



Frodi informatiche: cosa sono e come proteggerci

Rischi digitali: quali sono e come proteggere noi e i nostri figli.
Giovani Ambasciatori per la cittadinanza digitale.

11.04.2022



PERCHE' LA CYBER SECURITY?

“La grande opportunità offerta dalla tecnologia comporta un'enorme responsabilità per comprenderla e trarne vantaggio, nel modo giusto”

Luciano Floridi

Professore di Filosofia ed Etica delle Informazioni Università di Oxford



Grazie all'evoluzione tecnologica, la società sta affrontando un **cambiamento radicale** ricco di potenzialità..

La società *tradizionale*...



Identità fisica



Oggetti fisici



Interazione di persona



Lavoro presso i locali aziendali



...è sempre più una società *digitale*



Identità digitale

Segue approfondimento



Dati e asset virtuali



Interazione tramite social



Smart working

che porta con se anche **rischi anche dovuti al fattore umano**



..ma anche pericoli, spinti dalla digitalizzazione ed emergenza sanitaria..

Principali driver di crescita



Significativo **incremento della rilevanza dei canali digitali** per le interazioni con la clientela e i **servizi pubblici e privati**



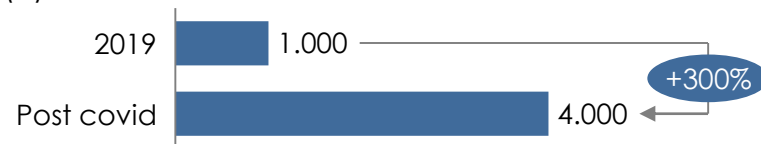
Cambio del modello operativo dovuto all'emergenza Covid, con ricorso massivo allo "smart working", estensione dei processi digitalizzati ed incremento delle interazioni digitali con le terze parti



Attacchi Cyber globali⁴

Frodi online globali

Segnalazioni giornaliere attacchi cyber all'FBI¹ (#)



~8,3k

Numero attacchi cyber gravi con danni significativi² dal 2017 al 2020 (~400M\$ per singolo attacco)

206B\$

Perdite per frodi stimate su pagamenti online a livello globale tra il 2021 e il 2025³



..Il **90%**¹ degli incidenti cyber è innescato dal **fattore umano** a causa di comportamenti inadeguati...

Il **90%**¹ di tutti gli incidenti di sicurezza deriva da una qualche forma di **errore umano**...

Click su link malevoli e cessione delle tue credenziali

Utilizzo delle medesime credenziali sui social network e mail (es. registrarsi a siti web o social network)

Navigazione su **siti web malevoli e connessione a reti poco sicure**

Gestione scorretta dei **dispositivi** (e.g. smarrimento, compromissione,...) e **disattenzioni durante la condivisione** di dati e informazioni

...con **potenziali impatti significativi**



Impatti **economici diretti**



Impatti **reputazionali**

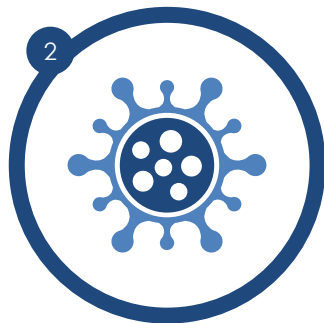


.. ci sono elementi che hanno favorito l'**aumento delle frodi**



Digitalizzazione

incremento superficie di attacco a causa dell'estensione e maggiore utilizzo dei canali digitali da parte dei cittadini



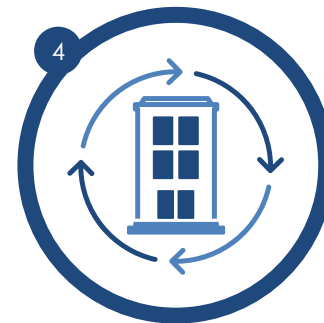
Covid-19

sfruttamento del contesto generato dall'emergenza per creare nuove "esche"



Disponibilità strumenti

facilità nel reperire strumenti gratuiti sul web per mettere in atto le frodi



Debolezze di sistema

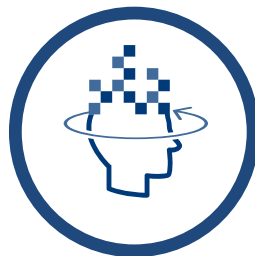
presenza di vulnerabilità fuori dal controllo delle istituzioni



Per questo è importante imparare ad avere maggiore
consapevolezza e responsabilità...



Singolo individuo



Identità Digitale



Proteggere i propri dati e asset virtuali (es. non utilizzare stesse credenziali su siti diversi) e gestire le proprie relazioni digitali in sicurezza (es. Social Media)



Diventa fondamentale **proteggere le informazioni di accesso** alla nostra identità digitale da **hacker** e **cyber criminali**.



I cyber criminali utilizzano varie tecniche, talvolta anche banali, per scoprire le nostre password

Segue approfondimento



Utilizzano l'ingegneria sociale

utilizzano tecniche di phishing, smishing, spoofing per fingersi persone / enti affidabili ed ingannarci ad inserirle su un sito falso



Indovinano le password

utilizzano informazioni personali come nome o data di nascita



Utilizzano il "shoulder surfing"

ci osservano di nascosto mentre le digitiamo e le registrano



Scoprono dove le salviamo

trovano un foglietto con le nostre password o le recuperano dalle note del nostro smartphone



Utilizzano attacchi di tipo "Brute Force"

utilizzano programmi che provano un gran numero di password in poco tempo finché non trovano quella giusta



Intercettano le password

intercettano i dati trasmessi su una rete, spesso se pubblica e poco protetta



Installano un malware

utilizzano dei programmi malevoli ad esempio per registrare ciò che viene digitato su tastiera



Compromettono un database

attaccano i sistemi contenenti dati personali, come le password, e le acquisiscono

Segue approfondimento

La maggior parte degli inganni avviene tramite **phishing**



Phishing

Truffa effettuata su Internet attraverso la quale **un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali**, dati finanziari o codici di accesso, **fingendosi un ente affidabile** in una comunicazione digitale



E-mail phishing

Invio di una **e-mail** per fingersi un ente / persona affidabile



Smishing

Invio di un **SMS** per fingersi un ente / persona affidabile



Vishing

Telefonata per fingersi un ente / persona affidabile

Come proteggersi

- **Non fornire mai dati personali** (username, password, numeri di carta, ecc.) via **email**, **sms**, **WhatsApp** o **telefonata**
- Fai attenzione che **l'SMS spesso si colloca nella chat legittima della banca**
- Prenditi il tuo tempo prima di rispondere ad una comunicazione e **controlla attentamente che l'indirizzo del mittente sia quello legittimo**
- **Non cliccare sui link** contenuti nelle **mail** o negli **SMS**

I frodatori utilizzano varie tecniche combinate (es. Swap ALIAS, Spoofing) **per fingersi entità / persone affidabili** e far "abboccare" le vittime



Alcuni **semplici consigli** per proteggersi dalle e-mail di phishing



Controlla attentamente l'indirizzo mittente per esteso **ed il dominio di provenienza**

Adotta tutti gli accorgimenti anche se il dominio è corretto (es. @intesasanpaolo.com)



Diffida delle e-mail di mittenti sconosciuti che ti chiedono di cliccare un link e/o di eseguire azioni con urgenza



Posiziona il cursore del mouse sui link per vedere l'indirizzo esteso



Non cliccare su eventuali allegati se non sei sicuro

Gli allegati potrebbero anche contenere malware che infettano il tuo dispositivo



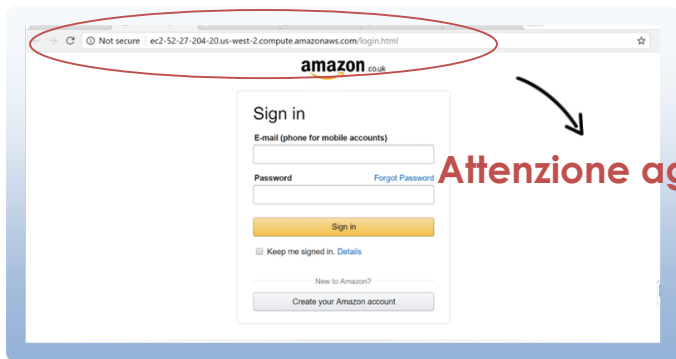
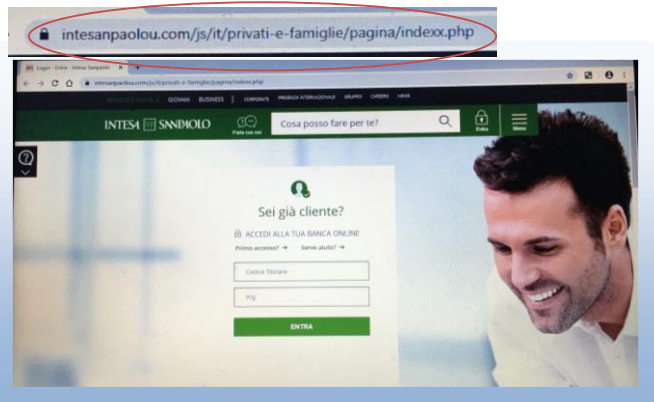
Eventuali **errori grammaticali** sono sinonimo di phishing, come la **mancaanza di firma e logo**



Applica queste semplici regole anche su smartphone e tablet

Ricordati di segnalare le e-mail sospette con il bottone outlook

Cliccando sui link di **siti falsi** vengono carpite le credenziali o installati **malware**



Attenzione agli URL!

Come proteggersi

- **Non installare mai software** i cui provenienza non è sicura **e scaricali solo da store ufficiali**
- Prenditi il tuo tempo prima di rispondere ad una comunicazione e **controlla attentamente che l'indirizzo del mittente sia quello legittimo**
- Quando sei su un **sito web**, controlla sempre che ci sia **l'icona del lucchetto** a fianco all'URL
- **Non cliccare sui link** contenuti nelle **mail** o negli **SMS**



Facciamo la nostra parte!



Sono sempre **più numerose le famiglie italiane** che, accedendo tramite computer, tablet e smartphone, scelgono i canali digitali

Cresce l'impegno delle Istituzioni e del settore bancario, finanziario per la sicurezza informatica, per la **prevenzione e il contrasto degli attacchi** e per la **protezione dei clienti** dalle frodi online.

Obiettivo della campagna è **aumentare la consapevolezza e sensibilizzare i clienti e i cittadini** ad un uso informato e sicuro degli strumenti e dei canali digitali, per non cadere nelle trappole di quanti sfruttano la tecnologia e fanno leva sulle vulnerabilità del fattore umano.

Protagonista della campagna, che durerà fino alla fine dell'anno, è la famiglia "Navigati": grazie all'informazione anche il web diventa un **luogo familiare** in cui si può **navigare in sicurezza**.





Sei semplici regole ci permettono di proteggere la nostra password



Utilizzare password diverse	Non riutilizzare mai la stessa password per siti e servizi differenti per evitare che, violata una, siano violate tutte.
Costruire password complesse	Utilizzare password lunghe (se possibile almeno 12 caratteri), miste (es. lettere, numeri, caratteri speciali) e senza senso compiuto (evitare parole da dizionario, nomi, date)
Digitare le password di nascosto	Prestare attenzione durante la creazione delle nostre password che nessuno ci stia osservando sia fisicamente che virtualmente (es. schermo condiviso durante una videoconferenza)
Aggiornare le password	Modificare le password almeno ogni 60 giorni senza riutilizzare le precedenti per garantire elevati livelli di sicurezza anche nel caso di password frodata
Custodire le password	Utilizzare un Password Manager (software che permette di gestire tutte le password attraverso un'unica password centrale) evitando di memorizzarle su carta, note dello smartphone , etc.
Rinforzare le password	Abilitare sempre , se consentito, la Multi-Factor Authentication che permette di affiancare alla password qualcosa che abbiamo (es. token via SMS) e/o qualcosa che siamo (es. fingerprint)



La password più sicura è la numero 4!



Esempi psw

Livello di sicurezza

- | | | | |
|---|-------------|---|-----------------------------|
| 1 | 987654321 | × | Sequenza numerica |
| 2 | password | × | Parola a dizionario (ovvia) |
| 3 | Marco210295 | × | Nome / data nascita |
| 4 | EnTrOp!497 | ✓ | Rispetta tutti i requisiti |

- ×

Livello di sicurezza basso

✓

Livello di sicurezza elevato

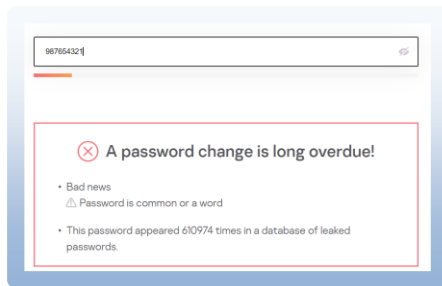
Utilizza i **servizi online gratuiti per verificare la complessità delle tue password,**



Controlla la sicurezza delle tue credenziali e verifica **se sono al sicuro**

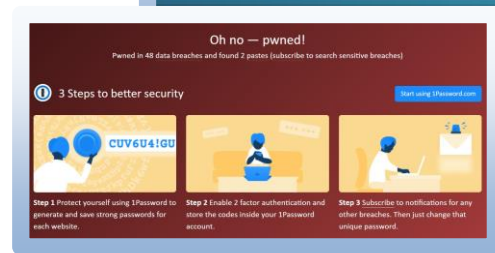
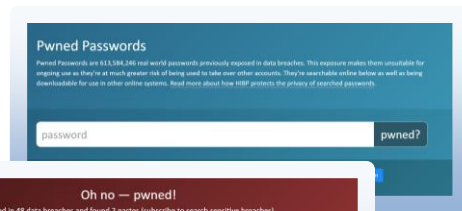
Testa la sicurezza delle tue password

- Visita un sito **password check** per testare la **sicurezza** delle tue password



Verifica se le tue credenziali sono al sicuro

- Inserisci **la tua password** sul sito **haveibeenpwned.com** e clicca su "pwned?"
- Puoi anche controllare se **il tuo indirizzo e-mail o numero di cellulare** sono stati compromessi
- In caso di compromissione, segui i consigli di sicurezza e **adotta le contromisure consigliate**



Ricordiamoci..



Società digitale, opportunità e pericoli.



Cybersecurity, comportamenti adeguati.



Strumenti per la nostra sicurezza.

Grazie.