Piccola Guida Pratica alla

SICUREZZA INFORMATICA

7 COSE DA FARE PER DIFENDERTI DAGLI HACKER ANCHE SE NON SEI UN TECNICO

Aggiornata a: dicembre 2022

LUCA GIULIANI

Benvenuto!

Al termine della lettura di questa piccola guida saprai **come eliminare 7 brutte abitudini** che mettono a rischio la tua sicurezza informatica.

Come scoprirai tra poco, preferisco esporre gli argomenti adottando uno stile ironico perché dopo molti corsi di formazione ho verificato che **così i concetti rimangono ben impressi,** e nel caso delle guide le persone tendono a leggere fino all'ultima pagina. E non è poco.

So di cosa parlo.

Una volta ho lasciato in bianco le ultime pagine di una guida consultabile solo online. Poi ho collegato alla guida un piccolo automatismo che mi avrebbe inviato una notifica ogni volta che qualcuno avesse cercato di leggere le pagine in bianco.
La guida era destinata a 12.000 impiegati sparsi in tutta Italia e spiegava l'utilizzo di un nuovo software di lavoro realizzato appositamente per loro. Ebbene: quasi tutti hanno iniziato la lettura ma **nessuno ha mai letto quella guida fino in fondo**, infatti non ho ricevuto nemmeno una notifica.

Ciò che ho imparato quella volta è che anche un argomento serio, se esposto nel modo sbagliato, rischia di fare la fine degli avvertimenti sui pacchetti di sigarette.

Il furto d'identità o le truffe online sono argomenti seri. Ci sono in ballo la tua reputazione, il tuo conto in banca e il tuo cane. Una delle voci l'ho inserita solo per incuriosirti.

Molte guide rendono questi argomenti n-o-i-o-s-i e spesso solo per dirti cose come "aggiorna sempre l'antivirus" oppure "non cliccare sui link sospetti". Io credo si possa fare di meglio.

Questa piccola guida è parte di un libro molto più completo dal titolo "Sicurezza Informatica Pratica" in vendita su Amazon a questo link:
https://www.amazon.it/dp/B09HSLYLTB

Forse dovresti dare un occhiata alla guida completa o forse no. Come puoi capirlo?

Ti propongo una sfida.

Ho raccolto alcune brutte abitudini molto pericolose per la tua sicurezza. Al termine di ciascun argomento, ti chiederò di **dare un voto alla soluzione che ti propongo**, a scelta tra: "la sapeva anche il mio cane", "vabbé questa non è male" e "ok, lo farò".

Se riuscirò ad assegnarti almeno un paio di cose da fare, beh... ci siamo capiti.
La sfida ha inizio.

Ora dovresti stampare questa pagina.

Sappi che **stampandola presterai automaticamente il seguente giuramento** (se non hai ancora un cane sei autorizzato a usarne uno immaginario):

> *Giuro che userò questa pagina per dare un voto a tutti gli argomenti della Guida.*
> *Giuro che assegnerò il voto "la sapeva anche il mio cane" solo ed esclusivamente a cose che io e il mio cane già sapevamo e che uno di noi due fa già abitualmente.*
> *Giuro che assegnerò il voto "vabbè questa non è male" solo a cose che ho capito di dover fare ma che poi non farò ma in compenso avrò dei sensi di colpa.*
> *Giuro che assegnerò il massimo voto solo a cose che mi impegno a fare sul serio.*
> *Questo io stampo e giuro.*

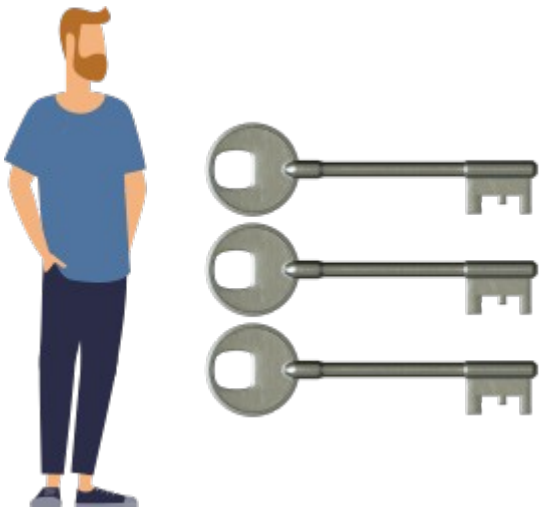
Le 7 brutte abitudini	Il tuo voto sulla soluzione proposta		
	La sapeva anche il mio cane	**Vabbè questa non è male**	**Ok, lo farò**
1: usare la stessa password su siti diversi			
2: conservare le password dove capita			
3: digitare la password del bancomat senza coprire mano e tastierino			
4: non sfruttare l'autenticazione a due fattori nella posta elettronica			
5: non svuotare mai la casella di posta elettronica			
6: rispondere in modo banale alle Domande di Sicurezza			
7: non proteggere i messaggi di conferma delle transazioni			

Premessa: chi è l’Uomo Incappucciato

Quando i media parlano di hacker e truffe informatiche usano spesso l’immagine di un losco figuro con il cappuccio della felpa calato sulla testa e il viso in ombra.

A forza di vederlo ho cominciato a pensare a lui come all'**Uomo Incappucciato** e voglio avvertirti che lo incontrerai spesso anche in questa piccola guida, dato che deciso di considerarlo una sorta di archetipo rappresentativo del Pericolo Informatico. Insomma è tutta colpa sua.

Brutta Abitudine 1: usare la stessa password su siti diversi



Consideriamo due qualsiasi servizi online come ad esempio Facebook e Linkedin, che forse già utilizzi.

Quando hai registrato il tuo account personale su questi servizi ti è stato chiesto di scegliere un *nome-utente* che fosse diverso da quello di qualsiasi altro utente già registrato, e di decidere una qualsiasi *password*.

All'inizio la maggior parte dei servizi online permetteva di scegliere un nome-utente di fantasia. In questo modo però il processo di registrazione diventava molto più lento perché spesso i nomi desiderati erano già in uso e le persone dovevano fare diversi tentativi prima di trovarne uno libero (e come se non bastasse dopo qualche tempo tendevano a dimenticarlo).

Oggi la maggior parte dei servizi online chiede ai propri utenti di usare come *nome-utente* il proprio indirizzo di posta elettronica, perché non esistono al mondo due persone che ne abbiano uno uguale ed è più difficile che l'utente lo dimentichi.

E qui iniziano i problemi: l'indirizzo email è un dato pubblico e non è difficile da scoprire, perciò **quello che separa realmente** il tuo account Facebook dal tuo account Linkedin **è solo la password**.

Perbacco, e se la password fosse la stessa? Oh, beh…

Facciamo finta che la password della tua pagina Facebook sia **dadada** e poniamo che un **Uomo Incappucciato** la scopra. La sua prossima mossa sarà quella di provare quella

stessa password sui più diffusi servizi online di qualsiasi genere: social, ecommerce, gestori di posta elettronica, fornitori di hosting, aste online e così via.

Se stai usando la stessa password su tutti i tuoi account, l'Uomo Incappucciato prenderà in pochi minuti il controllo della tua intera vita digitale.

Tutto questo succede più spesso di quanto immagini. E' successo anche al buon Mark Zuckerberg che per chi non lo sapesse è l'ideatore di Facebook, nonché uno degli uomini più ricchi del pianeta. E si, la sua password era veramente *dadada*.

Se un Uomo Incappucciato riuscisse a prendere il controllo dei tuoi social, lo userà per contattare amici e conoscenti a tuo nome per tentare diversi tipi di truffe online (io ne ho identificati 11 tipi diversi e te ne parlerò nella guida completa). Oppure potrebbe chiederti un riscatto per la loro restituzione.
Tutto questo si chiama **furto d'identità** ed avviene più spesso di quanto immagini.

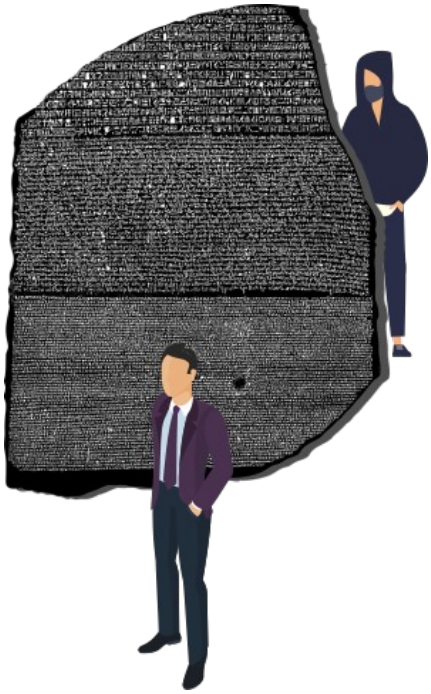
Se un Uomo Incappucciato riuscisse invece a prendere il controllo della tua casella di posta elettronica le conseguenze sarebbero ancora peggiori, ma forse non immagini ancora quanto. Te lo spiegherò meglio in uno dei prossimi capitoli. Per ora torniamo a parlare di password.

La soluzione a questo problema è semplice: **modifica le password che usi attualmente in modo tale che siano tutte diverse**.

Se ora stai chiedendo: **ma poi come farò a ricordarle tutte?** Ebbene, lo scoprirai nel prossimo capitolo.

Ora però è il momento del voto.

Brutta Abitudine 2: conservare le password dove capita



Nella vita digitale di chiunque le password si moltiplicano come conigli e con il tempo memorizzarle tutte diventa sempre più difficile. Per questo l'umano medio cercherà immediatamente strategie più comode. Tra cui:

- tatuarsi le password con l'henné in punti intimi del proprio corpo;
- scriverle su un post-it attaccato all'angolo inferiore sinistro del monitor;
- scriverle in una nota sul computer o nello smartphone, se il monitor è già pieno di post-it;
- scriverle in un'agenda cartacea;
- **usare un password-manager.**

E si, la soluzione corretta era l'ultima ma tu l'hai capito solo perché era in neretto perciò non è il caso di vantarsene. E dimentica il tatuaggio.
Dimentica anche i post-it e le note, per piacere. Tutte le volte che qualcuno scrive una password su un post-it o in un file di testo, da qualche parte nel mondo un informatico si accascia al suolo e muore. E ci crederesti che esistono in commercio delle agendine fatte apposta per conservare le password, con le pagine piene di diciture del tipo *sito web, username, password e note* già belle e pronte? Simpatiche, vero? Beh, dimentica anche

quelle. Potresti perderle o potrebbero esserti rubate e finiresti solo per facilitare il lavoro dell'Uomo Incappucciato.

Perciò per memorizzare le tue password puoi utilizzare un **Password Manager**. Urrah! Ma di cosa si tratta?

Un Password Manager è un software in grado di archiviare in modo sicuro e crittografato tutte le tue credenziali e gli eventuali dati associati ad esse, come username, password, indirizzi web, note, ecc... Questi software sono disponibili sia per computer che sotto forma di app per smartphone.

L'accesso ai dati memorizzati nel Password Manager è protetto da una password (che da ora chiameremo Master-Password) che è l'unica che non dovrai mai dimenticare.
Se la Master-Password viene persa non ci sarà più nessun modo per poter accedere all'archivio perché i Password Manager degni di questo nome **non prevedono** una funzione di recupero password.

I buoni Password Manager salvano l'archivio "offline" in un singolo file crittografato di cui dovrai fare diverse copie di backup, perché perdendo il file perderesti tutte le tue password.

Ultimamente vanno molto di moda i Password Manager "**online**" che ti **sconsiglio fortemente** di utilizzare. Salvare le tue password online è un rischio che non hai alcun bisogno di correre: gli archivi online delle password sono il bersaglio ideale di tutti gli Uomini Incappucciati del mondo.

Personalmente KeePassXC https://keepassxc.org un software Open Source gratuito disponibile per Windows, Mac e Linux, in grado di salvare le password offline sul mio computer, all'interno di un unico file crittografato.
Invece per il mio smartphone ho scelto ma preferito **non** creare alcun account e **non** attivare le opzioni di salvataggio online, in modo tale che le password siano conservate offline, ossia solo nel mio smartphone (il Password Manager del produttore di antivirus Avast https://www.avast.com ma preferito **non** creare alcun account e **non** attivare le opzioni di salvataggio online, in modo tale che le password siano conservate offline, ossia solo nel mio smartphone (e ovviamente in forma crittografata).

Prima di lanciarti su internet, ricordati che ora è il momento del voto.

Brutta Abitudine 3: digitare la password del bancomat senza coprire la mano e il tastierino

Si, il PIN del bancomat è una password ed è anche una delle peggiori perché:

- è corta
- è composta solo di numeri
- si utilizza in pubblico
- non viene mai cambiata

La prossima volta che sei in fila alla cassa del supermercato, guarda il modo in cui le persone utilizzano il bancomat. La maggior parte di loro digita il PIN completamente allo scoperto, con il tastierino in piena vista e l'indice della mano ben visibile.

L'hai fatto anche tu, moltissime volte. E proprio dietro di te c'era un uomo con la felpa del cappuccio calata e il viso in ombra. Era **l'Uomo Incappucciato** e ora anche lui conosce il tuo PIN. Adesso però non ci pensare.

I tastierini dei POS di pagamento sono tutti uguali e hanno uno schema che conosci benissimo. E' lo stesso delle calcolatrici o di certe tastiere per computer. Se non ne hai una sottomano ti basterà ricopiare questo schema su un foglio:

7	8	9
4	5	6
1	2	3
	0	

Ecco una semplice tecnica che avresti dovuto usare per digitare il tuo PIN in pubblico:

- Posiziona indice, medio e anulare rispettivamente sui numeri 4,5,6
- Copri la mano e il tastierino con l'altra mano, per nascondere tutte le operazioni che seguono.
- Ora digita il tuo PIN usando il dito che si trova già sul numero giusto. Se i numeri da digitare sono su una altra fila, sposta tutte e tre le dita sulla fila giusta. Continua così fino a digitare l'intero PIN.

Se vuoi complicare ulteriormente le cose all'Uomo Incappucciato, puoi divertirti a spostare per qualche istante le tue dita anche su file di numeri che in quel momento non ti servono. Visto che non hai più bisogno di guardare il tastierino, potresti anche controllare le persone che hai intorno. Potresti persino fare nuove amicizie.

Tutto chiaro? E' un abitudine molto semplice da prendere e **impedirà a chiunque di capire cosa stai digitando**. Potrebbe impedirti di essere scippato dopo l'uscita del supermercato dall'Uomo Incappucciato. Dico sul serio. Prova a fare una semplice ricerca su Google News e scoprirai che le cronache locali sono piene di storie di persone scippate all'uscita di un negozio, subito dopo aver usato in pubblico il proprio bancomat.

Questa tecnica ti proteggerà anche dagli Uomini Incappucciati particolarmente pigri, che hanno ideato un modo per derubarti rimanendo comodamente sdraiati sul proprio divano. La loro truffa funziona così. I ladri visitano nella notte un negozio, compiendo quella che sembra solo una piccola rapina. All'insaputa dei proprietari nel negozio viene nascosta una microtelecamera puntata sul tastierino del lettore, mentre un piccolo circuito detto "skimmer" viene invece nascosto nella fessura in cui si inserisce la carta.
La microcamera ha il compito di riprendere il PIN, mentre lo skimmer legge le informazioni memorizzate nella carta. Il vero furto avverrà quindi a mesi di distanza dal primo, quando il truffatore avrà raccolto le informazioni necessarie a clonare abbastanza carte.
E' così che l'Uomo Incappucciato ha comprato il suo bel divano.

E' il momento del voto. Sai cosa fare.

Brutta Abitudine 4: non sfruttare l'autenticazione a 2 fattori nella posta elettronica

Subire il furto della propria casella di posta elettronica è un problema grave perché da quel momento Uomo Incappucciato potrebbe sfruttarla per commettere truffe e raggiri a tuo nome. Nel prossimo capitolo di spiegherò in che modo potrebbe riuscirci, ora voglio spiegarti come potresti aumentare il tuo livello di sicurezza per prevenire il furto.

Per poter rubare la tua casella di posta, l'Uomo Incappucciato deve riuscire a indovinare le tue credenziali. Se la tua password è *batman* forse c'è già riuscito, ma anche le password più complesse possono essere rubate. Cosa dovresti fare allora?

La soluzione si chiama **autenticazione a due fattori**, ma cosa si intende per fattori?

Il **primo fattore** è **qualcosa che conosci.**
Invece il **secondo fattore** è **qualcosa che possiedi**.

Nel processo di autenticazione **a un solo fattore**, l'unico elemento necessario per effettuare il login è la tua password. Che sicuramente conosci a memoria e che sicuramente non è scritta su un file "password.txt" in bella mostra sulla scrivania di Windows o nell'app note dello smartphone. O almeno spero.

Invece il **processo di autenticazione a due fattori** è basato sia sulla *conoscenza* di una password che sul *possesso* di qualcosa. Che potrebbe essere sia un generatore di password fisico (spesso chiamato "token" o "chiavetta") che una semplice app (spesso chiamata "token virtuale") installata sul tuo smartphone. Che sicuramente è protetto da una password d'accesso diversa da 12345. O almeno spero.

L’autenticazione a due fattori ha lo svantaggio di essere scomoda, dato che ci costringe a utilizzare due password conservate in due modi diversi ma in compenso è maggiormente sicura. Perché l’Uomo Incappucciato, per riuscire a entrare sul nostro account, dovrebbe riuscire a scoprire la nostra password e contemporaneamente a rubare il nostro generatore di password (fisico o virtuale che sia).

Se hai un conto corrente gestibile online, sicuramente stai già utilizzando l’autenticazione a due fattori. Perché allora non estenderla anche alla tua posta elettronica?

Forse ti interesserà sapere che i principali gestori di posta elettronica, tra cui Google e Microsoft offrono da tempo e gratuitamente un servizio di autenticazione a due fattori, fantasiosamente e rispettivamente chiamato “Google Authenticator” e “Microsoft Authenticator”. Malgrado i loro servizi siano gratuiti, le loro statistiche dicono che la stragrande maggioranza degli utenti trova scomodi questi servizi e che per questo NON li utilizza.

Le mie personali statistiche dicono che tu **non seguirai** questo consiglio **ma in compenso ti sentirai in colpa per non averlo fatto**. Perciò ora hai l’occasione di stupirmi.

Ora pensa bene all’Uomo Incappucciato e poi dai un voto a questo argomento.

Brutta Abitudine 5: non svuotare mai la casella di posta elettronica

Capisco che per alcuni sarà un brutto colpo ma devo dirlo: **le caselle di posta hanno una capienza limitata** e ogni tanto andrebbero svuotate.

In genere ce ne ricordiamo ogni 2 o 3 anni, più o meno quando ci ricordiamo di spolverare dietro il mobile grosso del salotto. Forse dovresti mettere un post-it dietro quel mobile per ricordarti di pulire anche la tua casella di posta. Fammi sapere se lo farai davvero.

Nel nostro caso, svuotare periodicamente la casella della posta elettronica non è solo una questione di praticità ma anche di prudenza.

Ecco un piccolo elenco di alcune delle cose che probabilmente giacciono nella tua casella di posta:

- quel documento che hai spedito una volta, insieme a una fotocopia della tua carta d'identità creata con lo scanner e digitalizzata in un file;
- le bollette delle utenze di casa e del cellulare;
- le tracce digitali di tutti i servizi online che utilizzi;
- gli estratti conto bancari e la pubblicità della tua banca;
- certi dati che preferiresti mantenere riservati;
- altre cose importanti che hai spedito alcuni anni fa e di cui non ricordi assolutamente niente (si, è un colpo basso).

Hai mai sentito parlare di **furto d'identità**?

Funziona così: supponiamo che un Uomo Incappucciato riesca ad accedere alla tua casella di posta. Rovistando nelle tue email, scoprirà ben presto un mucchio di cose su di te, come ad esempio: nome, cognome, luogo e data di nascita, residenza, coordinate bancarie, documenti di identificazione, professione, ecc… Tutte queste **informazioni**, unite alle **copie dei tuoi documenti** e al **controllo della tua posta**, lo renderanno molto credibile quando farà finta di essere te**,** e gli permetteranno di fare **COSE BRUTTE** a tuo nome. Cose che vanno dall'attivazione di servizi, ai noleggi di merce, ai prestiti o alle truffe nei confronti di amici e partenti. Il tutto a tuo nome.

Inoltre quasi tutti i servizi online offrono una funzione di "recupero password" per permettere a chi ha dimenticato le proprie credenziali di impostare una nuova password d'accesso.

Di solito questa procedura si attiva con un semplice click sulla classica domanda "Hai dimenticato la tua password?" spesso riportata sullo stesso modulo con cui effettui il login. Con un semplice clic ti verrà inviata un'email con le indicazioni per impostare la tua nuova password e il problema sarà risolto.

Questo però significa che chiunque abbia il controllo della tua casella postale avrà la possibilità di **modificare le password di tutti i tuoi servizi online, ottenendone il pieno controllo**.

Questo è il furto d'identità, baby.

Alcuni Uomini Incappucciati particolarmente pigri, si limitano a chiedere un riscatto per la restituzione delle proprietà digitali rubate. Con un piccolo versamento su una carta di pagamento potresti riavere tutto. Forse. Sei pronto a fidarti di loro? Io non credo.

Per prevenire il furto di un account potresti deciderti ad attivare l'autenticazione a due fattori di cui ti ho parlato nel capitolo precedente.

Invece per ridurre i danni di un eventuale furto della tua casella di posta **ti basterà diminuire la quantità di vecchie email che ti ostini a conservare senza una vera ragione**.

Anche una casella capiente come Gmail prima o poi sarà piena. Perché non fare pulizia oggi stesso?

Questo suggerimento vale perlomeno un "vabbè questa non è male". Ora tocca a te.

Brutta Abitudine 6: rispondere in modo banale alle domande di sicurezza

Molte banche obbligano i propri clienti a impostare la procedura delle Domande di Sicurezza.

Il funzionamento è semplice: inizialmente al cliente viene chiesto di fornire la risposta a una certa domanda. Se un giorno il cliente dovesse dimenticare la propria password di accesso, potrà dimostrare la propria identità rispondendo a quella stessa domanda. Se la risposta sarà corretta, il sistema gli darà nuovamente accesso e gli permetterà di impostare una nuova password al posto di quella dimenticata.

Questa procedura è sicuramente più sicura di quella adottata da molti servizi online, che prevedono unicamente che l'utente fornisca l'indirizzo email associato al proprio account, per poter ricevere per posta le indicazioni per impostare una nuova password.

La procedura delle Domande di Sicurezza ha però un problema: quasi sempre il cliente non può modificare la domanda, ma solo fornire una risposta a una o più delle domande preparate dal sistema e come se non bastasse queste domande regolarmente molto banali.

Se fossero del tipo: "qual'è l'equazione differenziale di terzo ordine più affascinante che tu conosca?" saremmo forse portati a dare risposte più articolate, piene di strani versi e punti interrogativi. E invece non è così.

Tipicamente, le domande sono del tipo:

- il tuo primo lavoro;
- il nome del tuo primo animale domestico;
- il nome della tua scuola elementare;
- la tua città preferita.

Queste domande sono così orribilmente banali che la maggior parte delle persone tende a fornire risposte altrettanto banali.

Mi spiego. La risposta a una domanda banale del tipo: "Come si chiama il tuo cane?" potrebbe essere: "Dako"

Oppure potrebbe essere: “nonvuolechesisappiaperchéèuncanedaguardia!”

La prima delle risposte potrebbe essere facilmente indovinata dai tuoi amici, dagli amici degli amici, dal tuo cane e da chiunque altro ti segua su Facebook. Sei pronto a fidarti completamente di tutti loro? Ti do un indizio: puoi fidarti completamente solo del tuo cane.
Invece la seconda delle risposte non sarebbe facile da indovinare nemmeno per il tuo cane perciò ora sapete entrambi cosa fare.

Adesso è di nuovo l’ora del voto.

Brutta Abitudine 7: non proteggere i messaggi di conferma delle transazioni

Se hai un conto corrente gestibile online, sai anche cosa sono i messaggi per la conferma delle transazioni bancarie. Parlo proprio di quei messaggi con cui una banca invia un codice monouso con cui puoi confermare la transazione bancaria che hai appena effettuato con il tuo computer.

Questi messaggi di conferma possono arrivare **sia sotto forma di notifica smartphone che come semplici sms** (a seconda del circuito bancario).

Il problema è che molto spesso questi messaggi sono visibili anche se lo smartphone è bloccato (!!!).

Finché ad essere visibili sono solo le notifiche di WhatsApp o quelle di Facebook poco male. Anzi la tua fidanzata\o lo apprezza molto. E così che ti tiene d'occhio da anni. Ma se anche i messaggi bancari sono potenzialmente leggibili da chiunque riesca a entrare in possesso del tuo smartphone, allora una delle tue linee di difesa è appena caduta.

Se desideri aumentare la sicurezza delle tue transazioni bancarie, ti invito a smanettare nella configurazione del tuo smartphone per fare i modo che questi messaggi siano visibili solo a smartphone sbloccato. Non posso illustrarti il procedimento perché varia a seconda del sistema operativo dello smartphone, ma sappi che questa precauzione serve a proteggere maggiormente il tuo denaro e che dovresti davvero attuarla.

Ora però dovresti mettere un voto a questo suggerimento. Così, tanto per ricordartelo.

Conclusioni e note folcloristiche

Sei giunto alla fine di questa piccola Guida e hai scoperto 7 brutte abitudini che forse riguardano anche te. Se è così, dovresti davvero valutare con attenzione le soluzioni che ti ho suggerito, perché **collezionare buoni consigli non ti aiuterà, metterli in pratica invece si**.

Per concludere voglio raccontarti una storia.

La dedico a tutte le guide alla sicurezza che ritengono che si possa capire se un email è falsa "*controllando con attenzione l'ortografia e l'aspetto grafico ed evitare assolutamente di usare i link contenuti in quelle* ***scritte male***".

Un giorno chiesi a un [NOTOGESTORE] di cui non faccio il nome, la modifica dell'iban su cui è domiciliato il pagamento delle mie bollette.

Alcuni giorni dopo, controllando periodicamente il mio account personale sul sito di [NOTOGESTORE] scoprii per caso che la modifica era stata effettuata.

Due giorni dopo ricevetti un'email con cui [NOTOGESTORE] mi confermava la suddetta modifica. Il fatto che l'avviso fosse arrivato con ben due giorni di ritardo rispetto all'aggiornamento delle informazioni era già, da un punto di vista informatico, alquanto inquietante. Ma sorvoliamo.
Dunque "*controllando con attenzione"* l'email di [NOTOGESTORE], mi accorsi che:

- l'immagine del logo del gestore era **sgranata e in bassa risoluzione**.
  A giudicare dalle linee di contorno era stata palesemente ritagliata con le forbici da qualche stampa cartacea e quindi passata allo scanner, solo per poterla trasformare in un file immagine e quindi incorporare nell'email.
- nell'email era presente una **frase sgrammaticata**.
- Inoltre nell'email **mancavano alcuni piccoli dettagli**, come ad esempio il mio indirizzo, il codice della fornitura e diverse date.
  In effetti i campi che avrebbero dovuto ospitare queste informazioni erano tristemente vuoti, tanto che alcune frasi si interrompevano nel nulla. Come ad esempio quella che mi informava acutamente che il mio nuovo iban sarebbe stato "utilizzato per il pagamento delle bollette emesse dopo il ."

Nell'email erano presenti anche alcuni link alla mia Area Personale sul sito di [NOTOGESTORE]. A questo punto avrei dovuto "*evitare assolutamente di usare i link*" in questo messaggio così orribilmente sospetto.

Disgraziatamente per tutti noi italiani l'email era autentica.

Anzi con il tempo ho scoperto che il livello di qualità delle comunicazioni ufficiali di [NOTOGESTORE] è talmente basso che mi sento di coniare la seguente regola aurea, di cui mi assumo la piena responsabilità: "*Nel caso di [NOTOGESTORE], controllate con attenzione l'ortografia e l'aspetto grafico, ed evitate assolutamente di usare i link delle email scritte* ***troppo bene***."

In conclusione...

Capire se un messaggio o un link siano realmente falsi è importante. Anzi la Sicurezza Informatica è un tema importate e **tu dovresti approfondirla**.
Io invece dovrei decidermi a cambiare gestore.

Tornerò su questo ed altri argomenti nel mio libro sulla Sicurezza Informatica Pratica.

E ora sipario.

Note sull'autore e saluti. Proprio come si usava una volta.

Sono Luca Giuliani, dottore in Informatica e amministratore di Seventylab. Ho deciso di promuovere la cultura della Sicurezza Informatica dopo aver visto amici e parenti diventare vittime di truffe online, e dopo aver rischiato di subirne una io stesso.

Questa piccola guida è parte di una guida molto più completa dal titolo "**Sicurezza Informatica Pratica:** *Scopri come proteggerti da frodi, phishing, ransomware, hacker e ladri d'identità anche se non sei un tecnico".*

E' in vendita su Amazon a questo indirizzo:

https://www.amazon.it/dp/B09HSLYLTB

Puoi arrivarci anche con il qrcode che segue. Finirai sulla stessa pagina di prima ma in modo molto più elegante.

Potresti anche contattarmi per farmi sapere che punteggi hai ottenuto in questa piccola sfida o per farmi domande sugli argomenti della Guida.
Sul mio sito aziendale https://www.seventylab.it troverai un comodo modulo di contatto che ho forgiato con le mie mani proprio a questo scopo, e anche altre piccole guide come questa.

Un saluto,
Luca