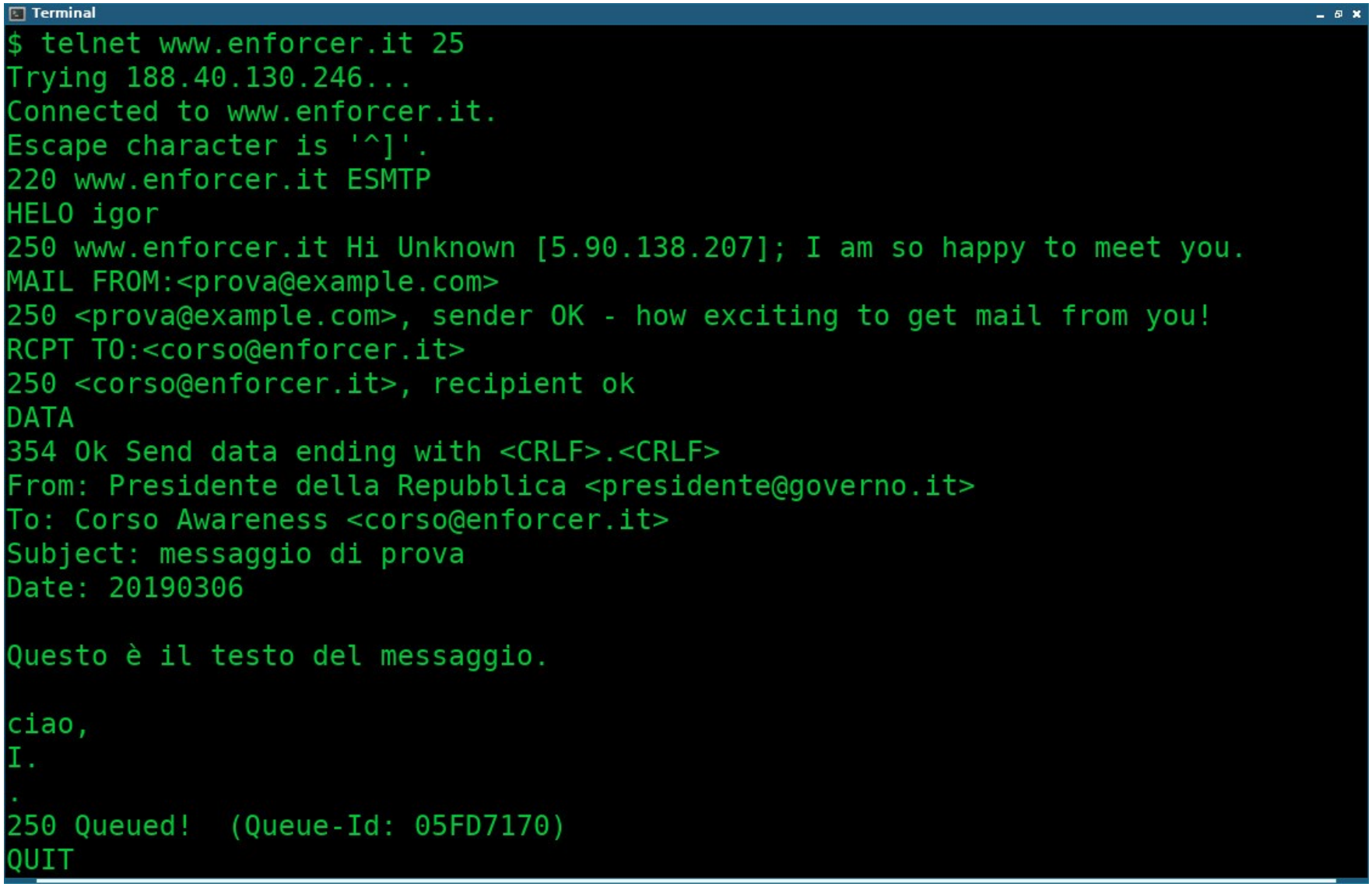
- **Non “regalare” i propri dati**
- **Leggere le informative**
- **Usare indirizzi “usa e getta”..**
- **..o almeno indirizzi diversi**
- **Segnalare i casi di SPAM**

Se è troppo bello per essere vero..

EMAIL false!

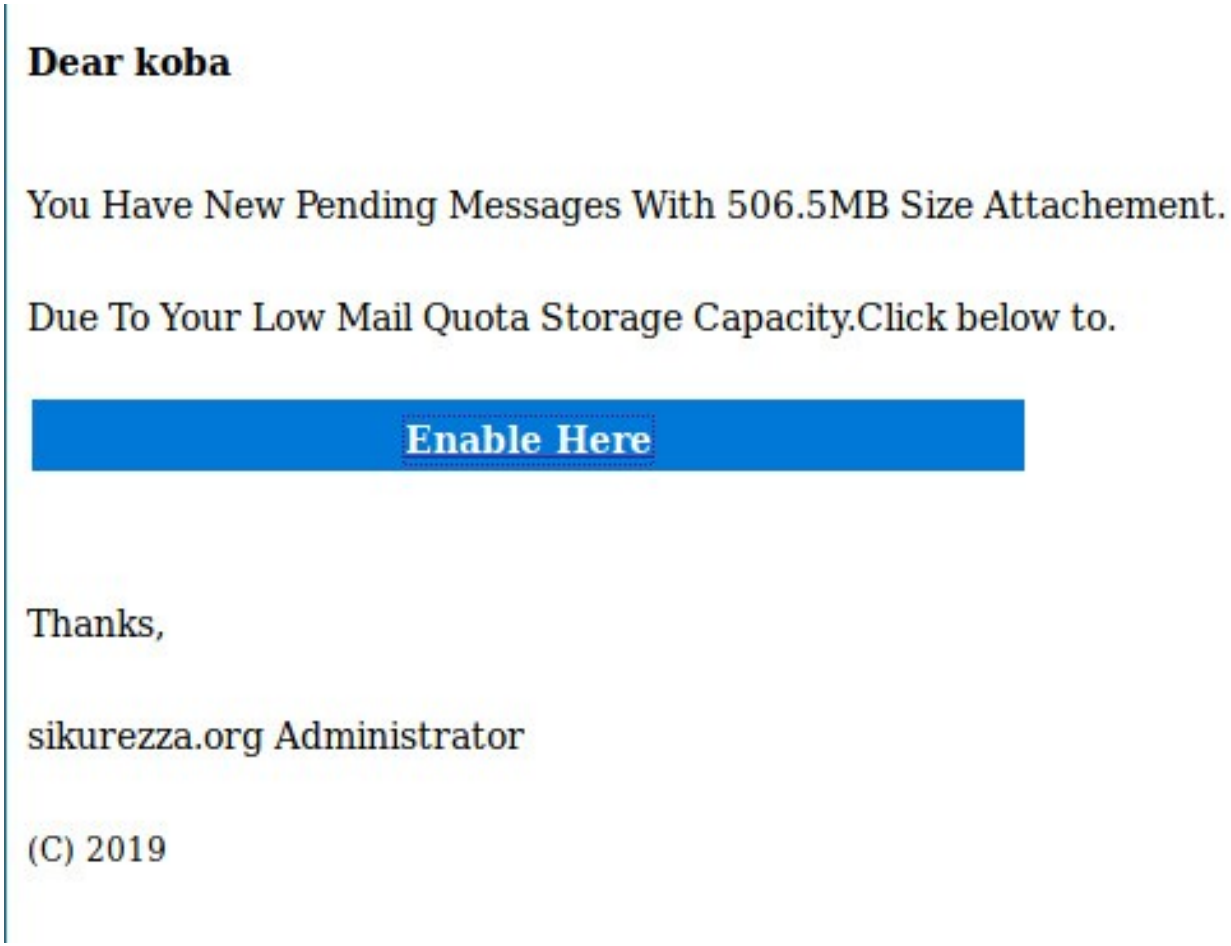

0 Nuovo | Message | Private server, unauthorized use prohibited. - Mozilla Firefox
0 Nuovo | Message | Priv
https://www.enforcer.it/wmail/?page=message&uid=15&mailbox_page=1&sort_by=
150%
Hm2
INBOX (0)
Vai
07/03/19
Marca come non letto: 0
Scrivi Cerca Contatti Preferenze Profilo Cartelle Esci
INBOX
Viewing message 1 / 1
Pagina 1
and
Nessuna azione
A:
Drafts
Oggetto:
messaggio di prova
Da:
Presidente della Repubblica <presidente@governo.it>
A:
Corso Awareness <corso@enforcer.it>
Data:
Wed, 06 Mar 2019 00:00:00 +0100 (1 day, 7 hours ago)
Contatti:
presidente@governo.it
Aggiungi
Rispondi Rispondi a tutti Inoltra Allega Modifica come nuovo || Intestazione completa Sorgente messaggio Stampa Raggruppa per discussione
Questo è il testo del messaggio.
ciao,
I.

Difficile? NO!



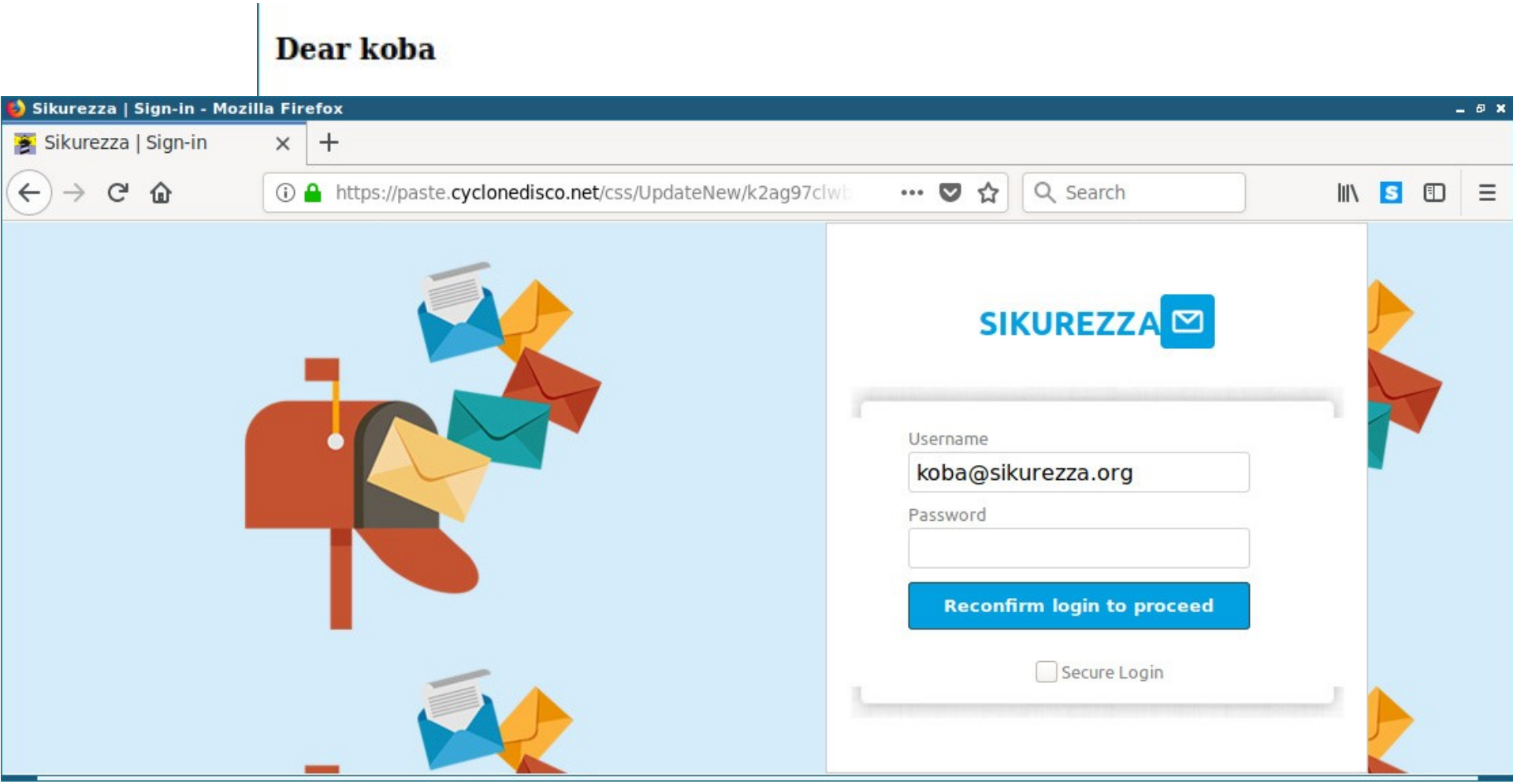
Phishing (generico)

vedi https://en.wikipedia.org/wiki/Phishing

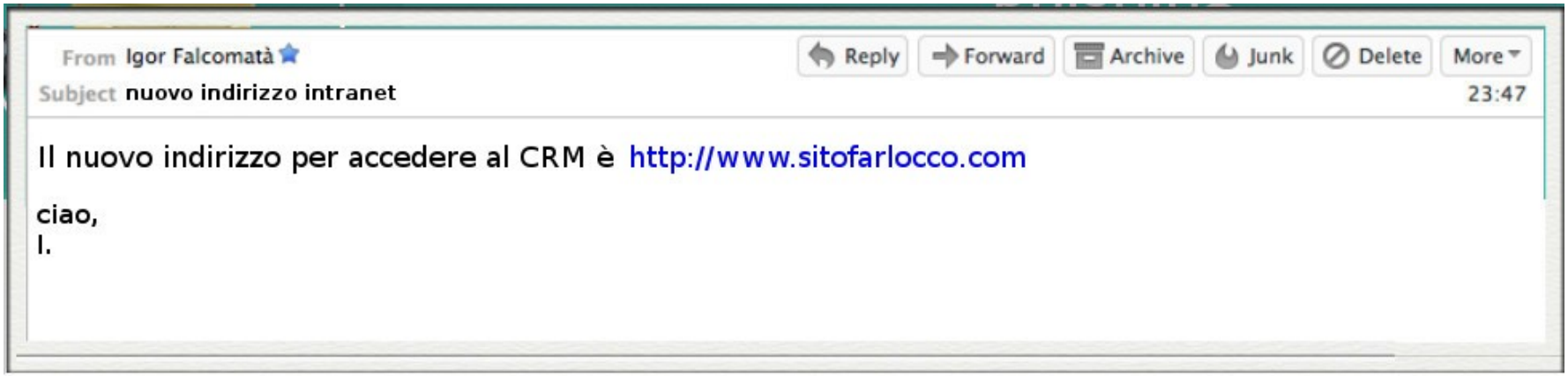


Phishing (generico)

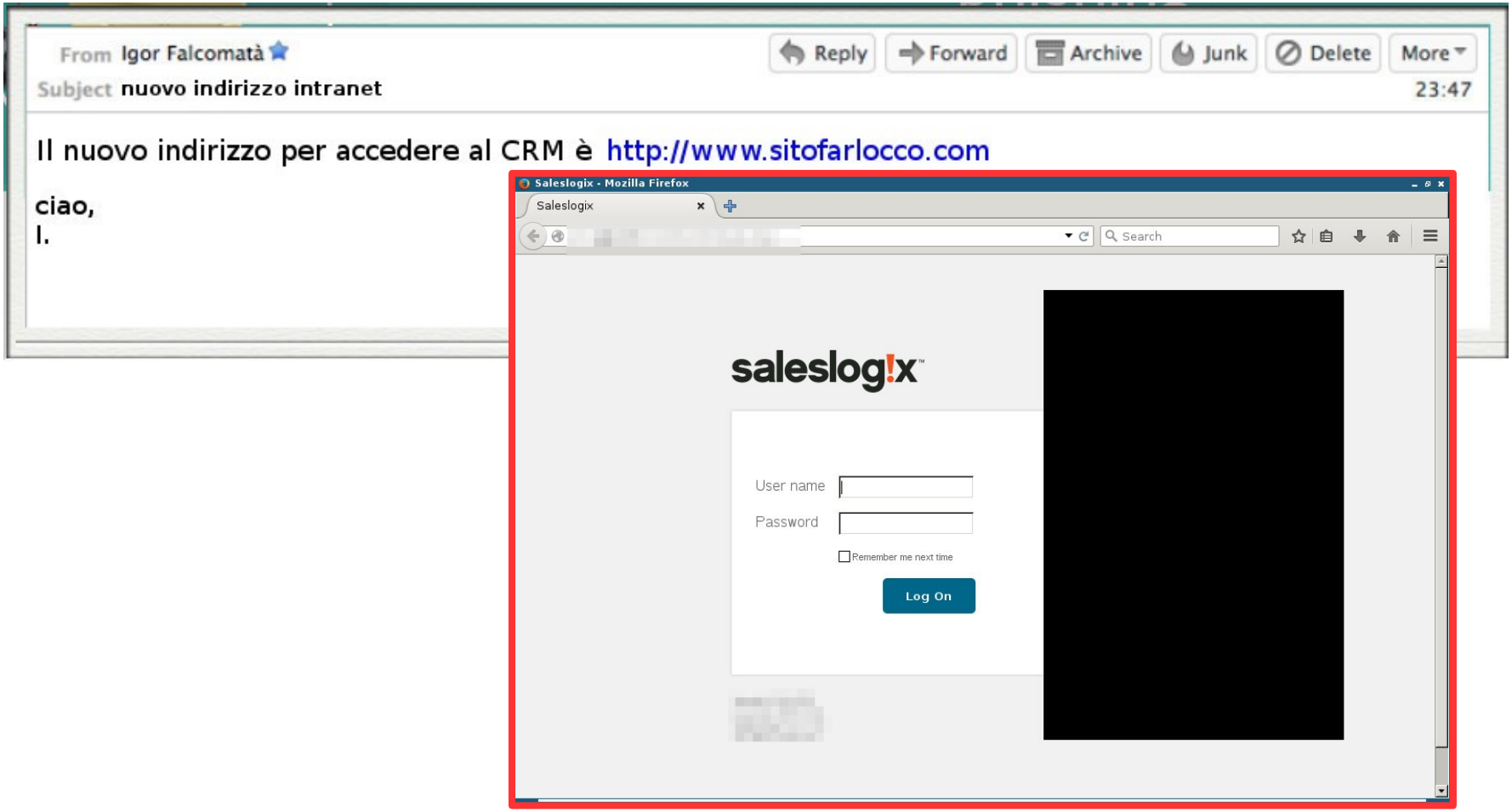
vedi https://en.wikipedia.org/wiki/Phishing



Phishing (mirato “spear phishing”)



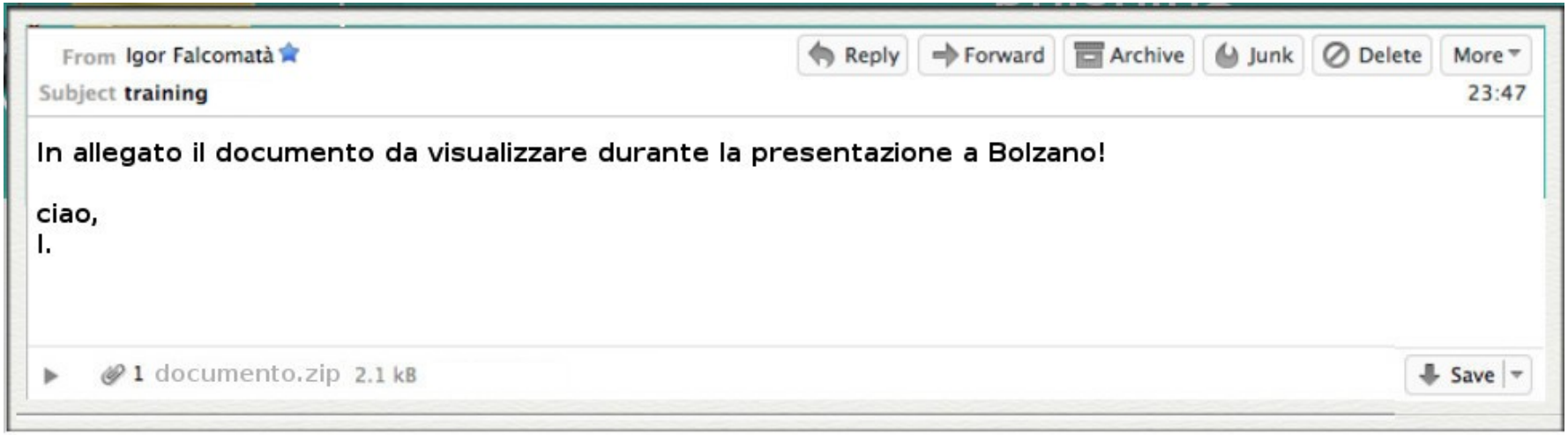
Phishing (mirato “spear phishing”)



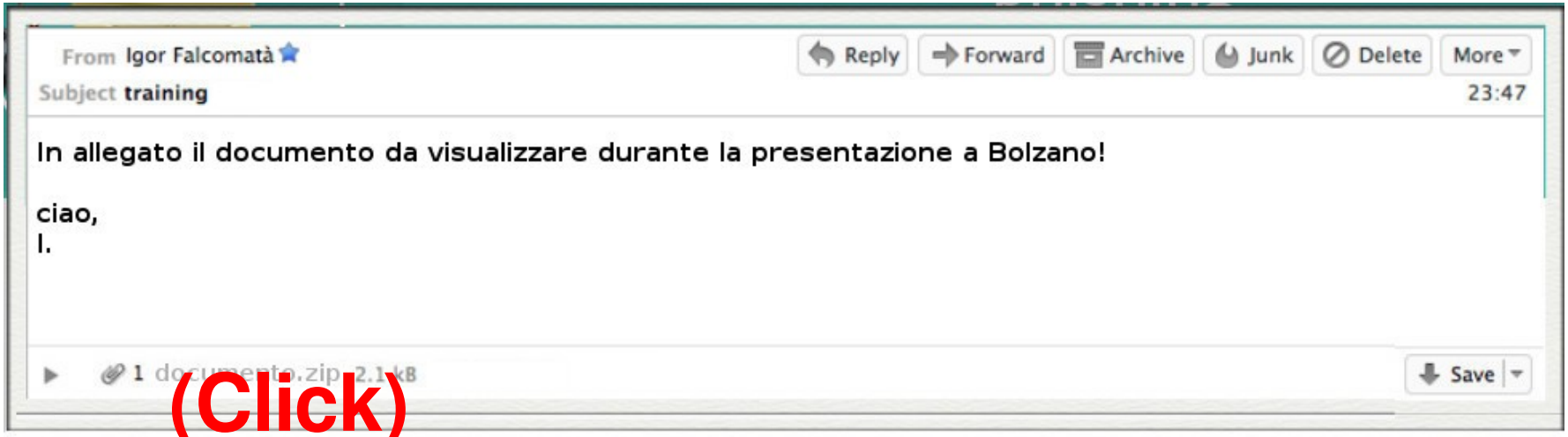
Difendersi

- **Le email potrebbero essere FALSE..**
- **..o arrivare da qualcuno che conoscete**
- **Mai inserire credenziali da link email**
- **Non cliccate su tutto quello che luccica!**
- **L'antivirus potrebbe non bastare..**
- **Se in azienda, segnalate mail sospette**

Malware (software malevolo)

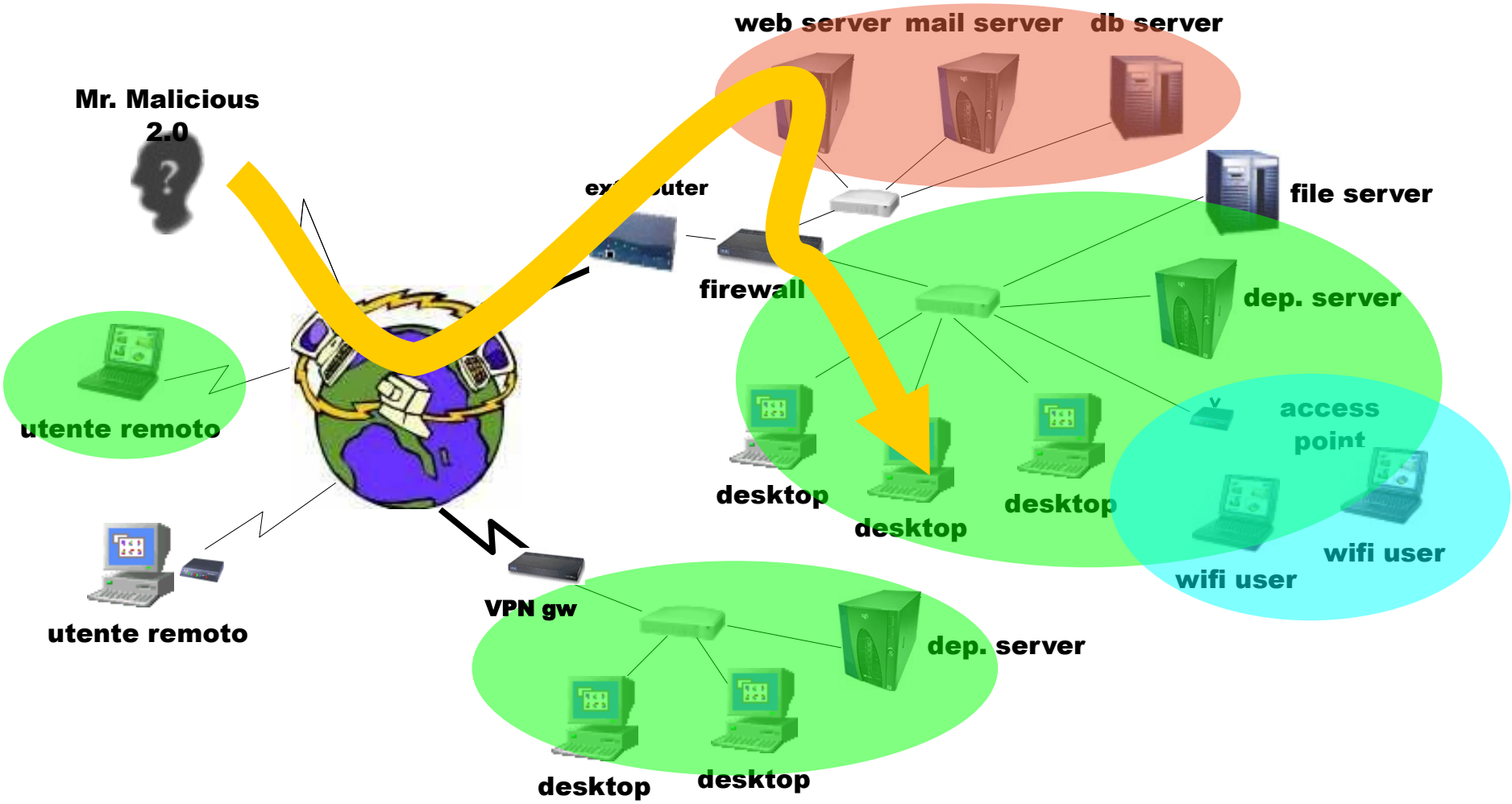


Malware (software malevolo)

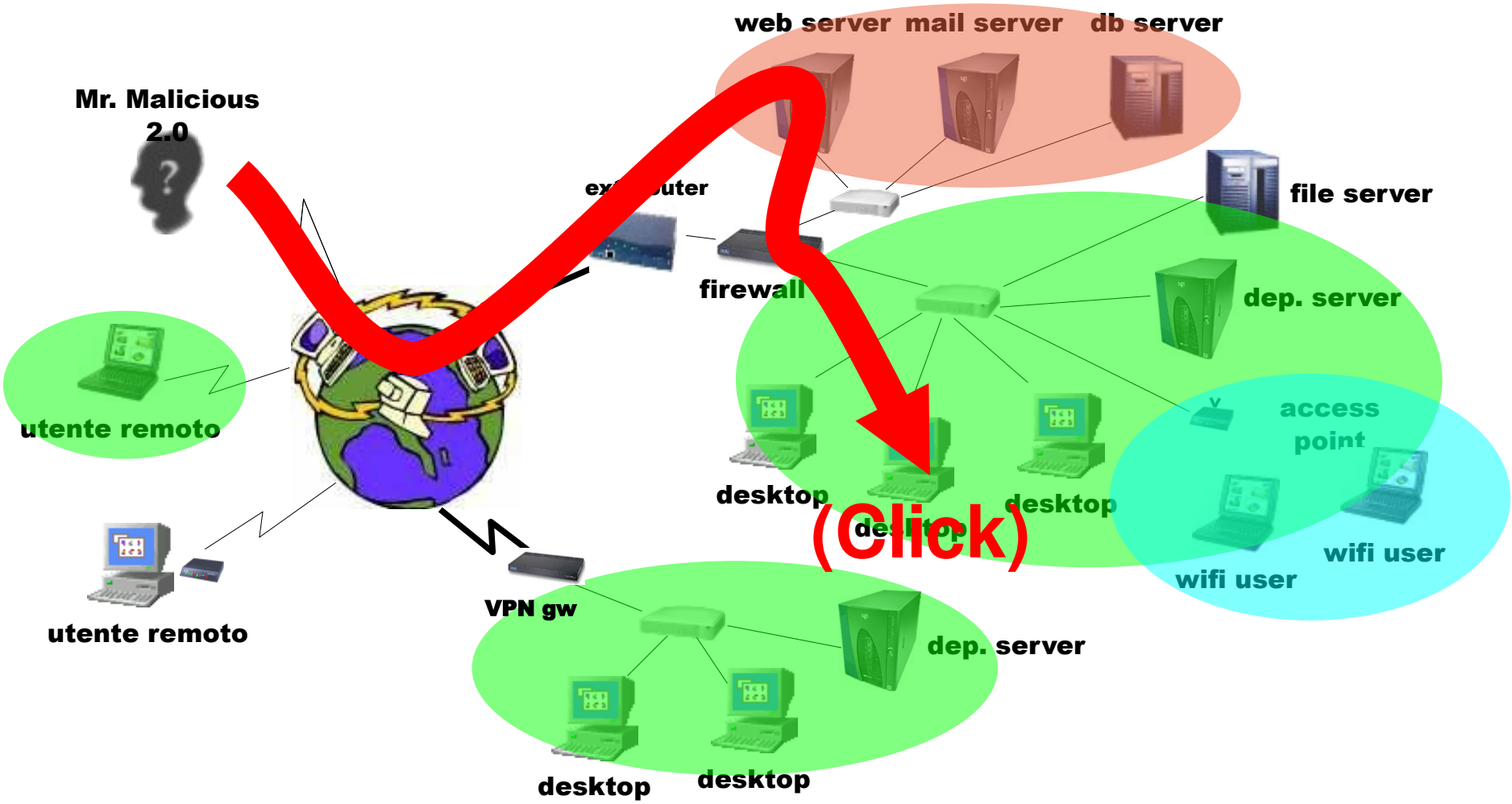



CryptoLocker
Your Personal files are encrypted!
Your personal files encryption produced on this computer: photos, videos, documents, etc. Encryption was produced using a unique public key RSA-2048 generated for this computer.
To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 1.00 bitcoin (~291 USD).
You can easily delete this software, but know that without it, you will never be able to get your original files back.
Disable your antivirus to prevent the removal of this software.
For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"
Do not delete this list, it will be used for decryption. And do not move your files.
Private key will be destroyed on
1/6/2015 1:11:17 PM
Time left
71:55:27
Checking wallet..
Received: 0.00 BTC
Show files
Pay with Bitcoin

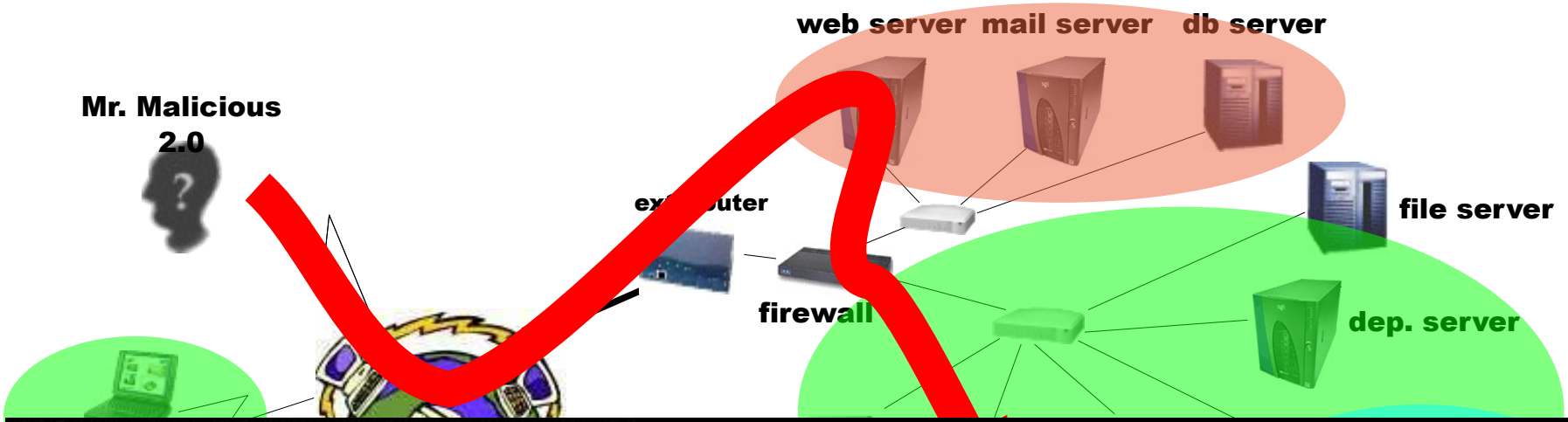
Malware (software malevolo)



Malware (software malevolo)

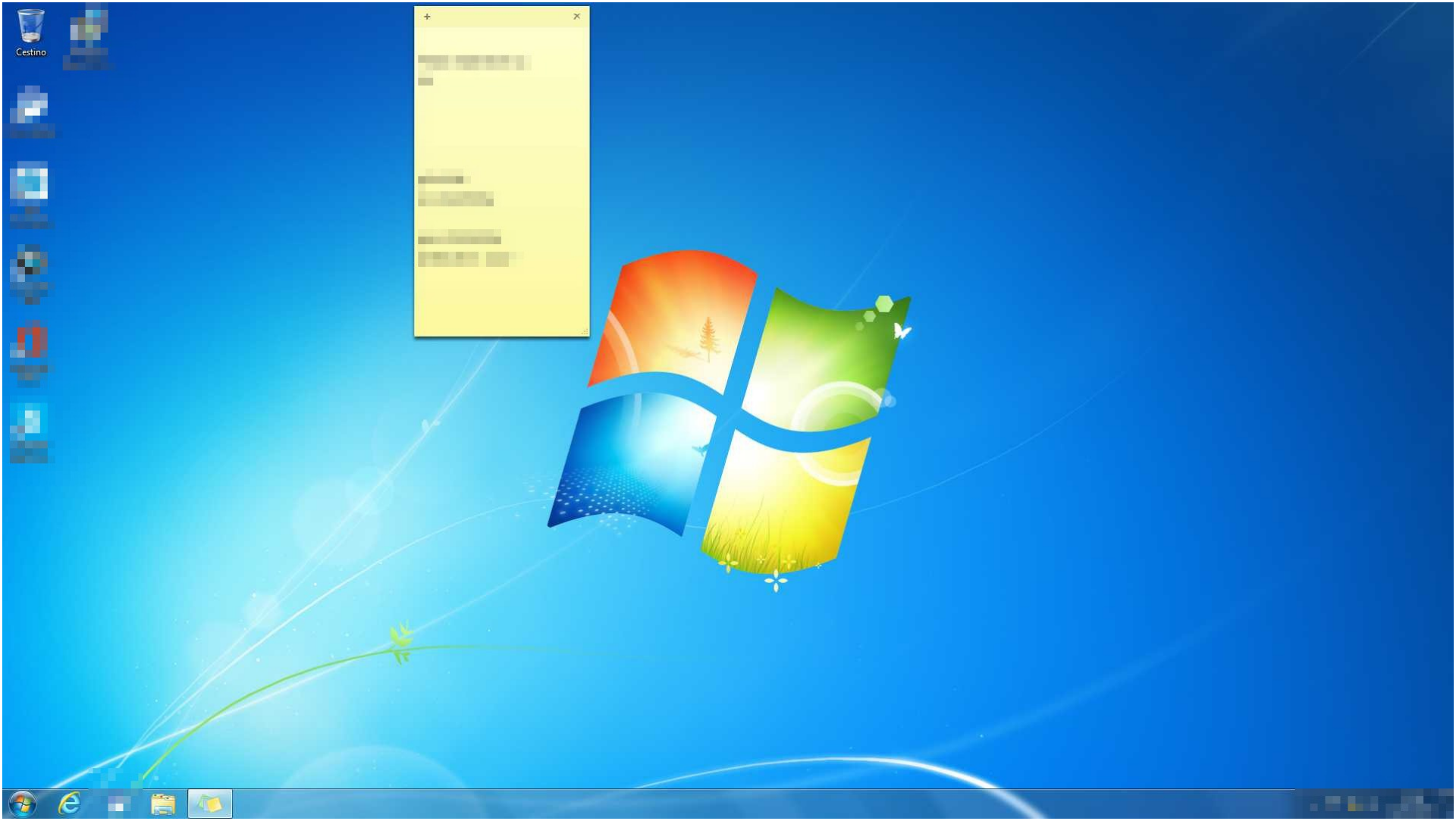


Malware (software malevolo)

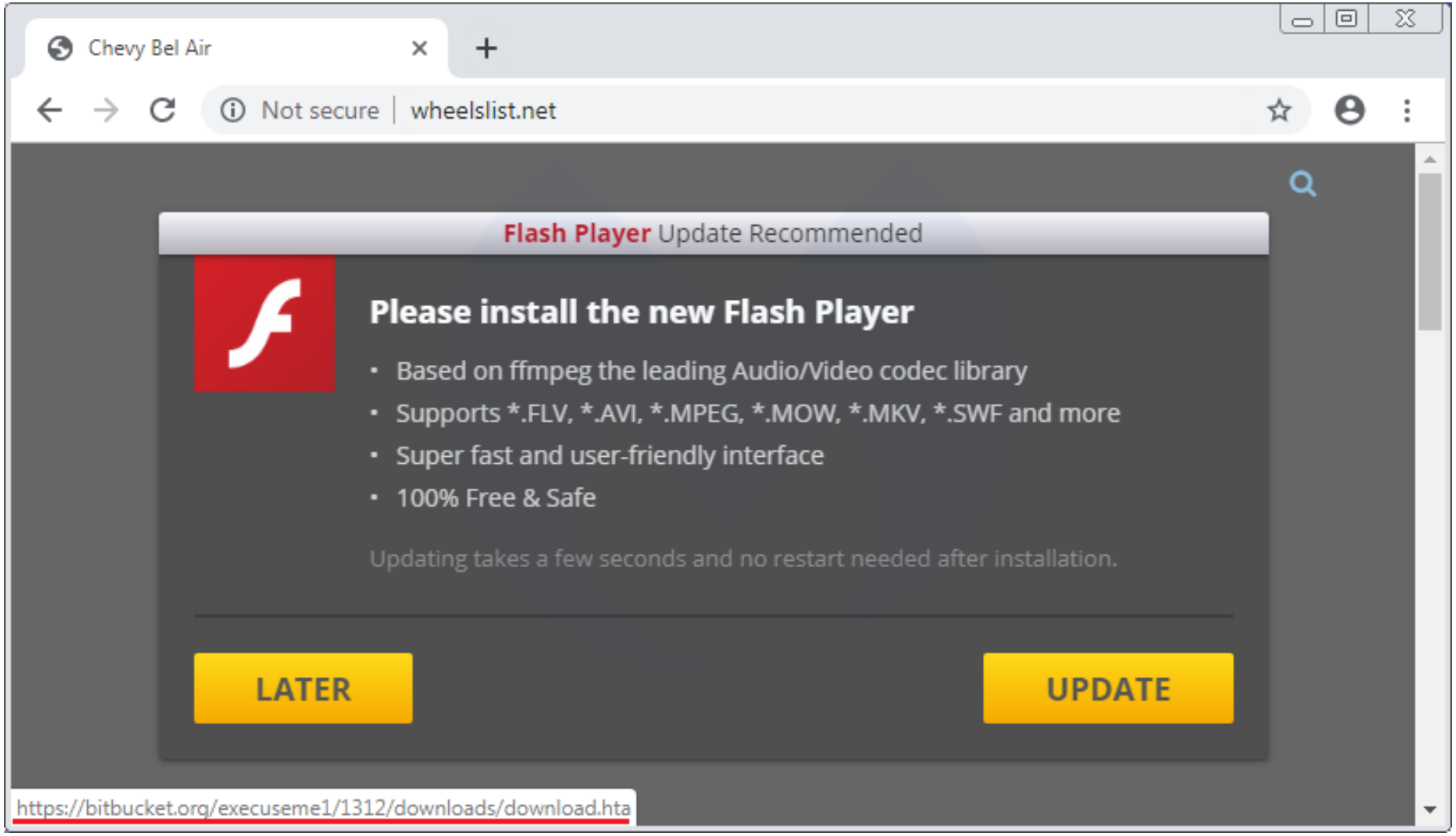



```
C:\Documents and Settings\baltar\Desktop>dir C:\
dir C:\
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 6813-B985

 Directory di C:\

21/10/2010  14.54                 0 AUTOEXEC.BAT
21/10/2010  14.54                 0 CONFIG.SYS
21/10/2010  15.11    <DIR>          Documents and Settings
21/10/2010  15.11    <DIR>          Programmi
21/10/2010  15.11    <DIR>          WINDOWS
               2 File              0 byte
               3 Directory   8.961.507.328 byte disponibili

C:\Documents and Settings\baltar\Desktop>
```

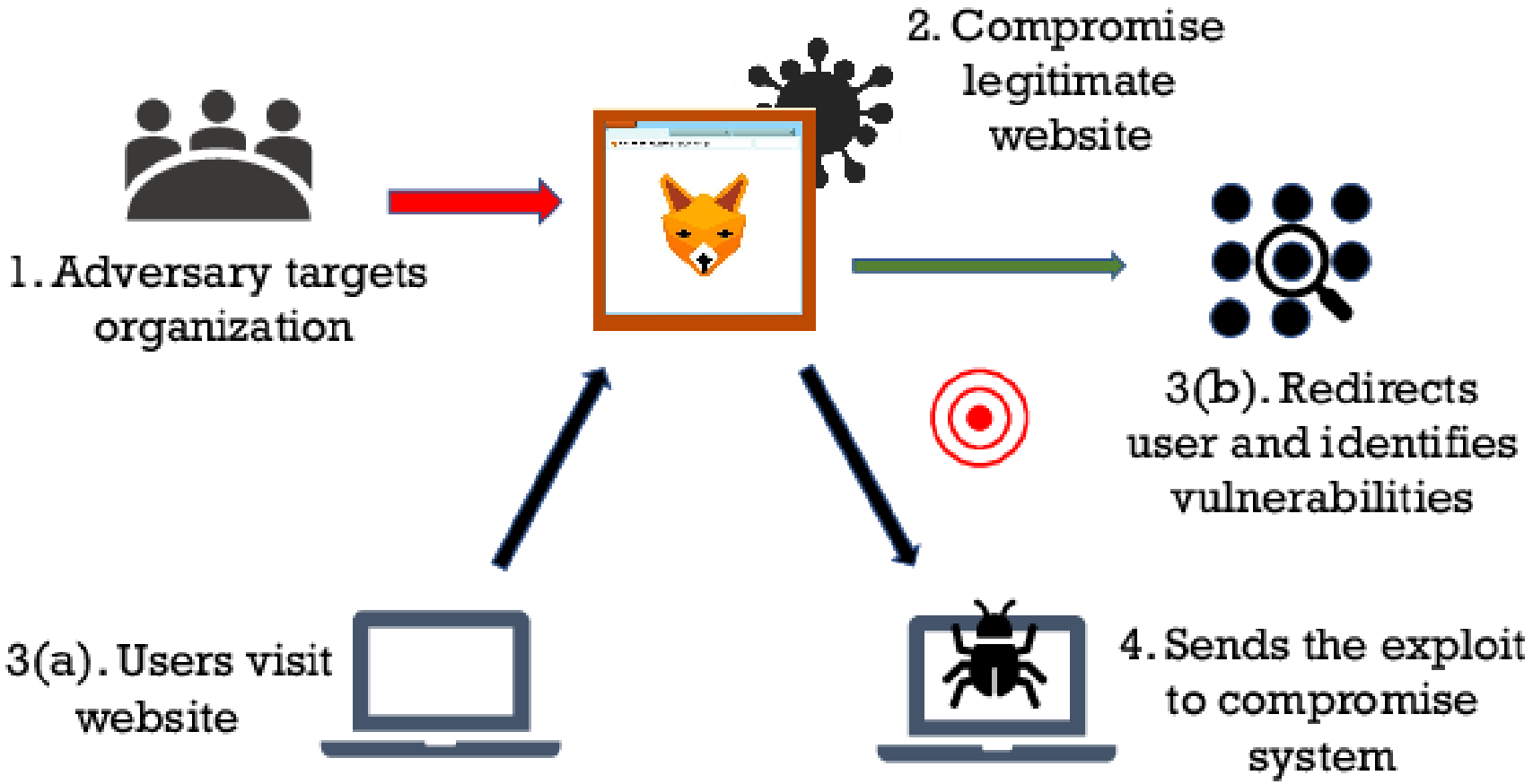
Malware (software malevolo)



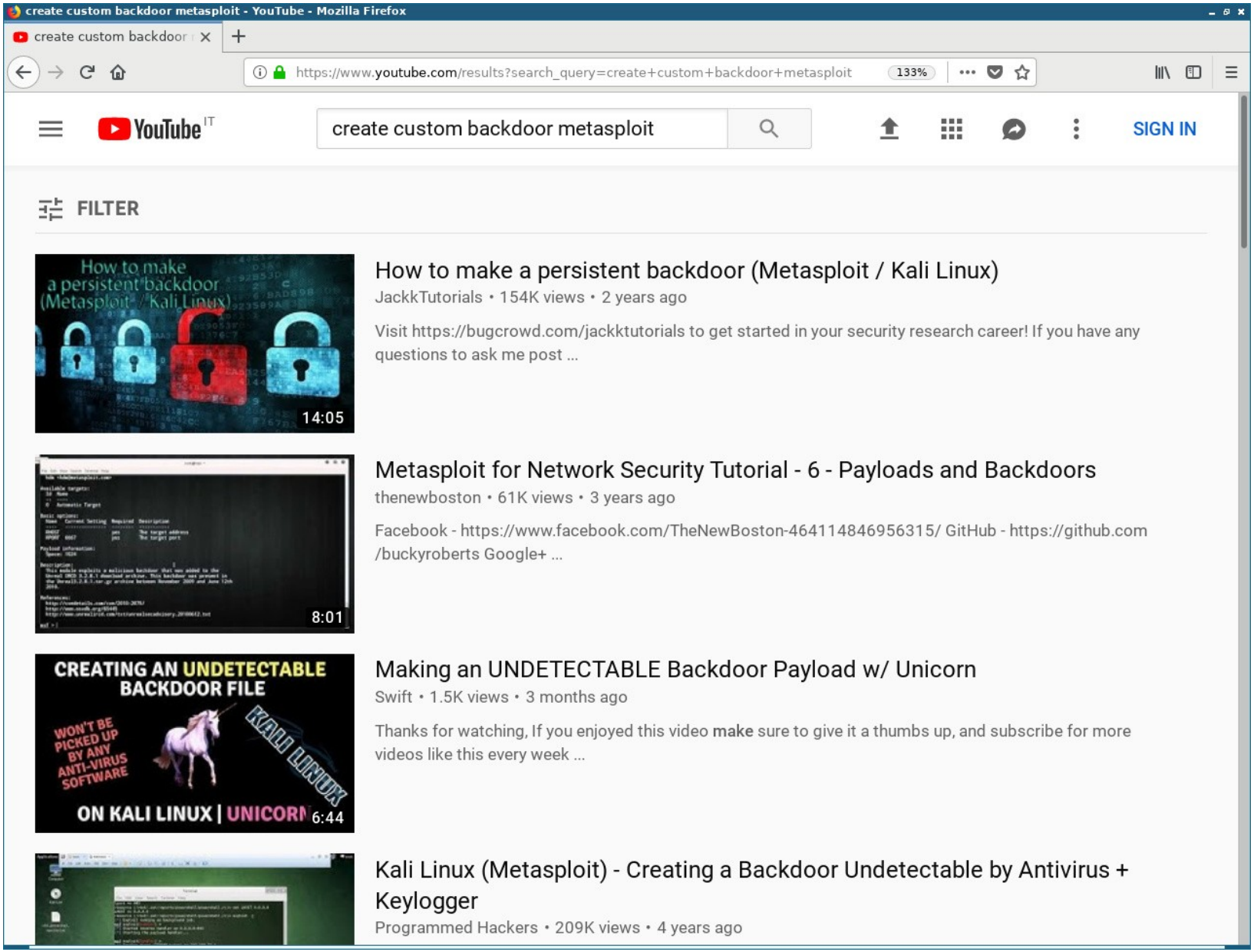
Non solo via email..



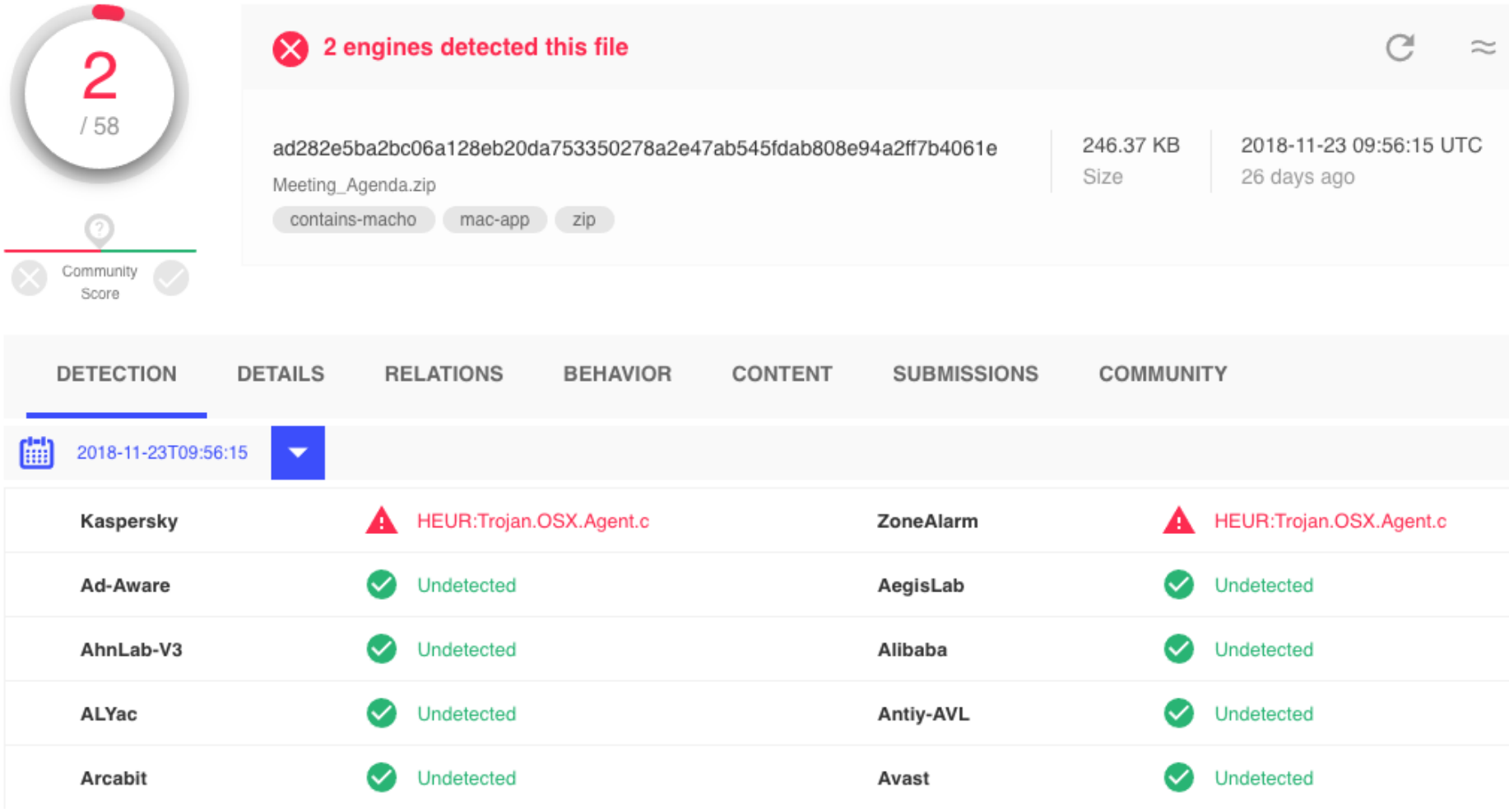
..anche da chi vi fidate..



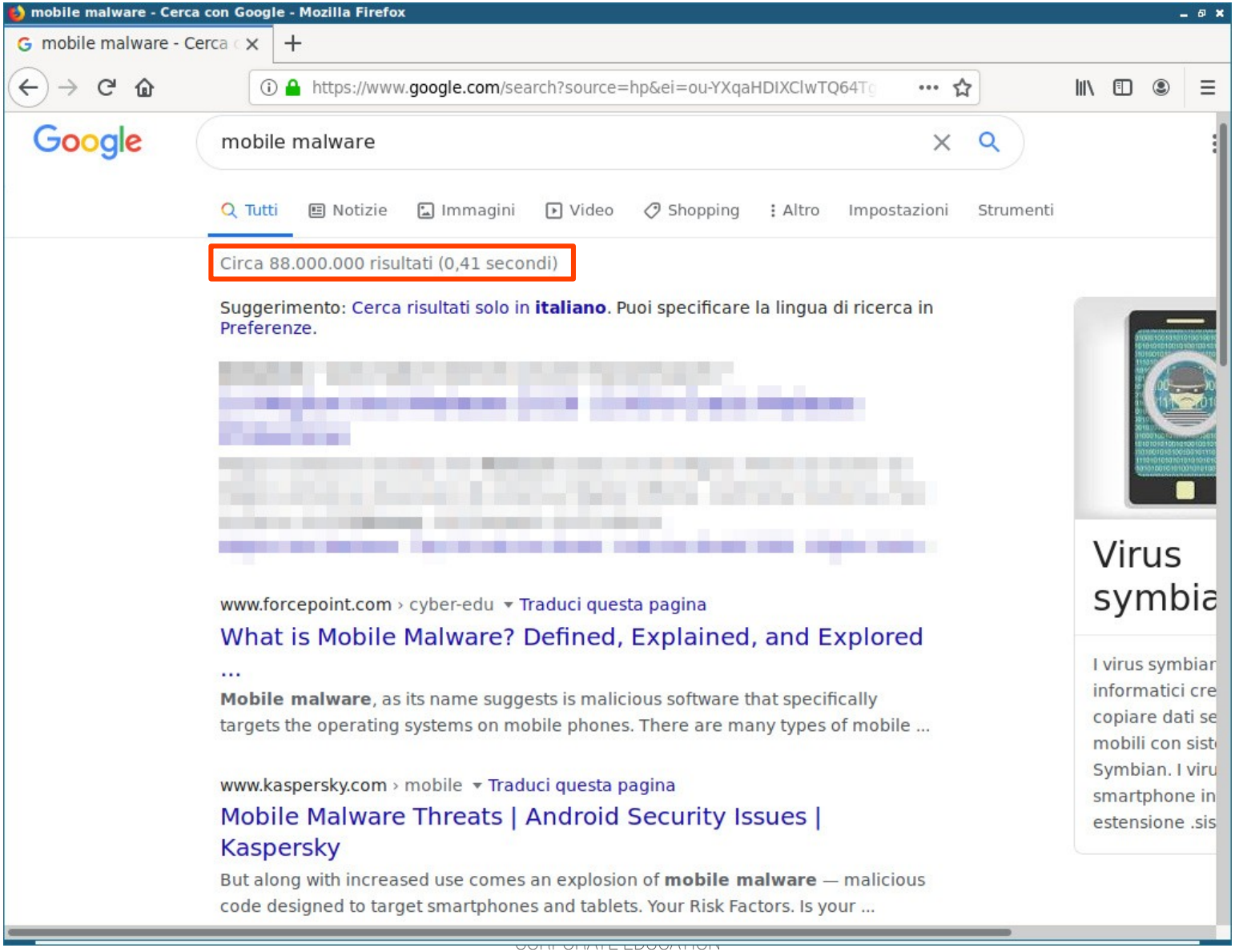
Difficile?


create custom backdoor metasploit - YouTube - Mozilla Firefox
create custom backdoor
https://www.youtube.com/results?search_query=create+custom+backdoor+metasploit
133%
YouTube IT
create custom backdoor metasploit
SIGN IN
FILTER
How to make a persistent backdoor (Metasploit / Kali Linux)
14:05
How to make a persistent backdoor (Metasploit / Kali Linux)
JackkTutorials • 154K views • 2 years ago
Visit https://bugcrowd.com/jackktutorials to get started in your security research career! If you have any questions to ask me post ...
8:01
Metasploit for Network Security Tutorial - 6 - Payloads and Backdoors
thenewboston • 61K views • 3 years ago
Facebook - https://www.facebook.com/TheNewBoston-464114846956315/ GitHub - https://github.com/buckyroberts Google+ ...
CREATING AN UNDETECTABLE BACKDOOR FILE
WON'T BE PICKED UP BY ANY ANTI-VIRUS SOFTWARE
KALI LINUX
ON KALI LINUX | UNICORN
6:44
Making an UNDETECTABLE Backdoor Payload w/ Unicorn
Swift • 1.5K views • 3 months ago
Thanks for watching, If you enjoyed this video make sure to give it a thumbs up, and subscribe for more videos like this every week ...
Kali Linux (Metasploit) - Creating a Backdoor Undetectable by Antivirus + Keylogger
Programmed Hackers • 209K views • 4 years ago

E gli antivirus?



E smartphone/tablet ?



Difendersi

- **Installate ed aggiornate l'antivirus..**
- **..meglio se con funzioni "evolute"**
- **Attenzione ad allegati e download..**
- **Non installare software "non fidato"**
- **Non usare "administrator"**
- **Usare VM o postazioni diverse per contesti diversi**

Difendersi

- **Dispositivo supportato e aggiornato**
- **Uno smartphone è “come un PC”**
- **Uno smartphone non è “smart”**
- **Non installate software “non fidato”**
- **Usate il PIN/blocco dello schermo**
- **Usate la cifratura del dispositivo**

src: https://toggl.com/blog/every-video-call-ever

Domande?

(grazie per l'attenzione)

Igor Falcomatà
CEO, Enforcer
ifalcomata@enforcer.it

easynet group | enforcer SECURITY

Qualche riferimento

- https://www.cert-pa.it/notizie/smart-working-il-vademecum-per-lavorare-online-in-sicurezza/
- https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza
- https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-teleworking-tips-and-advice
- https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-awareness-roles/security-awareness-issues-for-remote-workers/