Fattore umano

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

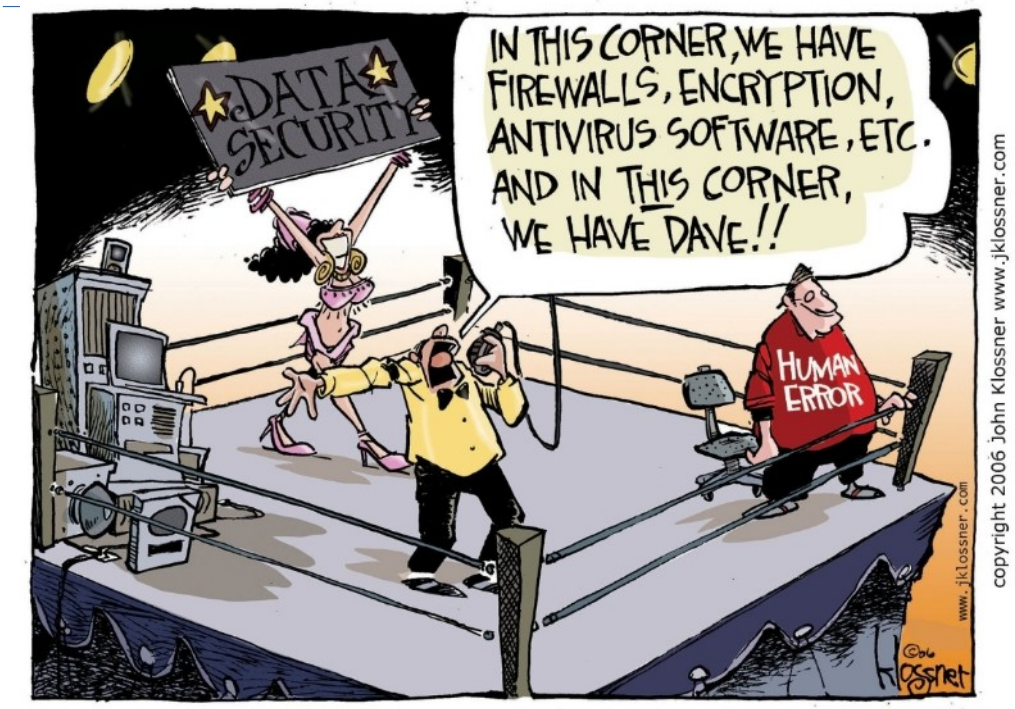
"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Fattore umano

- Il fattore umano
- BYOD e Shadow-IT
- Social Engineering
- Spam, Phishing e dintorni
- La gestione delle password

..

Il fattore umano



Ma siamo sicuri che l'utente "sbagli"?
O forse usiamo due modelli/linguaggi diversi?
Più che di "human error" spesso dovremmo parlare di "misunderstanding".
"Stop trying to fix the user"
https://www.schneier.com/blog/archives/2016/10/security_design.html

L'utente è inarrestabile! :-)
https://www.youtube.com/watch?v=84gvEKJiJzc

Il fattore umano

Poi c’è chi scrive le interfacce...

Annullo le modifiche ai contatti oppure annullo il comando di annullamento?
Si poteva scrivere in 1000 modi, invece...
E l’utente così si perde i dati.

Il fattore umano

Tecnologia vs uomo/organizzazione

Anello più debole della catena = client/utente

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.”
(Sun Tsu - L’arte della guerra)

Molti temi tecnologici hanno una loro controparte umana/organizzativa: sicurezza della navigazione, gestione dispositivi mobili, la posta elettronica, l'antivirus i salvataggi dei dati ecc.

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.” (Sun Tsu - L’arte della guerra)

Attaccare i server e i DataCenter sta diventando sempre più complesso; è più facile provare a passare dal client e dall'utente finale, normalmente molto più fragili e attaccabili.

Problemi non tecnologici

- Awareness
- Fallibilità degli esseri umani
- Tendenza alla fiducia
- Interfacce/architetture complesse
- Prestazioni vs sicurezza
- Shadow IT
- BYOD

Problemi base (non tecnologici)

- Scarsa comprensione del problema (awareness)
- Fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, …)
- Gli esseri umani hanno una naturale tendenza alla fiducia
- Interfacce/architetture complesse che facilitano gli errori e lo stress nell'utente
- Calo di prestazioni dovuto all'applicazione delle misure di sicurezza (es. antivirus)
- Shadow IT (chi usa Dropbox in azienda? Il mio PC/smartphone/tablet personale è meglio di quello aziendale! A volte il personale IT è fra i più indisciplinati!)
- da cui segue --→ BYOD

Shadow IT

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

Le applicazioni “consumer” ormai sono diventate più funzionali e performanti di quelle aziendali.

Social (Facebook) e posta personale completano il quadro.

Sono applicazioni non facilmente identificabili ed eliminabili.

Spesso vanno incontro ad esigenze reali dell’utente ma introducono problemi di sicurezza.

Anche una chiavetta USB è “Shadow IT”.

Anche gli acquisti “extra IT” lo sono.

AWS può diventare un nemico dell’IT aziendale.

Inutile approcciarlo con le cattive, meglio collaborazione e dialogo (“se non puoi combatterli unisciti a loro” … ma entro certi limiti)

Shadow IT Managers

Anche detti “technology leaders”.
Lo “smanettone” di reparto.
Quello a cui chiedere consigli per il prossimo smartphone.
Coinvolgerli, farseli amici, pericoloso averli contro!

Bring your own device (BYOD)

- BYOT – BYOP – BYOPC - BYOC
- COPE vs POCE
- Aggredire il problema tecnologico ma anche quello organizzativo (e legale)

http://en.wikipedia.org/wiki/Bring_your_own_device

Varie declinazioni: “Bring your own technology (BYOT)”, “Bring your own phone (BYOP)”, “Bring your own PC” (BYOPC), “Bring your own cloud (BYOC)” ecc.

COPE (Company Owned, Personally Enabled) vs POCE (Personally Owned, Company Enabled)

Esistono strumenti per aggredire il problema tecnologico (ad esempio software di Mobile Device Management tipo AirWatch http://www.air-watch.com/), è molto più complesso aggredire quello organizzativo (e legale, ad esempio GPS)

BYOD e Shadow IT

Bring your own device

- Limiti e modalità di utilizzo
- Responsabilità
- Servizi, Applicazioni, Dati
- Analisi dei rischi dell'adozione
- Infrastruttura tecnologica
- Misure di sicurezza
- Politiche di licensing
- Sistemi di monitoraggio
- Procedure di gestione
- Strumenti di supporto

Definire i limiti e le modalità di utilizzo dei dispositivi mobili non aziendali (o aziendali, quando abilitati anche all'uso personale).

Definire le responsabilità aziendali e quelle personali nell'uso dei dispositivi misti (responsabilità diverse nei casi di POCE vs COPE).

Definire i servizi, le applicazioni e i dati che devono essere accessibili dai dispositivi.

Fare un'analisi dei rischi dell'adozione del BYOD.

Definire l'infrastruttura tecnologica, le misure di sicurezza, le politiche di licensing, i sistemi di monitoraggio, le procedure di gestione e gli strumenti di supporto

BYOD e Shadow IT

Quindi sei l'Amministratore Delegato e vorresti installarti Instagram sullo smartphone aziendale?

- Identità = so chi sei
- Contatti = so chi conosci
- Posizione = so dove sei
- Fotografie = so cosa ti piace (cosa mangi)
- Archivio = so tutta la tua storia
- Fotocamera = magari ti faccio anche una foto
- Microfono = ti ascolto durante un CDA
- Batteria = so quando sei irraggiungibile (o posso renderti tale)
- Vibrazione/notifiche = so quando ti chiamano

Sono te!

BYOD e Shadow IT

Esistono anche strumenti più sofisticati di controllo dei dispositivi.

App che consentono il controllo totale da remoto di un dispositivo. Serve un breve contatto fisico con il dispositivo sbloccato. Illegali in Italia senza il consenso del controllato (se dipendente deve essere avvertito, comunque da contrattare con i sindacati come i sistemi di video sorverglianza, applicabile ai figli minorenni).

- https://www.flexispy.com/
- https://www.theonespy.com/iphone-spy-software/
- http://spyera.com/iphone-spy-app/
- https://www.mspy.it/
- http://www.highstermobi.com/

Social engineering

- Sfruttare l'utente
- Attaccare i punti deboli
- Pressione psicologica
- Utenti esperti!
- Molteplici canali di attacco
- Studio e analisi
- Conoscenza porta a fiducia

http://en.wikipedia.org/wiki/Social_engineering_(security)

Sfruttare la partecipazione (inconsapevole) dell'utente per un attacco.
Si cerca di attaccare i punti deboli dell'utente (vedi dopo).
Meccanismi di pressione psicologica (Nigerian Scam http://en.wikipedia.org/wiki/419_scams)
A volte ci cascano anche utenti esperti.
Sfrutta molteplici canali di attacco (mail, telefono, comunicazioni cartacee, chiavette USB ecc.).
Per riuscire bene richiede una fase di studio e di analisi molto accurati (attenzione a quello che racconta di noi il nostro sito web, i social ecc.)
Dimostrare di conoscere bene l'azienda, le persone, le procedure porta istintivamente il target dell'attacco ad abbassare la guardia.

Sito molto interessante
https://www.social-engineer.org/framework/general-discussion/

Social engineering

I punti deboli dell'utente

- Coerenza
- Curiosità
- Validazione sociale
- Liking
- Autorità/Autorevolezza
- Scarsità
- Altruismo

Elementi comportamentali attaccabili:

- Coerenza: stabilità dei propri comportamenti e delle proprie convinzioni
- Curiosità: "chissà cosa c'è in questa chiavetta che ho trovato al bar..."
- Validazione sociale: "lo fanno tutti..."
- Liking: si tende a dare fiducia a chi è simpatico, bello o gentile
- Autorità/Autorevolezza: esiste una sudditanza di base verso l'autorità vera o presunta
- Scarsità: si tende a sovrastimare il valore di una cosa potenzialmente scarsa
- Altruismo: siamo tendenzialmente portati ad aiutare una persona in difficoltà

Social engineering

I punti deboli dell'utente

- Reciprocità
- Senso di colpa
- Paura
- Ignoranza
- Avidità

Elementi comportamentali attaccabili:

- Reciprocità: se mi fai un regalo o mi risolvi un problema sono predisposto a ricambiare
- Senso di colpa: mi fai sentire in colpa per spingermi ad un comportamento
- Paura: reazioni istintive prevedibili in situazioni di panico
- Ignoranza: sfrutto la tua ignoranza per farti sbagliare
- Avidità: ti prospetto una situazione apparentemente interessante

Social engineering

La ricostruzione di un attacco reale (sembra un film ma è basato su una storia vera):

Targeted Cyber Attack Reality - Trend Micro
https://www.youtube.com/watch?v=0hs8rc2u5ak

Costruire un attacco mirato partendo da quanto ricavabile dai Social Network:

Amazing mind reader – Safe Internet Banking - Belgio
https://www.youtube.com/watch?v=F7pYHN9iC9I

https://www.youtube.com/watch?v=0hs8rc2u5ak

https://www.youtube.com/watch?v=F7pYHN9iC9I

..

Social engineering

Un esempio personale:

Esempio di social engineering telefonico
https://www.youtube.com/watch?v=lc7scxvKQOo

Social engineering

Lettura istruttiva

L'arte dell'inganno - Kevin David Mitnick

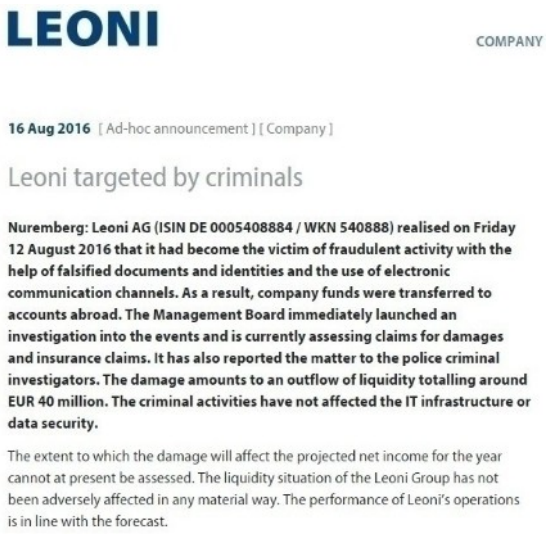
https://it.wikipedia.org/wiki/L%27arte_dell%27inganno

Oppure Robert B. Cialdini: Le armi della persuasione.
https://www.youtube.com/watch?v=CdZrgnf12v0

A seguire: Kevin David Mitnick, L'arte dell'intrusione
https://it.wikipedia.org/wiki/L%27arte_dell%27intrusione

Social engineering

Social Engineering + domini DNS = colpo da 40M€



LEONI

COMPANY

16 Aug 2016 [Ad-hoc announcement] [Company]

Leoni targeted by criminals

Nuremberg: Leoni AG (ISIN DE 0005408884 / WKN 540888) realised on Friday 12 August 2016 that it had become the victim of fraudulent activity with the help of falsified documents and identities and the use of electronic communication channels. As a result, company funds were transferred to accounts abroad. The Management Board immediately launched an investigation into the events and is currently assessing claims for damages and insurance claims. It has also reported the matter to the police criminal investigators. The damage amounts to an outflow of liquidity totalling around EUR 40 million. The criminal activities have not affected the IT infrastructure or data security.

The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way. The performance of Leoni's operations is in line with the forecast.

https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/

"The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way."

Oltre al danno diretto anche i danni collaterali.

Tanti attacchi di questo tipo, Confindustria Bruxelles ad esempio.

https://ricerca.repubblica.it/repubblica/archivio/repubblica/2017/10/06/sessanta-mail-una-telefonata-due-bonifici-cosi-la-truffata12.html

Spam

http://en.wikipedia.org/wiki/Email_spam

Lo spam, o “Unsolicited Commercial Bulk Email”, è un fenomeno largamente diffuso.

Consiste nel pubblicizzare prodotti e servizi a scopo commerciale o di phishing, o nell'indurre il destinatario della mail a visitare siti o pagine compromessi al fine di catturare dati o credenziali.

Produce danni sia come perdita di tempo che, a volte anche direttamente economici.

Non vi sono rimedi particolarmente efficaci o applicabili con elevato successo; tenendo alta l’attenzione all’evolversi del fenomeno si mettono in atto diverse pratiche, non ultima la “semplice” educazione degli utenti.

Spam, phishing e dintorni

Figure 10. This spam service offers support, just like many legitimate online offers.

Anche questo è ovviamente un business

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Antispam

(strumenti base)

- Filtri sui contenuti
- Black&white-listing dei mittenti
- Graylisting

Vengono utilizzate varie metodologie per mitigare gli effetti dello spam (il punto finale dell'attacco rimane sempre l'utente finale):

Filtri sui contenuti (probabilistici e comunque sempre un passo indietro rispetto all'attaccante)

Black&white-listing dei mittenti (aggiornamento delle liste, rischio DOS per mittenti inconsapevoli)

Graylisting (rifiuto la prima mail con un “temporary error”)

Siti per verificare se sono finito nelle liste degli spammer (ad esempio http://mxtoolbox.com/blacklists.aspx)

Antispam

(strumenti avanzati)

- Sender Policy Framework
- DKIM
- DMARC (DKIM+SPF+Regole)

Sender Policy Framework (Controllo incrociato IP: se IP mittente non corrisponde IP in SPF record allora spam.)
https://en.wikipedia.org/wiki/Sender_Policy_Framework
Tool per validare:
http://www.kitterman.com/spf/validate.html
Problemi: gestione e propagazione

DKIM (DomainKeys Identified Mail) è un metodo tramite il quale il proprietario di un dominio “certifica” di prendersi la responsabilità di quella specifica email.

DMARC: DKIM+SPF+regole ulteriori
Va oltre SPF ma è ancora poco diffuso
Tool per validare o costruire record DMARC
https://dmarcian.com/dmarc-inspector/

Antispam

… oppure tenere occupato lo spammer

Chat/mail bot che tengono impegnato lo spammer in conversazioni fingendo di essere il target.
https://spa.mnesty.com/

Oppure se volete divertirvi…
https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email?language=it#t-16339

Mail Marketing

Il confine fra SPAM e Mail Marketing può essere sottile.
"Mail non richiesta", ma siamo sicuri che la richiesta sia sempre così esplicita? (Iscrizione a siti, scaricare documentazione, rispondere ad un invito ecc.)
Perché una email non finisca nello spam sono necessarie due condizioni:

1. Il server di invio deve **avere buona reputazione**, essere configurato correttamente e evitare di "infastidire" i domini di destinazione (nello spam ci mette il provider)
2. Il messaggio deve **essere non fastidioso** per i destinatari (nello spam ci mette l'utente)

Ricordarsi di mettere sempre le modalità di cancellazione dalla lista di distribuzione.

Phishing

http://en.wikipedia.org/wiki/Phishing

Neologismo, assonanza con “fishing” → “Andare a pesca di ingenui”. Via mail ma anche via IM.

Social Engineering di massa, spesso poco mirato, si lanciano milioni di esce sperando che qualcuno abbocchi.

Utilizzo di “shadow server”.

Metodologie di difesa simili a quelle contro lo SPAM.

Ancora più importante però la consapevolezza dell'utente.

A differenza dello SPAM la minaccia è nascosta e richiede un'azione da parte dell'utente.

Insegnare all'utente di cercare sempre il “lucchetto chiuso”.

Insegnare all’utente di diffidare di mail “strane” (“se non ho un contratto perché ricevo una fattura?”)

URL Shortner: http://www.trueurl.net/

Phishing

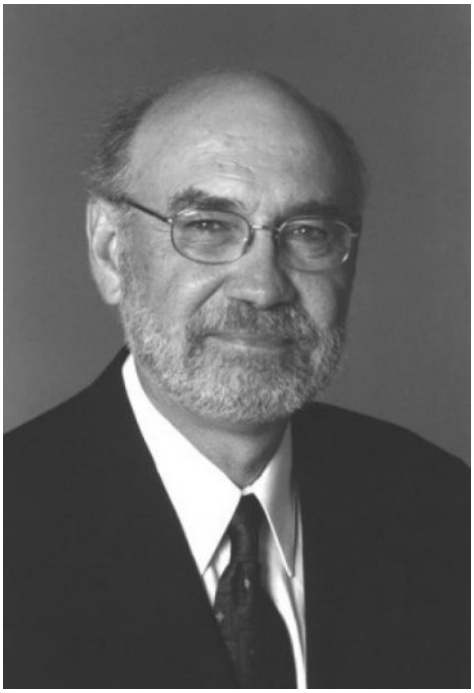
- Whaling
- Spear Phishing

Whaling: phishing mirato a CIO/CEO, molto sofisticato. C'è chi si è giocato il posto (FACC aerospatial Austria, frode da 40M€, licenziato CEO https://businessinsights.bitdefender.com/cyber-fraud-ceo-fired)

Spear Phishing: attacchi molto mirati a singole persone o gruppi, non necessariamente in alto nella catena gerarchica, ma potenzialmente canali di intrusione in azienda. Spesso l'anello debole della catena, alta percentuale di successo. Non esiste una risposta tecnologica → Awareness !

Verificate la vostra resistenza al phishing: https://www.opendns.com/phishing-quiz/

La gestione delle password



L’uomo che ha consentito il maggior numero di furti di password: Spencer Silver, l’inventore dei Post-it (RIP 2021)

La gestione delle password

Le password:

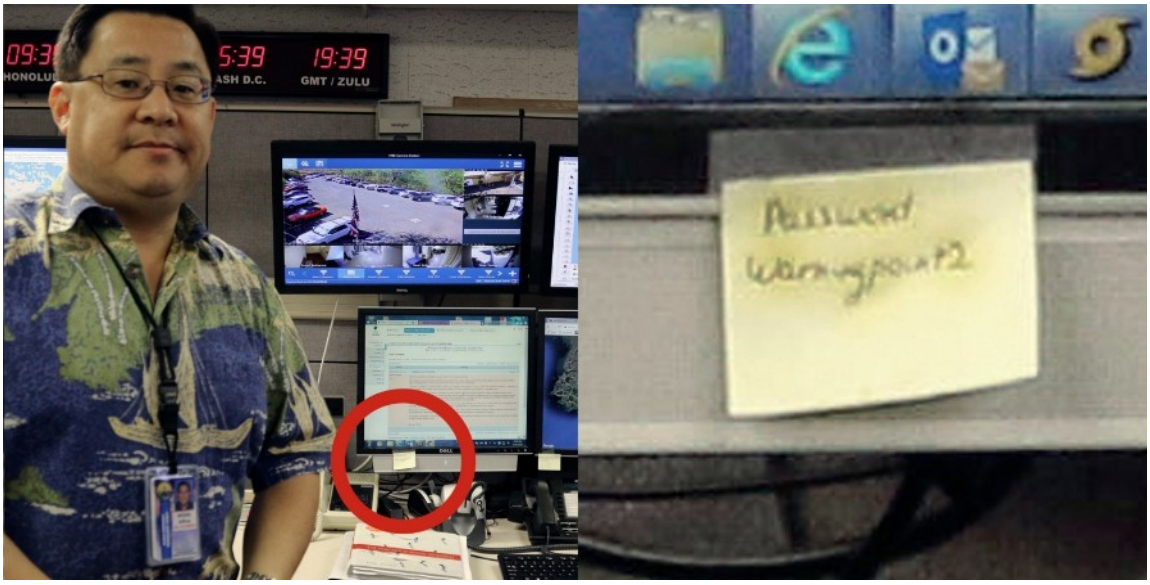
- Sono tante
- Non debbono essere ripetute
- Vanno conservate
- Andrebbero cambiate (NO! NO! NO!)
- Debbono essere difficili da indovinare

- Dobbiamo ricordare tante password (non usate la stessa in tutti i siti, vero?)
- Se vi beccano quella di un sito debole siete finiti (oppure se vi beccano quella del “recupera la tua password”)
- Non le scrivete su un foglietto giallo o sotto la tastiera vero? Dove le conservate?
- Aveva senso una volta, ora non ha più senso, anzi induce confusione e abbassa la sicurezza. Vedi anche: https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html

- No il nome del cane/gatto/figlio/moglie ovviamente

La gestione delle password

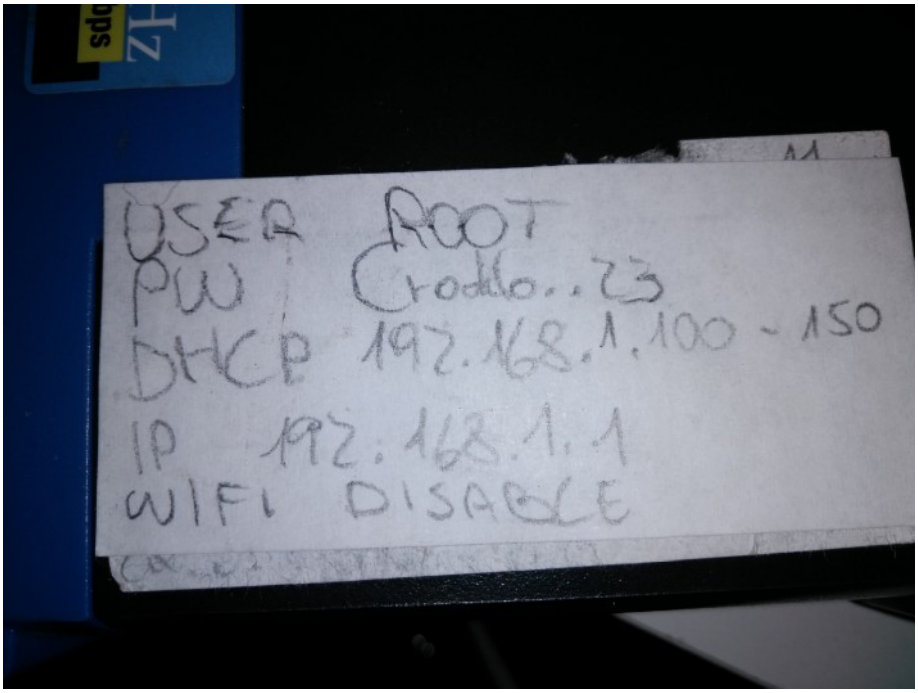
I foglietti gialli causa di allarmi nucleari



Gestisci gli allarmi nucleari degli USA nelle Hawaii, vieni intervistato e sui giornali di tutto il mondo si vede la tua password.

http://uk.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?IR=T

La gestione delle password



.....

La gestione delle password

Approfondimento Governo

Governo, Draghi invita Salvini alla prudenza sul coronavirus. E circola l'ipotesi di nuove strette

23 FEBBRAIO 2021

.....

La gestione delle password

Una soluzione: Password manager

(in ordine casuale)

- KeePass (Open source) KeepassXC
- 1Password (Cloud)
- LastPASS (Cloud)
- BitWarden (Open source)
- DashLane (Cloud)
- ecc.

Ovviamente se vi perdete la master password siete finiti!

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

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

Possono essere in locale oppure nel cloud, alcuni esempi:

http://keepass.info/
https://keepassxc.org/
https://bitwarden.com/
https://1password.com/
https://www.lastpass.com
https://www.dashlane.com/

La gestione delle password

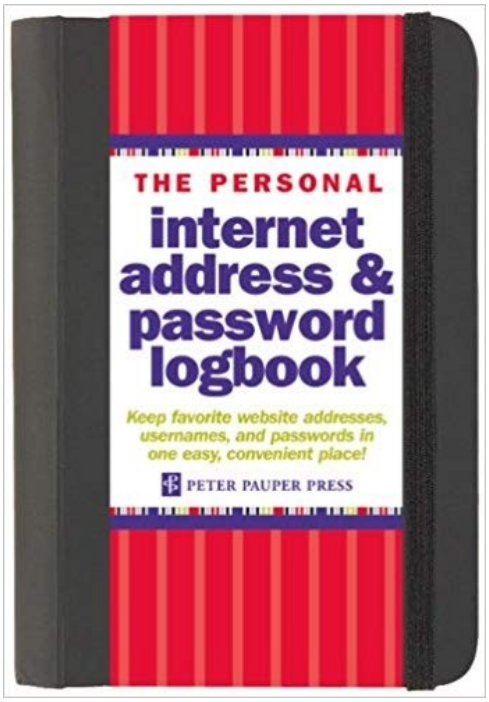
	Built in			Stand alone					
					Commercial			Open Source	
	Chrome	Edge	Keychain (Safari)	1Password	Dashlane	Keeper	LastPass	KeePass	PasswordSafe
Generates passwords for you	✔	✘	✔	✔	✔	✔	✔	✔	✔
Verifies that site isn't impostor	✔	✔	✔	✔	✔	✔	✔	✔[1]	✘
Identifies re-used passwords	✘	✘	✔	✔	✔	✔	✔	✔[1]	✘
Blinded to customer support	✘	✘	✔	✔	✔	✔	✔	✔	✔
Recovery via physical object	✔	✔	✘	✔	✘	✘	✘	✘	✔
Recovery via trustee	✘	✘	✘	✘	✔	✔	✔	✘	✘
Published security architecture	✘	✘	✘	✔	✔	✔	✔	✔	✔

Tabella riassuntiva dei principali password manager

Video pubblicità password manager
https://www.youtube.com/watch?v=B5lslSPfhkg

La gestione delle password

Altra soluzione



Perchè no, se lo tenete in cassaforte…
(non è proprio comodo).
https://www.amazon.com/Personal-Internet-Address-Password-Book/dp/1441303251

La gestione delle password

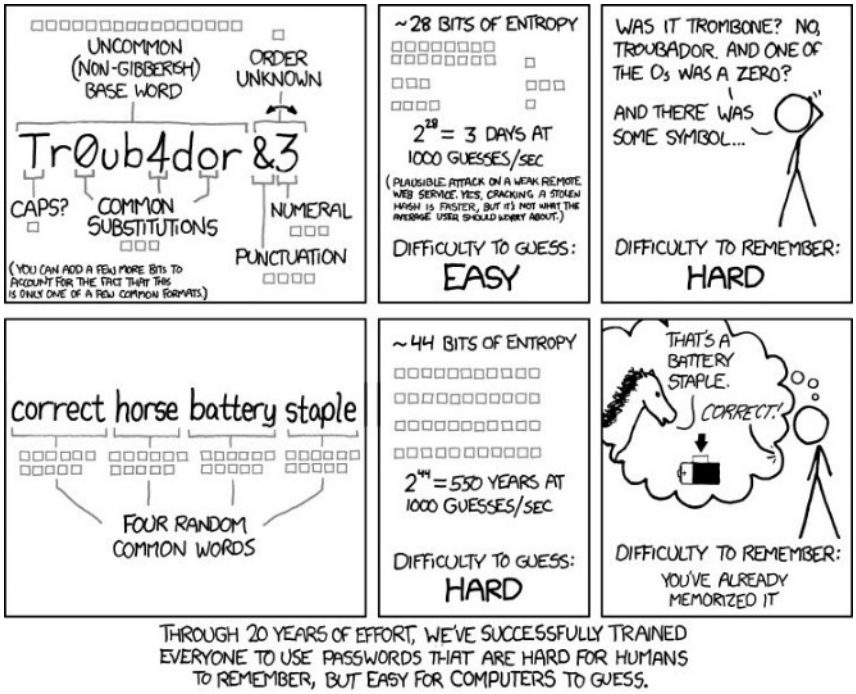
Ma se invece voglio avere una password sicura e memorizzabile? (master password ad esempio)

Almeno la master password però debbo ricordarmela e deve essere sicura.

Siamo certi che maiuscole/minuscole/caratterispeciali/numeri servano davvero?

La gestione delle password

Il falso mito delle password complesse



http://xkcd.com/936/
Vedi anche questo video:
https://www.youtube.com/watch?v=0SkdP36wiAU
Lo ha ammesso anche il suo creatore:
https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

Anche il NIST lo ha tolto come requisito.

La gestione delle password

Esempio:

- Password di tre caratteri lettere o numeri = 42.875
- Se impongo almeno una lettera e un numero = 26.250
- Risparmio il 40% del tempo

Disposizioni con ripetizione

il numero delle possibili sequenze di k oggetti estratti dagli elementi di un insieme di n oggetti, ognuno dei quali può essere preso più volte = n elevato alla k

password di tre caratteri lettere o numeri
25+10 oggetti = n = 35
k=3
disposizioni = 42.875

almeno una lettera e un numero
42.875 - (password di sole lettere 25 alla 3) - (password di soli numeri 10 alla 3)
42.875 - 15.625 -1000 = 26.250 = 40% di tempo in meno attacco a forza bruta

La gestione delle password

Nuove regole del NIST

- Chiedere di cambiare password ogni x mesi è dannoso, cambiare solo se compromessa
- Le regole per password complesse sono dannose
- Minimo 8 caratteri, massimo 64, consigliati 32
- Accettare tutti i caratteri (speciali, spazi ecc.)
- No alle domande di recupero della password (facilmente attaccabili)
- Sì al copia-incolla e alla visualizzazione della password
- Autenticazione a due fattori, meglio con app (no token, no SMS)
- Memorizzazione con hash+salt+iterazioni (PBKDF2 con 10.000 iterazioni)

National Institute of Standards and Technology

https://www.cybersecurity360.it/soluzioni-aziendali/sicurezza-delle-password-le-nuove-regole-del-nist-per-renderle-inattaccabili/

https://pages.nist.gov/800-63-3/sp800-63-3.html

La gestione delle password

Meglio se non contiene un segreto personale
Non deve dire la verità
Non deve avere senso
Non deve essere prevedibile
Le sostituzioni ovvie sono ovvie

E allora giochiamocela ai dadi!

- “amo Maria” ma mia moglie si chiama Giovanna
- Esiste una verità e tante bugie
- Per ogni frase sensata ne esistono di più senza senso
- “e poi ci troveremo come le ...”
- “s1cur0” non è più sicuro di “sicuro”

Diceware.
https://blog.agilebits.com/2011/06/21/toward-better-master-passwords/

*"'Source:'" Alexander Dreyer Two dices, all combination of eyes. Photographed by myself. {{self2|GFDL|cc-by-2.5}}

La gestione delle password

1) Lancio 5 dadi
2) Guardo la parola corrispondente nella tabella
3) Ripeto 4-5 volte
4) Costruisco una frase/immagine con le parole ottenute
5) (opzionale) sostituisco una delle parole con una mia personale (caratteri speciali ecc.)

4 parole + personale = 74 bit entropia
(500 Milioni anni a 1 milione tentativi/sec)

Diceware.
http://world.std.com/~reinhold/diceware.html
https://en.wikipedia.org/wiki/Diceware

Se interessa il calcolo dell'entropia e la matematica che c'è dietro:
https://blog.agilebits.com/2011/08/10/better-master-passwords-the-geek-edition/

La gestione delle password

One Time Password (password usa e getta)

OTP https://en.wikipedia.org/wiki/One-time_password
Con “token” fisico oppure con app su dispositivo.
Scomode, costose, deve essere un algoritmo veramente casuale
Problema allineamento dei clock (dispositivo-server, app-server, esempio token cambia ogni 60 secondi, deriva annua 15 secondi, ogni 4 anni debbo cambiare dispositivo)
Attacco DOS con ripetuti errori di chiave.
Attacco di Social Engineering per farsi sostituire la chiave.
2FA con SMS si attacca facendosi cambiare la SIM da un negozio compiacente/ingannato.
In via di dismissione da parte delle banche

La gestione delle password

Dispositivi HW o app

Ad esempio https://www.yubico.com
Bisogna averne almeno una di riserva.
Forte come il suo sistema di backup (“se hai perso la chiave ti faccio una domanda di recupero della password”)

Ad esempio Google Authenticator
Sostituisce chiavetta ed SMS, più affidabile se non perdo il telefono (che deve avere il pin ed essere cifrato ovviamente...)