Internet ai tempi del COVID-19

Come sono cambiati i nostri modi di comunicare, di interagire e di lavorare ai tempi del COVID-19

Chi siamo

- Francesco Palmerio
- Ing. Informatico
- Responsabile Information Security in un gruppo assicurativo
- francescopalmerio@gmail.com

- Paolo Perotti
- Perito in elettronica industriale
- Progettista Elettrico/Elettronico libero professionista
- paoloperottiperind@gmail.com

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.

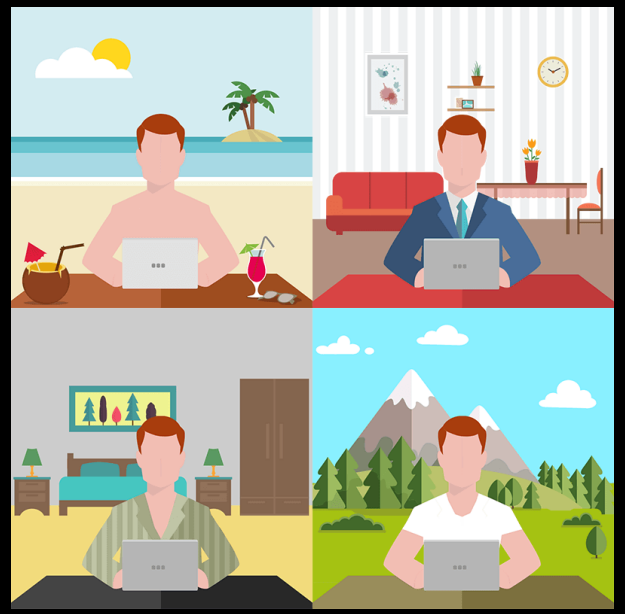
L’Associazione è animata dalla passione per tutto quello che concerne la sicurezza informatica e ha lo scopo di:

- diffondere la cultura della privacy e della sicurezza informatica
- 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»**. L'evento unisce specialisti, professionisti e appassionati di tutto il mondo operanti nell'ampio mondo della sicurezza informatica e della privacy.

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.



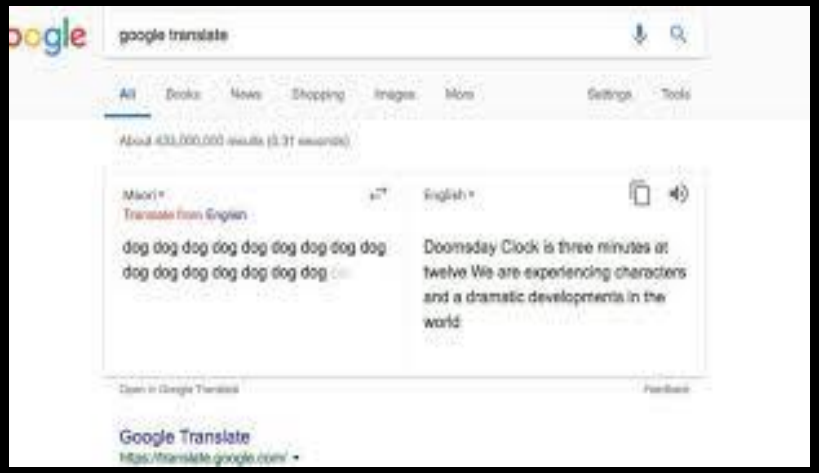
Prestiamo attenzione a:

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. 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

3. HTTPS cosa significa

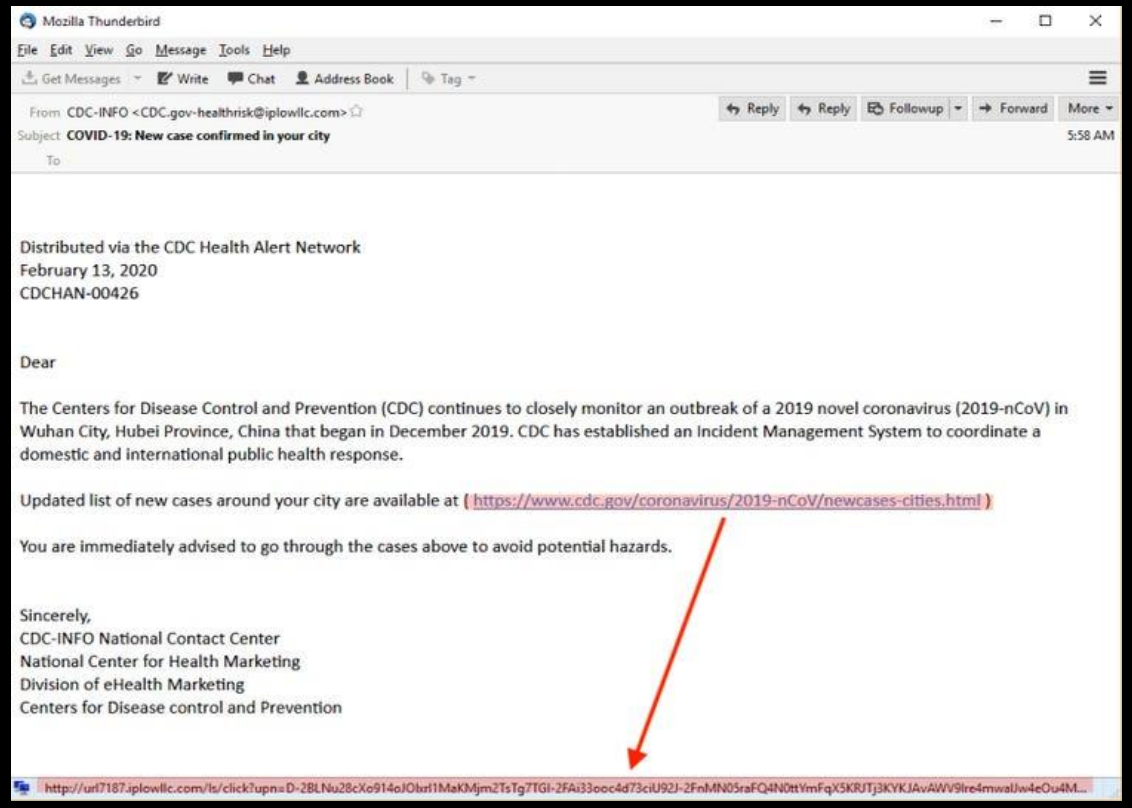
- S sta per Sicuro in ***https://*** e tu vuoi essere al sicuro!
- È vero che ogni indirizzo inizia con http://, ma oggi la maggior parte dei siti che richiede uno scambio di informazioni utilizza il protocollo ***https*** che protegge meglio dalla fuga di dati: Questo protocollo cifra la comunicazione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

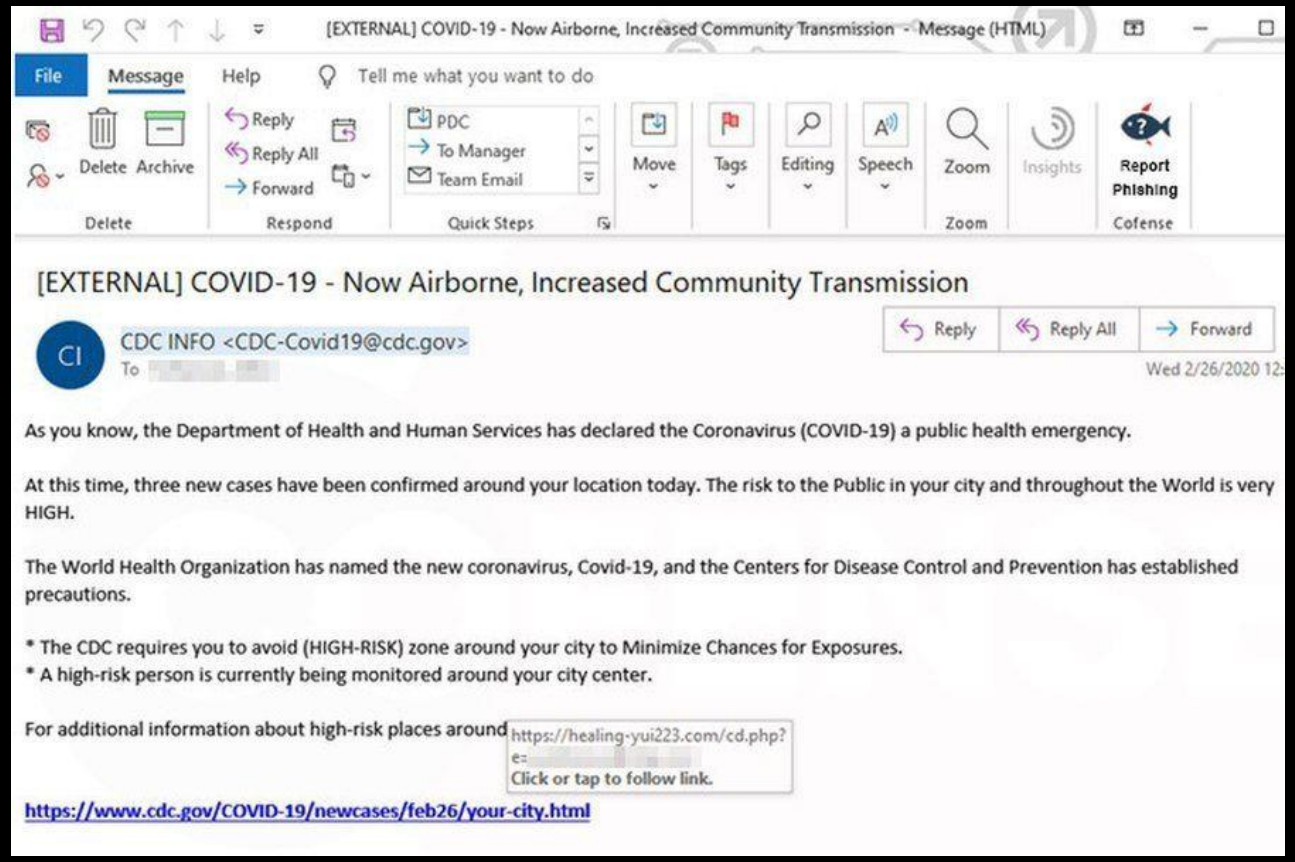
Phishing come evitarlo

- 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 email effettivo del mittente
2. Passa il mouse sopra al link contenuto nel testo della email 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

Password come sceglierla?

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt 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.

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.

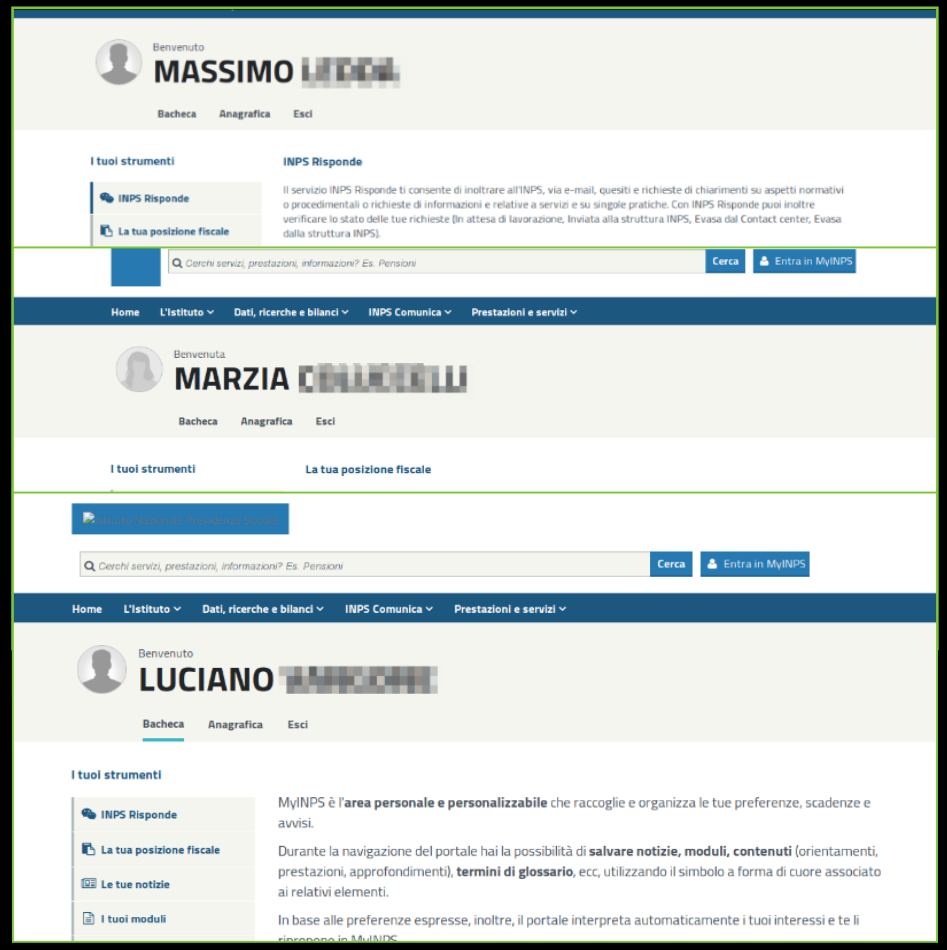
Reti Wi-Fi sono sicure?

- 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 (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.

Fake news cosa sono e come difendersi

- La produzione di disinformazione è ormai una fatto globale. Coinvolge decine di attori ed addirittura governi che usano metodi sofisticati per mascherare le loro identità e le loro posizioni.
- Dietro le fake news possono nascondersi sia organizzazioni che singoli utenti. Agiscono per interessi politici e/o economici, magari dietro commessa. Possono essere messi in campo centinaia di bot e falsi account.
- **Debunker**, in italiano **demistificatore** è una persona che con l'analisi, la verifica dei fatti e delle fonti: prova o smaschera ciarlatanerie, bufale, affermazioni o notizie false, esagerate, antiscientifiche, dubbie o tendenziose.

Caso INPS – cosa è successo?



- Pronti via, dalle 0:00 del 1 aprile era possibile collegarsi al sito dell'INPS ed inserire la propria richiesta per avere 600€.
- Dopo pochi minuti il sito è diventato indisponibile, non ha retto il numero di richieste.
- Per tentare di gestire il numero di richieste è stata attivata la funzione di *cache* (invece di ricreare la pagina ogni volta, viene creata e poi messa in memoria) ma in maniera scorretta!
- Risultato: chi accedeva visualizzava le informazioni relative ad altri individui.

Caso INPS – tutta colpa degli hacker?

- Il presidente INPS ha dichiarato che è stata colpa di un attacco hacker, ecco come risponde uno dei più famosi gruppi hacker, in Italia.
- In questa situazione sono stati commessi almeno **3 errori gravi**:
  1. Non è stato dato un **tempo sufficiente** a chi gestisce il sito per prepararsi al boom di richieste.
  2. La **funzione di caching** è stata configurata in maniera molto superficiale.
  3. **Dare la colpa** a qualcun altro è esattamente una cosa da non fare durante una crisi, soprattutto se quel qualcun altro è totalmente estraneo alla faccenda!

Domande

?