MEF Dipartimento del Tesoro

Newsletter

Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

UFFICIO VI

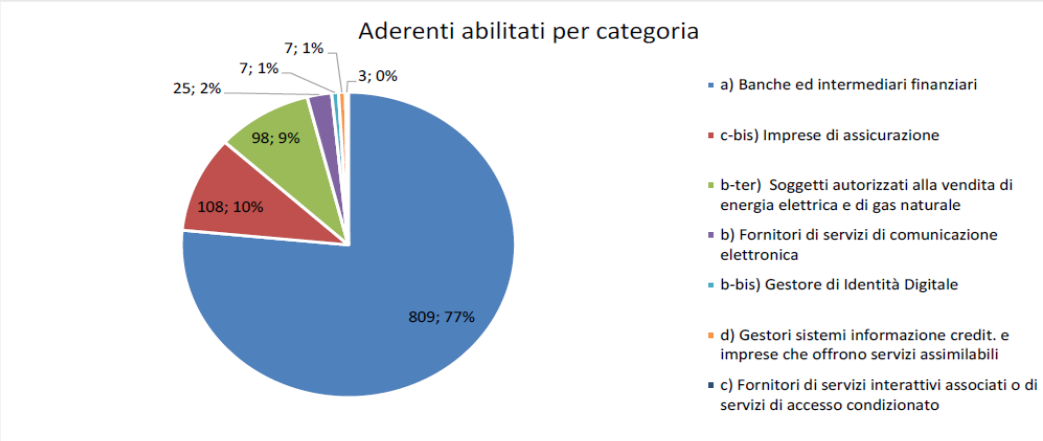
Newsletter n° 19 - Novembre 2018

In questo numero:

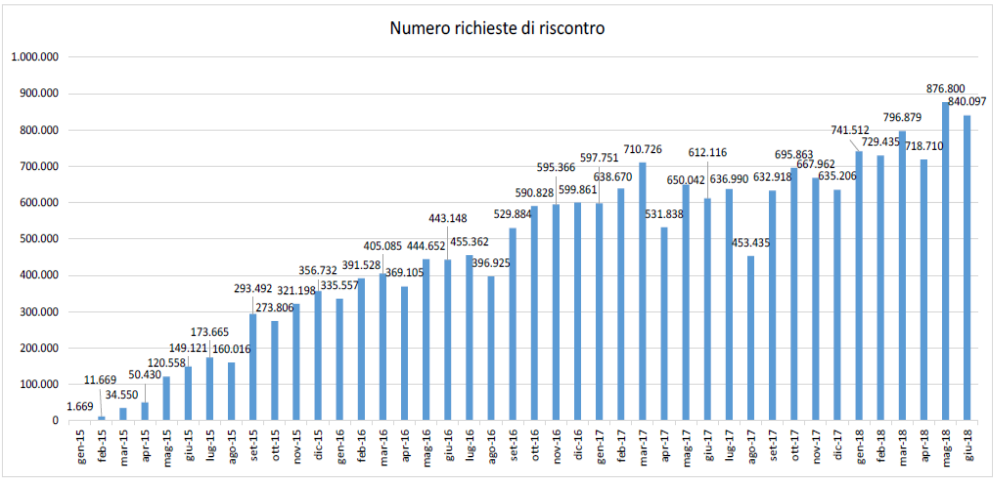
FURTO DI IDENTITÀ: I NUMERI DI SCIPAFI

In continuo aumento interrogazioni e numero di aderenti nel primo semestre 2018

Al 30 giugno 2018 il numero complessivo di aderenti al Sistema SCIPAFI di lotta al furto di identità risulta pari a 1.057 di cui 7 indiretti (1.017 a giugno 2017, di cui 7 indiretti).

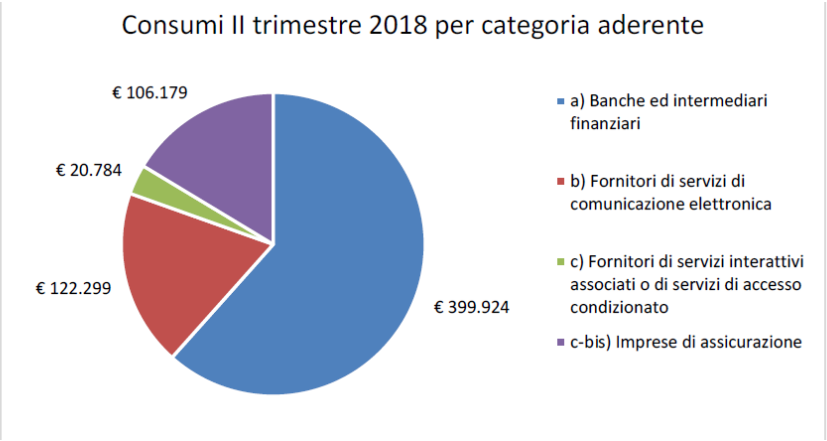


Dal 19 gennaio 2015 – data di inizio dell'operatività – a fine giugno 2018 il Sistema ha registrato un totale di 19.671.157 riscontri.



Nel mese di giugno 2018 sono stati effettuati dagli aderenti 840.097 riscontri, in crescita del 37% rispetto a quanto registrato a giugno 2017. Tale crescita è dovuta essenzialmente all'aumento dei riscontri effettuati dagli aderenti già attivi nel 2017. Relativamente alle diverse categorie di aderenti:

- *le Banche e gli Intermediari finanziari* rappresentano la categoria di aderenti che effettua globalmente il maggior numero di riscontri sul Sistema (59% su totale, ovvero 497.451 su 840.097). Si registra per questa categoria un tasso di crescita del numero di riscontri di giugno 2018 (497.451) rispetto a giugno 2017 (366.035) pari al 36%. Il dato di giugno conferma il trend positivo del numero di riscontri di Intesa San Paolo e Credito Emiliano, e l'intensificarsi dell'operatività sul Sistema per Unicredit e ING. Bank registrata a partire da gennaio 2018;
- i *Fornitori di servizi di comunicazione elettronica* effettuano il 17% dei riscontri totali (140.750 su 840.097), riducendo di 14 punti percentuali la loro quota sul totale rispetto a giugno 2017 (31%, ovvero 192.673 su 612.116); il dato di giugno 2018 conferma il trend negativo registrato a partire dalla seconda metà del 2017, imputabile principalmente alla fusione di Wind Telecomunicazioni e H3G in Wind Tre;
- le *Compagnie di assicurazione* passano da una quota del 6% sul totale di richieste di riscontro di giugno 2017 (36.112 su 612.116) al 17% di giugno 2018 (137.704 su 840.097). Per questa categoria si conferma sia il trend positivo del numero di riscontri effettuati da Genialloyd, che la recente operatività sul Sistema da parte di Allianz;
- i *Fornitori di servizi interattivi associati o di servizi di accesso condizionato* effettuano il 4% dei riscontri totali (34.786 su 840.097), quota superiore rispetto a giugno 2017 (3%, ovvero 17.296 su 612.116);
- i *Gestori di identità digitale* effettuano il 3% dei riscontri totali (28.466 su 840.097) e al 30 giugno 2018 il numero totale di riscontri registrati (123.835);
- le *Utilities di gas ed elettricità* effettuano una quantità di riscontri ancora trascurabile, per via della solo recente attivazione del processo di convenzionamento (12 dicembre 2017).



Per maggiori info:

http://www.dt.tesoro.it/it/attivita_istituzionali/antifrode_mezzi_pagamento/furto_identita/

CRIF, IN AUMENTO FRODI CREDITIZIE MEDIANTE FURTO IDENTITÀ

Perdita di 153 MLN nel 2017, vittime tra 41 e 50 anni, salgono giovani

Le frodi creditizie perpetrate mediante furto di identità continuano a crescere e a incidere pesantemente sul comparto del credito al consumo.

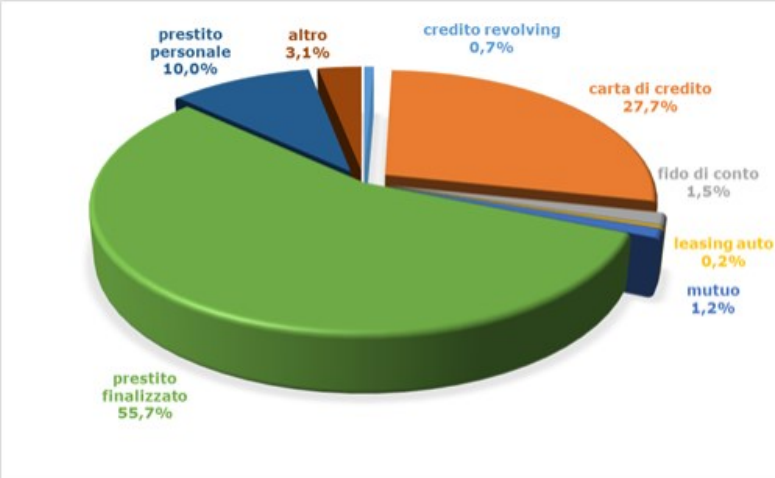
Le rilevazioni presentate nella 26^ edizione dell'Osservatorio CRIF - Mister Credit sui furti di identità e le Frodi Creditizie confermano, infatti, che nel 2017 i casi rilevati sono stati più di 26.600 per un importo medio pari a oltre 5.700 euro e una perdita economica complessivamente pari a circa 153 milioni di euro.

La distribuzione delle frodi per sesso evidenzia che la maggioranza delle vittime (il 57,8% del totale) sono ancora una volta uomini ma, rispetto all'anno precedente, si registra un cospicuo aumento delle vittime di sesso femminile (+18,1%).

Dato ancor più significativo emerge dall'osservazione della distribuzione delle frodi per età della vittima: se la classe in cui si concentra il maggior numero di casi rimane quella compresa tra i 41 e i 50 anni (con il 25% del totale), quella nella quale si rileva il maggior incremento rispetto alla precedente rilevazione è quella dei 18-30enni (+9,3%), che dimostrano di essere particolarmente esposti forse anche a causa della scarsa consapevolezza e di una eccessiva disinvoltura nell'utilizzo dei canali digitali (con la relativa disseminazione di informazioni personali sovente utilizzate dai criminali per ricostruire identità false). In crescita anche il peso degli over 60, che vedono un incremento del +7,1%.

Il prestito finalizzato, come già osservato anche negli anni scorsi, risulta ancora una volta essere la tipologia di finanziamento maggiormente esposta alle frodi, con una quota pari al 55,7% dei casi, seppur in calo rispetto all'anno precedente.

Al contempo si registra un significativo incremento delle frodi perpetrate sulle carte di credito, che arrivano a spiegare il 27,7% dei casi totali a fronte di una crescita che nel 2017 è stata pari addirittura al +49% rispetto all'anno precedente.

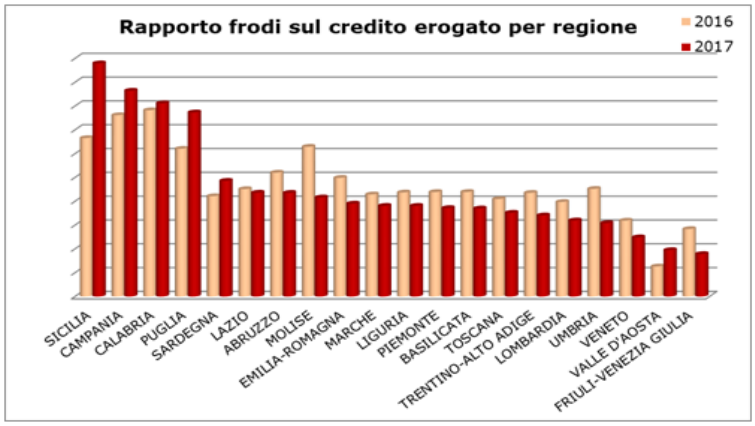


Fonte: Osservatorio CRIF – Mister Credit sui furti di identità e le frodi creditizie

La ripartizione percentuale delle frodi per regione di residenza dichiarata al

momento della richiesta del finanziamento vede al primo posto del ranking la Sicilia, con il 16% del totale, seguita dalla Campania, con il 15,9%.

Nella sostanza si tratta delle stesse regioni che occupavano i primi posti di questa



Fonte: Osservatorio CRIF – Mister Credit sui furti di identità e le frodi creditizie

poco invidiabile classifica anche nell'anno precedente ma con la novità della Sicilia che sorpassa la Campania in virtù di una significativa crescita dei casi rilevati.

Rapportando il numero di casi rispetto ai contratti di finanziamento alle famiglie erogati in regione, invece, la Calabria scala la classifica passando dalla ottava posizione alla terza. Nel complesso, ancora una volta la Sicilia e la Campania si confermano le regioni caratterizzate dalla maggiore incidenza del fenomeno, anche se alcune regioni più piccole, come il Molise e l'Abruzzo, spiccano nella classifica per una incidenza particolarmente elevata rispetto ai volumi di credito.

BCE: ECCO LE NUOVE BANCONOTE DA 100 E 200 EURO

Presentate a Francoforte, in circolazione dal 28 maggio

Il 17 Settembre la Banca centrale europea (BCE) ha presentato le nuove banconote da € 100 e € 200, che entreranno in circolazione il 28 maggio 2019. Dopo i € 5, € 10, € 20 e € 50, le banconote da € 100 e € 200 sono le ultime due denominazioni della serie Europa, e quindi segnano il suo completamento.

Le nuove banconote da € 100 e € 200 si avvalgono di nuove e innovative funzionalità di sicurezza. Proprio come le altre denominazioni, le nuove note sono facili da controllare quando si utilizza il metodo "feel, look and tilt". Nella parte superiore della striscia argentata un ologramma satellitare mostra piccoli simboli € che si muovono intorno al numero e diventano più chiari sotto la luce diretta. La striscia argentata mostra anche il ritratto di Europa, il motivo architettonico e un grande simbolo di €. Le nuove banconote da € 100 e € 200 presentano anche un numero smeraldo migliorato. Mentre il numero dello smeraldo stesso è presente su tutte le altre note della serie Europa, questa versione avanzata mostra anche i simboli € all'interno dei numeri.

Le nuove banconote da € 100 e € 200 sono di dimensioni diverse rispetto alle vecchie banconote da € 100 e € 200. Entrambe le denominazioni hanno ora la stessa altezza della banconota da € 50. Tuttavia, la loro lunghezza rimane invariata: più lunga è la nota, maggiore è il valore. Poiché le banconote da € 50, € 100 e € 200 ora hanno la stessa altezza, possono essere più facilmente gestite e lavorate da macchine. Inoltre si adatteranno meglio ai portafogli delle persone e dureranno più a lungo, poiché saranno soggetti a minore usura.

Oltre alle caratteristiche di sicurezza che si possono vedere ad occhio nudo, le banconote in euro contengono anche caratteristiche di sicurezza leggibili meccanicamente. Sulle nuove banconote da € 100 e € 200 queste funzionalità sono state migliorate e ne sono state aggiunte di nuove per consentire alle banconote di essere elaborate e autenticate rapidamente. Come ha sottolineato il membro del consiglio di amministrazione Yves Mersch nel suo discorso che svela le nuove banconote, con il passaggio ai nuovi € 100 e € 200 l'intera serie di banconote in euro continuerà a offrire una forte protezione contro la contraffazione. Ciò rende le banconote in euro ancora più sicure, ma anche più facili da controllare e gestire.

L'Eurosistema - la BCE e le 19 banche centrali nazionali dell'area dell'euro - sostiene i produttori e i proprietari di macchine per la gestione di banconote e dispositivi di autenticazione nella preparazione delle nuove banconote. Ciò include l'agevolazione della verifica delle attrezzature e la pubblicazione di un elenco di macchine per l'elaborazione di banconote che hanno dimostrato con successo che possono elaborare le nuove banconote della serie Europa.

Per saperne di più

https://www.ecb.europa.eu/euro/banknotes/html/index.en.html

BCE, MONITORAGGIO I SEMESTRE 2018 SU BANCONOTE SEQUESTRATE

Si riducono i sequestri, ritirati dalla circolazione 301 mila esemplari

Nella prima metà del 2018 le banconote in euro false ritirate dalla circolazione sono state circa 301.000, in calo del 17,1% rispetto alla seconda metà del 2017 e del 9,1% rispetto alla prima metà del 2017. Le probabilità di ricevere una banconota falsa sono veramente molto scarse. Il numero di falsi resta molto basso rispetto al totale dei biglietti autentici in circolazione, che mostrano un costante incremento sin dalla loro introduzione, registrando ritmi di crescita più elevati di quelli del PIL.

Nel 2017, ad esempio, il volume e il valore delle banconote in euro in circolazione sono aumentati rispettivamente di circa il 5,9% e il 4% .
La tavola seguente riporta i dati dei falsi per semestre:

Periodo	1° sem. 2015	2° sem. 2015	1° sem. 2016	2° sem. 2016	1° sem. 2017	2° sem. 2017	1° sem. 2018
N. di falsi	454.000	445.000	331.000	353.000	331.000	363.000	301.000

cui segue la ripartizione in base al taglio:

Taglio	€ 5	€ 10	€ 20	€ 50	€ 100	€ 200	€ 500
%	1,20%	1,90%	23,80%	59,30%	10,90%	0,80%	2,10%

Nella prima metà del 2018:

- i tagli da €20 e €50 hanno continuato a far registrare il numero più elevato di falsificazioni fra le banconote; nell'insieme questi due tagli rappresentano circa l'83% del totale dei falsi;
- la maggior parte delle banconote falsificate (88,8%) è stata rilevata in paesi dell'area dell'euro; circa il 10,3% dei falsi proviene dagli Stati membri dell'UE non appartenenti all'area dell'euro, mentre lo 0,9% da altre parti del mondo.

Fin dall'emissione della prima serie di banconote in euro, l'Eurosistema (costituito dalla Banca centrale europea e dalle banche centrali nazionali dei 19 paesi dell'area dell'euro) ha incoraggiato i cittadini ad avere un atteggiamento vigile quando ricevono una banconota.
È facile riconoscere i biglietti autentici con il metodo basato sulle tre parole chiave "toccare, guardare, muovere", illustrato nella sezione "The €uro" del sito Internet della BCE e nei siti delle banche centrali nazionali. Se una banconota appare sospetta, può essere subito confrontata con un'altra di autenticità comprovata. Se il sospetto di falsificazione trova quindi conferma, occorre contattare le forze dell'ordine o, a seconda della prassi vigente nel paese, la banca centrale nazionale o una banca commerciale. L'Eurosistema sostiene le forze dell'ordine nella lotta alla falsificazione di valuta.

L'Eurosistema svolge varie attività di comunicazione per aiutare i cittadini a riconoscere le falsificazioni e per assistere le categorie professionali che operano con il contante, affinché le apparecchiature di selezione, verifica e accettazione delle banconote riescano a individuare i falsi e a trattenerli in maniera affidabile.
L'Eurosistema ha il dovere di salvaguardare l'integrità dei biglietti in euro e di continuare ad affinare la tecnologia delle banconote. La seconda serie di banconote in euro, anche nota come "serie Europa", risulta ancor più sicura e contribuisce pertanto a preservare la fiducia dei cittadini nella loro moneta.

Per ulteriori approfondimenti:
https://www.ecb.europa.eu

INTERNET, QUALCHE PRECAUZIONE

Key Words contro le frodi dal sito web della Polizia Postale

Il New Hacker´s Dictionary di Eric S. Raymond definisce un hacker come qualcuno che ama esplorare le possibilità offerte da un sistema informativo e mettere alla prova le sue capacità, in contrapposizione con la maggior parte degli utenti che preferisce apprendere solo lo stretto indispensabile. Questo è, ovviamente, il concetto di hacker espresso con un valore positivo. Vi è tuttavia da segnalare che dell´intento puramente ludico che spingeva i primi hacker ad agire poco è rimasto. I sistemi informatici custodiscono, infatti, dati sempre più preziosi e la loro violazione arreca ormai danni notevoli ad aziende ed istituzioni pubbliche e governative. Vi è infine da segnalare che si usa distinguere tra la figura dell´hacker e quella del cracker. I cracker sono coloro che fanno attività di hacking a scopo di lucro. Entrambe le figure, per la legge italiana, sono punibili.

Utilizzare i firewall. I firewall sono degli strumenti, sia di tipo hardware che software, che permettono di vigilare sullo scambio di dati che intercorre tra il nostro pc o la nostra rete locale ed il mondo esterno. Essi sono programmabili con una serie di regole così da inibire, ad esempio, il traffico di dati proveniente dall'esterno e diretto verso alcune porte del nostro pc solitamente utilizzate per porre in essere intrusioni telematiche. Permettono inoltre la visualizzazione sul monitor dei tentativi di intrusione verificatisi, comprensive dell'indirizzo telematico utilizzato dall'autore di questi. In Rete possono essere facilmente reperiti numerosi software di tipo “firewall” gratuitamente.

Utilizzare un software di tipo antivirus e aggiornarlo regolarmente. Il virus informatico non é altro che un programma che ha la capacità di auto-replicarsi e, una volta scrittosi sui dischi, di effettuare una serie di operazioni sul pc ospitante più o meno dannose che vanno dalla visualizzazione sul video di un messaggio fino alla cifratura del contenuto del disco fisso, rendendolo così illeggibile.Considerato che ogni giorno vengono creati nuovi virus e che, con lo sviluppo della rete Internet, questi si diffondono con eccezionale rapidità, risulta fondamentale non solo installare sul proprio pc un buon antivirus, ma anche aggiornarlo frequentemente.

Non aprire gli allegati ai messaggi di posta elettronica se non dopo averli esaminati con un antivirus. Il principale veicolo di diffusione dei virus é la posta elettronica. Per essere più precisi dovremmo dire i messaggi allegati ai messaggi di posta elettronica. Infatti, un virus può trasmettersi unicamente tramite file eseguibili (programmi con estensione exe,com,drv e dll) o contenenti una parte di codice che viene eseguita (es. documenti in formato word che contengono macro). Non é quindi possibile “infettare” il nostro computer leggendo semplicemente il testo di una e-mail, ma é necessario eseguire il file infetto

allegato alle e-mail che riceviamo. Va inoltre precisato che l'aprire un file allegato ad un messaggio di posta elettronica anche se si conosce il mittente non é di per se sufficiente a metterci al riparo dal contagio, poiché alcuni tipi di virus prelevano dal pc infettato gli indirizzi di posta elettronica registrati nel client di posta ed inviano a questi una mail a nostro nome contenente in allegato il virus. I destinatari di tali messaggi potrebbero aprirli senza utilizzare alcuna precauzione, forti della sicurezza che gli deriva dal conoscere il mittente. E' il modo con cui il virus "Melissa" ha contagiato milioni di computer! D'altro canto non possiamo neanche cestinare tutti gli allegati che riceviamo presumendo che siano infetti. Vale quindi sicuramente la pena di perdere qualche secondo per salvare l'allegato in un supporto di memoria, per poi analizzarlo con un antivirus. Va infine segnalato che vi sono alcuni programmi che, una volta eseguiti sul vostro pc, ne permettono il controllo da una postazione remota. Anche questi possono essere contenuti nei file allegati ai messaggi di posta elettronica e possono essere segnalati da un buon antivirus.

Non eseguire programmi prima di averli analizzati con un antivirus. Abbiamo visto che cos'é un virus e come si trasmette. Ciò vale, ovviamente, non solo per gli allegati dei messaggi di posta elettronica ma anche per tutti quei file eseguibili contenuti in cd rom o dispositivi USB. É quindi opportuno, in ogni caso, analizzare tali file con un antivirus prima di eseguirli.

Effettuare copie di backup. Gli antivirus riducono drasticamente i rischi di contagio ma bisogna anche tener presente che se un antivirus riconosce un virus é perché precedentemente c'é stata qualche vittima. Ciò significa che si potrebbe anche verificare il caso che il nostro antivirus, poiché non aggiornato o poiché deve analizzare un virus nuovissimo, non riconosca quel file come uno contenente un virus. In questo caso potremmo, a seguito del contagio, anche perdere i dati contenuti sul nostro disco fisso. In tale sventurato caso sarà di vitale importanza avere effettuato, nei giorni precedenti il disastroso evento, una copia di backup dei nostri dati.

Non fornire nelle chat i propri dati personali. Non cedere alla tentazione durante le conversazioni virtuali (chat) di fornire ad ignoti utenti i propri dati personali. Questo per un duplice motivo: non possiamo sapere chi c'é dall'altra parte della tastiera e i nostri dati potrebbero essere utilizzati come punto di partenza per ricavare le nostre password.

Scegliere una password efficace e non comunicarla a nessuno. Per creare una password efficace bisogna seguire i seguenti accorgimenti. La password deve essere della lunghezza massima permessa dal sistema ed almeno di otto caratteri. Infatti, i programmi utilizzati per forzare le password richiedono, per riuscire nell'opera, un tempo direttamente proporzionale alla lunghezza delle password da violare. La password non deve essere un termine di senso compiuto contenuto in un dizionario poiché esistono dei programmi che, supportati dalla potenza di calcolo degli elaboratori, provano tutte le parole contenute in un dizionario. É preferibile che la password non contenga esclusivamente lettere minuscole o maiuscole ma che le contenga entrambe, possibilmente unitamente a simboli alfanumerici come, ad esempio, asterischi e trattini. In questo modo, i programmi di forzatura delle password dovranno provare tutte le combinazioni di caratteri

possibili richiedendo così, nel caso venga adottata una password lunga, molto tempo per trovarla. La password non deve essere in alcun modo collegata alla vita privata del titolare ed a ciò che lo circonda. Non deve quindi essere costituita dalla targa della sua auto, dalla sua squadra del cuore, dal suo nome, dalla sua data di nascita etc. Questo perché i primi tentativi fatti da chi vorrà indovinare la password saranno legati alla vita privata del titolare della stessa. La password non deve essere scritta da nessuna parte. Per creare una password che possa essere ricordata facilmente si può utilizzare la così detta "frase password" composta dalla prima lettera di ogni parola che compone una frase. É preferibile utilizzare una password diversa per ogni applicazione. Infatti, nel caso in cui fosse scoperta, i danni derivati sarebbero minori. La password di default, assegnata dai sistemi la prima volta che vengono utilizzati, deve essere sostituita subito. La password deve essere cambiata periodicamente.

Utilizzare, per le comunicazioni riservate, software di cifratura. Quando si inviano dati riservati é opportuno affidarsi ad un software di cifratura che permetta di criptare i messaggi da noi trasmessi. Questo perché, se anche il messaggio venisse intercettato, senza la chiave utilizzata per criptare il documento si avrebbero solo una serie di caratteri privi di alcun senso compiuto. Vi sono numerosi programmi che offrono questo tipo di protezione, prelevabili dalla rete Internet, disponibili gratuitamente.

Le considerazioni ed i consigli elencati in questo articolo sono sicuramente basici eppure, se ognuno di noi si attenesse a queste elementari “misure di sicurezza” nell’utilizzo e nell’interazione con la rete Internet, assisteremmo ad una drastica riduzione dei crimini informatici e soprattutto dei danni da essi arrecati.

Per maggiori info:

https://www.commissariatodips.it/approfondimenti.html

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI

Redazione: Dott. Augusto Santori
Funzionario Ufficio VI

Via XX Settembre, 97
00187 – Roma
Tel. 06 47610488
Web: http://www.dt.tesoro.it
E-mail: augusto.santori@mef.gov.it