



CORPORATE EDUCATION

Smartworking & Cybersecurity

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

Igor Falcomatà
CEO, Enforcer

MP

POLITECNICO DI MILANO
GRADUATE SCHOOL
OF BUSINESS

FT Executive Education
Ranking 2019

FT European Business Schools
Ranking 2018

2018
BEST
B-SCHOOLS

EFMD
EQUIS
ACCREDITED

ASSOCIATION
AMBA
ACCREDITED

EFMD
EQUIS
ACCREDITED

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

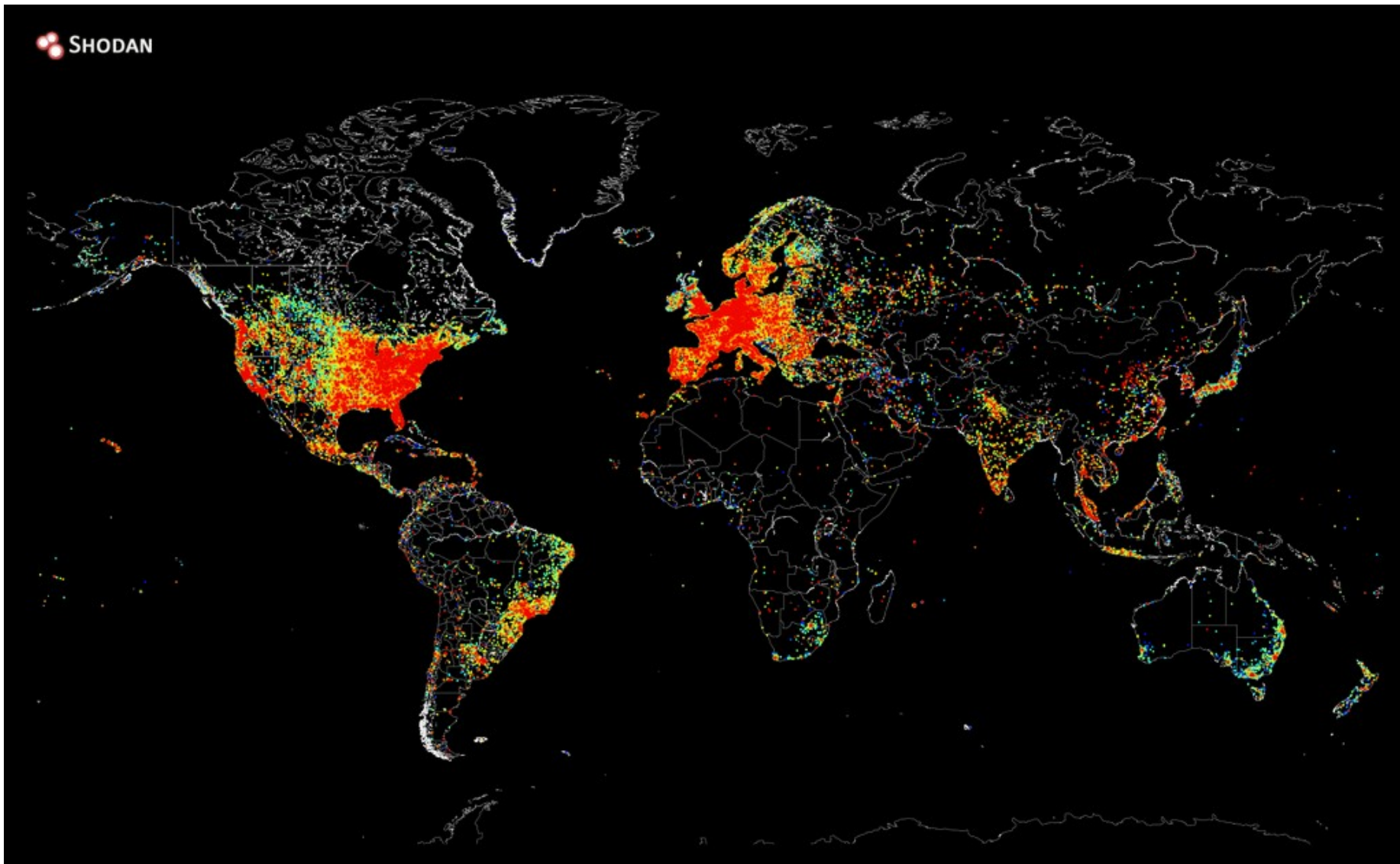


Agenda

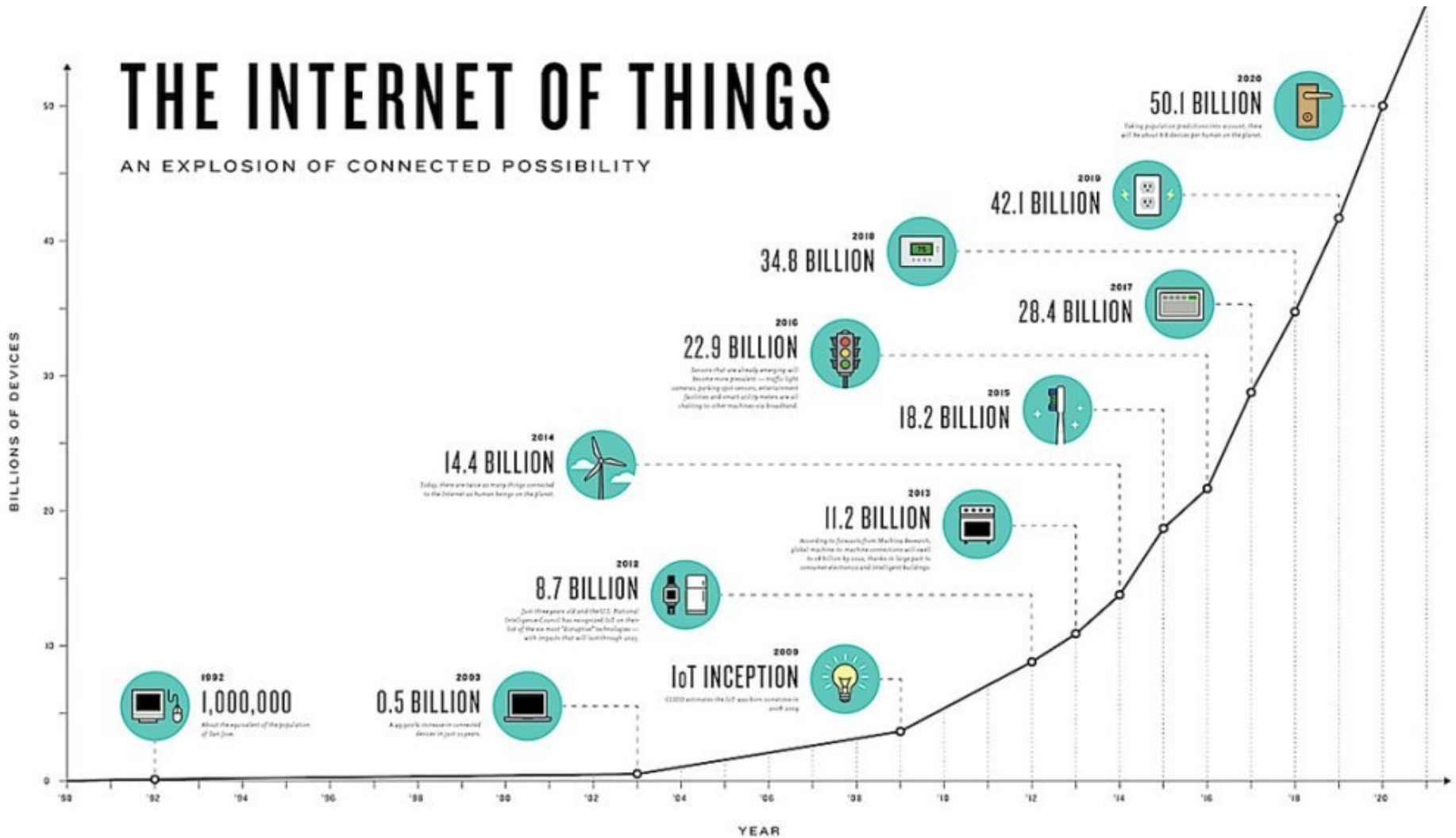
- Il contesto
- Smartworking
- Password
- Email
- Domande & Risposte

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



Created By:
@LoriLewis
@OfficiallyChadd

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 crimine"

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 richiesta di un **riscatto milionario**. Vittima dei pirati informatici, la **Bonfiglioli Rid** poche ore ha visto l'attività di vari stabilimenti compromessa; con la 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

the hardest hit was Copenhagen-based Maersk, which moves about one million containers at Maersk terminals in four continents, 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



CORPORATE EDUCATION



Il contesto (particolare)

{* 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.

> 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 sabotori al **San Camillo**.



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..

The screenshot shows a Twitter post from the account LulzSecITA (@LulzSec_ITA). The tweet text reads: "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...? Dobbiamo rilasciare tutti i dati per ottenere qualche risposta?". Below the text is a list of CSV files and a PDF document, all of which are heavily blurred for redaction. The list includes: 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, and COVID19vademecum2.0.pdf. The tweet is dated 9:28 AM on May 21, 2020, and has 155 retweets and 482 likes. On the right side of the interface, there are promotional cards for "New to Twitter?" and "Relevant people" featuring the profiles of LulzSecITA and San Raffaele Milano.

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...? 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

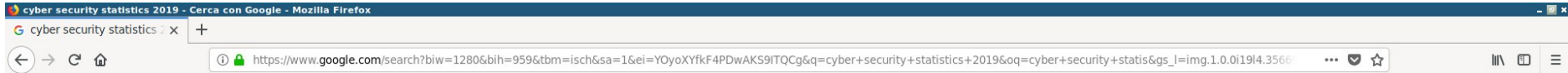
New to Twitter?
Sign up now to get your own personalized timeline!
[Sign up](#)

Relevant people

LulzSecITA
@LulzSec_ITA
Official Account! #LulzSecITA & #Italy
[Follow](#)

San Raffaele Milano
@SanRaffaeleMI
L'IRCCS Ospedale San Raffaele, parte del Gruppo San Donato, è una struttura clinica-scientifica-universitaria di rilievo internazionale e alta specializzazione.
[Follow](#)

Prima dello smartworking..



60 Must-Know Cybers...

varonis.com

Malicious Email Per User by Industry (per year)

Industry	Users Targeted (%)
Wiring	37.5%
Wholesale Trade	36.6%
Construction	36.6%
Non-classifiable Establishments	31.2%
Retail Trade	27.2%
Agroforestry, Forestry & Fishing	21.1%
Manufacturing	20.4%
Public Administration	20.2%
Transportation & Public Utilities	19.0%
Services	17.7%
Finance, Insurance & Real Estate	17.6%

States have improved the frequency of application security testing

How often does your state perform application security vulnerability testing and code review? (Q1 2018)

Frequency	2016	2018
Monthly	33%	33%
Quarterly	11%	11%
Semiannually	2%	2%
Annually	17%	17%
Ad hoc	40%	40%
Never	4%	4%
Do not know	4%	4%

Companies increased spending on IT security in 2018

80 Eye-Opening Cyber Security Statistics for 2019 - Hash... thessistore.com

300+ Terrifying Cybercrime & Cybersecurity Stati... comparitech.com

Insider Threat Statistics fo... ekransystem.com

Breach Notifications

12.4 29.97 48.11 82.42 165.81 288.54 588.48 792.81 912.47

2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

Total Malware Infection Growth Rate (In Millions)

2019 Cyber Security Statistics Trends & Data: ...

purpelsec.us

Cyber Security Statistics ...

testbytes.net

Cybersecurity Statistics for 2019 - ...

topvpn.review

Cybersecurity Industry Size by Year

2013: \$161.39 billion
2014: \$171.01 billion
2015: \$181.02 billion
2016: \$191.03 billion
2017: \$201.04 billion
2018: \$211.05 billion
2019: \$221.06 billion
2020: \$231.07 billion
2021: \$241.08 billion
2022: \$251.09 billion
2023: \$261.10 billion

Growth in ransomware damage and costs worldwide

2015: \$325 MILLION
2017: \$5 BILLION
2019: \$11.5 BILLION
2021: \$20 BILLION

Malware Statistics: You Need to Know

Hackers Going Stealth ...

smallbiztrends.com

2018 CYBERSECURITY STATISTICS

28% of breaches involved internal users
24% of breaches involved third-party vendors
49% of breaches involved individual email
76% of breaches involved multiple channels
12% of breaches involved physical access

Web applications and malicious code are the leading sources of security breaches

Source	2018	2017	2016	2015	2014
Web applications	20	25	19	16	14
Malicious code	24	17	8	15	6
Malware for end users	2	8	6	0	8
Electronic attack	4	3	5	1	0
Physical attack	0	0	0	0	0

10 CYBERSECURITY STATISTICS IN 2019

Just 2% Of the average IT Budget gets spent on cybersecurity

7 Cybersecurity statistics in the past year that y...

200+ Terrifying Cybercrime & Cybersecurity Stati...

10 Cybersecurity Stati...

80 Eye-Opening Cyber Security Stati...

Alarming Cyber Security Statistics 2019

- 70% of the companies agreed that cyber attack is imminent
- 67% increase in security breach over 5 years
- More than 4,000 ransomware attacks occur everyday
- 91% of the attacks are caused by spear phishing mails
- 90% of hackers cover their trail with encryption

Precautionary Measures

- Tighten your security system after thorough testing
- Raise the awareness about strong credentials among employees
- Encrypt your company data
- Learn about how cyber attacks work

testbytes
Making Quality a Habit
info@testbytes.net
+91 811 386 5000

Cyber Security Statistics 2019 | Testbytes

Le immagini potrebbero essere soggette a copyright. Scopri di più

Attacchi.. automatizzati



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

Attacchi.. mirati

The image shows a stack of four Mozilla Firefox browser windows. The top window is a Google search for 'igor falcomata'. The second window is a LinkedIn profile for 'Igor Falcomatà'. The third window is a Facebook search for 'john smith', showing a search bar with 'john smith' and a 'Sign Up' button. The bottom window is a Skype 'Add a Skype Contact' dialog box. It features a search bar with 'falcomata' and a table of search results.

Full Name	Skype Name	City, Country
Anna Falcomata	annafalco1	Sydney, AU
Cinzia Falcomatà	cinzia.falcomata	Torino, IT
Elisa Falcomatà	elisa.falcomata	pesaro, IT
Roberto Falcomatà	errefesi	Milano, IT
Joseph Falcomata	jofalco	Sydney, AU
Gabriella Falcomatà	lady_hawk5	Reggio Calabria, IT
Loretta Falcomata	loretta.falcomata	AU
Miriam Falcomatà	miriam.falcomata	Reggio Calabria, IT




Competenze tecniche necessarie.. nessuna!

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

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

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

May 29, 2015 Swati Khandelwal



SHARE

- f
- t
- in
- Share icon
- Comment icon

Create a virus

Ransom - \$

Notes

Captcha

"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!



Bitcoin - Wikipedia - Mozilla Firefox

W Bitcoin - Wikipedia x +

← → ↻ 🏠

🔒 https://en.wikipedia.org/wiki/Bitcoin#Privacy 170%

Privacy

Bitcoin is [pseudonymous](#), meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses.^[127] Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information.^[128] To heighten financial privacy, a new bitcoin address can be generated for each transaction.^[129]

Fungibility

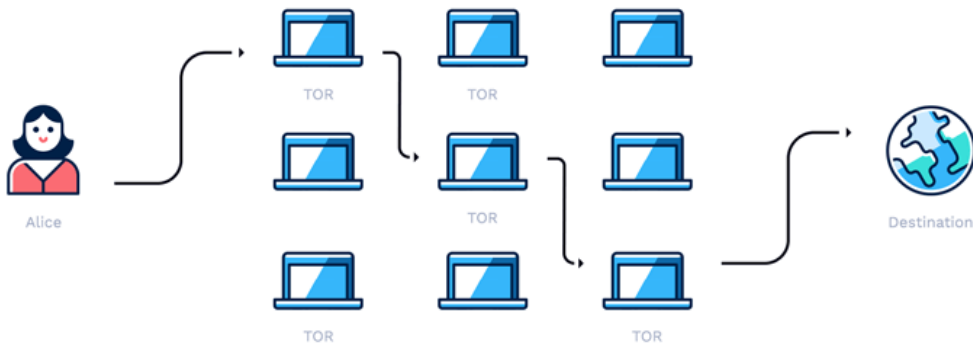
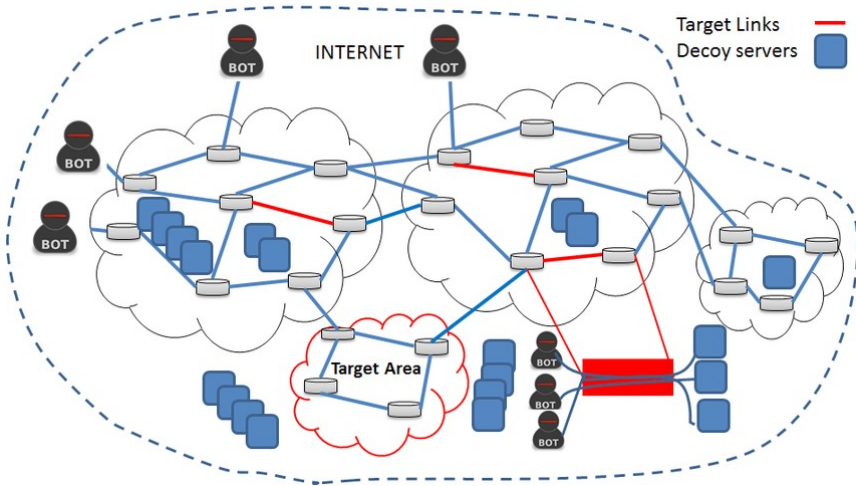
Wallets and similar software technically handle all bitcoins as equivalent, establishing the basic level of [fungibility](#). Researchers have pointed out that the history of each bitcoin is registered and publicly available in the blockchain ledger, and that some users may refuse to accept bitcoins coming from controversial transactions, which would harm bitcoin's fungibility.^[130] For example, in 2012, Mt. Gox froze accounts of users who deposited bitcoins that were known to have just been stolen.^[131]

Scalability

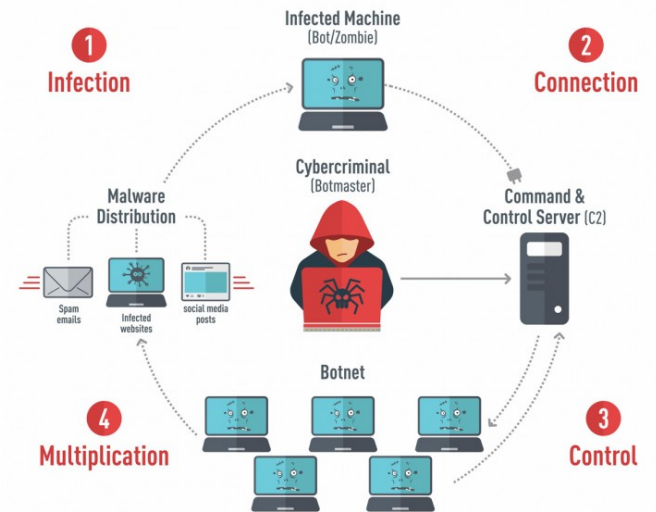
Main article: [Bitcoin scalability problem](#)

The blocks in the blockchain were originally limited to 32 [megabytes](#) in size. The block size limit of one [megabyte](#) was introduced by Satoshi Nakamoto in 2010. Eventually the

Facile rendersi anonimi..

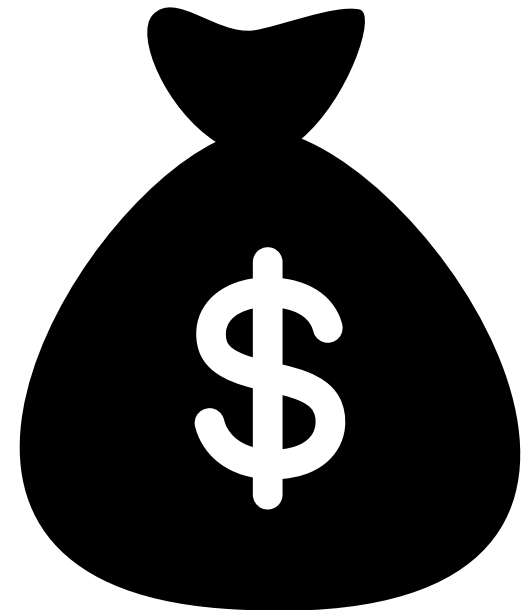


How a Botnet works

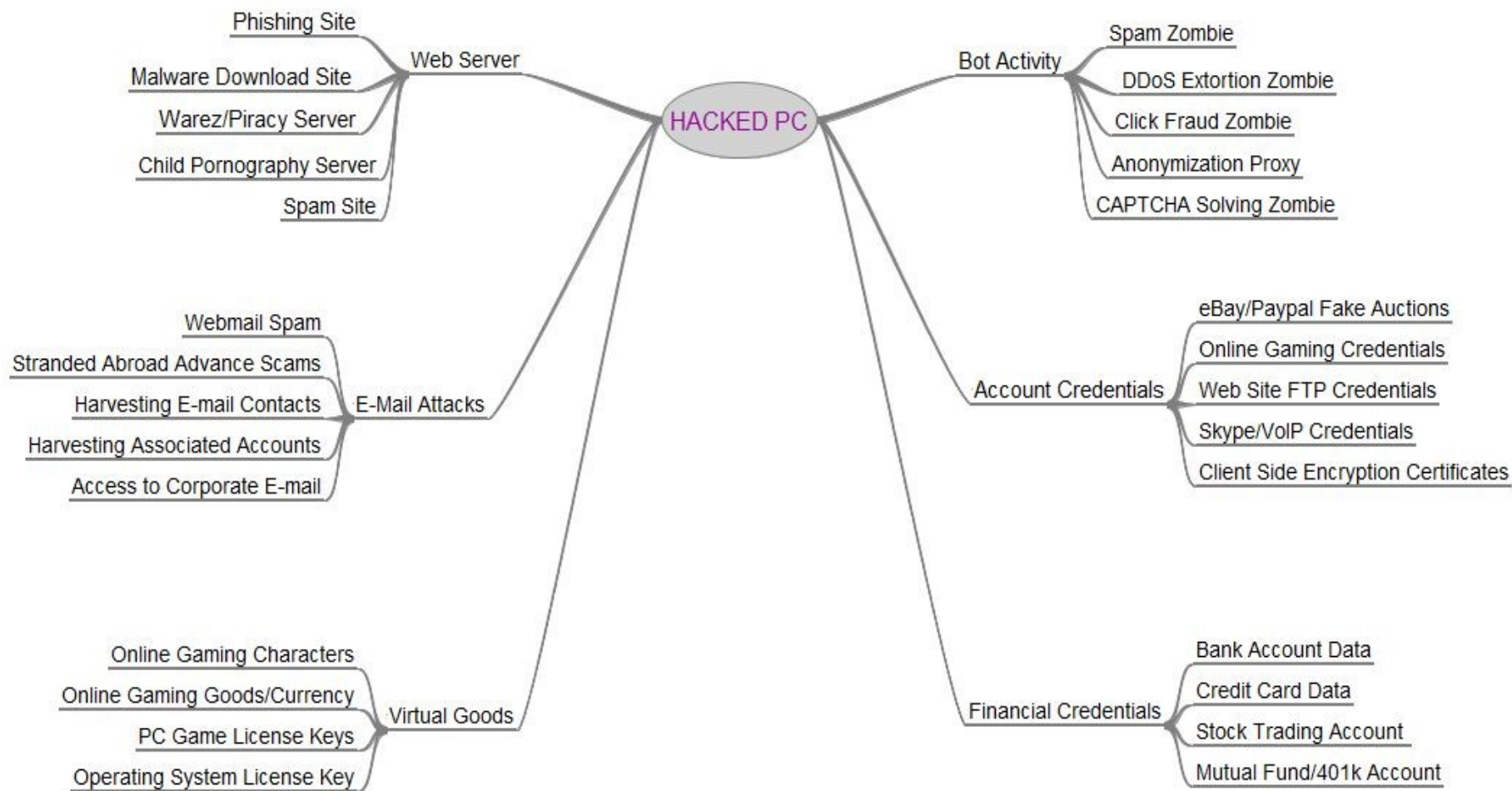


EMSISOFT

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/>



Non cliccare su link o allegati contenuti in email **sospette**.



Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) **di cui conosci la provenienza** (nuovi, già utilizzati, forniti dalla tua azienda).



Blocca l'accesso al sistema e/o configura la modalità di blocco automatico dello schermo.



Utilizza l'accesso a connessioni **Wi-Fi adeguatamente protette**.



Effettua sempre il **log-out** dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.



Segui prioritariamente le **policy** e le **raccomandazioni** dettate dalla tua azienda.

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.

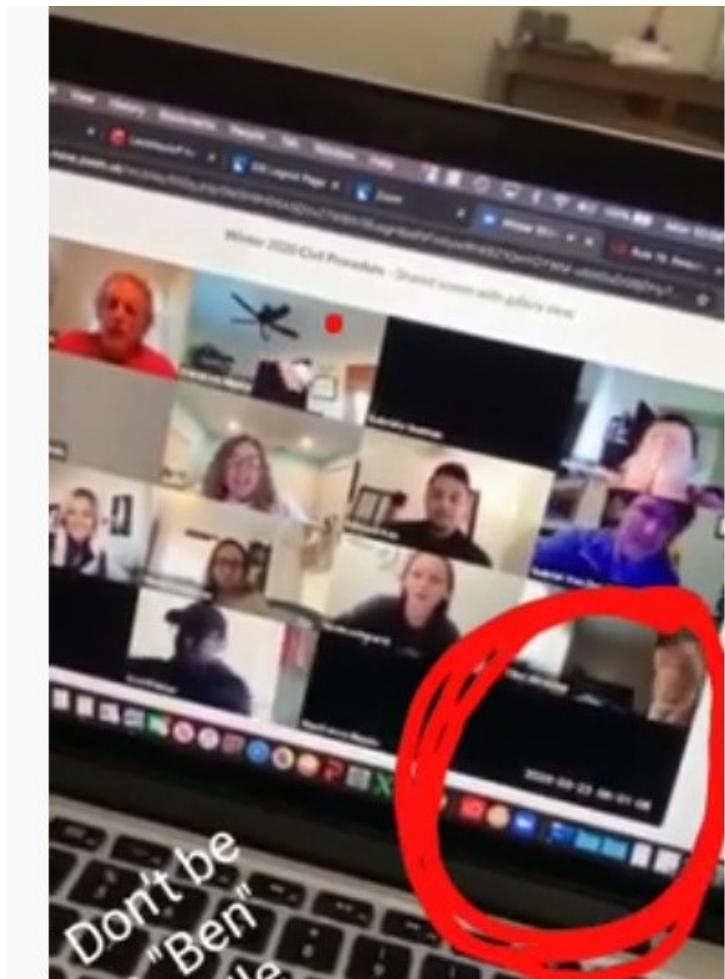


Assicurati che i **software di protezione** del tuo sistema operativo siano abilitati e **costantemente aggiornati**.



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

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 ?

The screenshot shows the 'Have I Been Pwned' website interface. At the top, it displays four statistics: 408 pwned websites, 8,506,873,299 pwned accounts, 102,441 pastes, and 122,480,433 paste accounts. Below these are two columns of breach information: 'Largest breaches' and 'Recently added breaches'. Each breach entry includes a logo, the number of accounts affected, and the name of the breach.

Largest breaches		Recently added breaches	
	772,904,991 Collection #1 accounts		988,230 StreetEasy accounts
	763,117,241 Verifications.io accounts		780,073 Sephora accounts
	711,477,622 Onliner Spambot accounts		23,165,793 Wanelo accounts
	593,427,119 Exploit.In accounts		15,453,048 Lumin PDF accounts
	457,962,538 Anti Public Combo List accounts		4,606 KiwiFarms accounts
	393,430,309 River City Media Spam List accounts		396,533 Minehut accounts
	359,420,698 MySpace accounts		95,431 Void.to accounts
	234,842,089 NetEase accounts		36,395,491 Poshmark accounts
	164,611,595 LinkedIn accounts		89,388 Mastercard Priceless Specials accounts
	161,749,950 Dubsmash accounts		561,991 XKCD accounts

Maybe I don't saccio!

Хакерский форум Free Hacks - Все хакерские направления в одном месте!
Добро пожаловать на Хакерский форум Free Hacks - Все хакерские направления в одном месте!

Администрация		Последнее сообщение
 Новости сайта и форума (4 Просматривает) Новости администрации сайта и форума Сервисы FreeHacks.ru (11/113)	Тем: 28 Сообщений: 296	🔔 sata-ata - новый администратор форума >>> от admin 10.06.2018, 15:20
 Уважаемая администрация! (4 Просматривает) Жалобы, предложения и ошибки сообщаем администрации сайта Предложения по сайту (29/454) Ошибки и баги сайта (22/142) Жалобы и Нарушения (3/19) Вакансии и заявки (3/29)	Тем: 57 Сообщений: 644	Важное >>> от admin 01.06.2018, 15:55
Форумы FreeHacks		Последнее сообщение
 Общение (74 Просматривает) Курилка (271/2480) Новости хакерского мира (449/1270) Турниры и Конкурсы (20/668) Юмор (32/453) Вопросы / Попрошайки (312/1725) Видео (45/166)	Тем: 1,133 Сообщений: 6,775	Услуги взлома ,переписка whats app/viber >>> от olyazimq Сегодня, 20:32
 Обсуждение форумов смежной тематики Вся правда о ресурсах	Тем: 3 Сообщений: 9	Кидальные борды >>> от poloz 24.03.2018, 11:01
 Хакерство и Безопасность (48 Просматривает) Безопасность и взлом (155/871) Тестирование на уязвимости (5/21) Анонимность и приватность (73/474) Вирусология (41/216) Социальная инженерия (СИ) (16/83) Криптография (29/141) Спам, рассылки (32/152) Лента уязвимостей (57/203) Wardriving & Bluejacking / Wi-Fi (13/70) Софт (107/555)	Тем: 538 Сообщений: 2,837	Услуги взлома ,переписка whats app/viber >>> от olyazimq Сегодня, 20:36
 Кардинг (14 Просматривает) Реал кардинг (51/209) Новости в мире кардинга (8/21) Ботнет \ Трафик (37/236) Вещевуха (38/352) Виртуальный стафф (9/70) Безопасность (4/40) Софт (13/102)	Тем: 188 Сообщений: 1,139	Информация о шопах и возможность доставить через... >>> от Mark01 14.06.2018, 10:09
 Электроника и Фриинг (7 Просматривает) Сотовый фриинг (4/14) Железо (2/26) Схемы, программы, прошивки (1/1) Телефония и связь (1/13)	Тем: 8 Сообщений: 54	📄 Кто поможет разобраться с софтом и схемой? >>> от Mogoziy 27.04.2018, 00:37
 Брут (3 Просматривает) Статьи (8/27) Софт (57/172) Парсеры (2/20)	Тем: 68 Сообщений: 226	Brut Cheker Корикот.ru >>> от CLANDEX 17.06.2018, 15:48
 DoS / DDoS (5 Просматривает) Статьи (8/72) Софт (10/118) Защита от DoS / DDoS (4/39)	Тем: 25 Сообщений: 251	🔔 PyDoS - мощный стрессер в 40 строчек кода. >>> от Jorg_Kosmos 12.06.2018, 10:04

Password..



Password..

A wizard with a long white beard and a tall, pointed hat stands in a dark, rocky cave. He is holding a lit torch in his right hand, which illuminates the scene. The cave walls are covered in ancient-looking carvings. The overall atmosphere is mysterious and ancient.

**Dite amici
ed entrate!**

Password..

soleil123

amore3

bateau9

ytrewq

curval

Benvenuto

interface

Bruxelles

Mario123

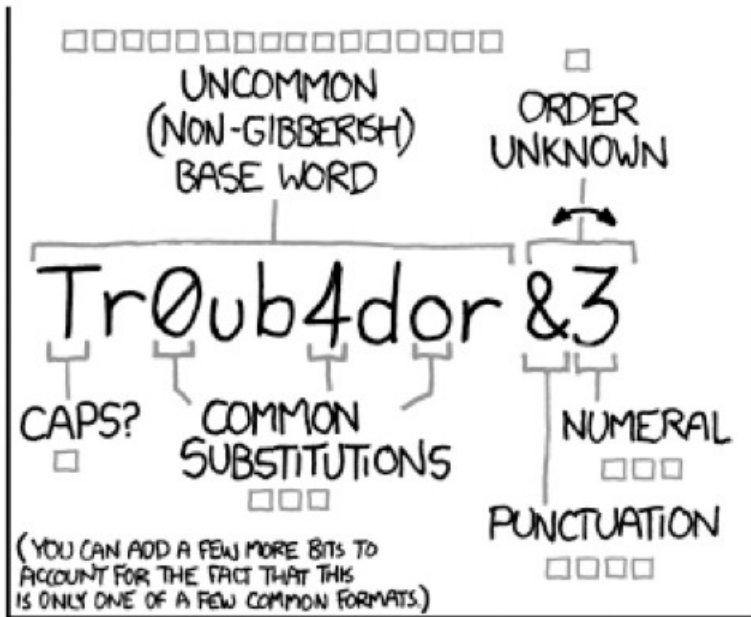
Password..

PASSWORDS ARE LIKE UNDERPANTS



Change them often, keep them private and never share them with anyone.

Password..



~28 BITS OF ENTROPY

□□□□□□□□ □

□□□□□□□□ □

□□□ □□□

□□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(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

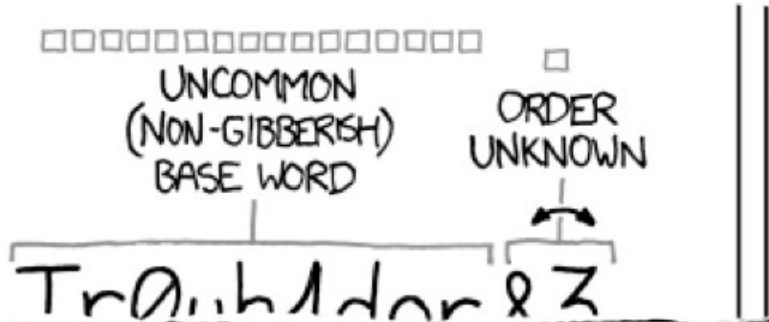
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD

Password..




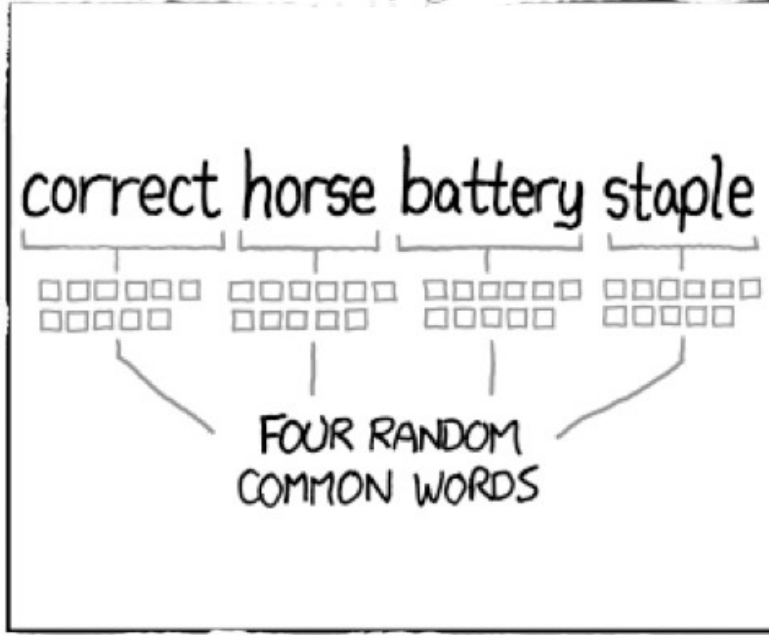
~28 BITS OF ENTROPY

□□□□□□□□ □
□□□□□□□□ □
□□ □ □ □ □
□□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL... 



~44 BITS OF ENTROPY

□□□□□□□□□□ □□□□□□□□□□
□□□□□□□□□□ □□□□□□□□□□
□□□□□□□□□□ □□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

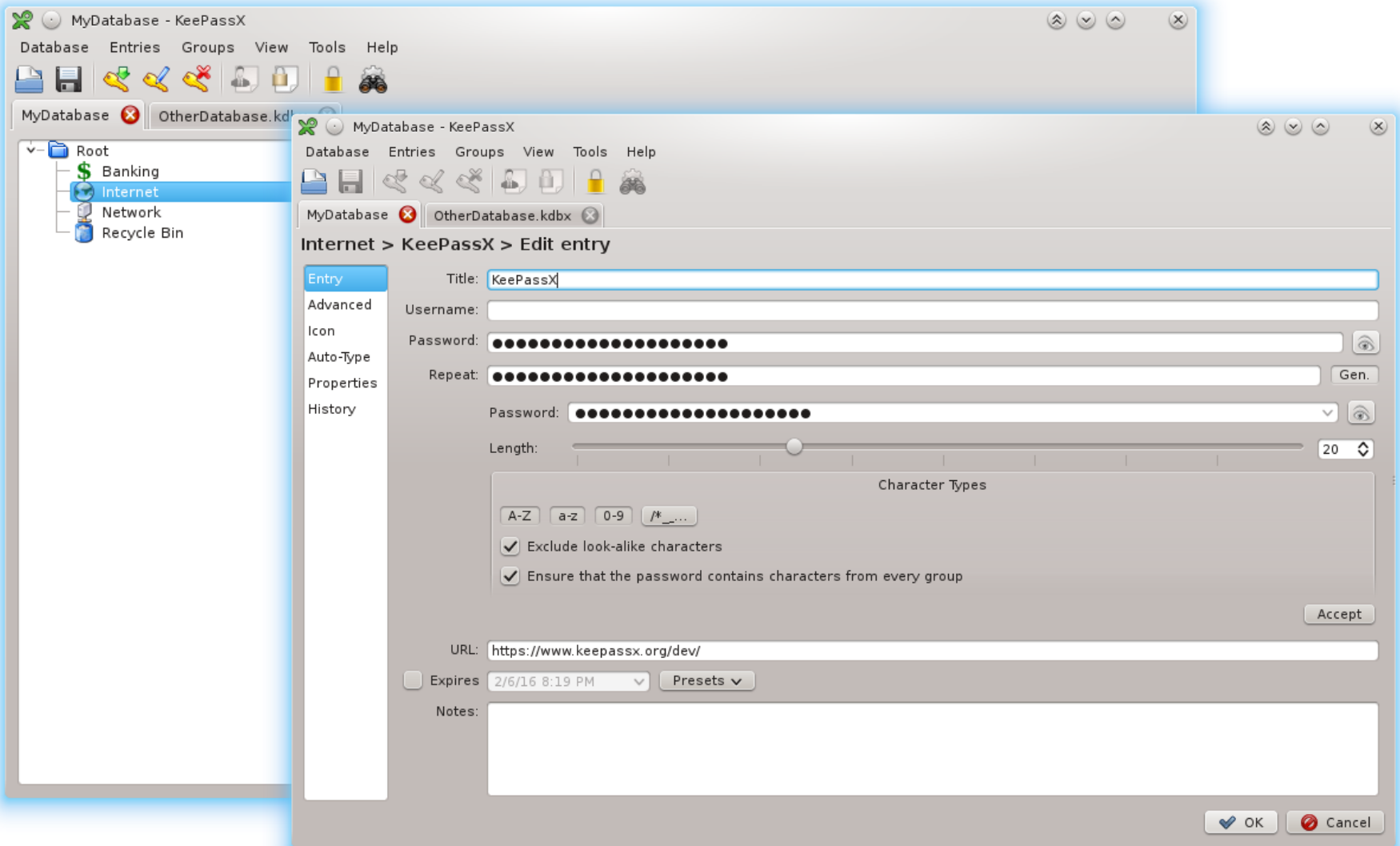
CORRECT!

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

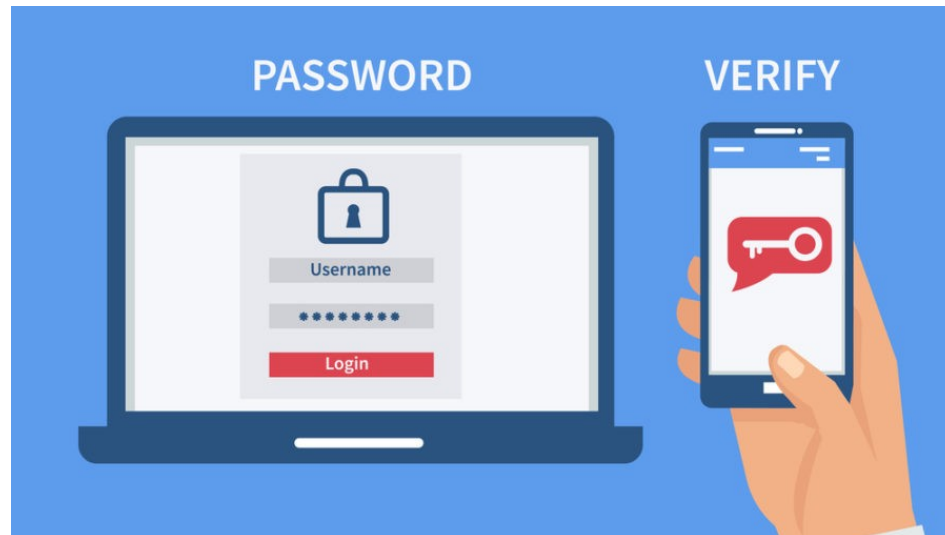


2FA, MFA, ..

token



app



MFA

A photograph of Gandalf the White from The Lord of the Rings, standing in a dark, rocky cave. He is wearing his characteristic white robes and a tall, pointed hat. He holds a long, glowing staff in his right hand. The background shows ancient stone carvings on the cave walls. The lighting is dramatic, with the staff providing a primary light source.

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

Email

SPAM

Important Information on your Life Insurance

SULLA POLIZZA AL
RISPARMIO
 FINO AL
40
 Dettaglio s

FAI IL PREVEN


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 ▶



IN PIÙ, CON



Risparmiare tempo

Fai tutto online, via telefono, email o fax. 24 ore su 24.



Avere tutta la sicurezza

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.

80% discount

Viagra Professional \$3.50
 Cialis \$1.99
 Cialis Professional \$4.07
 Viagra \$0.95

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 i 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 over 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 28,000 acres (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

H 0 Nuovo | Message | Priv: X +

https://www.enforcer.it/wmail/?page=message&uid=15&mailbox_page=1&sort_by=AR 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!

```
Terminal
$ telnet www.enforcer.it 25
Trying 188.40.130.246...
Connected to www.enforcer.it.
Escape character is '^]'.
220 www.enforcer.it ESMTP
HELO igor
250 www.enforcer.it Hi Unknown [5.90.138.207]; I am so happy to meet you.
MAIL FROM:<prova@example.com>
250 <prova@example.com>, sender OK - how exciting to get mail from you!
RCPT TO:<corso@enforcer.it>
250 <corso@enforcer.it>, recipient ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
From: Presidente della Repubblica <presidente@governo.it>
To: Corso Awareness <corso@enforcer.it>
Subject: messaggio di prova
Date: 20190306

Questo è il testo del messaggio.

ciao,
I.
.
250 Queued! (Queue-Id: 05FD7170)
QUIT
```

Phishing (generico)

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

Dear koba

You Have New Pending Messages With 506.5MB Size Attachement.

Due To Your Low Mail Quota Storage Capacity.Click below to.

Enable Here

Thanks,

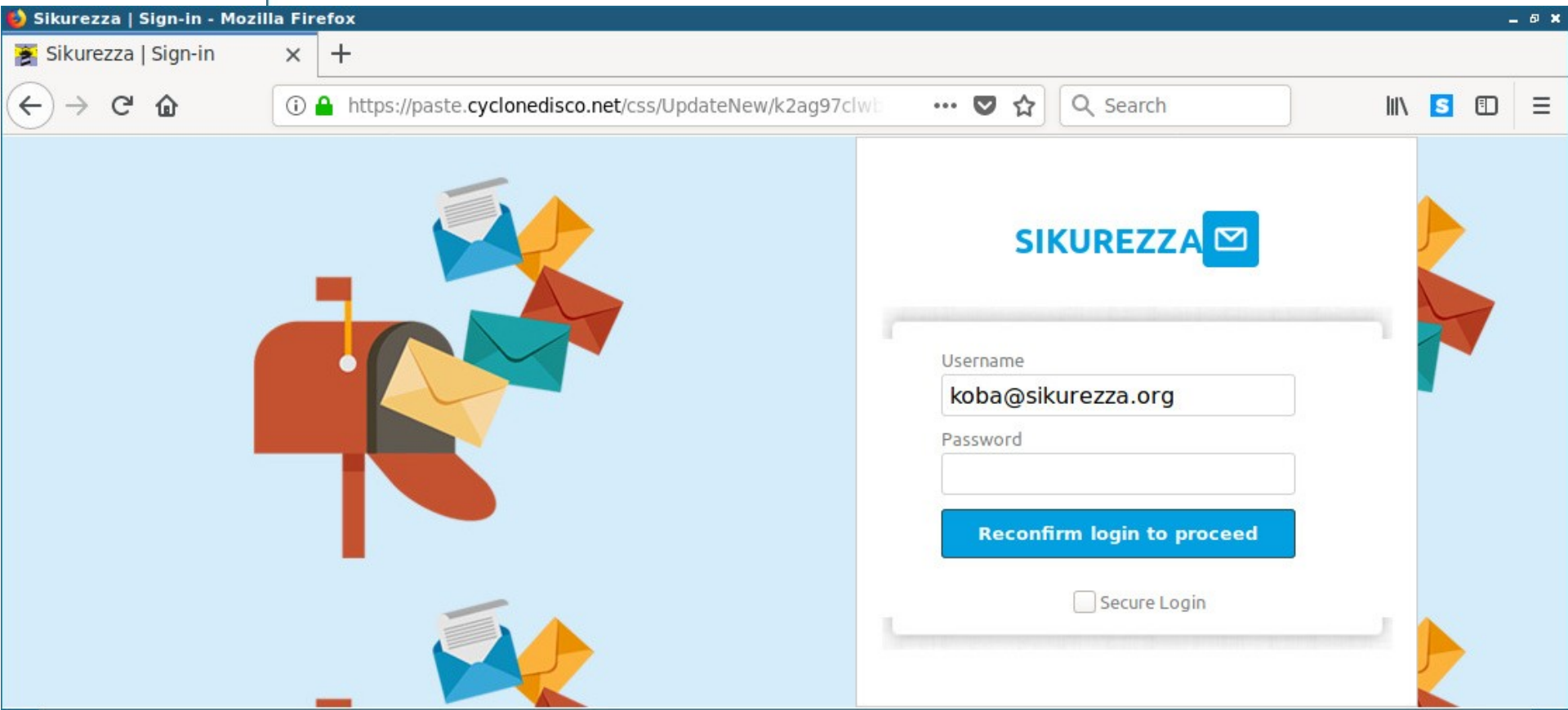
sikurezza.org Administrator

(C) 2019

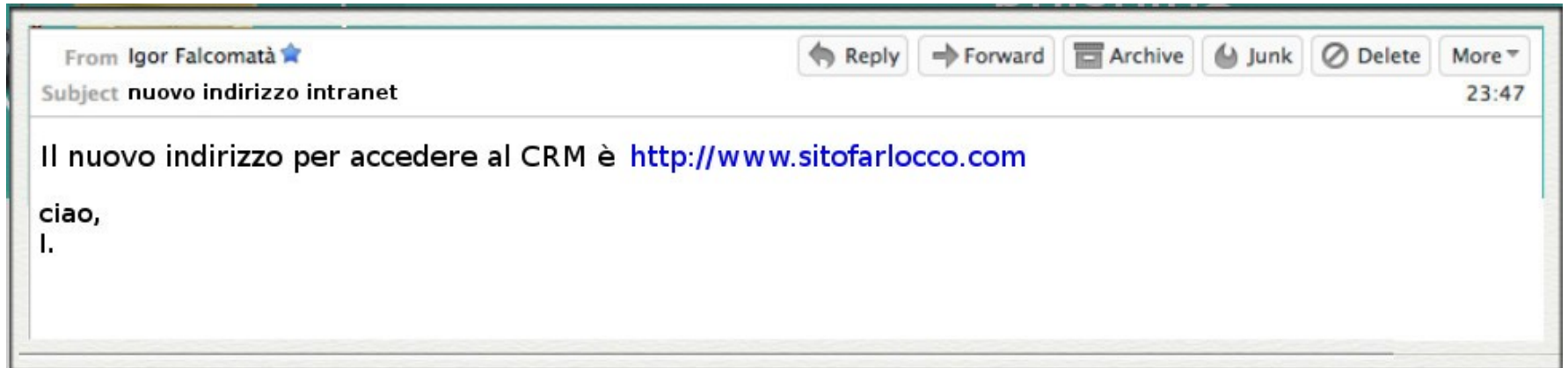
Phishing (generico)

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

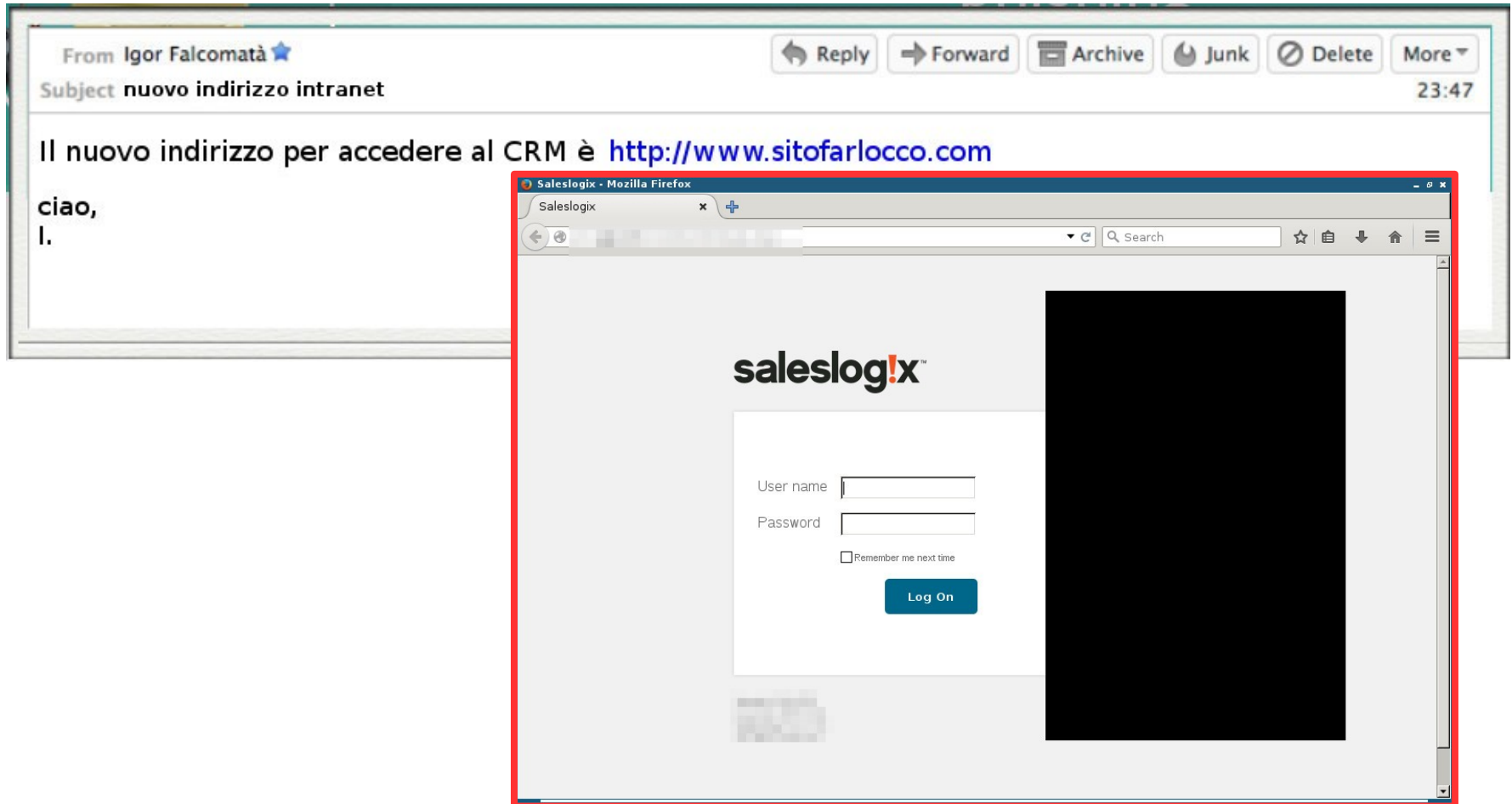
Dear koba



Phishing (mirato “spear phishing”)



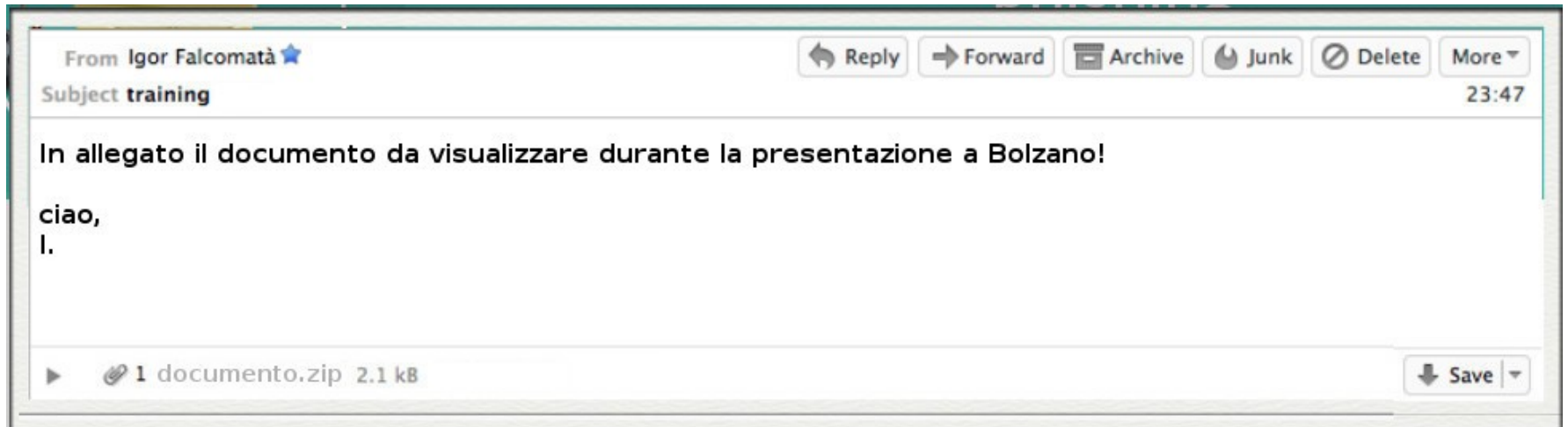
Phishing (mirato “spear phishing”)



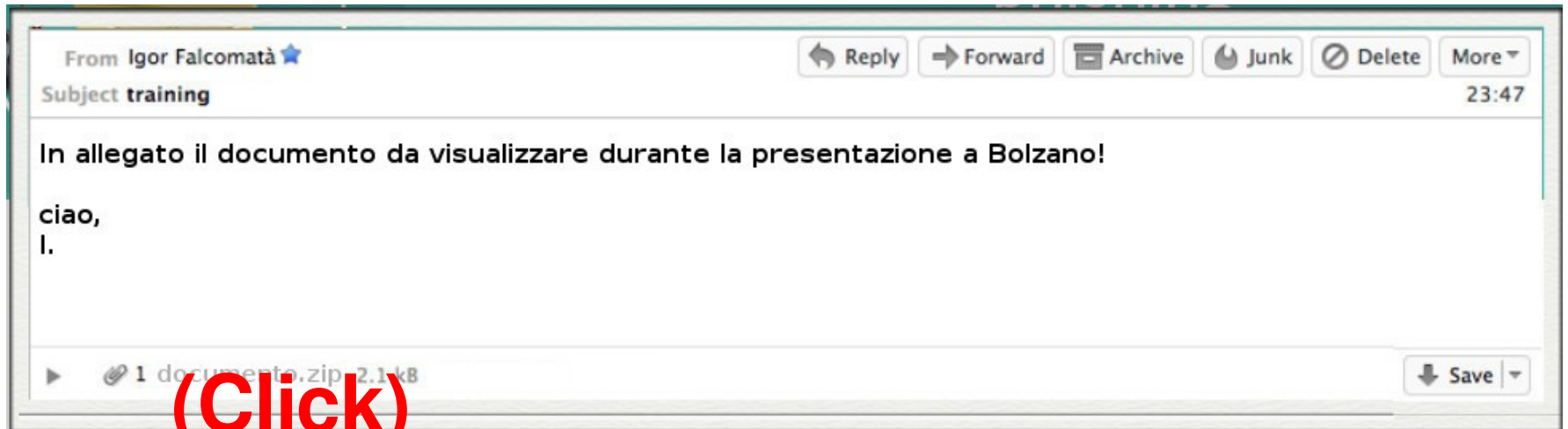
Difendersi

- 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



Private key will be
destroyed on

1/6/2015 1:11:17 PM

Time left

71:55:27

Checking wallet..

Received: 0.00 BTC

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.

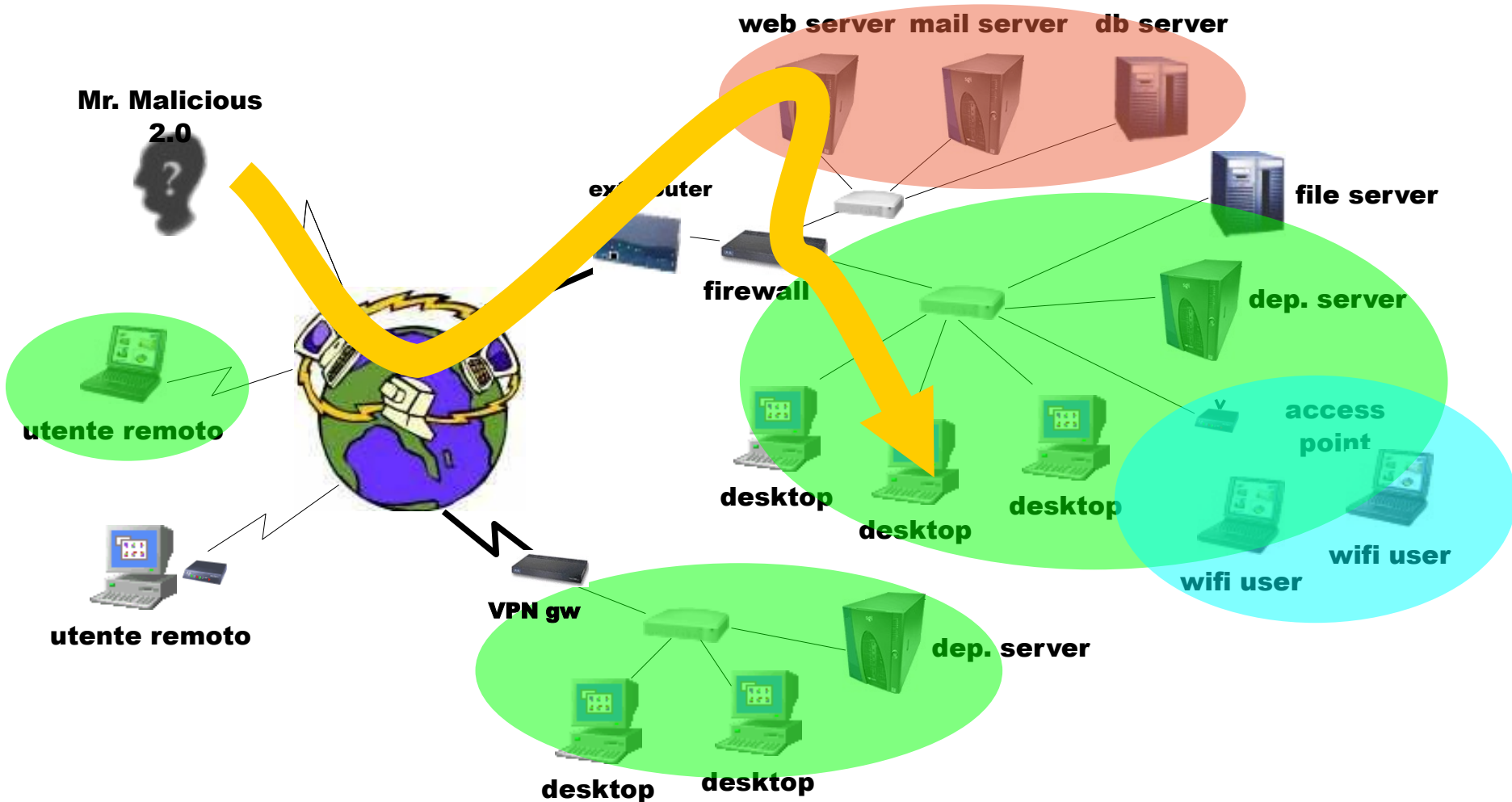
For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

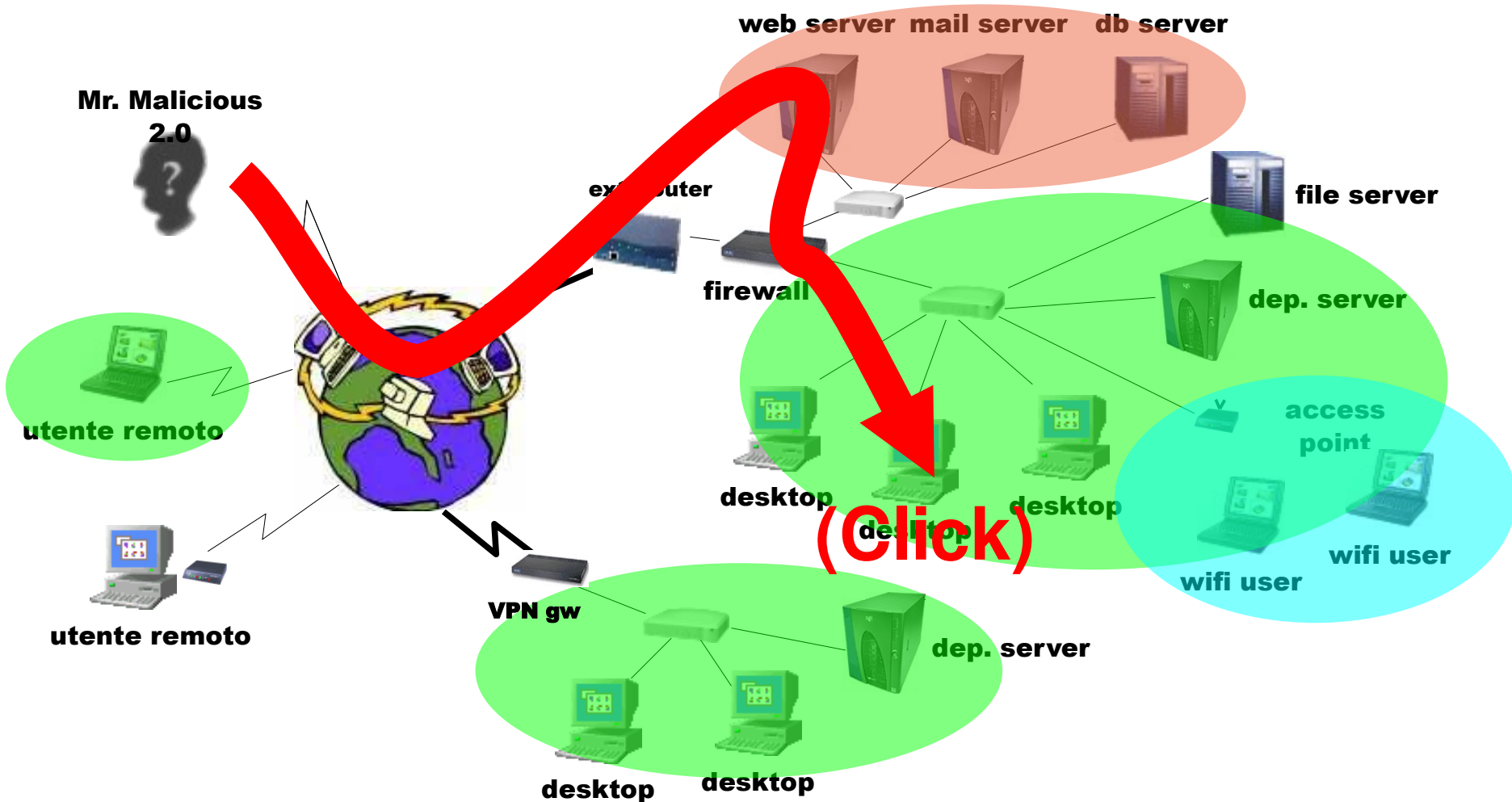
Show files

Pay with Bitcoin

Malware (software malevolo)

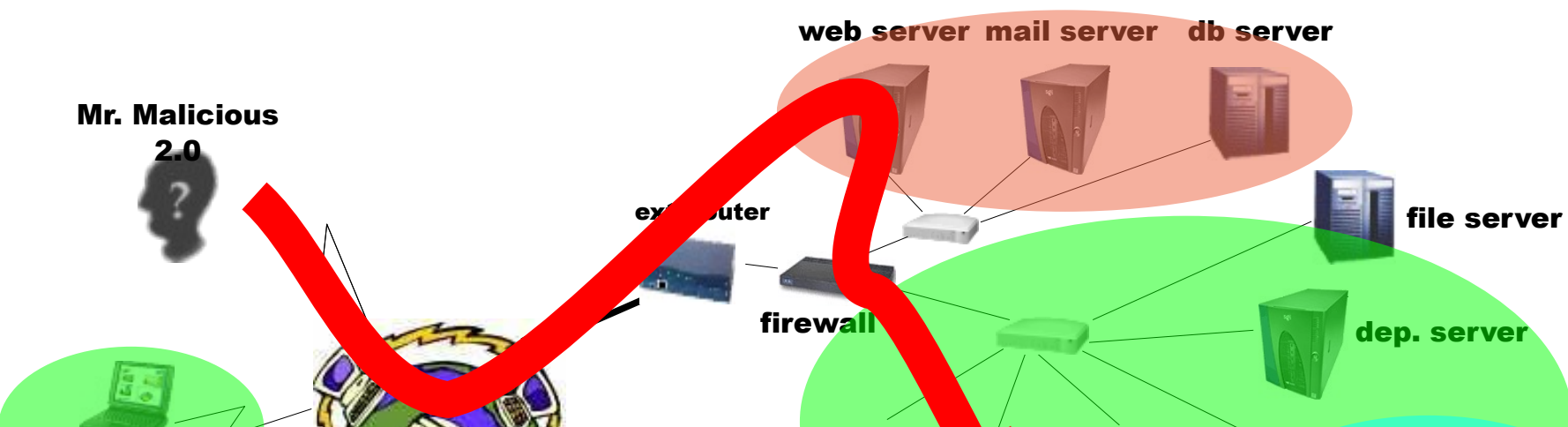


Malware (software malevolo)



Malware (software malevolo)

Mr. Malicious
2.0



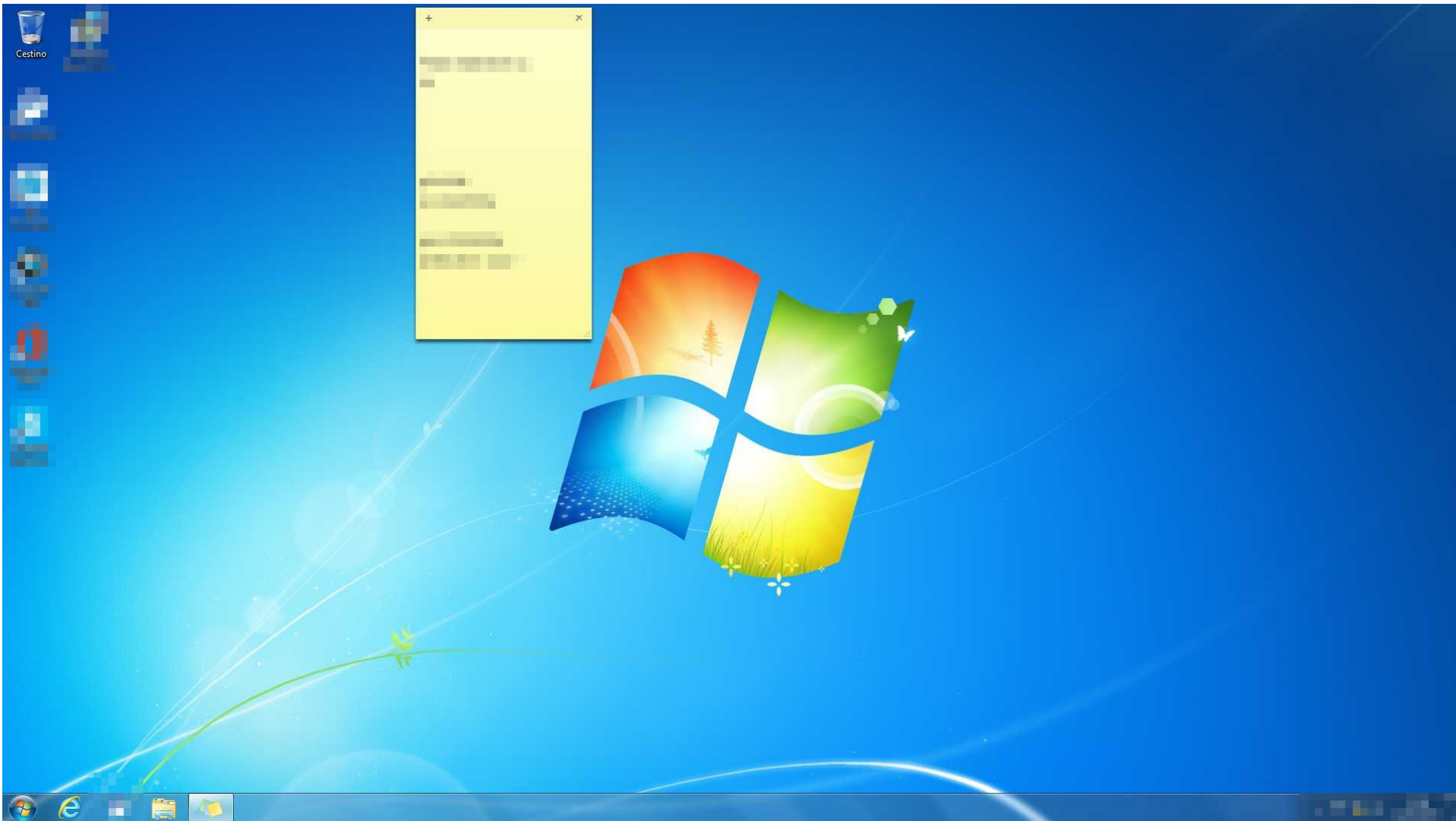
```
C:\Documents and Settings\baltar\Desktop>dir C:\
dir C:\
Il volume nell'unit# C non ha etichetta.
Numero di serie del volume: 6813-B985

Directory di C:\

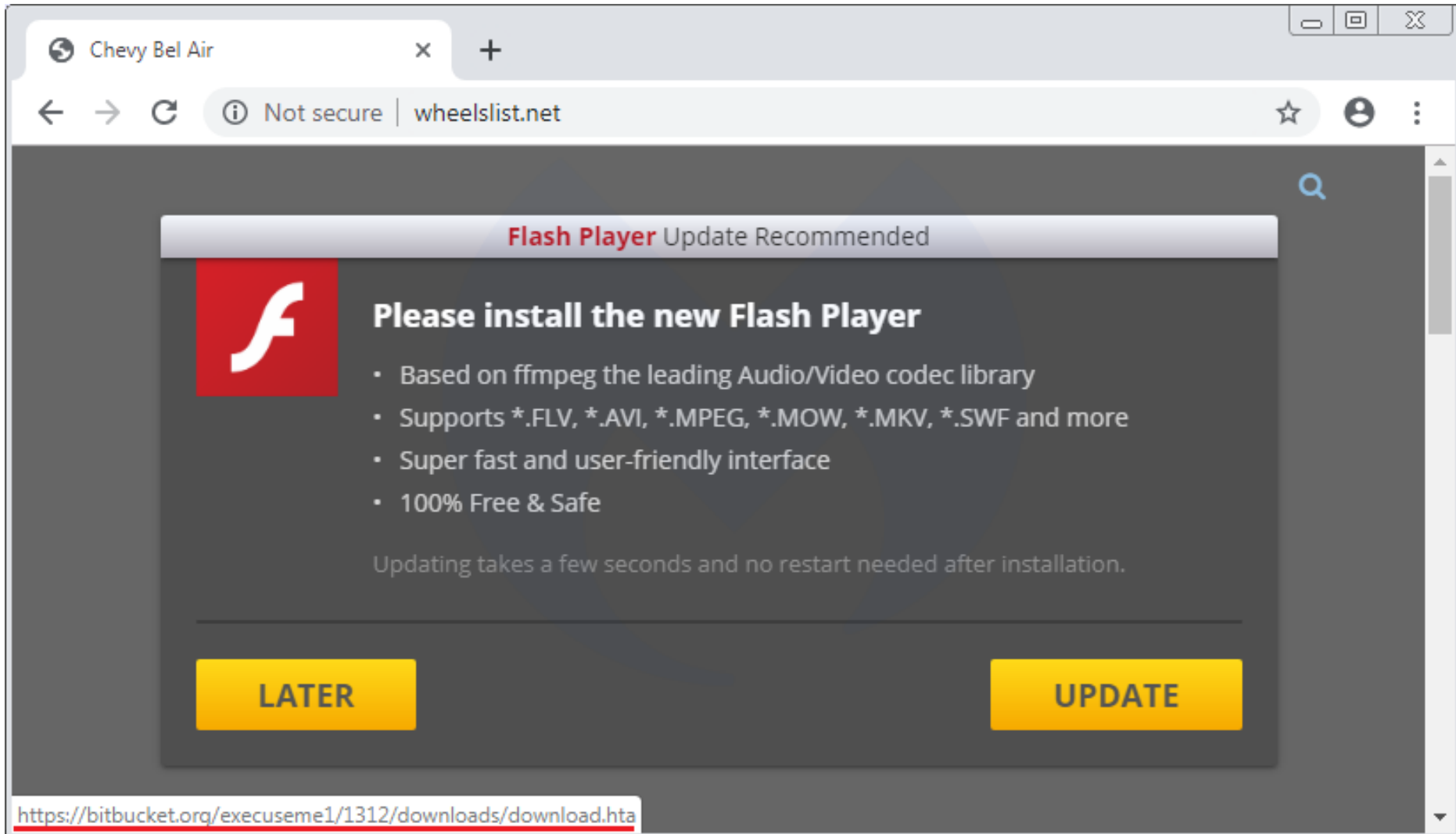
21/10/2010  14.54           0 AUTOEXEC.BAT
21/10/2010  14.54           0 CONFIG.SYS
21/10/2010  15.11    <DIR>      Documents and Settings
21/10/2010  15.11    <DIR>      Programmi
21/10/2010  15.11    <DIR>      WINDOWS
                2 File           0 byte
                3 Directory   8.961.507.328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

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

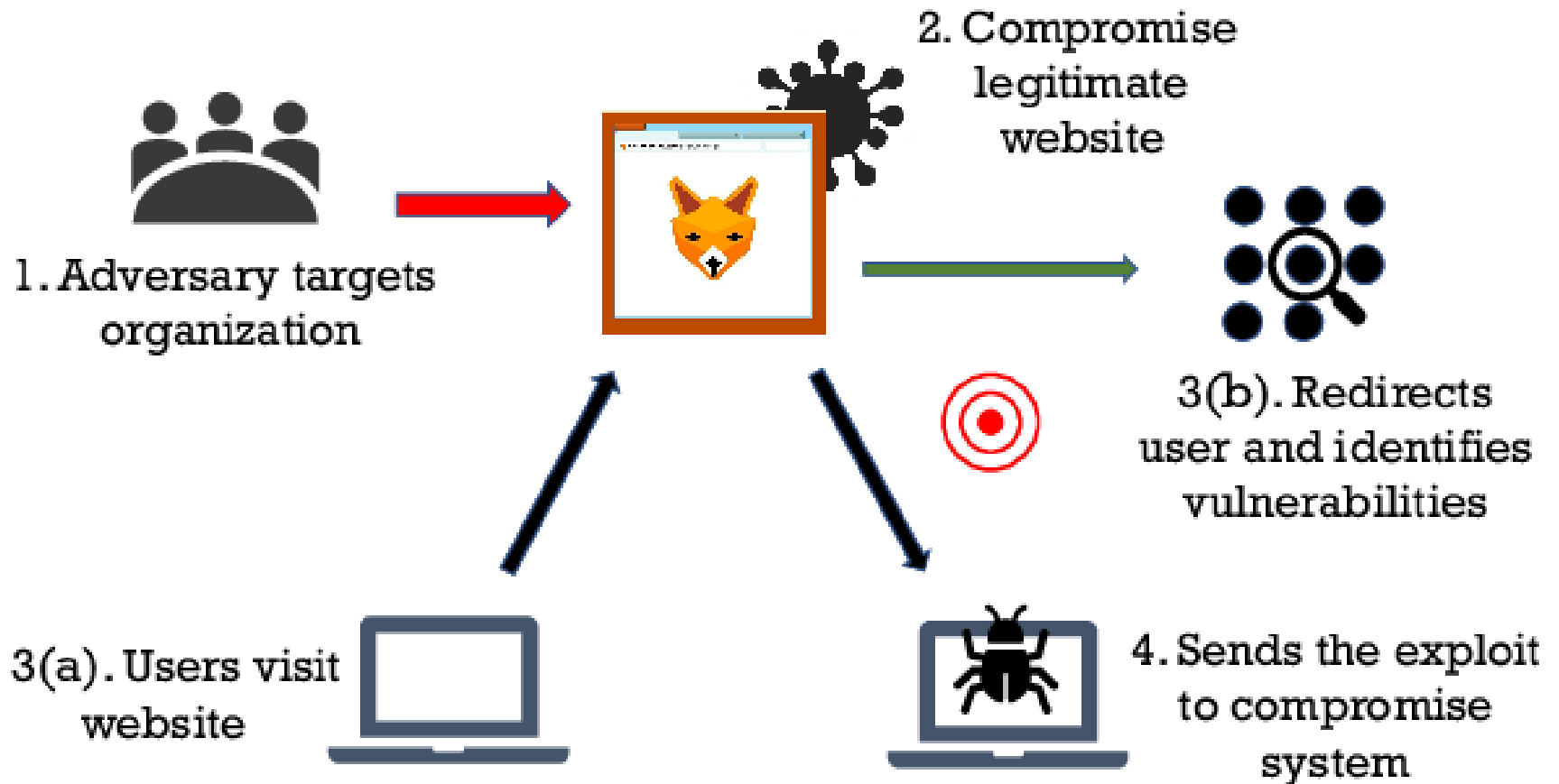
Malware (software malevolo)



Non solo via email..



..anche da chi vi fidate..



Difficile?

create custom backdoor metasploit - YouTube - Mozilla Firefox

create custom backdoor metasploit

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)
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 ...

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
ON KALI LINUX | UNICORN
KALI LINUX

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?



2

/ 58



Community Score



2 engines detected this file



ad282e5ba2bc06a128eb20da753350278a2e47ab545fdab808e94a2ff7b4061e

246.37 KB
Size

2018-11-23 09:56:15 UTC
26 days ago

Meeting_Agenda.zip

contains-macho

mac-app

zip

DETECTION

DETAILS

RELATIONS

BEHAVIOR

CONTENT

SUBMISSIONS

COMMUNITY



2018-11-23T09:56:15



Kaspersky



HEUR:Trojan.OSX.Agent.c

ZoneAlarm



HEUR:Trojan.OSX.Agent.c

Ad-Aware



Undetected

AegisLab



Undetected

AhnLab-V3



Undetected

Alibaba



Undetected

ALYac



Undetected

Antiy-AVL



Undetected

Arcabit



Undetected

Avast



Undetected

E smartphone/tablet ?

mobile malware - Cerca con Google - Mozilla Firefox

mobile malware - Cerca

https://www.google.com/search?source=hp&ei=ou-YXqaHDIXClwTQ64TQ

Google

mobile malware

Tutti Notizie Immagini Video Shopping Altro Impostazioni Strumenti

Circa 88.000.000 risultati (0,41 secondi)

Suggerimento: Cerca risultati solo in **italiano**. Puoi specificare la lingua di ricerca in Preferenze.

www.forcepoint.com > cyber-edu ▾ Traduci questa pagina

What is Mobile Malware? Defined, Explained, and Explored

...

Mobile malware, as its name suggests is malicious software that specifically targets the operating systems on mobile phones. There are many types of mobile ...

www.kaspersky.com > mobile ▾ Traduci questa pagina

Mobile Malware Threats | Android Security Issues | Kaspersky

But along with increased use comes an explosion of **mobile malware** — malicious code designed to target smartphones and tablets. Your Risk Factors. Is your ...

Virus symbian

I virus symbian informatici creano copie dei dati sensibili dei telefoni mobili con sistemi Symbian. I virus per smartphone in estensione .sis

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**

Domande?

(grazie per l'attenzione)

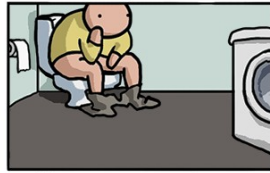
MART VIRKUS



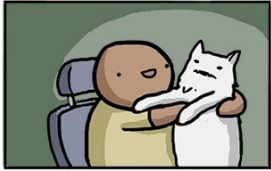
NO PANTS



OTHER TIMEZONE



FORGOT CAMERA ON



THE ONE WITH PETS



EVERY VIDEO CALL EVER



THE ONE WITH KIDS



TAKING NOTES OR GAMING?



LOOKING FOR MUTE



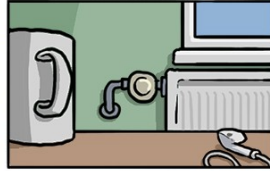
JOINS 10 MINS LATE



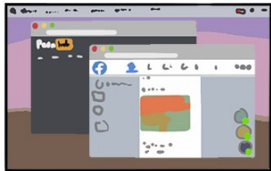
STUCK IN TRAFFIC



CONNECTION ISSUES



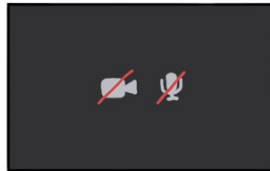
"I'M LISTENING"



ACCIDENTAL SCREENSHARE



GAVE UP



GAVE UP YEARS AGO



WHAT YOU THOUGHT IT WOULD BE



HOW IT WAS



WHAT IT COULD HAVE BEEN

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

Igor Falcomatà
CEO, Enforcer
ifalcomata@enforcer.it



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/>