Smartworking in an (in?)secure environment

Bruno Motta

Vodafone Partner markets

From Office to Home Hacking

Lo scenario NON e' semplice

Special Risks: COVID-19

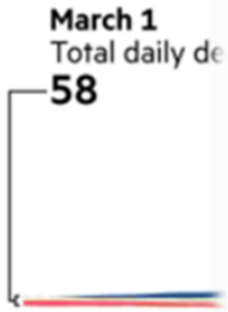
Global
Pandemic will prompt Western nations to shift spending priorities and reduce foreign troop deployments, allowing jihadists to extend operations

Global
Debt suspension for poorer countries will facilitate improved responses to COVID-19, but long-term risk of sovereign crises will persist

EU
Gradual lifting of COVID-19 restrictions in coming weeks to continue at varying pace across EU

China
COVID-19 will increase Western resistance to Chinese technology, raising challenges for foreign deals and partnerships

South Africa
Civil unrest to rise amid growing popular frustration at COVID-19 lockdown



The UK ha
daily d

NON partiamo da una cyber-situazione facile

E noi andiamo a *LAVORARE DA CASA*?

“Tutti Lavoreranno da Casa”

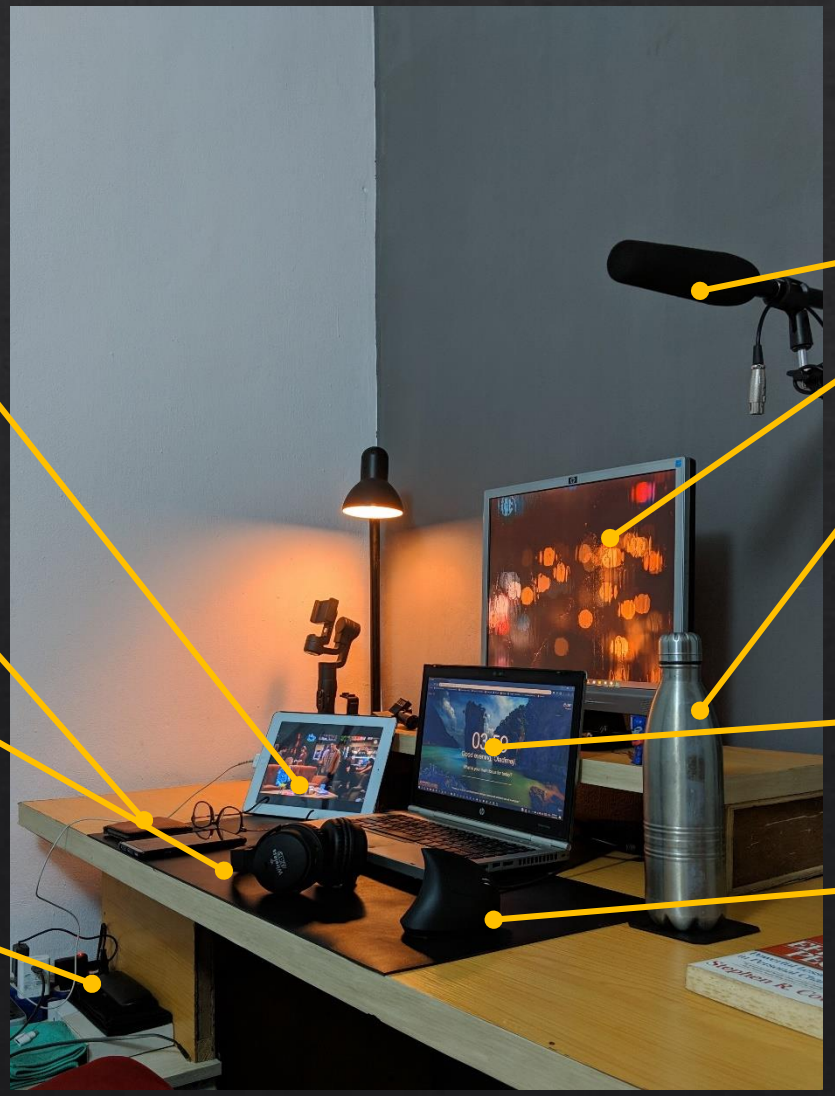
Il Dipendente

Come lo Pensiamo

La Sicurezza Aziendale

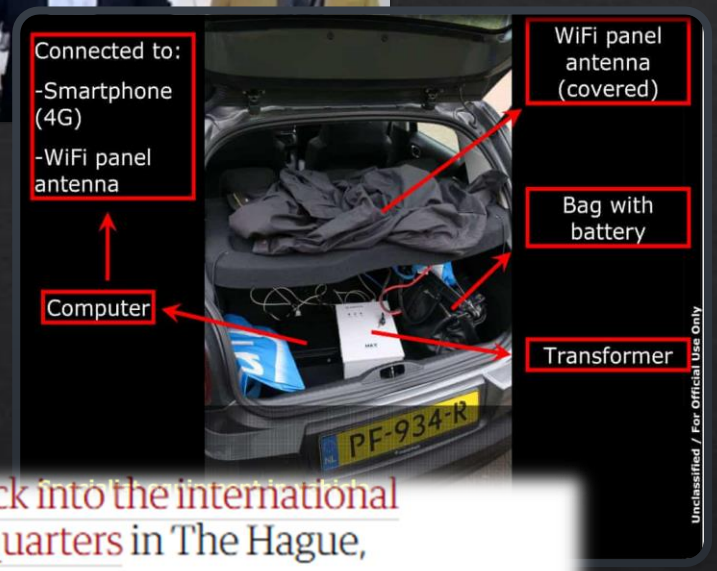
Come e’ Realmente

Ready? Smart Tools=Smart Working



…e i cattivi?…Smart Hacking!

- Smart Hacking
  - Il team raggiunge la vittima a domicilio se necessario
- No Intrusion
  - Il servizio puo' essere svolto dall'esterno
- Multi vector Attacks
  - Tutti abbiamo uno smartphone, WiFi a casa a qualche "Smart Device"



APRILE 2018

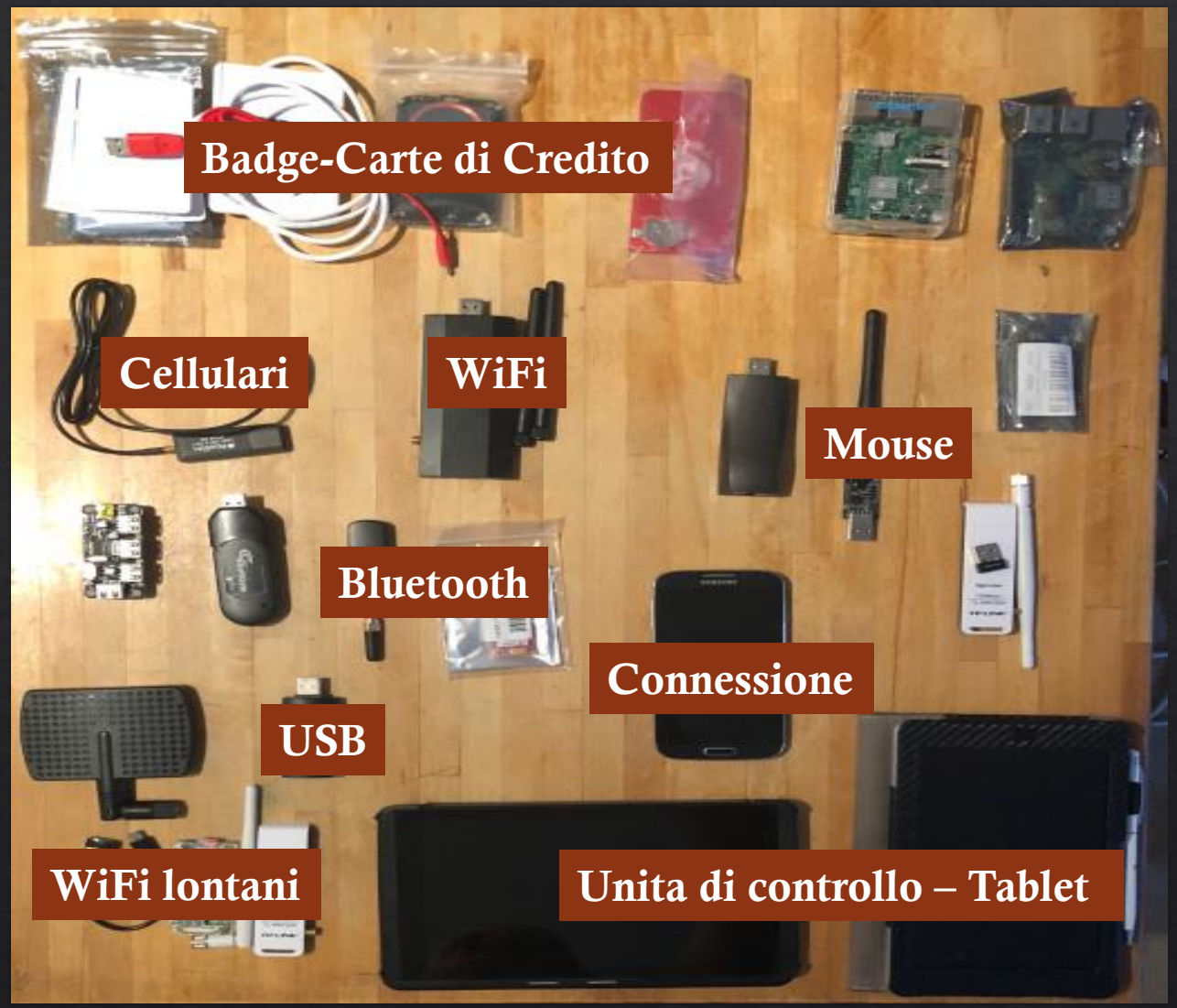
Four agents were caught trying to hack into the international chemical weapons watchdog's headquarters in The Hague, according to Dutch authorities

The four men, named as IT experts Aleksei Morenets and Evgenii Serebriakov, and support agents Oleg Sotnikov and Alexey Minin, travelled on diplomatic passports to Amsterdam's Schiphol airport on 10 April, and were met there by a Russian embassy official.

SOURCE: The Guardian - LINK

…smart Hacking???

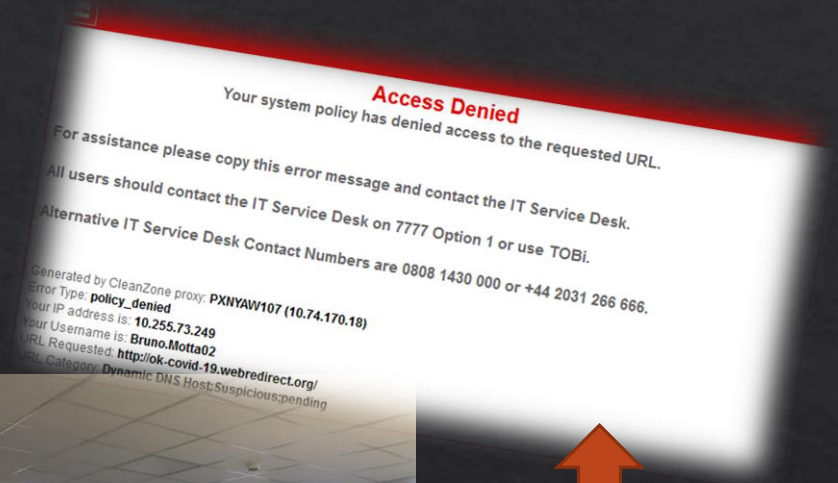
Bagaglio a mano sospetto…



…ma dobbiamo chiederci…

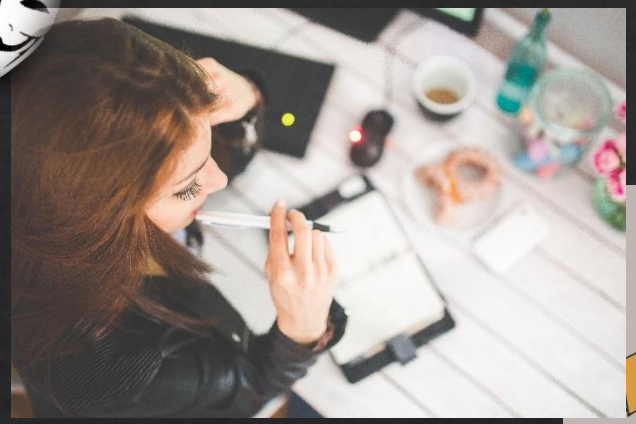
1. Lo smartworking, il lavorare da casa, rende la nostra azienda piu vulnerabile?
2. Ci sono nuovi tipi di attacchi hacker da cui dobbiamo difenderci?
3. La nostra casa e’ un ambiente sicuro per lavorare?

La Vulnerabilita’ in azienda



Un’azienda e’ strutturata per difenderci dagli attacchi esterni

La Vulnerabilita’ a casa

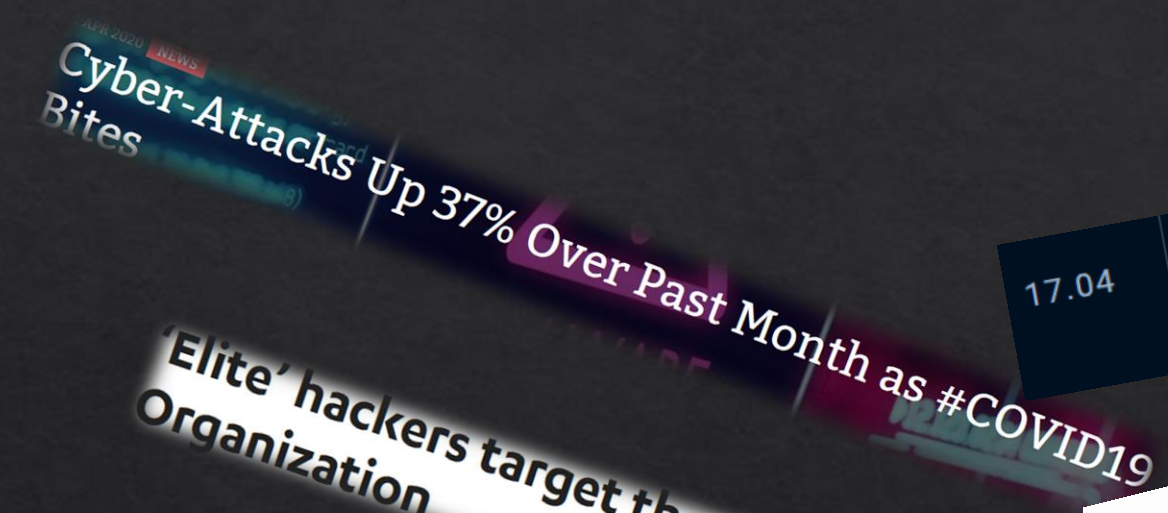


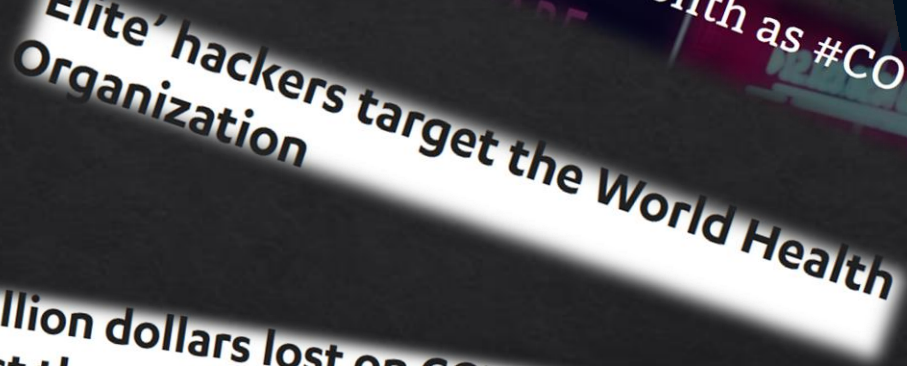
Ogni Home Office diventa una porta di accesso a tutta l’Azienda

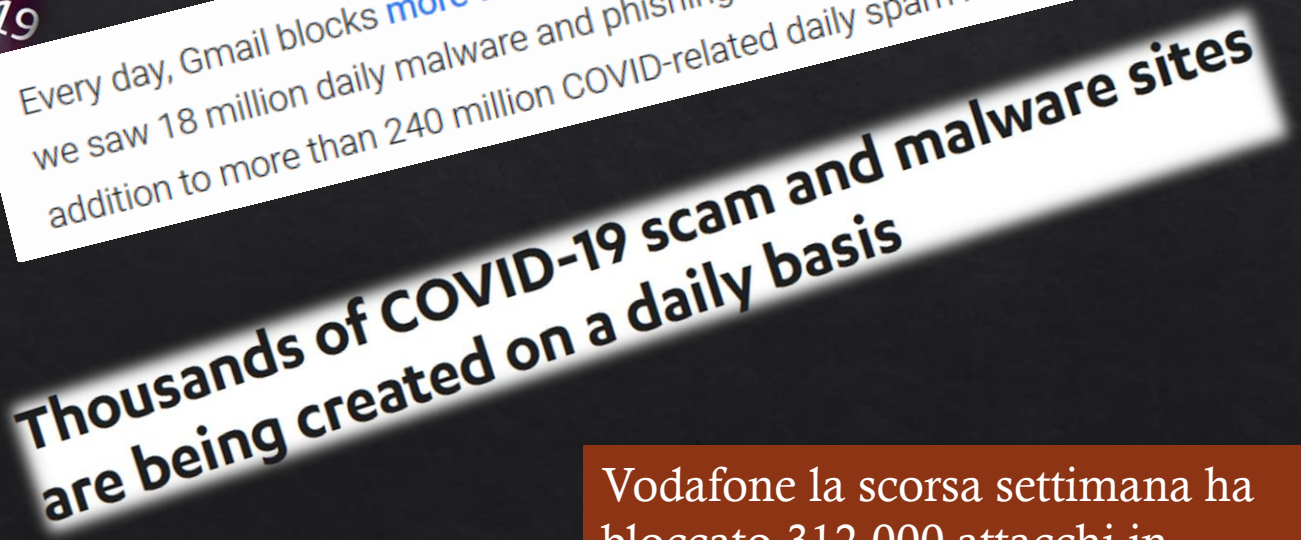
Lo smartworking, il lavorare da casa, rende la nostra azienda piu vulnerabile?

- L’ambiente di casa non e’ lo standard per il lavoro.
- Abbiamo sempre lavorato da casa per tempi brevi e spesso in modo non sistematico
- I protocolli aziendali non hanno mai considerato a fondo uffici stabili remote
- Gli strumenti e l’ambiente tecnologico del nostro lavoro a casa sono meno controllati e, spesso, piu “personali”

Ci sono attacchi hacker “COVID” da cui dobbiamo difenderci?







COVID-19-CTI-LEAGUE

[C-19-CTI](#) [WebARX](#) [F-Secure](#) [Google](#)

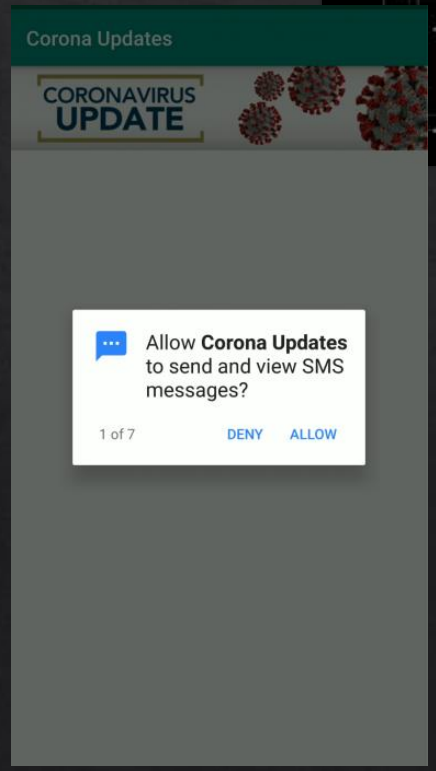
Vodafone la scorsa settimana ha bloccato 312.000 attacchi in Spagna e Germania

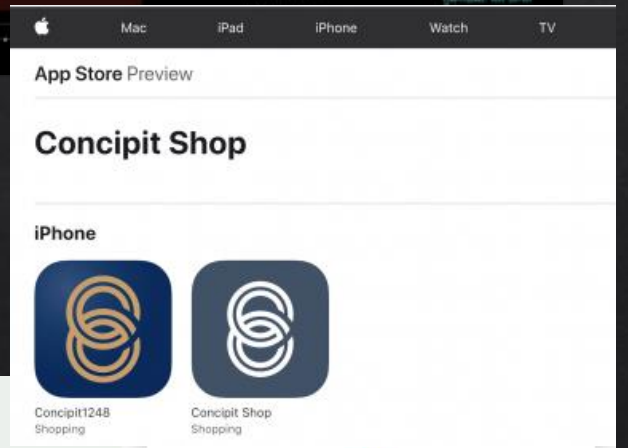
Project SPY

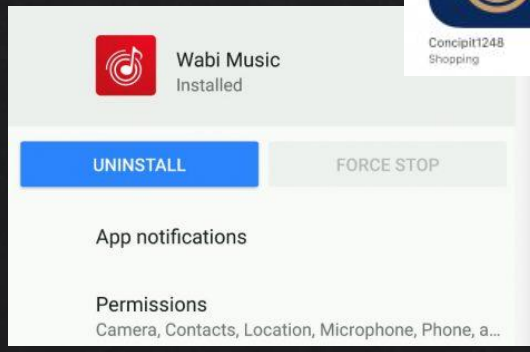
http://spy.cashnow.ee/

http://concipit1248.com/

- Dietro ad una azienda apparentemente legittima (Concipit) si nasconde un progetto di cattura di dati e informazioni personali
- **Corona Updates** sviluppato dalla stessa azienda e stato rimosso quasi subito

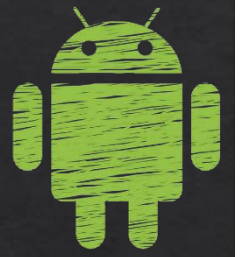






Cosa nascondono le APP per Android e iOS?

- In entrambi I casi le app permettono l'installazione di altre applicazioni e/o moduli all'insaputa dell'utente
- Possono avere accesso ai dati del telefono, agli SMS, alle chat e alle immagini.
- Possono attivare e disattivare il microfono
- Tutte queste applicazioni scaricano I dati su un server remota
- L'applicazione per iOS e' leggermente meno invasiva

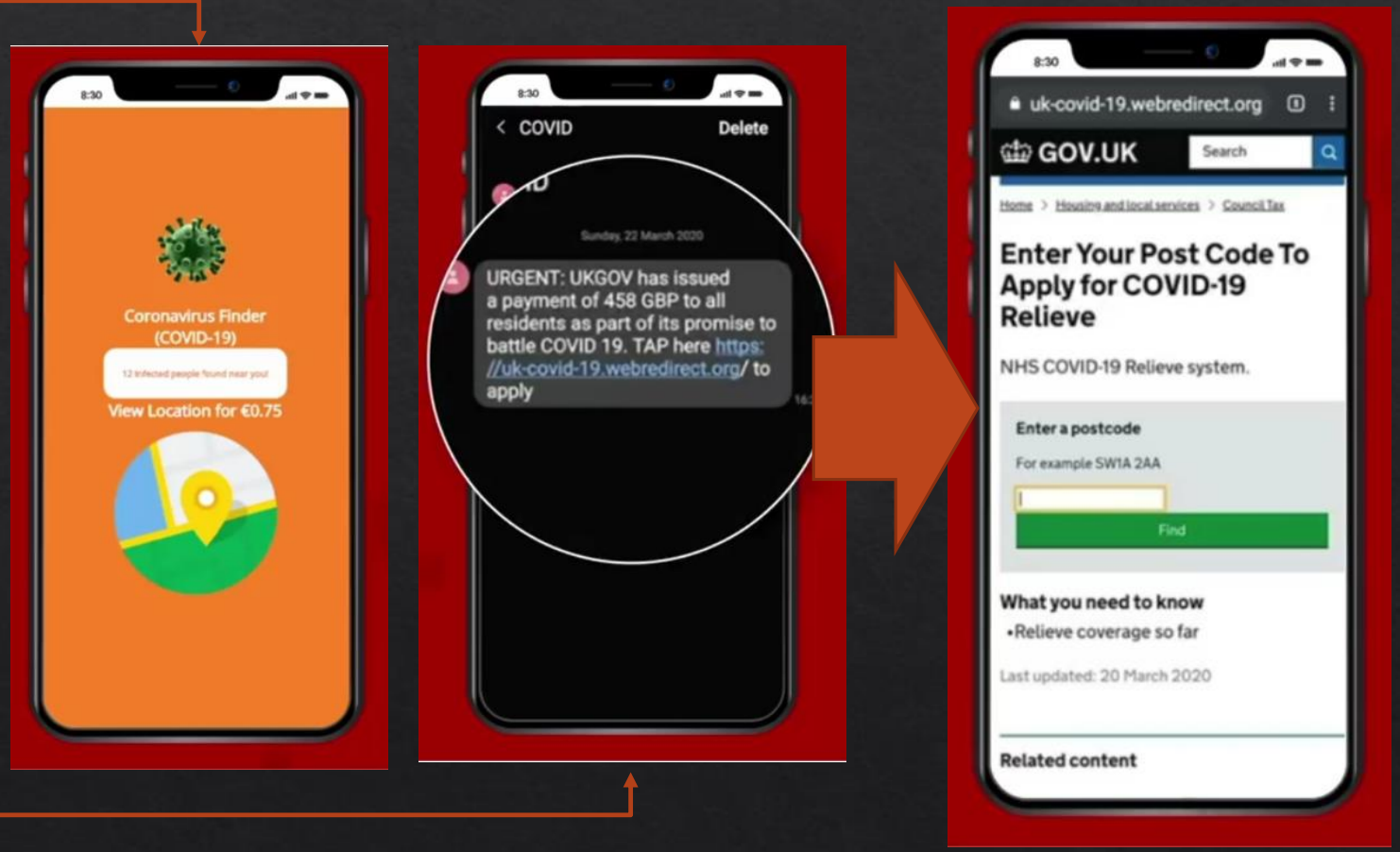


Initial Access	Persistence	Credential Access	Discovery	Collection	Command and Control
Deliver Malicious App via Authorized App Store	App Auto-Start at Device Boot	Access Notifications	File and Directory Discovery	Access Call Log	Commonly Used Port
Masquerade as Legitimate Application		Access Stored Application Data	Location Tracking	Access Contact List	Standard Application Layer Protocol
		Capture SMS Messages	System Information Discovery	Access Notifications	
			System Network Configuration Discovery	Access Stored Application Data	
				Capture SMS Messages	
				Location Tracking	
				Network Information Discovery	

Initial Access	Credential Access	Collection	Command and Control
Deliver Malicious App via Authorized App Store	Access Stored Application Data	Access Stored Application Data	Commonly Used Port
			Standard Application Layer Protocol

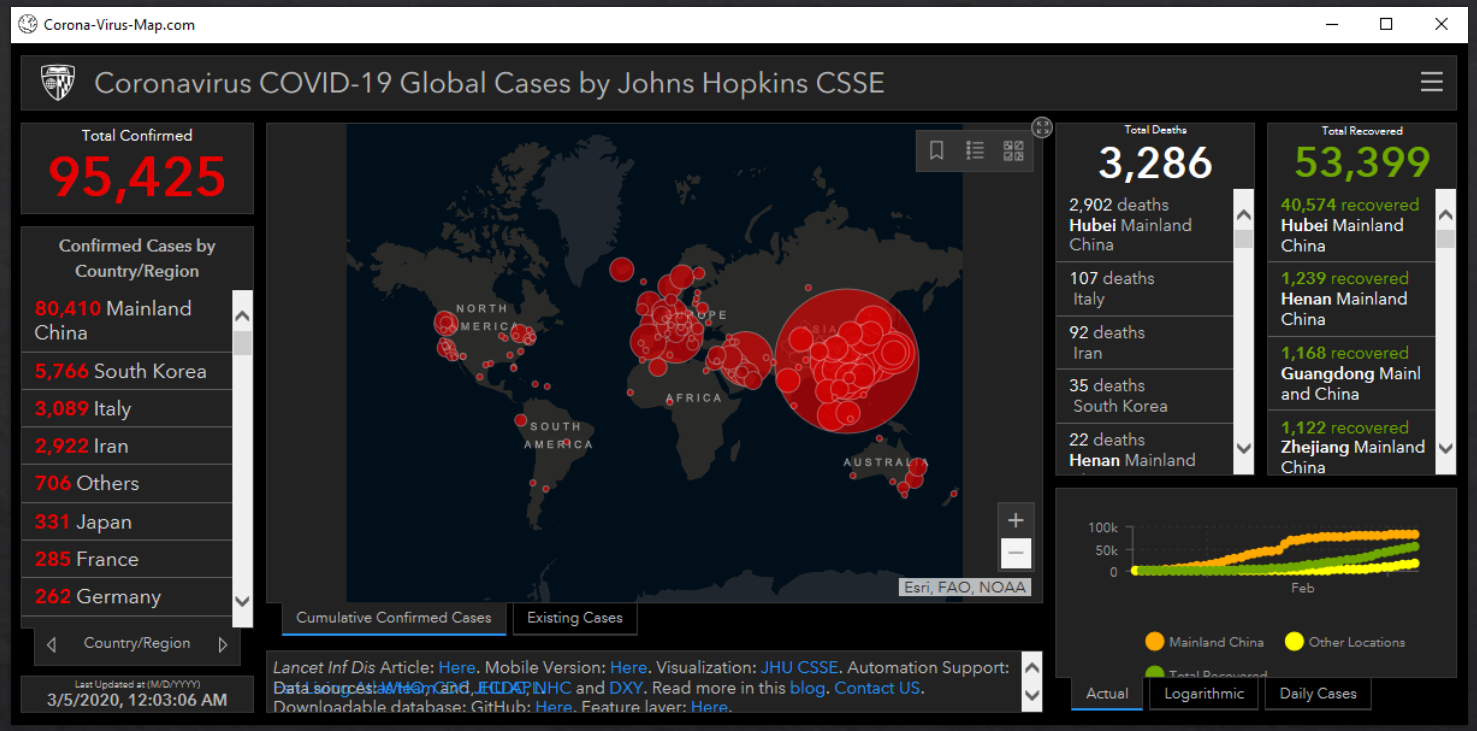
Ci sono altri casi?

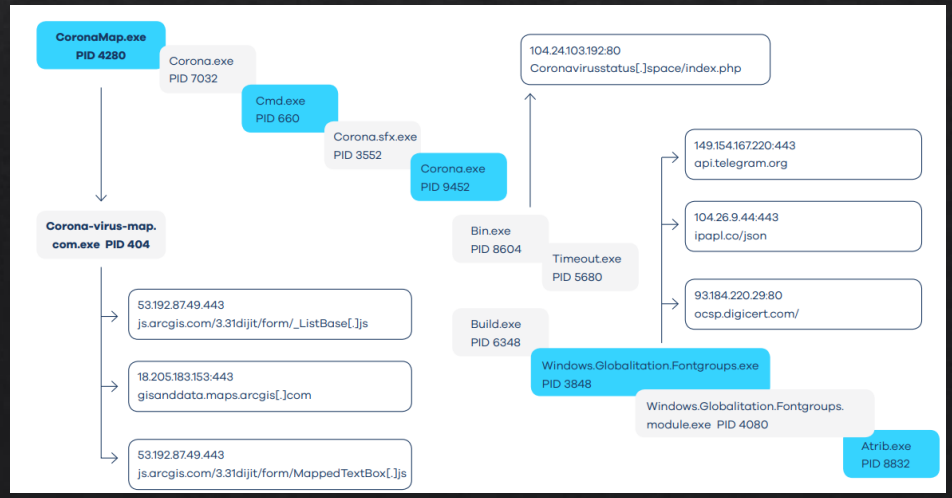
- **APP**
  - Vengono create app che chiedono il pagamento di PICCOLE somme di denaro per fornire informazioni importanti. Chiaramente NON forniscono informazioni attendibili
- **SMS**
  - Si possono ricevere SMS che includono messaggi trabocchetto con lo scopo di indirci a fornire le nostre informazioni personali



Coronavirus MAP

- Il Malware si presenta in modo molto convincente con una interfaccia simile a quella ufficiale
- Una vola attivato il programma legge I dati dal sito ufficiale
- ***…MA…***
- Nel frattempo scarica e installa moduli softwareche infettano in computer
- Il modulo installato e' AZORult, un information stealer



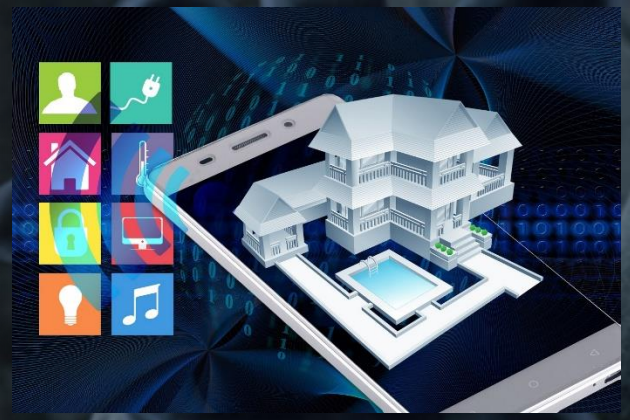


ReasonSecurity

Ci sono nuovi attacchi hacker da cui dobbiamo difenderci?

- **Allo Smartphone/Tablet**
  - SMS con link infetti che spesso promettono support da parte dello Stato o avvisi importanti
  - App che chiedono pagamenti per servizi inutile
  - App che catturano dati e prendono il controllo del telefono
- **Al Computer**
  - Programmi che informano sul virus ma nascondono altre funzioni maligne

La nostra casa e’ un ambiente sicuro per lavorare?



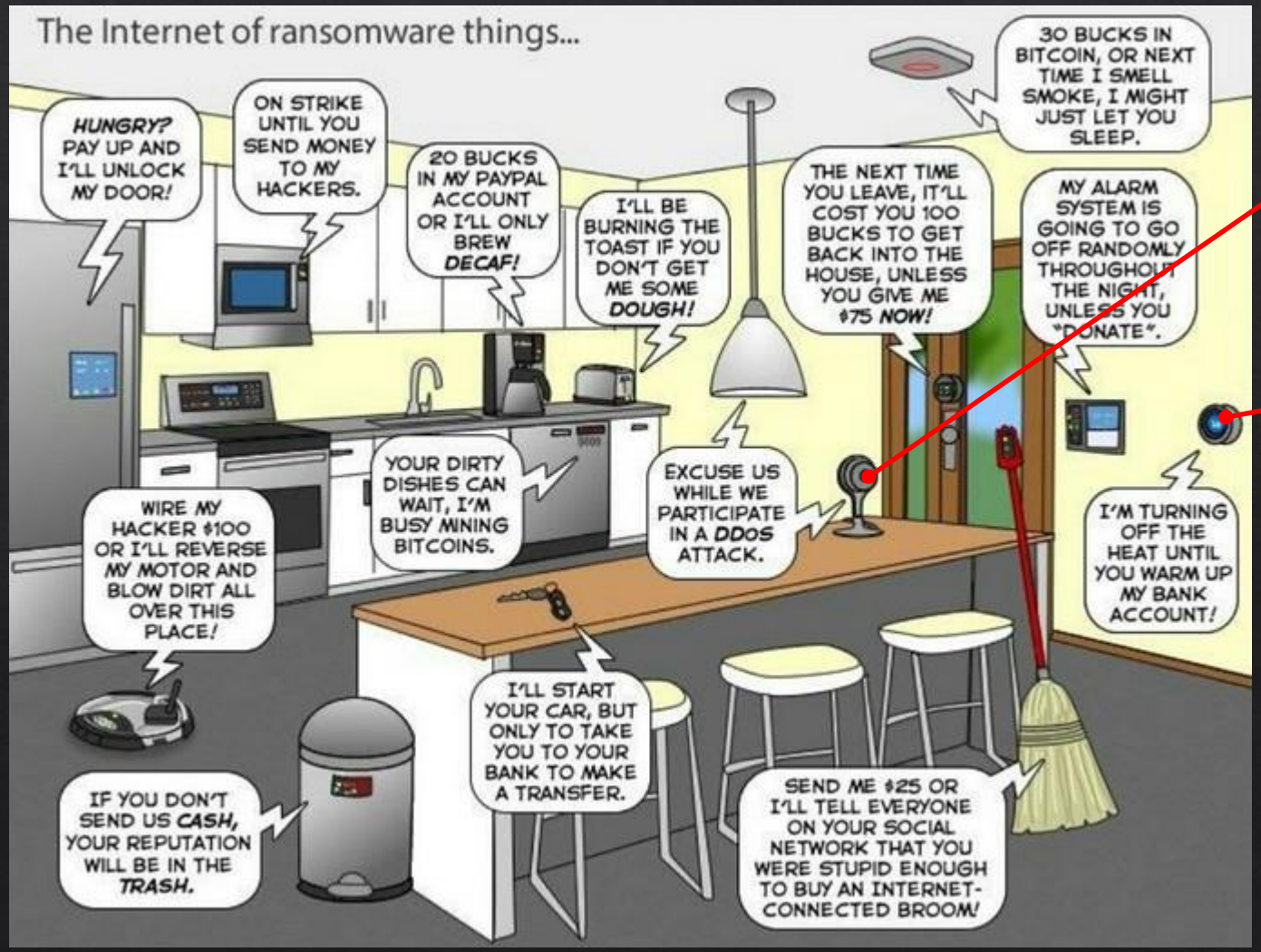
SMART Working in a SMART home

- La Casa e' oggi una vera RETE LOCALE con cavi, connessioni radio e dispositivi sempre connessi e di ogni tipo
- Ogni apparato ha un suo software, ha delle password che lo proteggono

Gli attacchi alla rete di casa

SHODAN

Starbucks ≠ Starbuck

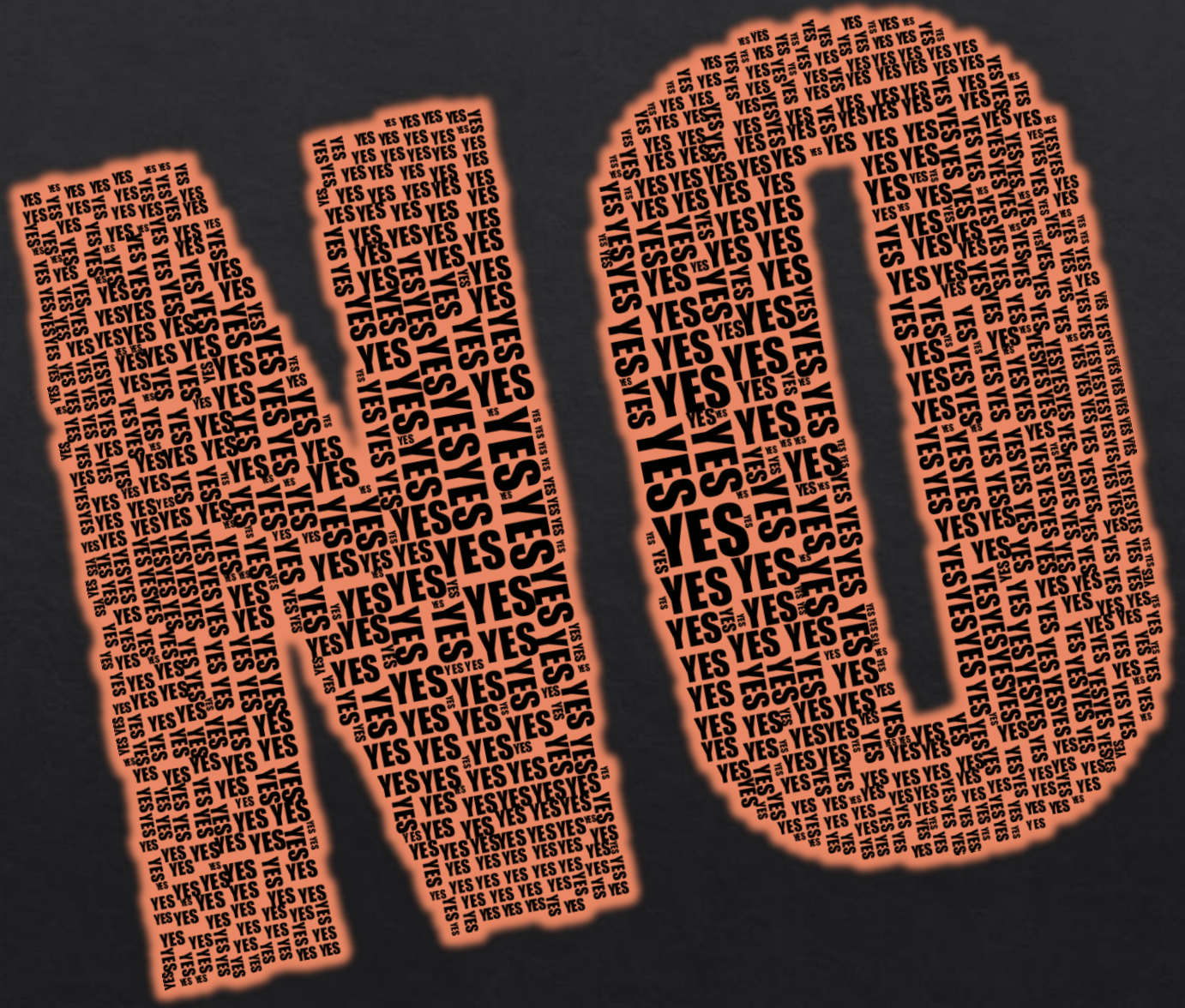


WEBCAM

Termostato

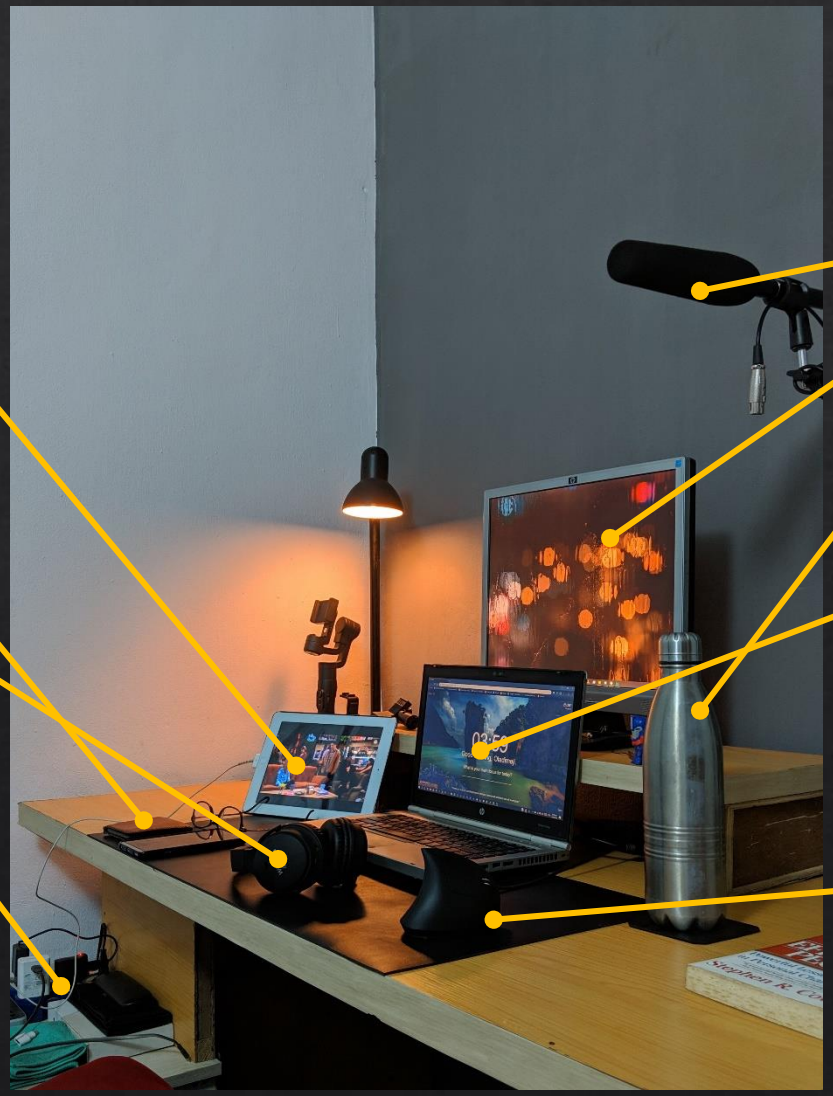
La nostra (smart) casa e' un ambiente sicuro per lavorare?

- WIFI
  - Le reti di casa sono spesso protette con password di accesso semplici e router non aggiornati
- SELF ISOLATION
  - Tutti I dipendenti sono a casa e quindi piu facili da tracciare
- SMART HOME VULNERABILTY
  - Le case, sempre piu' SMART offrono diversi vettori di attacco




...e comunque
DOBBIAMO
lavorare da casa...
MacBook Air

Ready? Smart Tools=Smart *Hacking*



Tablet

- Malicious Apps
- Fake SMS
- Fake Calls

Smartphone

Cuffie

Bluetooth can be spoofed

Router/Wifi

- Router has software on it
- WiFi has **just** password protection

Gadgets

- USB Gadgets can be weaponised

Laptop

- The main door to the heaven
- The REAL Pandora box

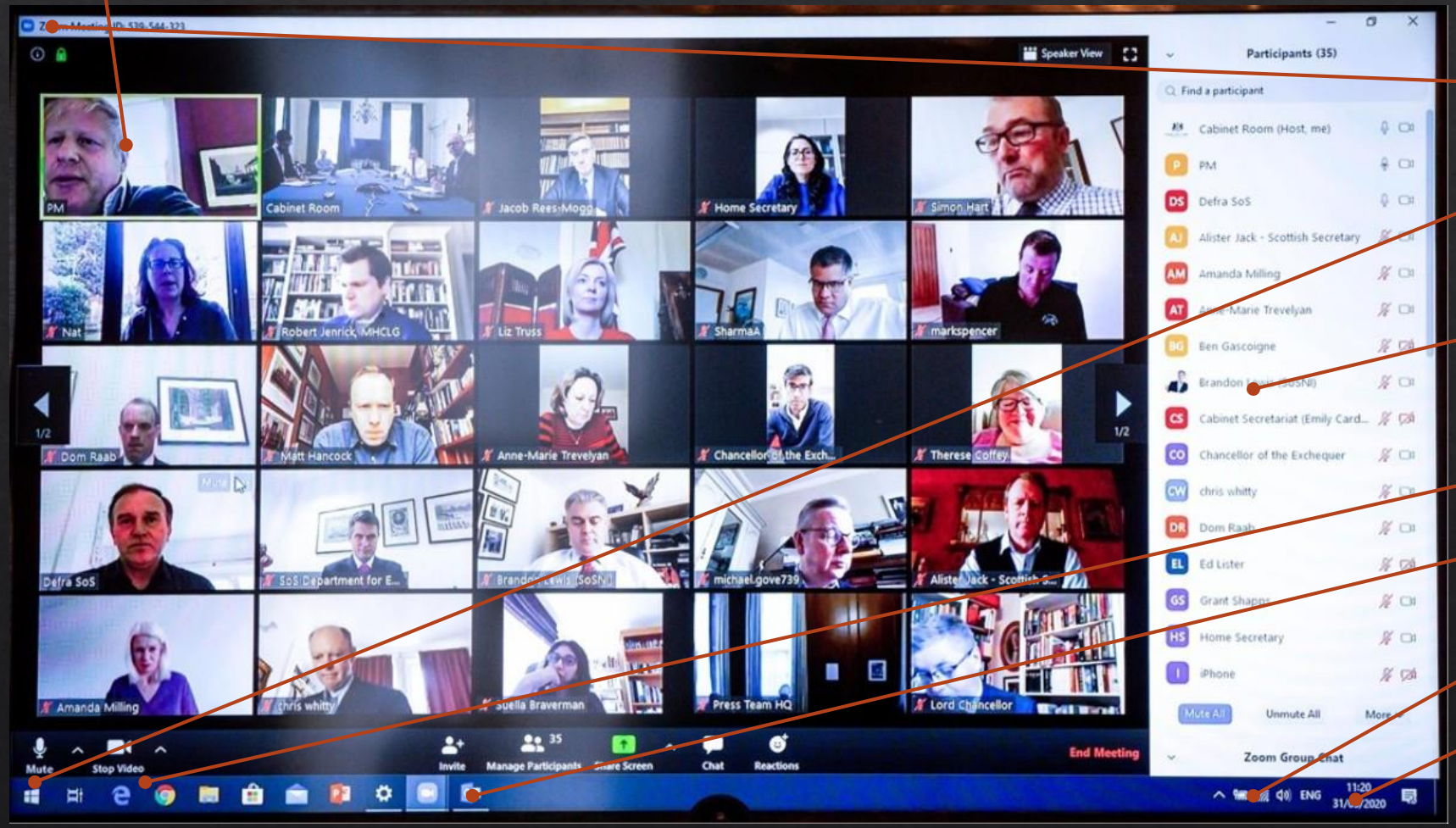
Mouse

- Wireless mice are vulnerable

Conference Calls

Chi Parla?

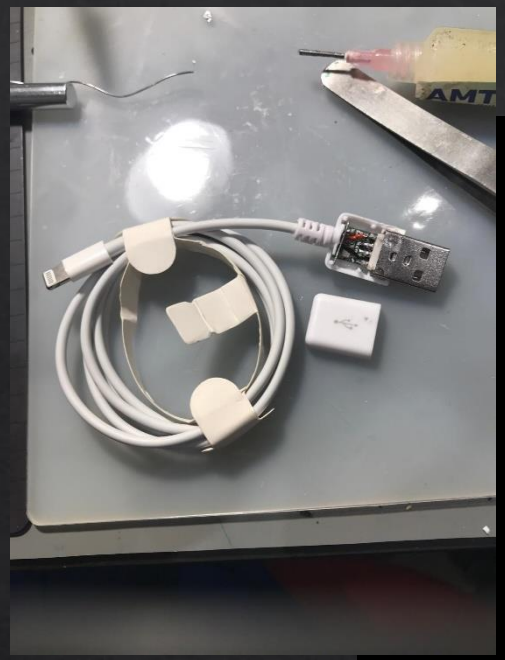
Meno EGO..please. E piu' sicurezza…



- Usa ZOOM (meeting N)
- Versione del Sistema Operativo
- Nomi "Zoom" dei partecipanti
- Browser Installati
- Client di posta
- WiFi attivo e connesso
- Orario esatto

Vi presento il PC di Boris Johnson!

Gadgets



Gadget

- **…E QUINDI?…**
  - NON fidiamoci di cio' che e' apparentemente sicuro
  - Le webcam oggi hanno anche un microfono… a buon intenditor…
  - NON e' la password della camera che conta, e' quella del sito a cui accediamo per vederla da remoto o dallo smartphone
  - Se non siamo sicuri… spegniamo quando siamo in casa!

Cybercriminal group mails malicious USB dongles to targeted companies

Trustwave

Il Computer

- **Se usiamo il computer di casa**
  - E' spesso uno strumento condiviso
  - Non sappiamo chi lo ha usato e per cosa
  - Come lo gestiamo?
  - L'azienda ha il controllo della sua sicurezza?
- **Se usiamo il computer di lavoro**
  - Come proteggiamo l'eccasso?
  - Siamo i soli utenti?
  - Cosa ci permette di fare?
- **E comunque**
  - Come ci colleghiamo all'azienda?

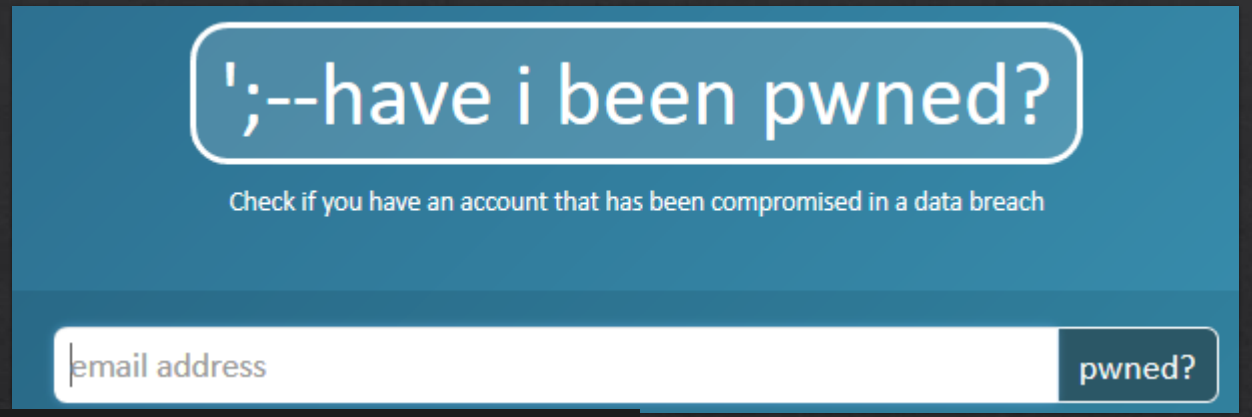
Laptop

- **…E QUINDI?…**
  - Gestione delle Password
  - Aggiornamenti software
  - L’antivirus NON e’ solo un software
  - Se possibile usate una VPN
  - Meglio una connessione via cavo

A proposito di password

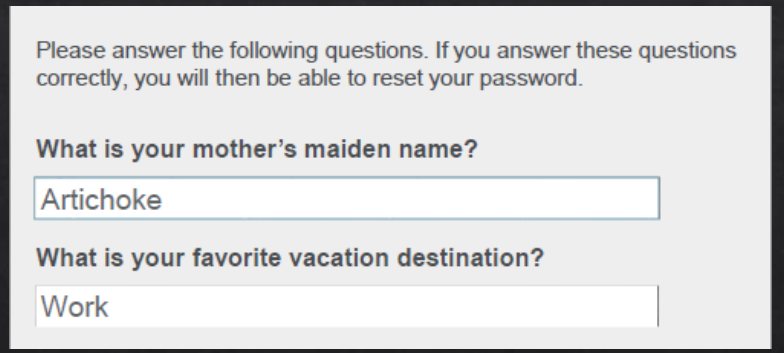
https://haveibeenpwned.com/

- **Scegliete bene le password!**
  - In questa situazione la protezione del perimetro da parte dell'azienda e' minore e quindi le password di accesso sono ancora piu importanti
- **Attenzione alle condivisioni**
  - Mai come in questo momento e' impotrante NON mescolare accessi di lavoro con quelli personali
- **Password per tutto!**
  - Ci sono password che proteggono anche le Camere WiFi e I sistemi di domotica – cambiatele e verificare che non siano troppo banali
- **2FA Please….**
  - L'autenticazione a due fattori non e' la soluzione ma aiuta moltissimo



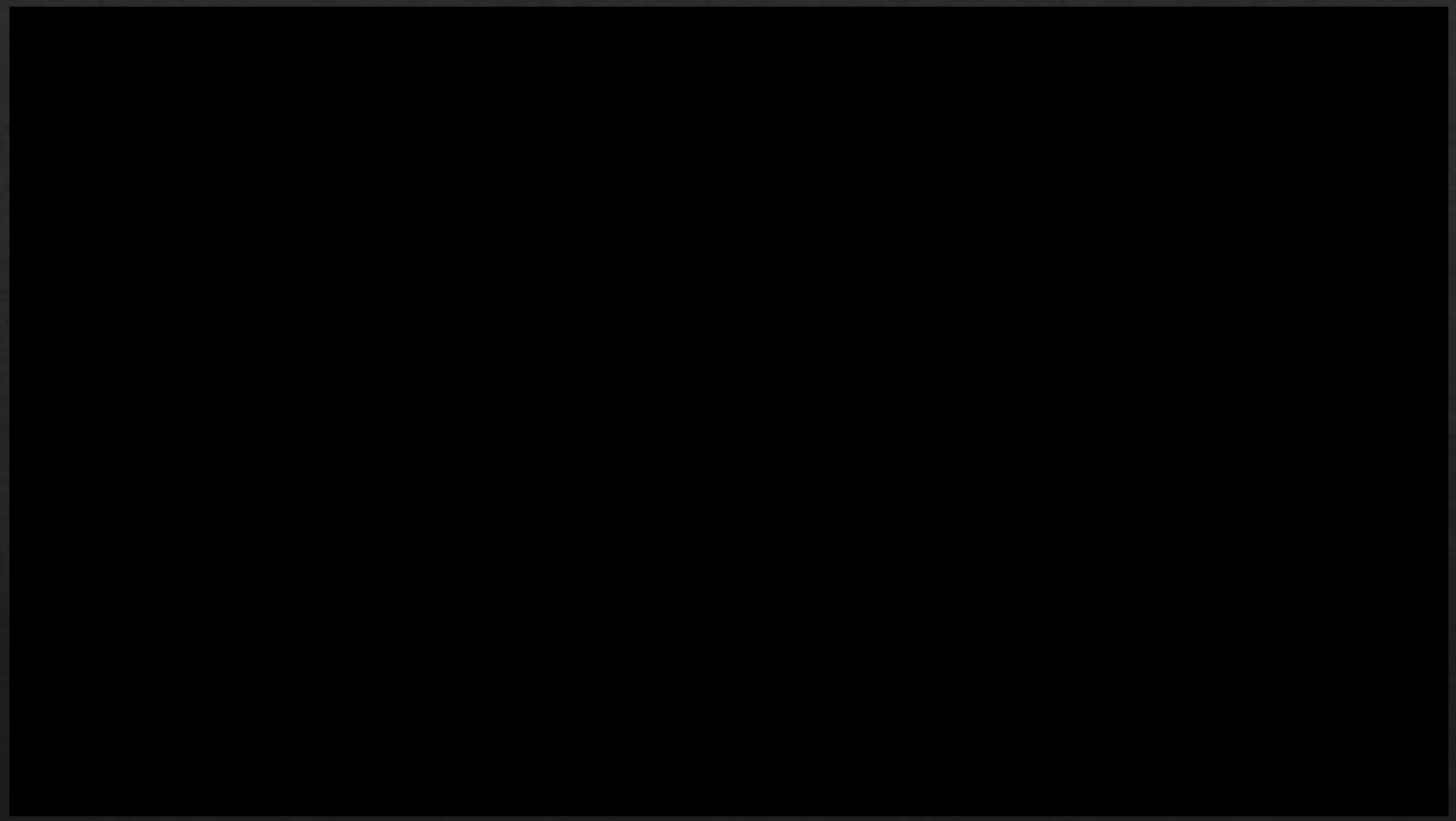

```
Session..........: hashcat
Status...........: Exhausted
Hash.Type........: MD5
Hash.Target......: hashes/hash5.txt
Time.Started.....: Mon May  6 23:28:38 2019 (1 min, 12 secs)
Time.Estimated...: Mon May  6 23:29:50 2019 (0 secs)
Guess.Mask.......: ?l?l?l?l?l?l?l?l [8]
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#2.....:   101.4 MH/s (3.72ms) @ Accel:16 Loops:8 Thr:512 Vec:1
Recovered........: 450/2069 (15.16%) Digests, 0/1 (0.00%) Salts
Recovered/Time...: CUR:0,N/A,N/A AVG:0,0,0 (Min,Hour,Day)
Progress.........: 8031810176/8031810176 (100.00%)
Rejected.........: 0/8031810176 (0.00%)
Restore.Point....: 456976/456976 (100.00%)
Candidates.#2....: wzvpfsz -> xqxqxqg

Started: Mon May  6 23:28:36 2019
Stopped: Mon May  6 23:29:51 2019
```

Dump file: 4k entries passwords
450 Passwords max 8 chars
Total cracking time: 15 minutes



Password	Cracking Time
Angel2018	Instantly
A0ngGEOS2$ch97L_	>100 years ?
Angel2018_Angel2018	>2 years ?
Angel2018_Bank	>2 years ?

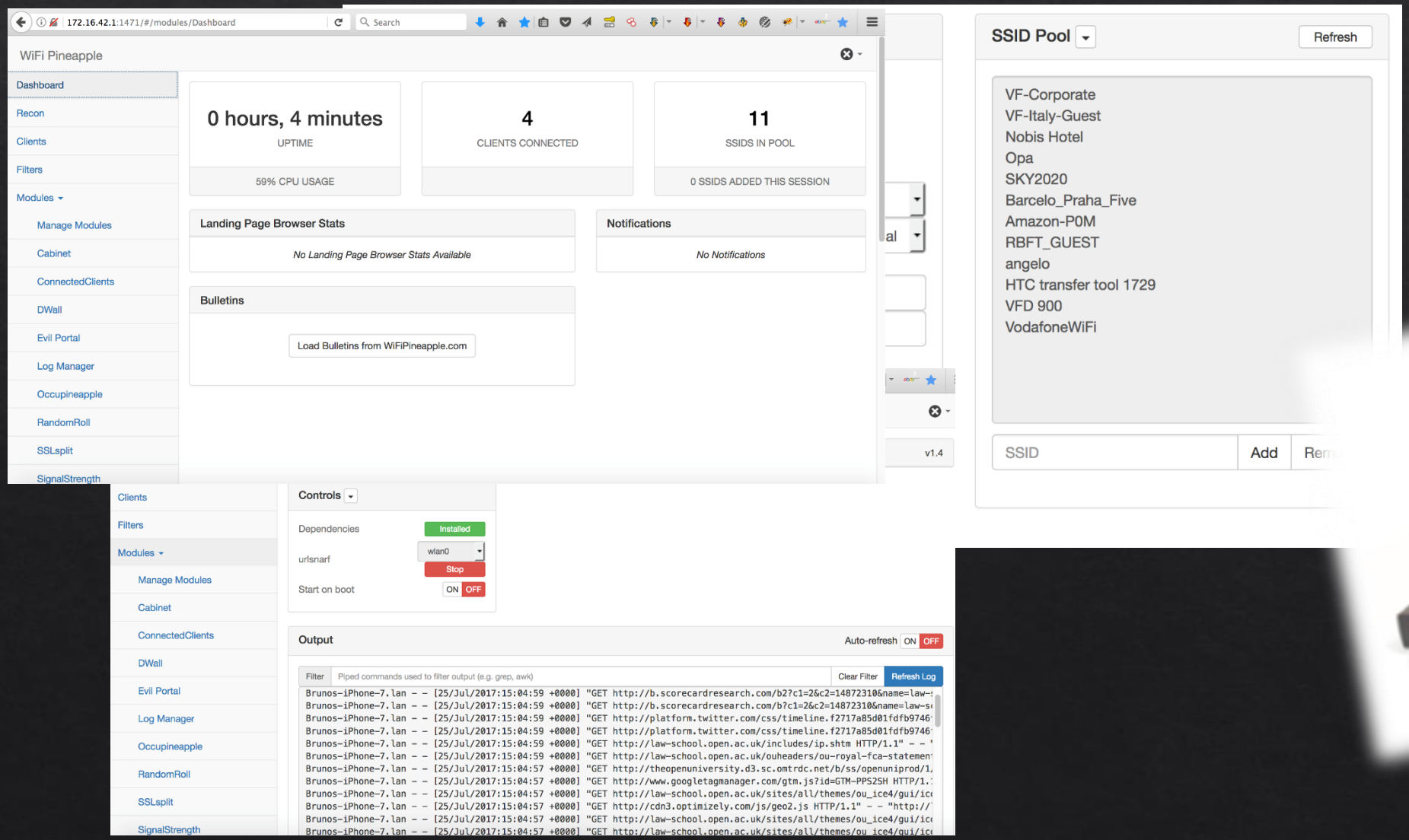
Mouse



Mouse

- **…E QUINDI?…**
- I topi hanno la coda.. Sarebbe bene ricordarlo anche adesso quando lavoriamo da casa – e non accettate topi dagli estranei
- Se il mouse deve proprio essere wireless che almeno non sia nella "lista nera"
  - https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices
  - Se e'nella lista "nera" aggiornatelo

Router/WiFi

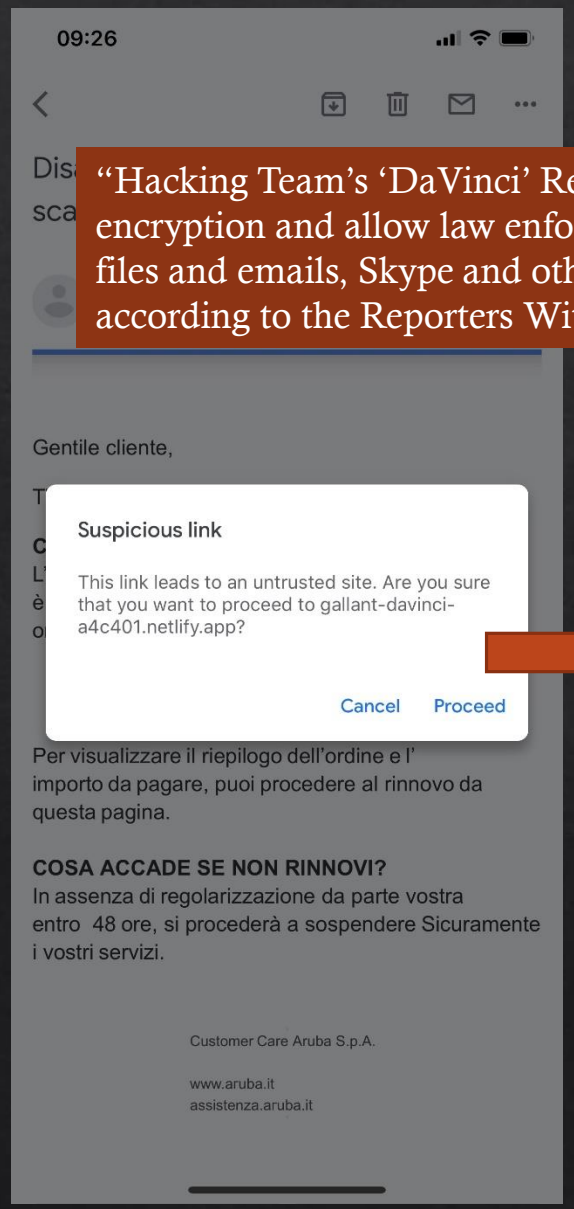

172.16.42.1:1471/#/modules/Dashboard
Search
WiFi Pineapple
Dashboard
Recon
Clients
Filters
Modules
Manage Modules
Cabinet
ConnectedClients
DWall
Evil Portal
Log Manager
Occupineapple
RandomRoll
SSLsplit
SignalStrength
0 hours, 4 minutes
UPTIME
4
CLIENTS CONNECTED
11
SSIDS IN POOL
59% CPU USAGE
0 SSIDS ADDED THIS SESSION
Landing Page Browser Stats
No Landing Page Browser Stats Available
Notifications
No Notifications
Bulletins
Load Bulletins from WiFiPineapple.com
v1.4
Clients
Filters
Modules
Manage Modules
Cabinet
ConnectedClients
DWall
Evil Portal
Log Manager
Occupineapple
RandomRoll
SSLsplit
SignalStrength
Controls
Dependencies
Installed
urlsnarf
wlan0
Stop
Start on boot
ON
OFF
Output
Auto-refresh
ON
OFF
Filter
Piped commands used to filter output (e.g. grep, awk)
Clear Filter
Refresh Log
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://b.scorecardresearch.com/b2?c1=2&c2=14872310&name=law-
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://b.scorecardresearch.com/b?c1=2&c2=14872310&name=law-s
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://platform.twitter.com/css/timeline.f2717a85d01fdfb9746
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://platform.twitter.com/css/timeline.f2717a85d01fdfb9746
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://law-school.open.ac.uk/includes/ip.shtm HTTP/1.1" - -
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:59 +0000] "GET http://law-school.open.ac.uk/ouheaders/ou-royal-fca-statemen
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://theopenuniversity.d3.sc.omtrdc.net/b/ss/openuniprod/1,
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://www.googletagmanager.com/gtm.js?id=GTM-PPS2SH HTTP/1.
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://law-school.open.ac.uk/sites/all/themes/ou_ice4/gui/ic
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://cdn3.optimizely.com/js/geo2.js HTTP/1.1" - - "http://
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://law-school.open.ac.uk/sites/all/themes/ou_ice4/gui/ic
Brunos-iPhone-7.lan - - [25/Jul/2017:15:04:57 +0000] "GET http://law-school.open.ac.uk/sites/all/themes/ou_ice4/gui/ic
SSID Pool
Refresh
VF-Corporate
VF-Italy-Guest
Nobis Hotel
Opa
SKY2020
Barcelo_Praha_Five
Amazon-P0M
RBFT_GUEST
angelo
HTC transfer tool 1729
VFD 900
VodafoneWiFi
SSID
Add

Router/WiFi

- **…E QUINDI?…**
- Il Router ha del **software** a bordo
  - Aggiornate il firmware del Router
- Il WiFi e’ protetto da password
  - Usate almeno WPA2
  - Cambiate la password di default
- Disabilitate la funzione WPS
  - Rende meno sicura la connessione di dispositivi al WiFi

https://en.wikipedia.org/wiki/Hacking_Team

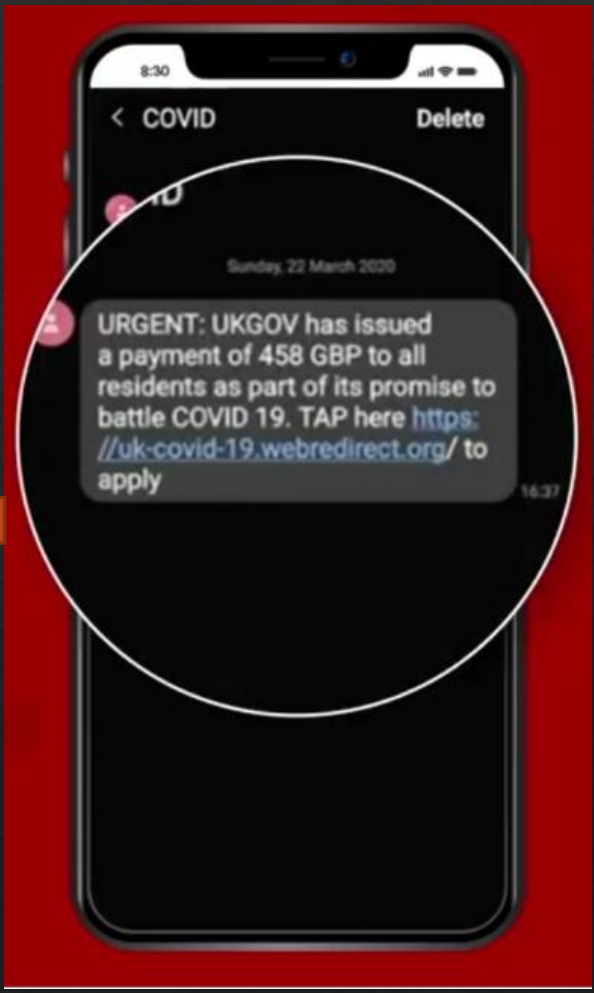
Smartphone/Tablet



"Hacking Team's 'DaVinci' Remote Control System is able to break encryption and allow law enforcement agencies to monitor encrypted files and emails, Skype and other Voice over IP or chat communication," according to the Reporters Without Borders advisory on DaVinci

gallant-davinci-a4c401.netlify.app

https://uk-covid-19.webredirect.org



Smartphone/Tablet

- **…E QUINDI?…**
- SMS
  - Attenzione agli SMS e al loro contenuto
- APP
  - Meglio un app di meno se non si e' sicuri al 100%
- TELEFONATE
  - Non date subito credito ad eventuali telefonate "strane" anche se provengono da un numero noto – nel caso RICHIAMATE
- ANTIVIRUS
  - Esistono antivirus per smartphone

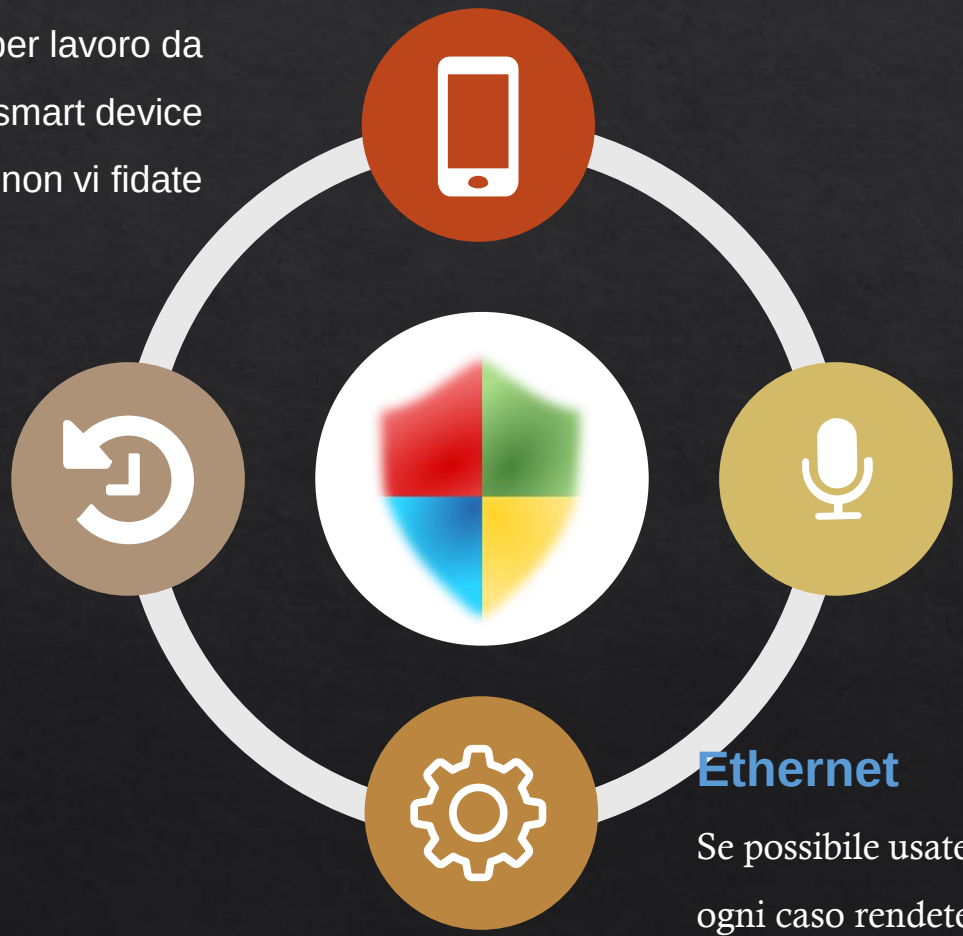
Office Checklist

DEVICES

Separate i computer e devices utilizzati per lavoro da quelli personali – Aggiornate o spegnete gli smart device di cui non vi fidate

VPN

Se vi viene fornita dall'azienda usate SEMPRE una VPN, altrimenti cercate una soluzione VPN affidabile su internet



IL ROUTER

E' la porta di accesso alla rete ed anche il punto piu debole. Mantenetelo aggiornato

Ethernet

Se possibile usate una connessione wired e in ogni caso rendete il piu possibile sicura quella WiFi (WPA2)

“

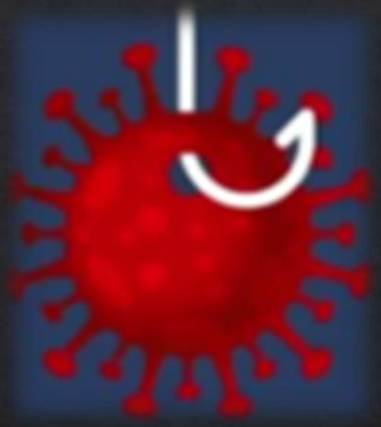
I dipendenti che lavorano da casa possono essere piu’ ***STRESSATI*** e piu’ ***DISTRATTI***

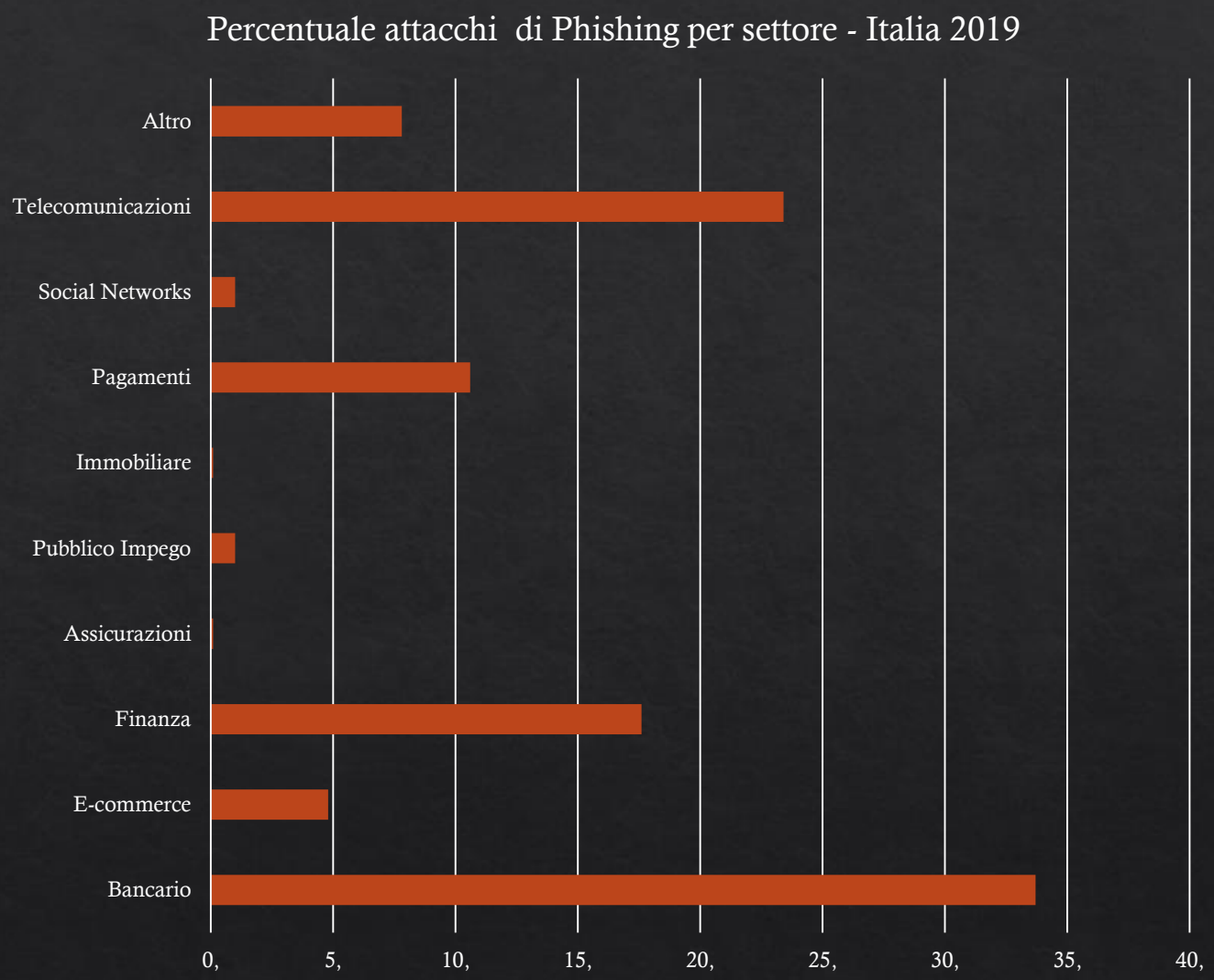
”

…e questo li rende **piu vulnerabili** che mai ad **attacchi personali**

L’ambiente non ci aiuta ma la situazione ce lo impone..

Phishing PRIMA di COVID-19





People Checklist

Attacchi in Aumento
il numero di attacchi connesso a COVID-19 e' in aumento esponenziale

Aspettiamoci di tutto
Gli attacchi possono essere SMS, APP, Telefonate, lettere, messaggi e-mail

Siamo parte del problema
ci viene chiesto di scaricare aggiornamenti, resettare password su siti fasulli, cliccare su link

Siate vigili!
Non cliccate su nessun link o scaricate alcuna applicazione senza essere sicuri – chiedete alla fonte prima – usate i VOSTRI contatti

Servizio Europeo
andate direttamente sui siti o sui portali per leggere le informazioni (WHO, siti Governativi, Istituzioni)

Seguite politiche aziendali
Verficate che l'azienda abbia protocolli certificati per la gestione del supporto tecnico e per fornire le comunicazioni su azioni da intraprendere

Mail Checklist

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

Link Utili

- Informazioni generali su COVID e Sicurezza
  - https://blog.f-secure.com/covid-19-cyber-security/
  - https://blog.reasonsecurity.com- Sull'attacco ai computer con la fake Covid Map
  - Spy-Cashnow e Concipit Website
- Testing
  - Have I been pwned? - Controllate la sicurezza della vostra mail
  - MouseJack - Controllate mouse e tastiera
- Antivirus per dispositive mobili
  - Mobile Antivirus for iOS – valutazione di piu'prodotti
  - Un Antivirus per Android – esempio
- COVID-19-CTI-League link alla lista aggiornata dei siti Blacklisted
- Un Sistema di protezione per I piu' esperti (o smanettoni) – PI-hole ->>

THANK YOU

I am a Hacker
I am a Criminal
AND
My crime is Curiosity
(The Mentor - January 8,1986)

bruno.motta@hackingcafe.com

Credits to my great Friends, Mentors and Teachers:
@lucabongiorni, FanLo, @evilsocket, @condor, @thedarktangent, @zerocool