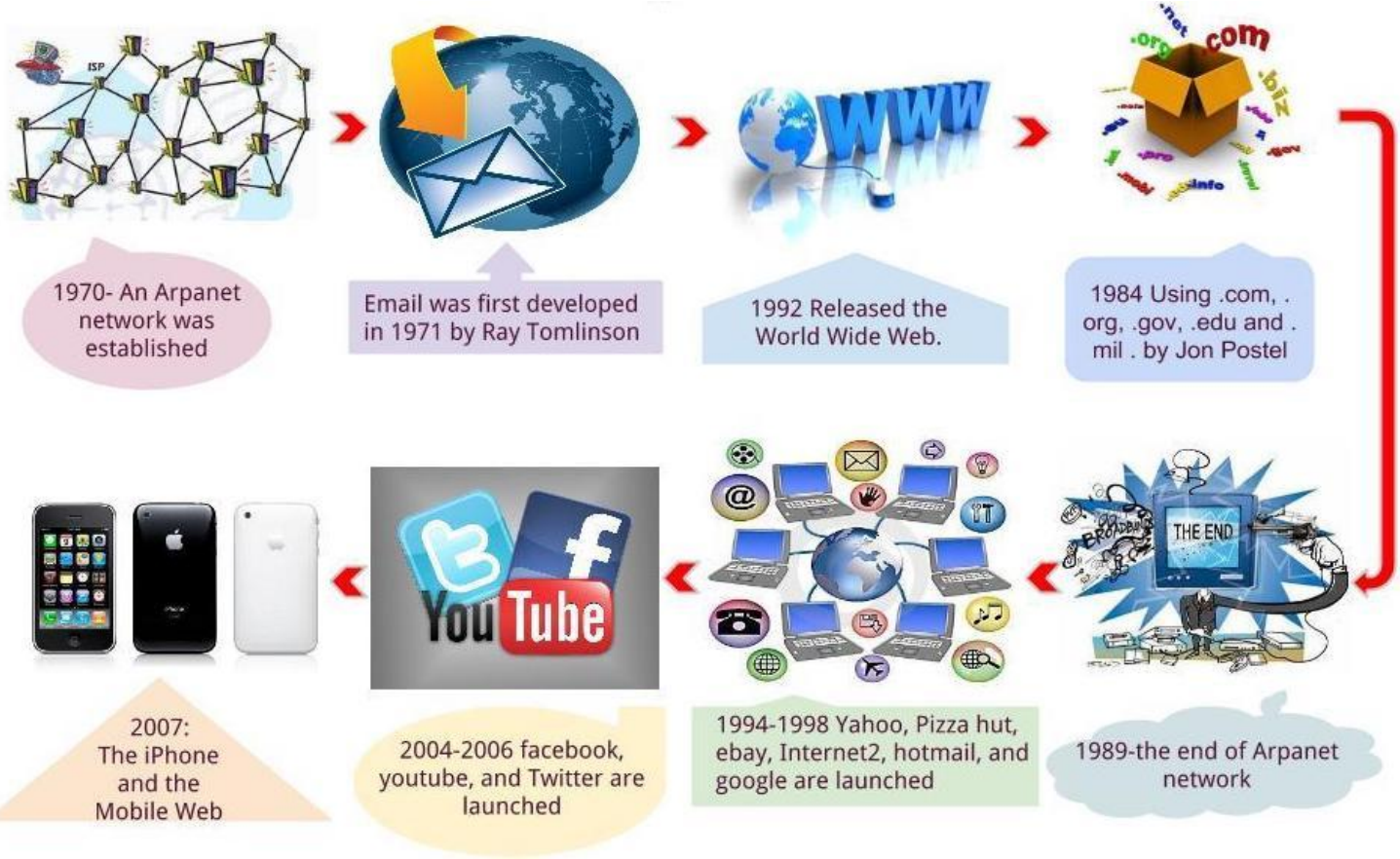
Mauro Giannandrea

Connessioni internet & sicurezza

Nascita di internet

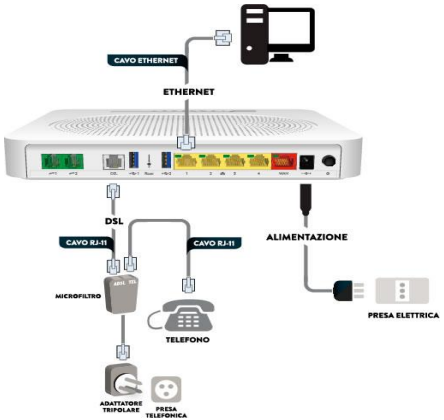
Usiamo Internet da molto tempo, ma non sappiamo nemmeno da dove viene.
Qui troverete la storia di internet ovvero la storia di diverse tecnologie che oggi compongono la rete come la conosciamo

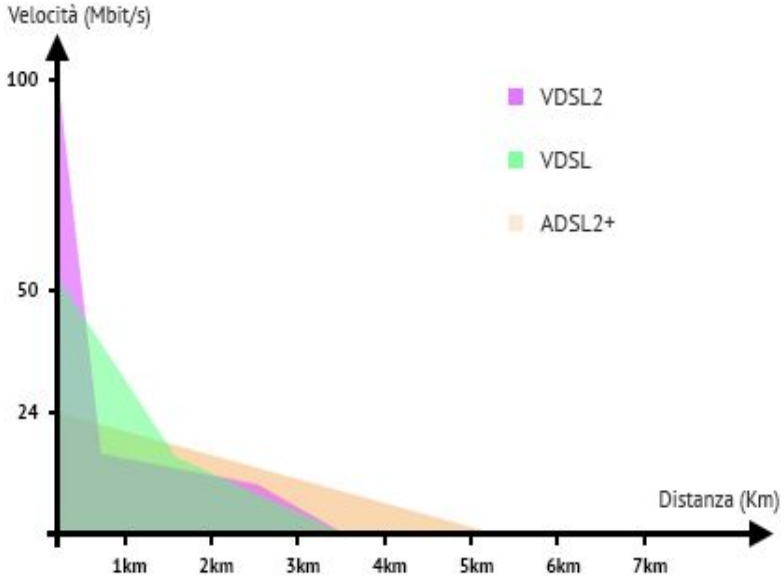


Connessioni internet (il Passato)

Dial-up: la più vecchia tipologia. Il modem effettua una vera telefonata al fornitore di internet parlandoci con segnali analogici (occupando la linea telefonica). La trasmissione di segnali analogici era lenta, un modem 56k, in media non superava 33 kbps.

ADSL: Le compagnie telefoniche quindi hanno sviluppato un modo di inviare un secondo segnale lungo le loro linee telefoniche, inviandolo a una frequenza più alta (e avere la cosiddetta banda larga). Per far funzionare la connessione DSL ancora meglio, è stata creata la **DSL Asincrona (ADSL)**, per migliorare la velocità di download (scaricamento) a scapito della velocità di upload.





Cable (cavo coassiale):
Il cavo coassiale era stato usato per decenni per inviare segnali digitali multipli a cui si è aggiunto internet. Per far ciò si lavora come per la DSL, utilizzando una frequenza più elevata per i dati e una bassa frequenza per la voce.
La connessione internet via cavo richiede modem speciali per funzionare e per separare i dati dai canali televisivi dai dati da trasmettere al computer.

Connessioni internet (il presente)

Fibra ottica: La connessione in fibra ottica ha un segnale di luce che passa attraverso un particolare tipo di vetro cavo flessibile o plastica trasparente. La fibra è costosa ed è più spesso utilizzata per collegare varie città tra loro in grossi tronconi che passano anche sotto gli oceani. La velocità di download arriva fino a 1 Gbps anche se la maggior parte dei servizi non offre più di 100 Mbps che è comunque tantissimo.

Wireless a banda larga: In questo caso il fornitore della connessione, si connette a Internet tramite una connessione cablata e trasmette poi tramite onde radio. Il cliente riceve questo segnale tramite un'antenna e un modem.
Le velocità del wireless a banda larga non raggiunge mai quella via cavo perchè il wifi è ancora meno veloce di un cavo di rete.

Internet mobile: Questo è il tipo di connessione usata da smartphone e dai modem portatili o chiavette con sim. Non è una vera connessione a banda larga ma ci si può collegare ovunque ci sia copertura della rete cellulare..
Internet Mobile funziona con le onde radio, con diversi tipi di velocità di trasmissione dati 3G, 4G, LTE.

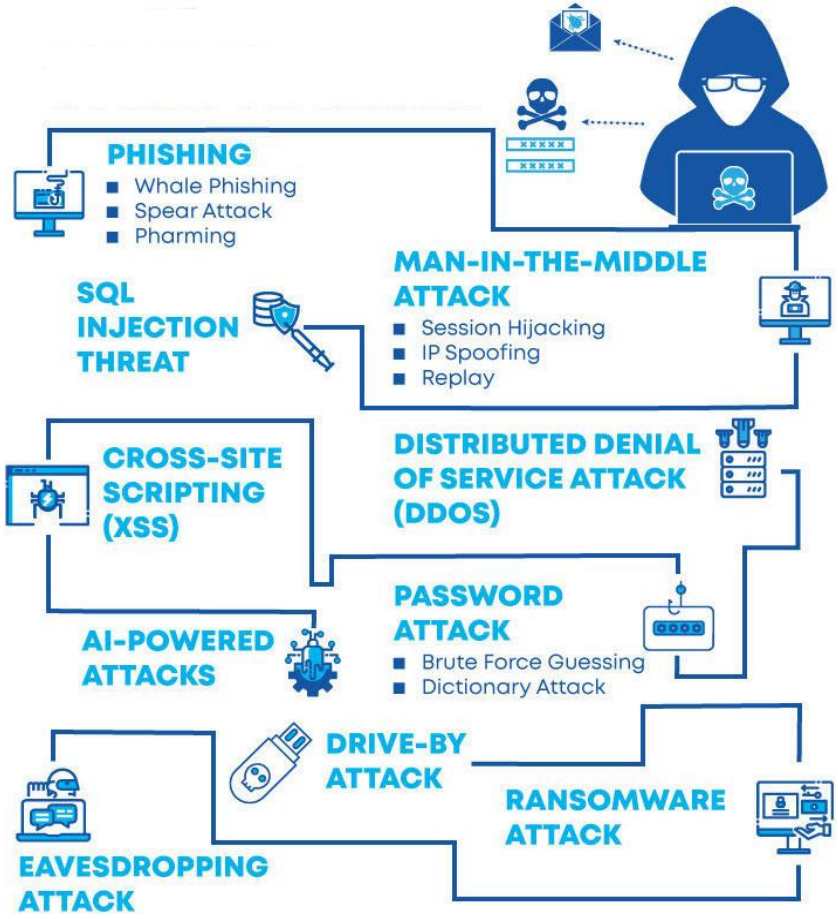
Internet satellitare: la connessione a internet satellitare funziona tramite un'antenna parabolica come quella della TV satellitare. Essendo il satellite lontano, questa connessione ha un upload lento, un download accettabile ma con un lag piuttosto alto e un costo superiore alle altre soluzioni.

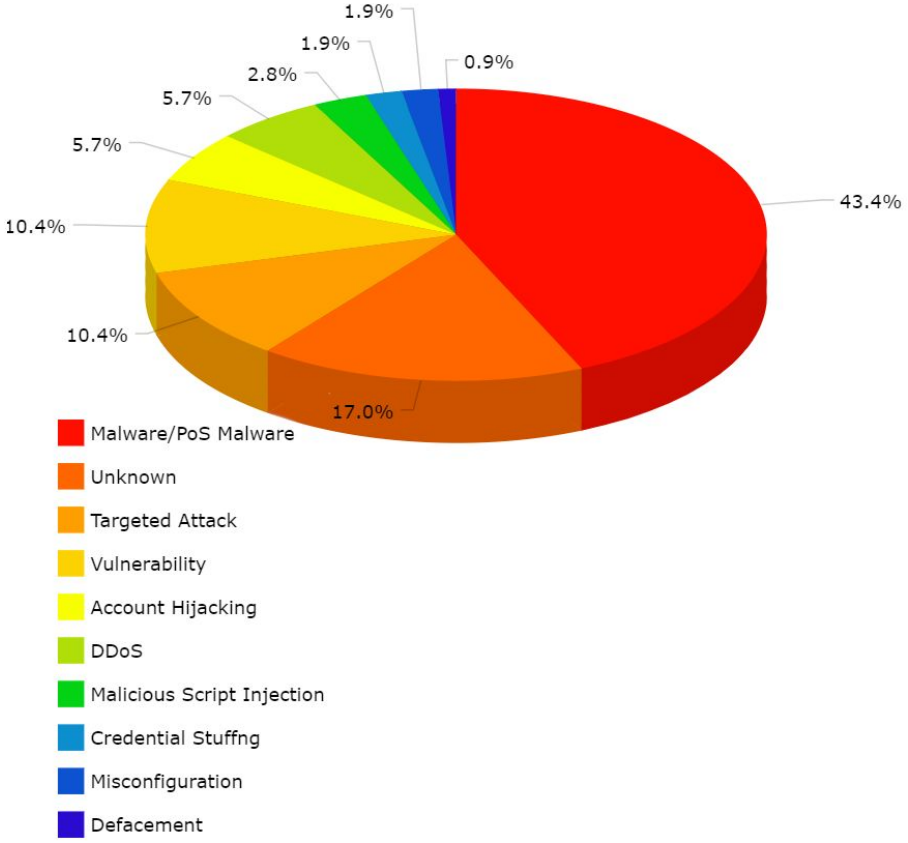
Sicurezza (anatomia di un attacco)

Un attacco informatico, nell'ambito della sicurezza informatica, indica una qualunque manovra, impiegata da individui od organizzazioni che colpisca sistemi informatici, infrastrutture, reti di calcolatori e/o dispositivi elettronici tramite atti malevoli, finalizzati al furto, alterazione o distruzione di specifici

Individuazione del target	**Intrusione**	**Studio del network**	**Accesso ai dati**
Si identifica l'obiettivo da colpire e se ne studiano le mosse. Attraverso tecniche come il social engineering si raccolgono informazioni sul target e sul sistema di sicurezza	Sulla base delle informazioni raccolte si cerca di prendere il controllo del dispositivo da remoto. Attraverso tecniche quali il phishing ci si può appropriare delle credenziali del network di protezione o tentare l'installazione di malware.	Si cerca di mappare la rete, le porte di accesso e le vulnerabilità, individuando il database e gli access points.	Ottenute le credenziali di accessi si prende il controllo dei sistemi informatici e quindi dei relativi dati. Per mantenere l'accesso, si cercherò di installare strumenti come backdoors rootkits o trojan.

Sicurezza (tipi di attacco)





Phishing

Il **phishing** è un tipo di 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

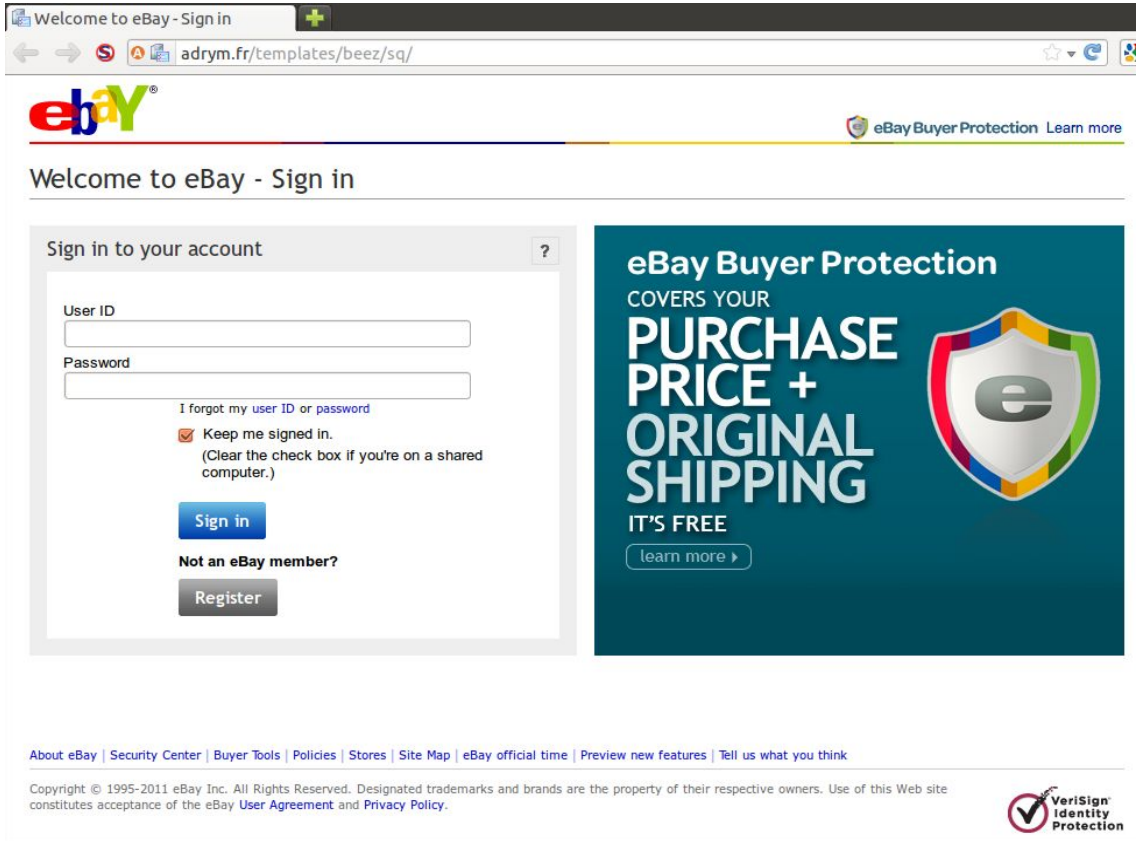
Si tratta di un'attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS.

Il phishing è una minaccia attuale, il rischio è ancora maggiore nei social media come Facebook e Twitter.

Riconoscere il Phishing

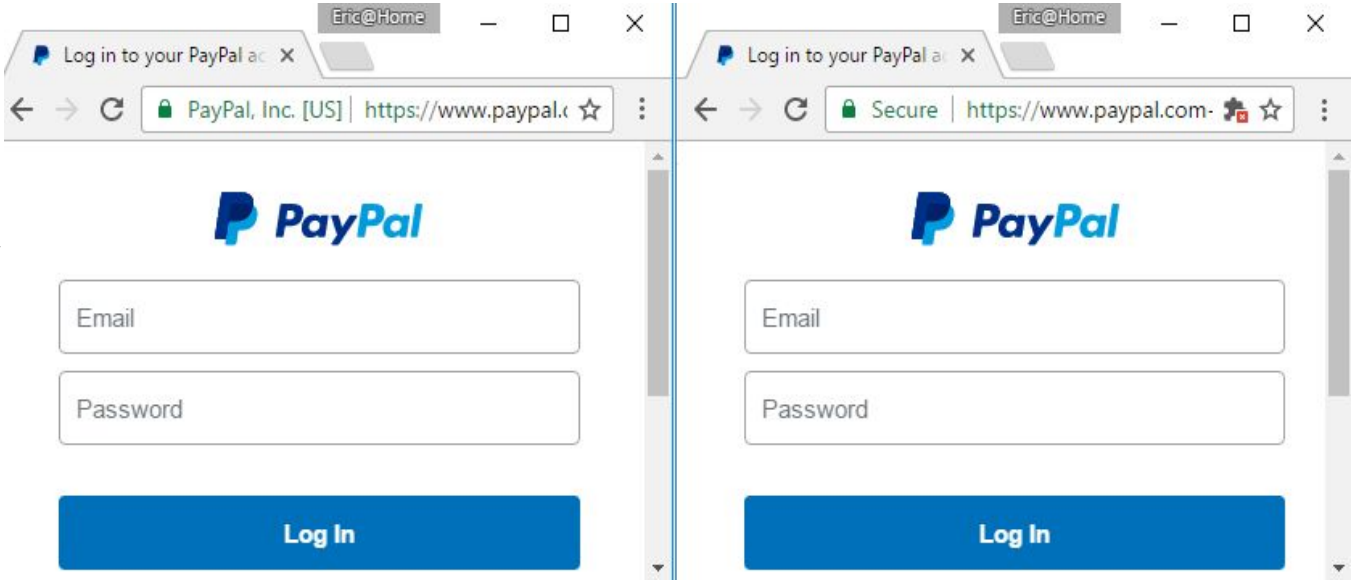
Non vi fidate della grafica del sito, i siti di phishing riescono ad essere identici all'originale tanto da ingannare anche gli utenti più assidui.

Il Browser è vostro amico.
Nella vostra barra degli indirizzi compare il nome del sito, se vi aspettare **ebay.com** non date i vostri dati ad **adrym.fr.**
Possono copiare tutto ma non il nome del sito nella barra degli indirizzi e il certificato ssl.



Riconoscere il Phishing 2

Il vostro browser vi aiuta anche indicando l'azienda proprietaria del certificato.
Come vedete in questo esempio è difficile distinguere la grafica del sito.



In questo caso l'indirizzo è molto simile entrambi contengono la parola paypal, questo potrebbe trarre in inganno un utente poco attendo che legga velocemente l'indirizzo.

Sicurezza delle password (bruteforce)

Ognuno di noi è inscritto ad una miriade di siti e questo aumenta le probabilità che almeno l'hash delle nostre password venga reso pubblico in seguito ad un data breach. Mentre il cracking di una password di lunghezza media 10 anni fa era piuttosto difficile ora serve molto meno tempo.

Years	Time x cracking "10051983"
1990	43 mesi
2000	5 settimane
2010	4 giorni
2020	45 ore

Password	Time x cracking
123456789	0,19 millisecondi
a23456789	9 settimane
A23456789	25 anni
A$23456789	80 000 anni

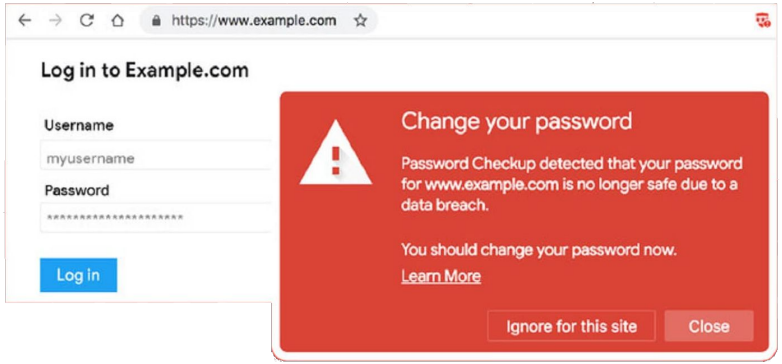
Sicurezza delle password (dictionary)

Un **attacco a dizionario** è una tecnica di attacco informatico mirata a "rompere" un meccanismo di autenticazione.
In pratica si tenta di accedere a dati protetti da password tramite una serie continuativa e sistematica di tentativi di inserimento della password, basandosi su uno o più dizionari di riferimento.
I dizionari, che sono normalmente semplici file composti da sequenze di parole divise da caratteri separatori, possono riferirsi a contenuti standard (dizionario della lingua inglese, della lingua italiana, dizionario dei nomi, ecc.) oppure essere creati appositamente a seconda del contesto di utilizzo.

```
C:\Users\Jake\Desktop\Passwords>python3 seclist_password_combiner.py -o combined_seclists_password_list.txt
[*] Processing file: .\bt4-password.txt
[*] Processing file: .\cirt-default-passwords.txt
[*] Processing file: .\clarkson-university-82.txt
[*] Processing file: .\combined_seclists_password_list.txt
[*] Processing file: .\darkc0de.txt
[*] Processing file: .\darkweb2017-top10.txt
[*] Processing file: .\darkweb2017-top100.txt
[*] Processing file: .\darkweb2017-top1000.txt
[*] Processing file: .\darkweb2017-top10000.txt
[*] Processing file: .\Keyboard-Combinations.txt
[*] Processing file: .\Most-Popular-Letter-Passes.txt
[*] Processing file: .\openwall.net-all.txt
[*] Processing file: .\PHP-Magic-Hashes.txt
[*] Processing file: .\probable-v2-top12000.txt
[*] Processing file: .\probable-v2-top1575.txt
[*] Processing file: .\probable-v2-top207.txt
[*] Processing file: .\twitter-banned.txt
[*] Processing file: .\unkown-azul.txt
[*] Processing file: .\UserPassCombo-Jay.txt
[*] Processing file: .\Common-Credentials\10-million-password-list-top-100.txt
[*] Processing file: .\Common-Credentials\10-million-password-list-top-1000.txt
[*] Processing file: .\Common-Credentials\10-million-password-list-top-10000.txt
[*] Processing file: .\Common-Credentials\10-million-password-list-top-100000.txt
[*] Processing file: .\Common-Credentials\10-million-password-list-top-1000000.txt
```

Sicurezza delle password (come difendersi)

Attivare su google chrome il check delle password che controlla la password salvata su un database di data breach per capire se la coppia mail e password è presente su internet.

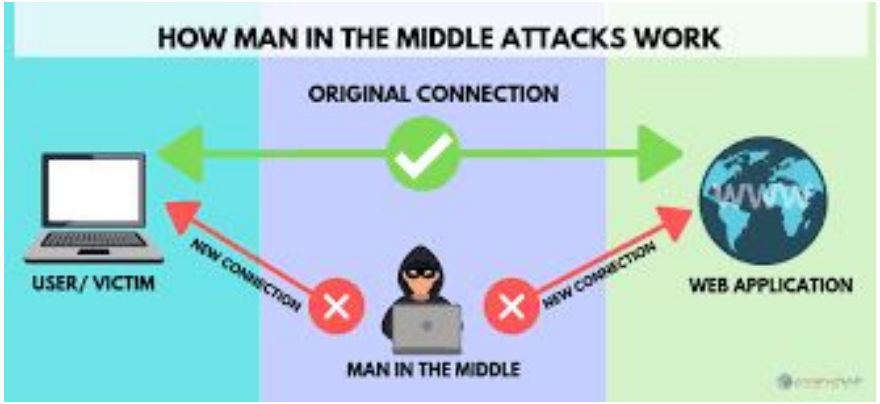


Come difendere le passwords
Aumentare la lunghezza delle password
Aumentare la complessità delle password
Limitare i tentativi di login
Usare captcha
Usare multifactor authentication
Non usare password comuni

Una password robusta è più sicura per il servizio dove viene utilizzata ma anche per tutti gli altri servizi in caso di data breach

Ransomware & Man in the middle

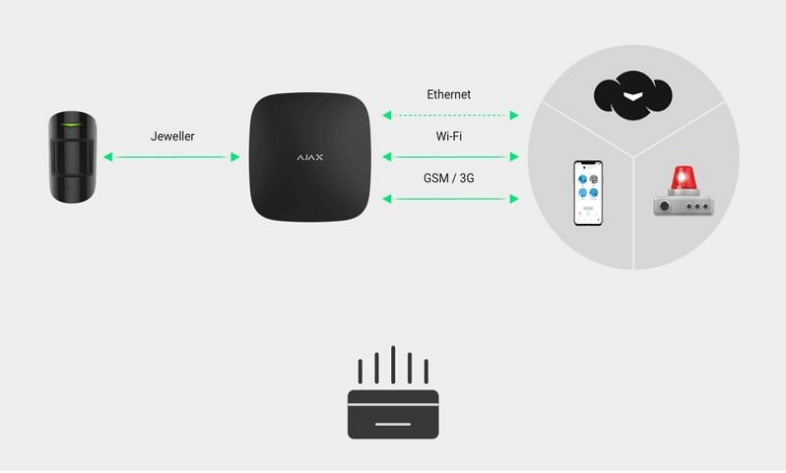
Ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, chiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione.

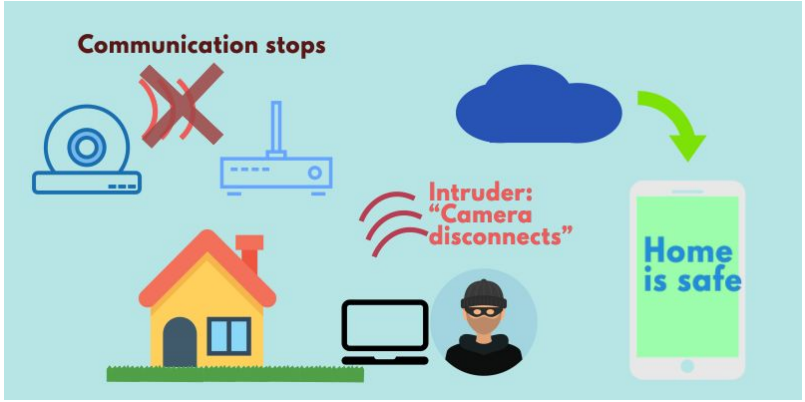


Man in the middle (*uomo nel mezzo)*
Una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

Sicurezza del wifi

Frequency jamming è l'atto di disturbare volutamente le comunicazioni radio facendo in modo che ne diminuisca il rapporto segnale/rumore, indice di chiarezza del segnale, tipicamente trasmettendo sulla stessa frequenza e con la stessa modulazione del segnale che si vuole disturbare.





Deauth attack
Il protocollo WiFi 802.11 contiene una feature di deautenticazione utilizzata per scollegare gli utenti dal network. Un hacker può inviare ad un router un frame di deauth in qualunque momento. Questo comando non ha nessuna cifratura o politica d sicurezza.
Questa vulnerabilità è stata trattata nella revision 802.11w-2009 per migliorare la sicurezza dei frame ma è raramente supportata e spesso disabilitata.

Sicurezza del contactless

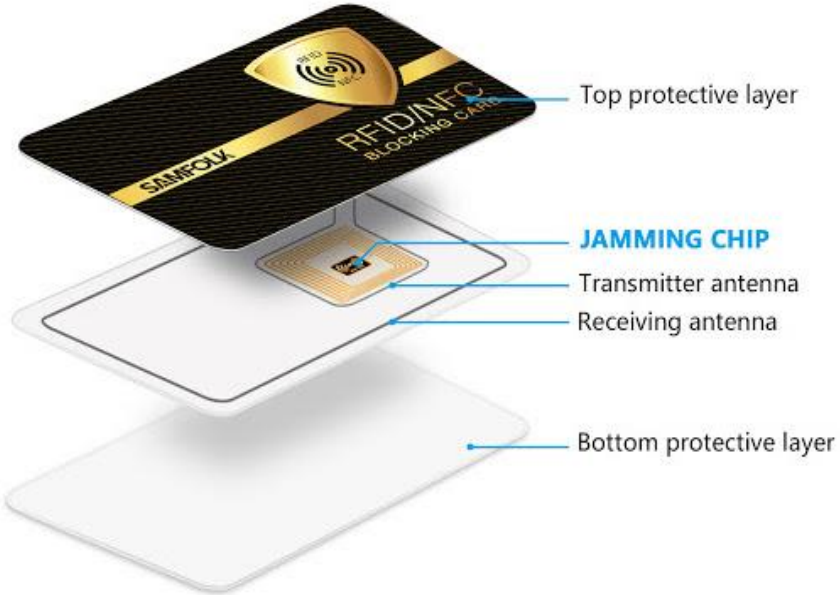
«Un ladro può rubare denaro avvicinando un terminale di pagamento alla carta o al dispositivo mobile mentre lo si tiene in tasca.»

Per alcune fonti come https://www.ccv.eu/ questo è un falso mito perché per avere un POS serve una registrazione.
Tuttavia non considerano che le carte di credito contactless funzionano in tutto il mondo e purtroppo non tutti gli stati e banche del mondo hanno una burocrazia così solerte.

Le ultime ricerche* di un duo di ricercatori dimostrano per la prima volta come aggirare il limite di $39 in UK per i pagamenti contactless effettuati con carte fisiche.
I ricercatori hanno anche scoperto problemi nel protocollo crittografico alla base dei pagamenti NFC, e queste lacune rendono possibile la clonazione delle transazioni.
"Visa è consapevole dei problemi, ma non vede alcun problema", ha detto Yunusov. Mastercard, che ha una maggiore presenza in Europa, è meno esposta.

*https://www.blackhat.com/eu-19/briefings/schedule/#first-contact---vulnerabilities-in-contactless-payments-17454

Sicurezza del contactless (soluzioni)



Soluzioni
Usare sempre le nuove carte aggiornate
Aggiornare il software dello smartphone
Disattivare l'NFC se non necessario
Utilizzare portafogli o coperture schermati
Utilizzare carte jammer