Cybersecurity… in pratica

Come applicare i principi base della cybersecurity nella vita di tutti i giorni

Chi siamo

- Francesco Palmerio
- Ing. Informatico
- Responsabile Cybersecurity in una azienda di servizi esternalizzati per il settore bancario
- Responsabile awareness per l'associazione BITM
- francescopalmerio@me.com

- Paolo Carrara
- Ing. Telecomunicazioni
- Cybersecurity Corporate Fastweb
- Responsabile IT e materiale per l'associazione BITM
- paolo.carrara80@gmail.com

Fastweb

Fastweb offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese.

Dalla sua creazione nel 1999, l'azienda ha puntato sull'**innovazione** e sulle **infrastrutture di rete** per garantire la **massima qualità** nella fornitura di servizi a banda ultralarga.

La società fa parte del gruppo Swisscom dal settembre 2007.

L’associazione

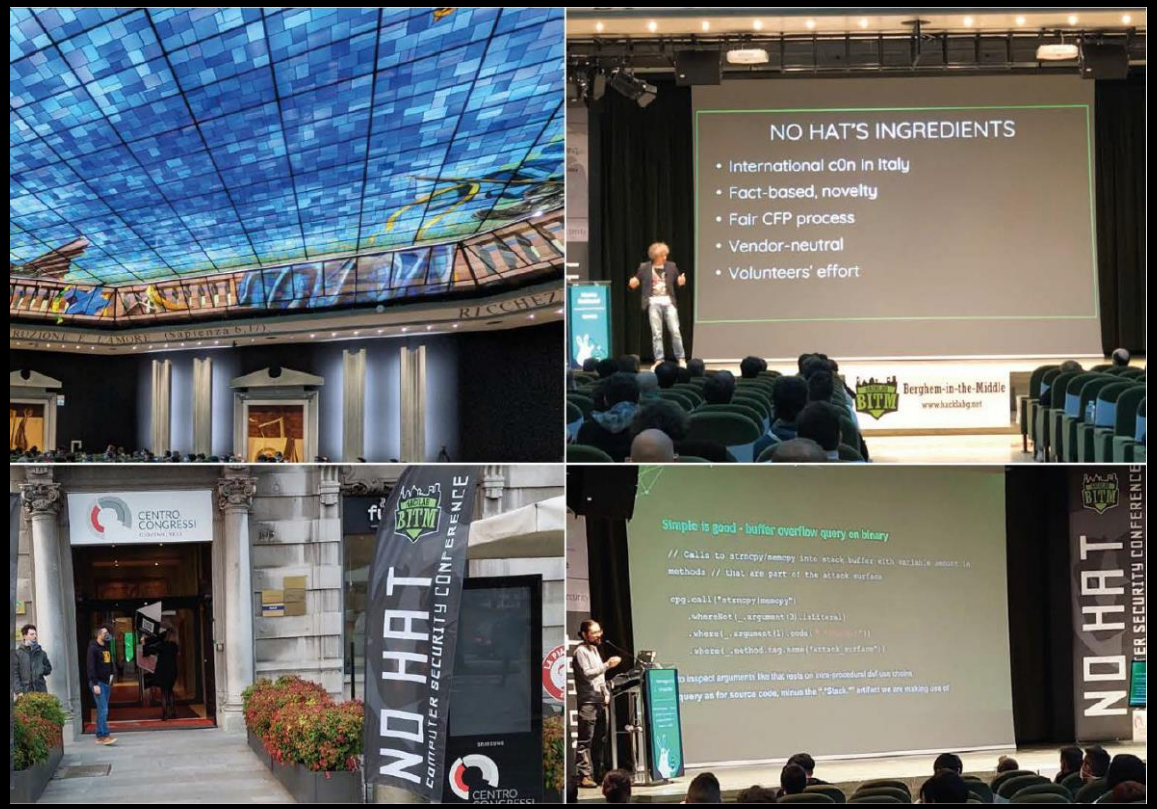
“Berghem-in-the-Middle ETS” l’**HackLab di Bergamo** è un’**Associazione senza fini di lucro** fondata nel luglio 2018 da un gruppo di appassionati e professionisti di sicurezza informatica e di informatica in generale: www.hacklabg.net

L’Associazione è animata dalla passione per tutto quello che concerne la sicurezza informatica e ha lo scopo di:

- diffondere la cultura della privacy e della sicurezza informatica
- essere punto di ritrovo per professionisti, studenti e appassionati di privacy e sicurezza
- sensibilizzare gli utenti alle tematiche della privacy e dell’anonimato

L’associazione **Berghem-in-the-Middle** organizza la conferenza annuale di sicurezza **«No Hat» (www.nohat.it).** Dopo 4 edizioni di successo, è ora riconosciuta tra le maggiori conferenze di Security a livello nazionale, e ha ottenuto rilevanza Europea grazie all’alto livello dei contenuti presentati da ricercatori e specialisti della scena internazionale.

No Hat 2022



- 9 talk con speaker internazionali
- 530 partecipanti in presenza
- 350+ visualizzazioni uniche dell'evento in streaming
- 17 sponsor
- 300+ litri di birra, 500+ caffè

www.nohat.it/2022

21 ottobre: No Hat 2023

Cosa è la cybersecurity

sicurézza informàtica

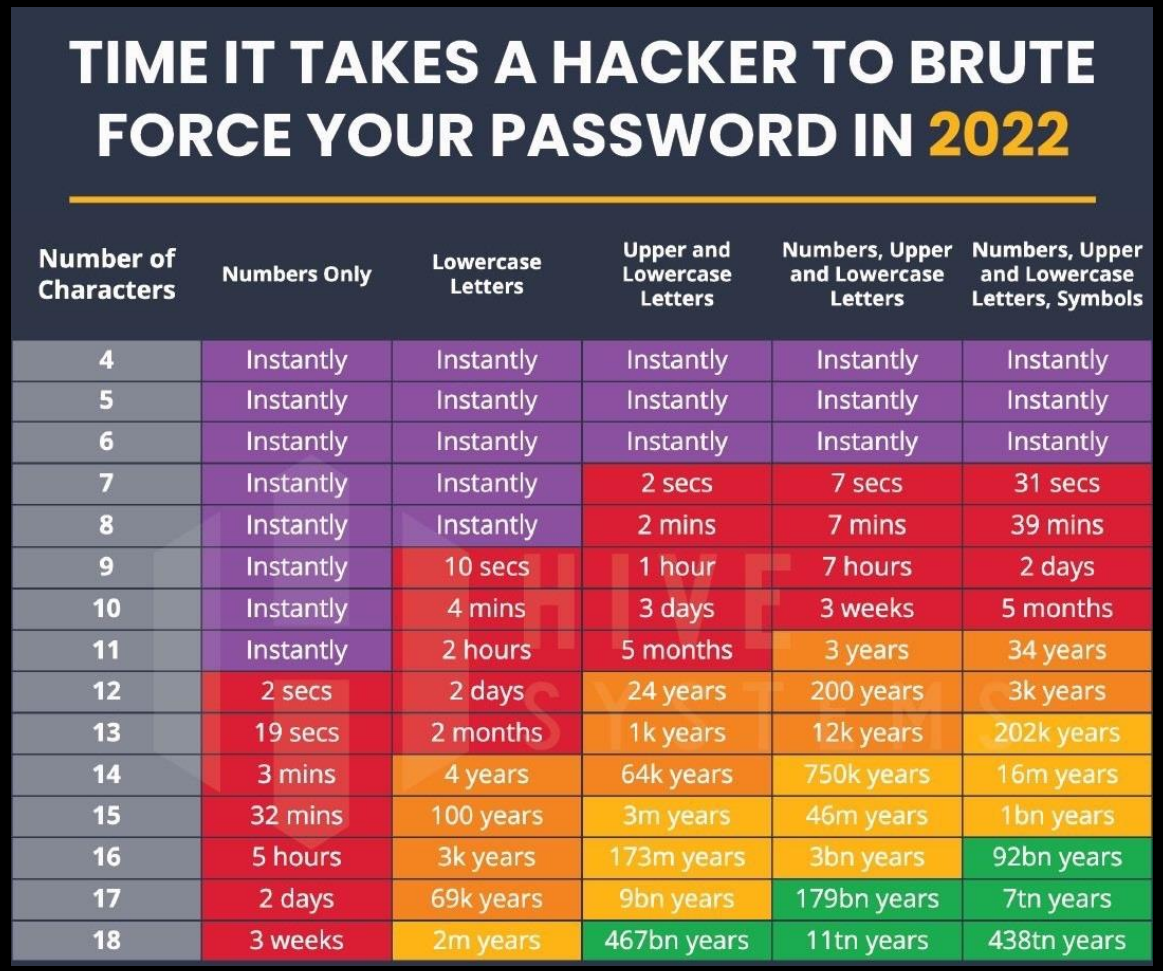
Ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. Tali tentativi di violazione possono essere contrastati sia mediante programmi sia mediante specifici strumenti hardware.

(https://www.treccani.it/enciclopedia/sicurezza-informatica)

Password e responsabilità

- La password è collegata alla login e rappresenta le tue **credenziali personali**: un modo per autenticarti inequivocabilmente sui sistemi e le applicazioni.
- Immagina che la password sia come una **chiave** per accedere al tuo armadietto. Se **duplichi la chiave** (in questo caso condividi la password), non sarai l'unico che potrà accedere all'armadietto per riporvi qualcosa, giusto? Ora, immagina che nel tuo armadietto venga ritrovato un oggetto rubato. Poiché si tratta del tuo armadietto che è sotto la tua **responsabilità**, sarai **la persona direttamente responsabile** di ciò che contiene.

Password come sceglierla?



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

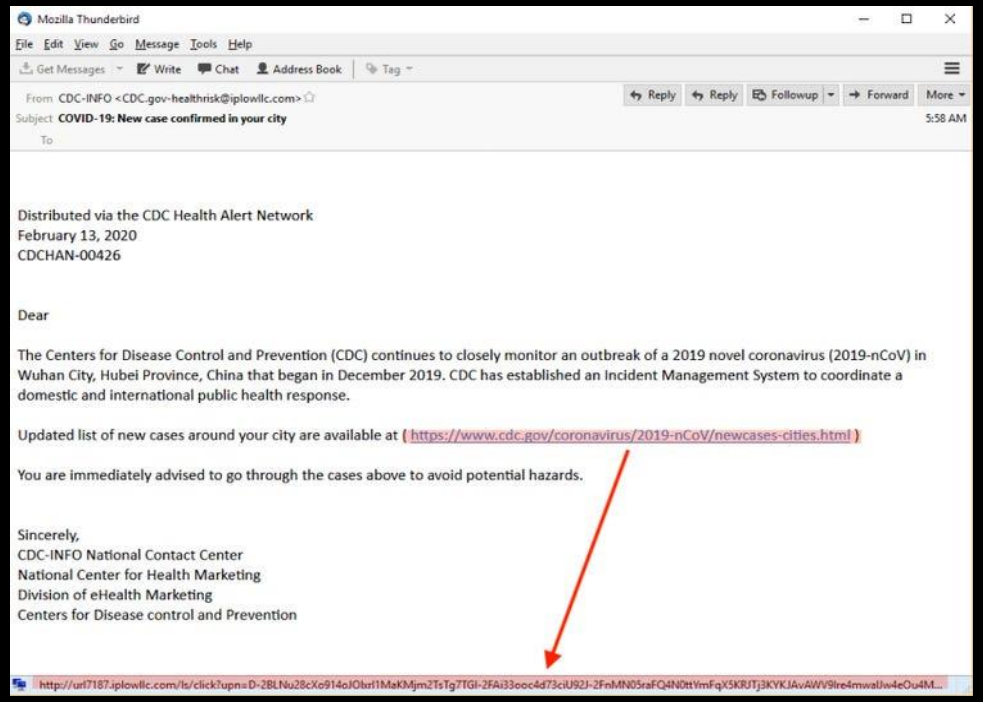
- Più la password è complessa più è difficile crackarla.
- Per sceglierne una sufficientemente **robusta** è bene comporla con **lettere maiuscole e minuscole, numeri e caratteri speciali.**
- Negli ultimi anni sta prendendo piede il termine ***passphrase*** con la quale si indica un insieme di parole oppure di stringhe alfanumeriche separate da uno spazio o da un carattere speciale.
- Utilizza sempre una **password diversa** per ogni servizio / sito web al quale ti iscrivi.
- **Aiutati con un password manager come LastPass, Keeper, 1Password, KeePass, …**

Oltre la password…
Multi Factor Authentication

- Ci sono diversi fattori di autenticazione:
  - Qualcosa che sai (es. la password)
  - Qualcosa che hai (es. un token)
  - Qualcosa che sei (es. impronte digitali)
- La combinazione di due o più di questi fattori si chiama **autenticazione multifattore**.
- Aggiunge un livello di sicurezza in più al furto delle credenziali (*rubare la password non è più sufficiente per poter accedere ad un servizio*)
- Tutti i principali servizi consentono di abilitare l'autenticazione a due fattori: **è molto importante usarla!**
- Di solito si può abilitare nella pagina di configurazione del proprio account.

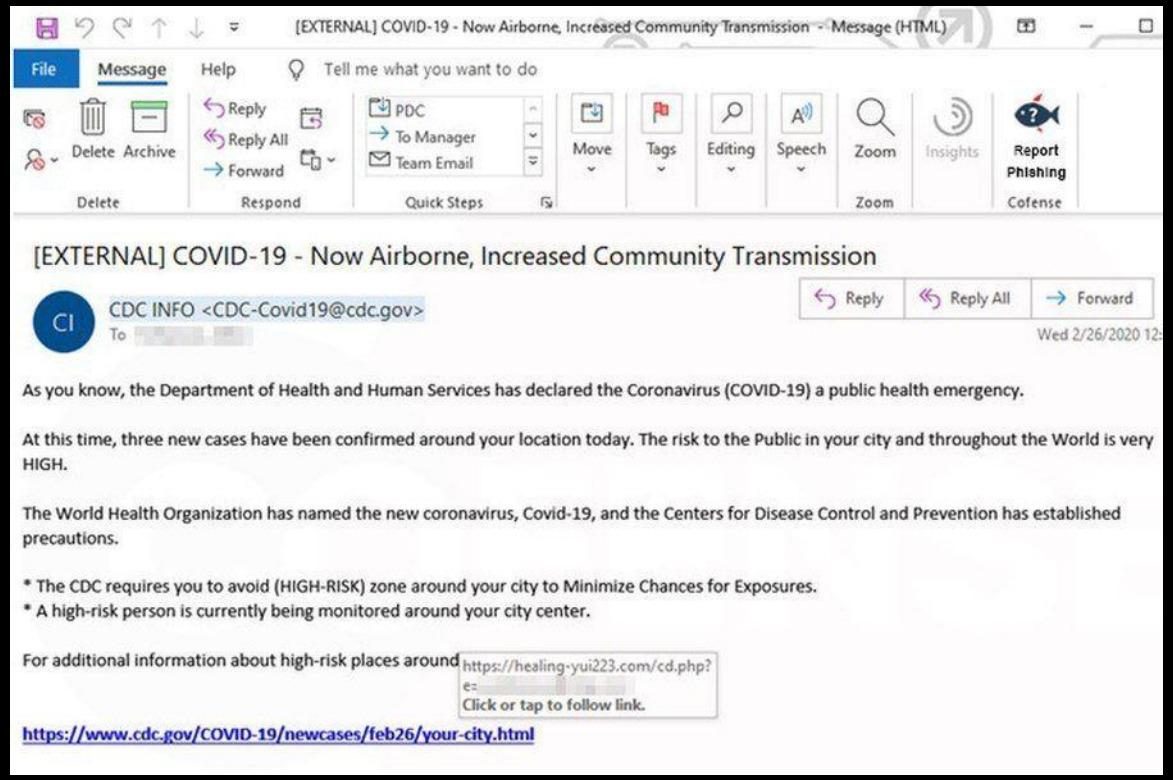
Phishing come evitarlo

- Le e-mail di phishing tentano di copiare, nel miglior modo possibile, la presentazione di un'e-mail autentica facendo anche riferimento a situazioni attuali.



1. Fai doppio click sul campo DA per visualizzare indirizzo e-mail effettivo del mittente
2. Passa il mouse sopra al link contenuto nel testo della e-mail per visualizzare la destinazione e verifica che sia coerente con il messaggio

Phishing come stanarlo

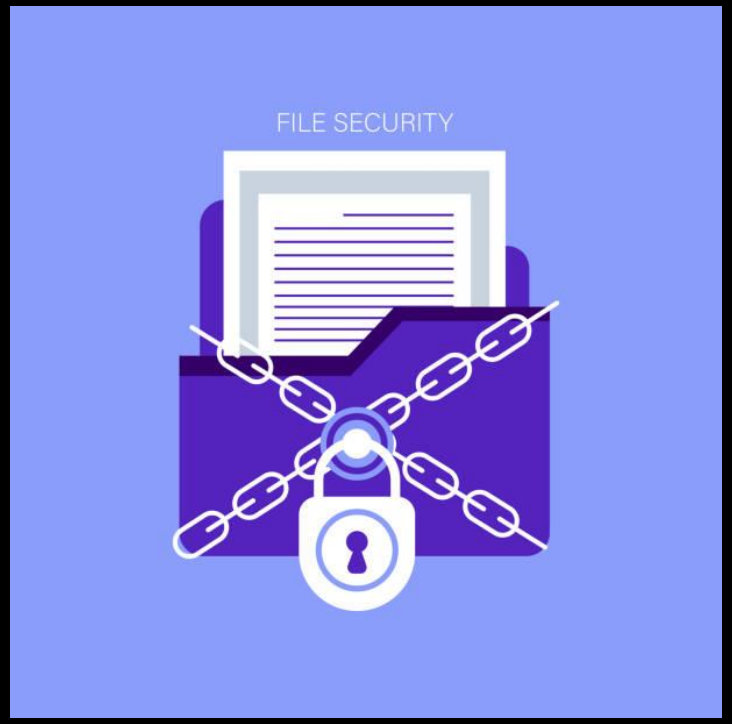


3. Presta attenzione agli elementi incoerenti: differenza tra il nome del mittente nella firma rispetto a quello nell'indirizzo e-mail; differenza tra il nome dell'azienda per la quale lavora il mittente nella firma e il nome di dominio dell'indirizzo e-mail; errori grammaticali, etc.
4. Fai una ricerca in internet

Reti Wi-Fi sono sicure?

- Le rete Wi-Fi sono sicure soltanto se l'accesso è protetto da un password piuttosto robusta e se il protocollo utilizzato per la cifratura è il WPA 2.
- Rispetto all'utilizzo di una rete Wi-Fi pubblica la rete dei provider (Fastweb, TIM, Vodafone, Wind, etc..) è sempre più sicura.
- Perché? Perché, ti proteggi da un attacco "***Man-in-the-Middle***": un hacker si inserisce tra te e l'hotspot pubblico cui sei connesso ed è in grado di intercettare tutto ciò che viene digitato, detto, ecc.
- Alcuni hotspot possono essere una "***honeypot***" utilizzati come esca per poter carpire informazioni personali.

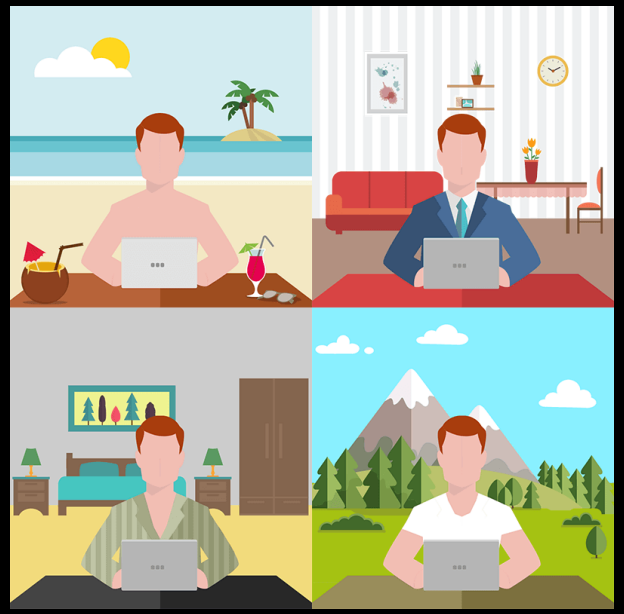
Comunicare informazioni «sensibili»



- Quando si devono inviare dei dati riservati (es. referti medici, la propria situazione finanziaria, …) via email bisogna assumere che i dati **NON siano protetti** e quindi potenzialmente visibili anche dal provider di posta.
- I dati importanti vanno **cifrati** prima di essere allegati all'email.
  - Cifrare un file è più semplice di quando si possa pensare: crea un file .zip e aggiungi una password
  - Allega il file .zip protetto all'email
- **La password NON deve essere scritta nell'email!** Usa un sms, un messaggio whatsapp o una telefonata.
  - *Il PIN del bancomat lo scrivi sul bancomat?*

Smartworking e lavoro Agile

- I benefici che derivano dallo Smart Working o lavoro Agile sono un fatto assodato per le aziende e per i lavoratori mentre non è chiaro a tutti a quali rischi legati alla cyber security ci si esponga.



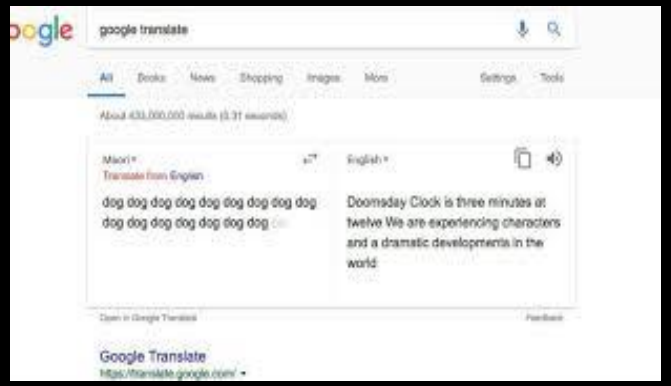
Prestiamo attenzione a:

1. Tenere sempre aggiornati il sistema operativo, l'antivirus e i software installati nel computer.
2. Salvare sul dispositivo soltanto i dati strettamente necessari soprattutto se il dispositivo non dispone di strumenti di sicurezza come cifratura del disco e/o blocco delle porte USB.
3. Fare molta attenzione ai documenti che si stampano, cercando di non lasciarli in giro e di distruggerli quando non sono più necessari.
4. Se non si lavora da casa o dall'ufficio, fare attenzione al fatto che nessuno possa leggere da lontano le informazioni che appaiono sullo schermo.

E più in generale prestare attenzione (1/2)

1. Inviti nei social network

- Accettare l'invito, sui Social network, di una persona che non ricordi di aver incontrato può essere molto pericoloso: è il primo passo di un attacco di phishing e si chiama **social engineering**.
- Il **social engineering** si riferisce a una manipolazione psicologica volta a indurre le persone a eseguire azioni o divulgare informazioni riservate, allo scopo di raccogliere dati, frodare o accedere a un sistema.



2. Tool on line gratuiti

- Quando si utilizzano servizi online gratuiti, come ad esempio di traduzione o per modificare i pdf, etc., il contenuto che inserite sarà inviato al server del provider e quindi potrebbe essere divulgato, se ce ne fosse l'intenzione, o semplicemente accessibile agli hacker.

E più in generale prestare attenzione (2/2)

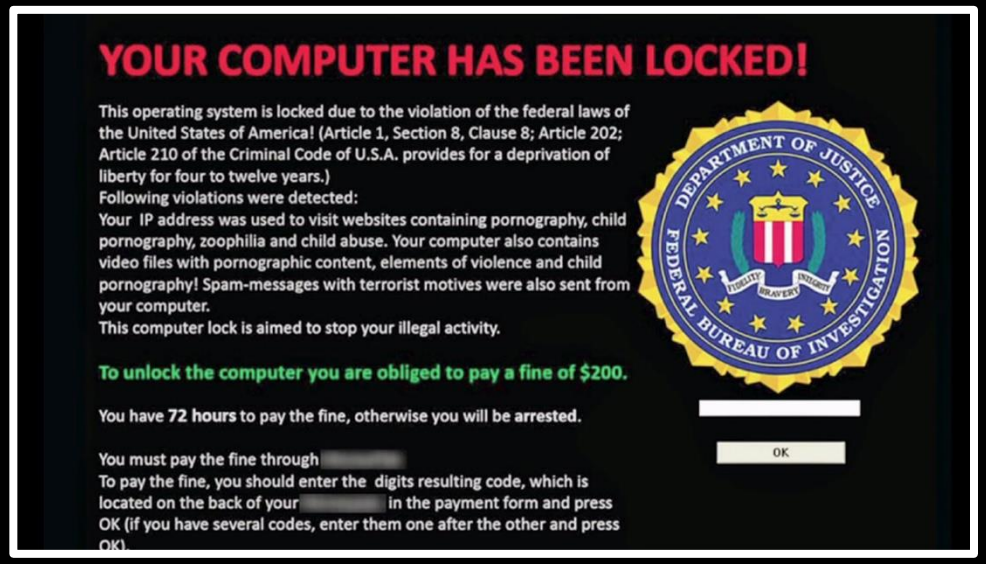
3. HTTPS cosa significa

- S sta per Sicuro in ***https://*** e tu vuoi essere al sicuro!
- È vero che ogni indirizzo inizia con http://, ma oggi la maggior parte dei siti che richiede uno scambio di informazioni utilizza il protocollo ***https*** che protegge meglio dalla fuga di dati: Questo protocollo cifra la comunicazione tra l'utente e il sito web.

4. Chiamata riservata in pubblico

- Se ricevi una chiamata riservata di lavoro mentre sei fuori ufficio o fuori casa, in un luogo affollato o sui mezzi pubblici, comunica al tuo interlocutore che lo richiamerai quando sarai in un posto isolato, anche se il chiamante fa pressione per avere subito le informazioni.

Cosa sono i ransomware? (e come difendersi)

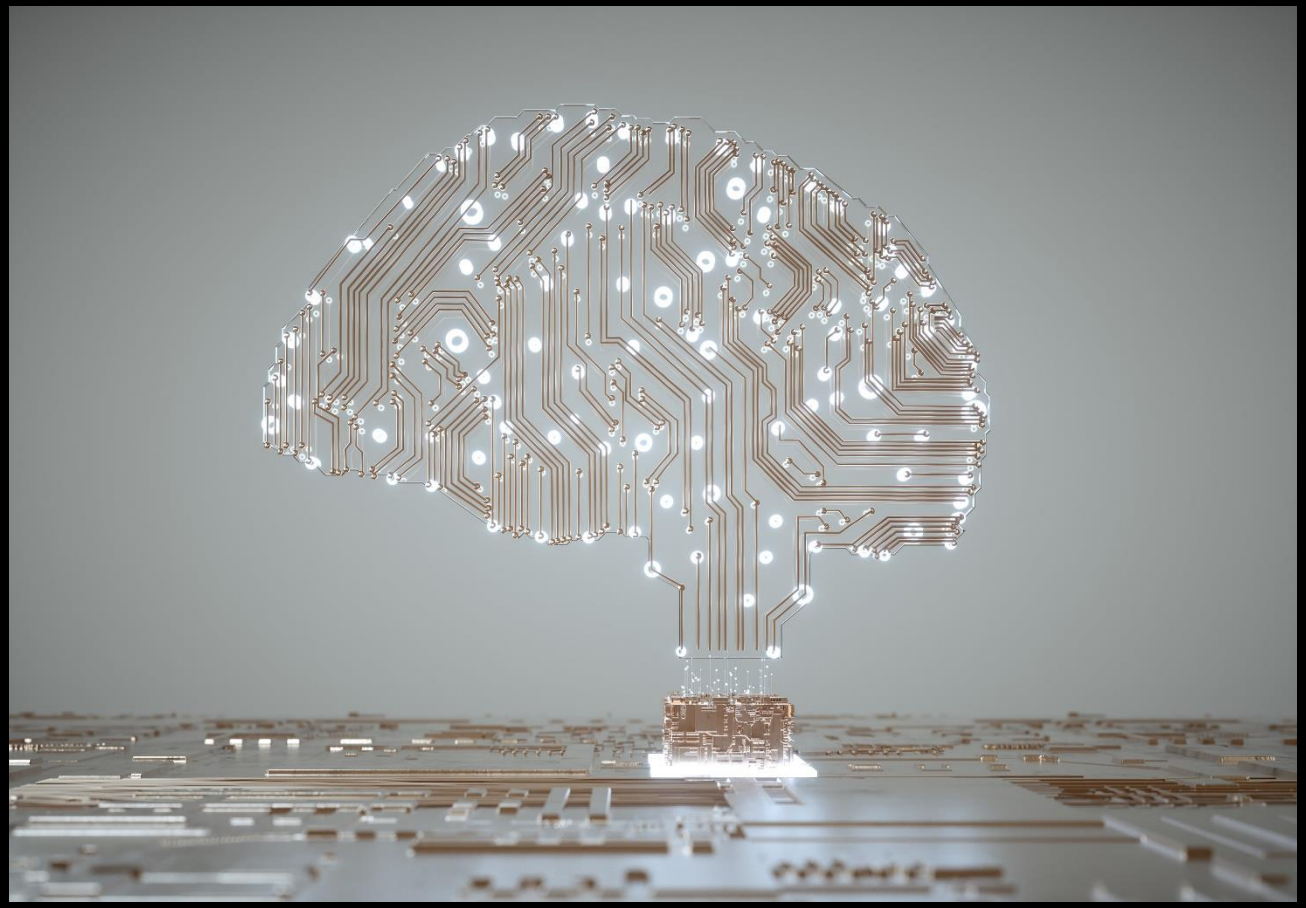


- Ransomware = software che chiede un riscatto (ransom)
- È un programma malevolo che è in grado di **cifrare** la maggior parte dei file presenti sul un computer impedendo quindi l'accesso. Per ottenere la chiave per decifrare i file viene chiesto di pagare una somma di denaro (tipicamente in criptovaluta)
- **Non sempre i criminali mantengono le promesse**… Se si paga si alimenta il mercato criminale.
- Per difendersi:
  - Occhio al phishing e ai link nelle email
  - Occhio ai programmi gratuiti scaricati da internet
  - Occhio ai programmi pirata scaricati da internet
  - Non installare nulla se non si è sicuri della provenienza del programma
- Per prevenire:
  - **Fare un backup** (tutti i giorni o le settimane) di tutti i dati importanti su un hard disk esterno non collegato al PC o su un servizio cloud

Strumenti che sarebbe meglio avere sul PC

- Antivirus per proteggerti dalle minacce più comuni (versioni a pagamento. Chiediti: quanto valgono i tuoi dati?)
- Password manager: per conservare tutte le tue password
- Programmi per cifrare documenti importanti (basta un semplice gestore di archivi .zip)
- Programmi per eseguire backup automatici
- Servizi cloud per salvare i tuoi backup (ne esistono anche con cifratura dei dati inclusa)

Lo strumento fondamentale della cybersecurity



Domande

?

Conflitto Russo-Ucraino

Agenzia per la cybersicurezza nazionale


Servizio · Allarme sicurezza

Milano, attacco hacker agli ospedali Fatebenefratelli e Sacco

L'attacco ai server dei siti di Fatebenefratelli e Sacco ha avuto conseguenze anche su altre sedi aziendali: i presidi Buzzi e Melloni e 33 sedi territoriali

2 maggio 2022

Ilsole24ore.com


MILANOTODAY

ATTUALITÀ

Attacco hacker agli ospedali milanesi, com'è la situazione

Gli aggiornamenti dopo l'attacco hacker del 1 maggio

milanotoday.it


Attacco hacker al sistema informatico degli ospedali Fatebenefratelli-Sacco: cartelle cliniche criptate e visite a rilento

di Alessandra Corica

Da domenica 1° maggio i sistemi sono in tilt. "Limitati" gli accessi al pronto soccorso e ai punti prelievi di Sacco, Fatebene, Buzzi e Macedonio Melloni. Medici e infermieri costretti a registrare a mano i dati dei pazienti

02 MAGGIO 2022 AGGIORNATO ALLE 17:03 · 2 MINUTI DI LETTURA

repubblica.it

- Il conflitto Russo – Ucraino si riflette all'interno del cyberspazio con attacchi giornalieri da entrambe le parti.
- Le aziende, per evitare impatti collaterali, devono giornalmente aggiornare i propri sistemi di protezioni informatica, attività che richiede un grande impegno da parte dei team tecnici.
- Perché? Perché purtroppo gli impatti collaterali accadono..

Conflitto Russo-Ucraino: caso Kaspersky

Si apre, o meglio si riapre il caso dell'antivirus russo Kaspersky, dopo l'intervista del *Corriere* a Franco Gabrielli. Il sottosegretario alla Presidenza del Consiglio con delega alla Sicurezza nazionale, rispondendo a Giovanni Bianconi, dice: «Dobbiamo liberarci da una dipendenza dalla tecnologia russa. Per esempio quella dei sistemi antivirus prodotti dei russi e utilizzati dalle nostre pubbliche amministrazioni, per evitare che da strumento di protezione possano diventare strumento di attacco». Gabrielli non fa nomi ma il riferimento a **Kaspersky** è chiaro. Le soluzioni antivirus di Kaspersky

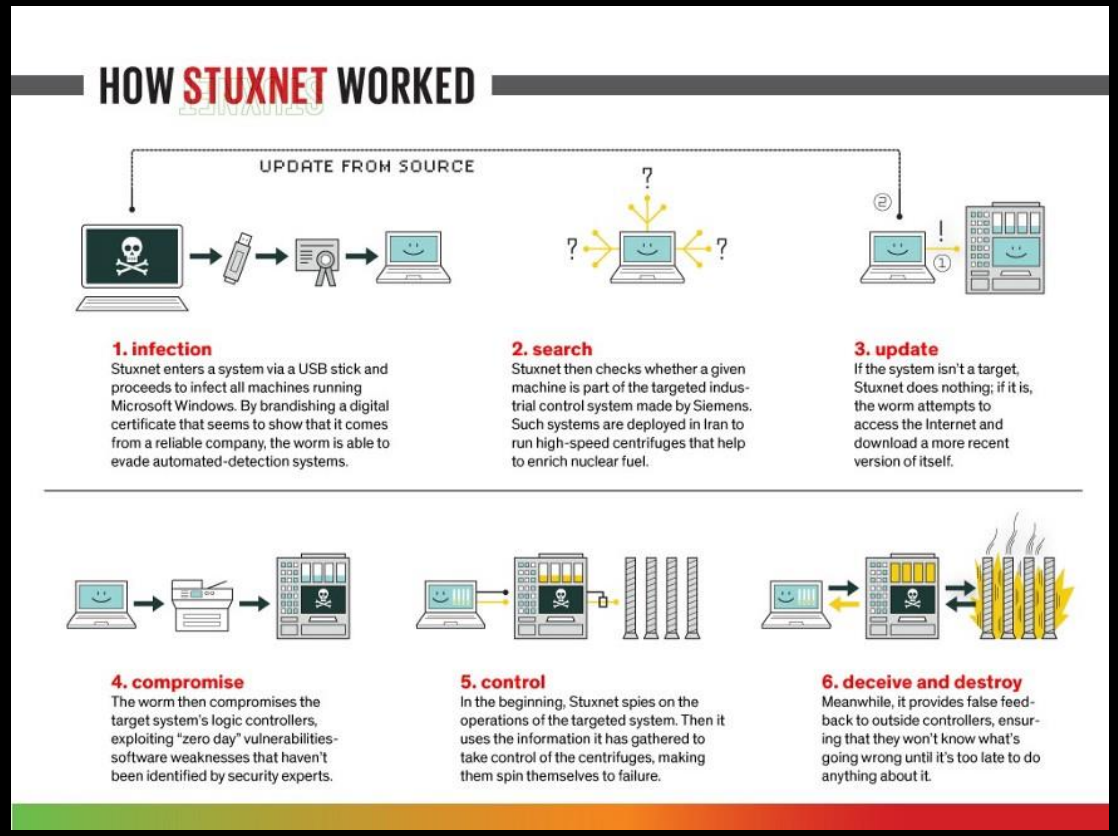
Corriere.it

La **FCC** (Federal Communications Commission) degli Stati Uniti ha inserito **Kasperky** nella "Covered List", ovvero l'elenco delle aziende che rappresentano un **pericolo per la sicurezza nazionale**. La software house russa ha dichiarato che la decisione è esclusivamente di natura politica. Anche il governo italiano ha chiesto alle amministrazioni pubbliche di acquistare un'altra soluzione di sicurezza.

Punto Informatico

- Kaspersky è un software antivirus che unisce una ottima qualità di funzionamento ad un costo molto competitivo.
- A causa di questo bando, e del bando da parte della FCC americana, Kaspersky deve essere rimosso in favore di altri strumenti.
- E un'azienda è praticamente costretta a chiudere i battenti..

BONUS: La storia dietro Stuxnet



- Stuxnet è da tutti riconosciuto come il malware che ha fatto conoscere al mondo la guerra informatica, scoperto per la prima volta nel 2010.
- All'incirca ogni 30 giorni, Stuxnet cambia la frequenza di uscita dei convertitori per brevi periodi di 15-50 minuti rispettivamente a 1410 Hz o 2 Hz, quindi torna a 1064 Hz (una frequenza normale).
- Stuxnet ha danneggiato circa **1000 centrifughe nell'impianto di arricchimento del combustibile di uranio a Natanz** ha rallentato di un anno il programma nucleare iraniano.