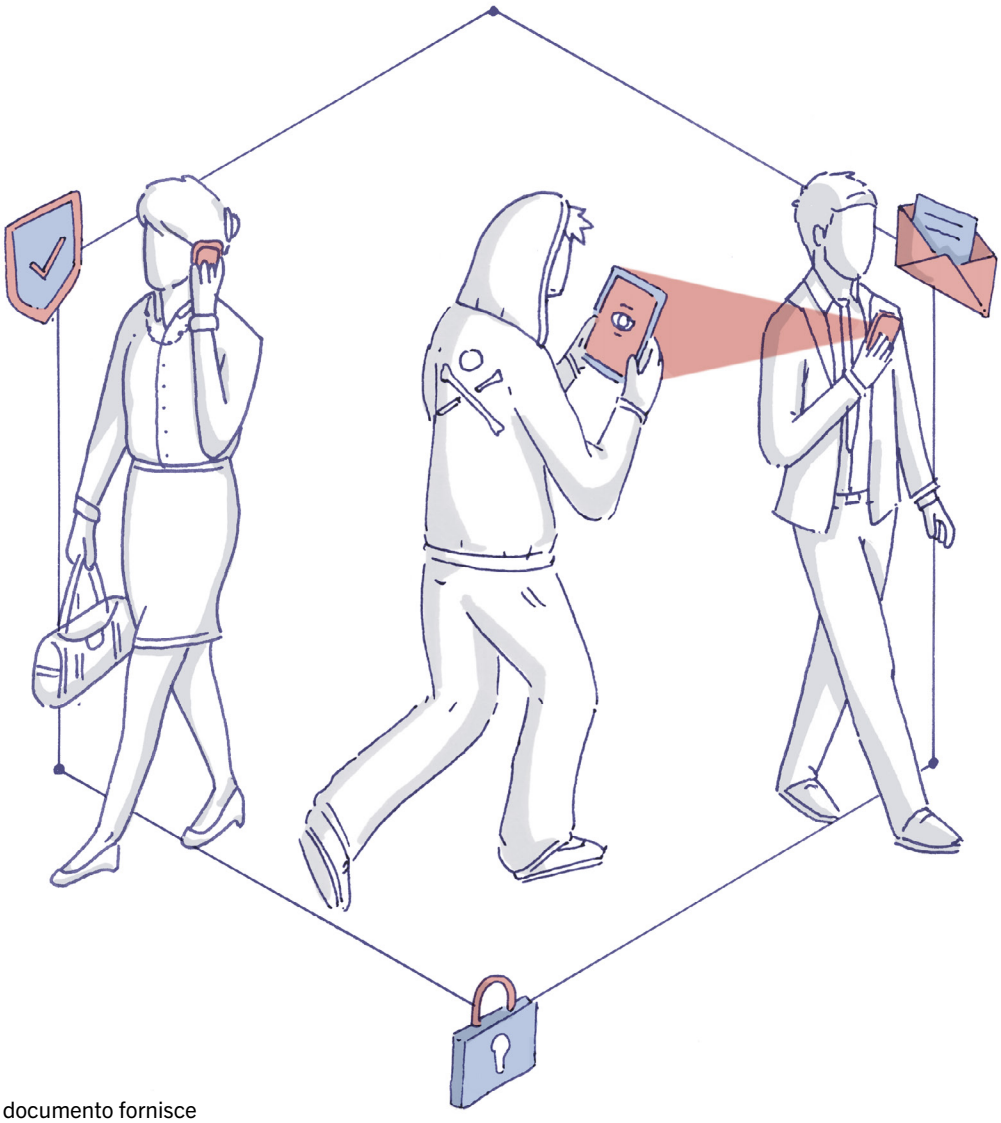
PICTET 1805

GENNAIO 2020

CYBERSICUREZZA

PROTEGGERSI DAI RISCHI DIGITALI



Il presente documento fornisce informazioni importanti riguardo ai rischi collegati alle comunicazioni digitali e propone misure facilmente applicabili per ridurli.

DATI PERSONALI: I RISCHI SONO IN FORTE AUMENTO

I dati personali sono divenuti una nuova forma di materia prima. Essi permettono di accedere a servizi gratuiti come social network, sistemi di messaggistica o reti wifi pubbliche, spesso senza che l'utilizzatore conosca le norme di sicurezza applicabili. Chi raccoglie i dati può sfruttarli commercialmente, sia in modo legale che illegale.

Bisogna pertanto essere particolarmente prudenti quando si comunicano informazioni personali. Le fughe di dati sono sempre più frequenti, anche quando ciò non è causato dal comportamento dell'utente. I giganti del web hanno mostrato la loro fragilità, come ad esempio Facebook (87 milioni di utilizzatori colpiti dallo scandalo Cambridge Analytica) e Google (52 milioni di persone coinvolte in una fuga di dati nel 2018).

L'obiettivo primario di Pictet è stabilire, in uno spirito di partnership, relazioni responsabili con i propri clienti. Teniamo ad assicurare la loro protezione e naturalmente ci preoccupiamo per i rischi collegati ai loro dati personali. È in quest'ottica che condividiamo le nostre raccomandazioni in materia di cybersicurezza.

Dati personali come identità, ubicazione o password possono facilmente cadere nelle mani di truffatori che se ne servono per accedere a un conto o ricattare le proprie vittime. Rispettando alcune semplici precauzioni è possibile ridurre considerevolmente tali rischi. Questo documento permette di rafforzare la sua sicurezza digitale (cfr. pagine 4-5) e di reagire in modo adeguato in caso di furto di dati (cfr. pagina 6). Le raccomandiamo di leggere attentamente questa pubblicazione e di conservarla in un luogo dove possa facilmente consultarla.

Gennaio 2020

COME OPERANO I PIRATI INFORMATICI?

Raccogliendo informazioni confidenziali, i cybercriminali possono accedere ai conti delle loro vittime o ricattarle.

I cybercriminali utilizzano tecniche sempre più ingegnose per appropriarsi dei dati personali. In alcuni casi per loro è sufficiente raccogliere informazioni che vengono rese pubbliche per negligenza o accidentalmente. In questa maniera, essi possono indovinare delle password, infiltrarsi nei sistemi informatici o ancora utilizzare indebitamente l'identità di altri.

Bisogna sapere che i truffatori utilizzano messaggi che fanno leva sull'emozione («il suo computer contiene un virus»), l'empatia («un amico si trova in una situazione difficile»), l'urgenza («richiesta di reazione immediata») o la promessa di guadagni («una opportunità da cogliere»).

Ecco qualche esempio di furto di dati o truffa:

1. ATTENZIONE AI DETTAGLI

Una e-mail proveniente da un mittente conosciuto invita l'utilizzatore ad andare su una copia contraffatta del sito Pictet, ospitata su un indirizzo simile all'originale, ad esempio picttet.com, pIctet.com o pic-tet.com. In questo modo, è possibile che la vittima arrivi a fornire informazioni che saranno poi utilizzate dai cybercriminali.

2. I DATI IN OSTAGGIO

L'utilizzatore riceve da parte di una persona la cui identità è stata usurpata un messaggio di posta elettronica contenente un allegato. L'apertura di questo allegato bloccherà il computer della vittima. A quel punto, un messaggio informa che il computer potrà essere sbloccato solo dopo il pagamento di un riscatto su un conto in cryptomoneta. Questa minaccia viene spesso menzionata dalla stampa con il termine «ransomware».

3. QUALCUNO CHE SI FINGE UN DIRIGENTE DELLA SOCIETÀ

Il contabile di una società riceve una chiamata da parte di un cybercriminale che finge di essere un suo superiore o un dirigente della società. Con il pretesto di una operazione urgente (acquisizione all'estero, controllo fiscale), il truffatore esige che gli vengano comunicate informazioni confidenziali.

RACCOMANDAZIONI IN MATERIA DI SICUREZZA

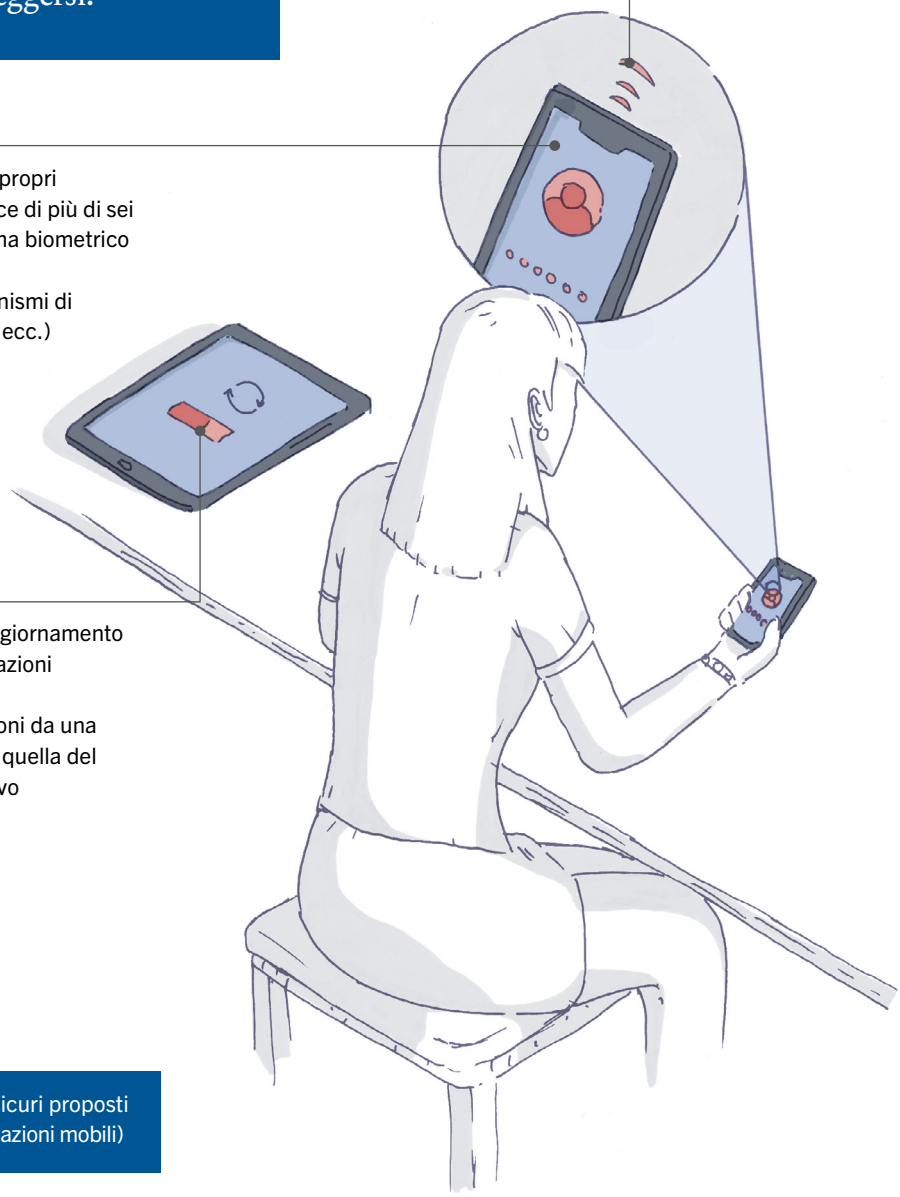
Vi sono diverse misure che permettono di evitare le fughe di dati e i rischi di truffa. Ecco alcune delle soluzioni per proteggersi.

Attivare le opzioni che permettono di resettare a distanza i dispositivi in caso di perdita o furto

Non conservare informazioni confidenziali nelle caselle di posta elettronica (password, transazioni finanziarie, ecc.)

Proteggere l'accesso ai propri apparecchi con un codice di più di sei caratteri o con un sistema biometrico

Non disattivare i meccanismi di protezione (codice PIN, ecc.)



Attivare le funzioni di aggiornamento automatico delle applicazioni

Non scaricare applicazioni da una piattaforma che non sia quella del costruttore del dispositivo

In ogni caso, preferire i canali sicuri proposti da Pictet (Pictet Connect, applicazioni mobili)

Verificare gli indirizzi dei siti

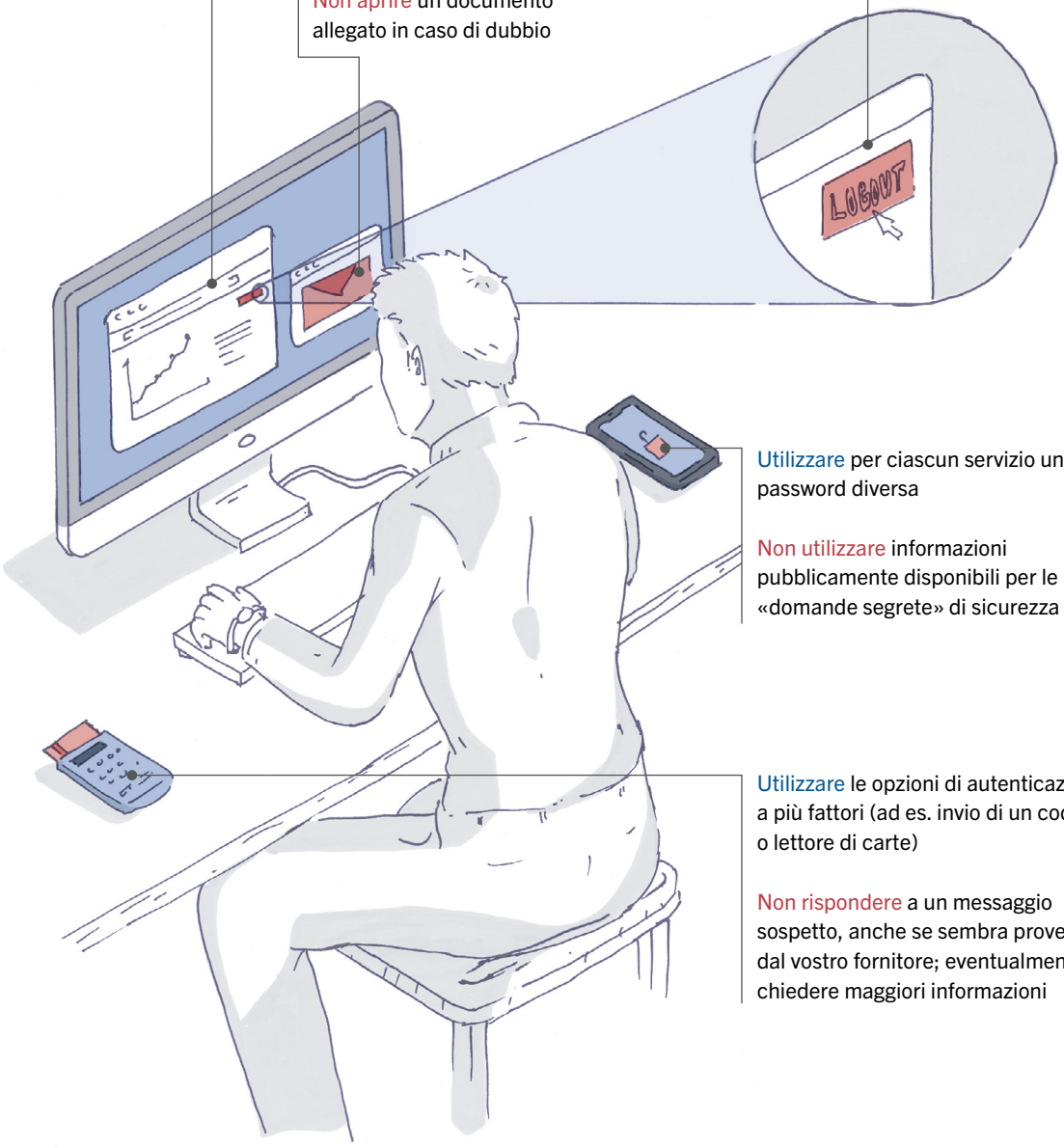
Non divulgare informazioni su un sito non sicuro, soprattutto quando si utilizza una rete pubblica

Adottare un atteggiamento saggiamente prudente nei confronti delle e-mail non richieste

Non aprire un documento allegato in caso di dubbio

Chiudere correttamente le sessioni tramite le apposite funzioni

Non lasciare aperta una sessione senza sorveglianza



Utilizzare per ciascun servizio una password diversa

Non utilizzare informazioni pubblicamente disponibili per le «domande segrete» di sicurezza

Utilizzare le opzioni di autenticazione a più fattori (ad es. invio di un codice o lettore di carte)

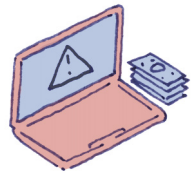
Non rispondere a un messaggio sospetto, anche se sembra provenire dal vostro fornitore; eventualmente chiedere maggiori informazioni

COSA FARE IN CASO DI FURTO DI DATI?

In caso d'incidente, vanno prese immediatamente le seguenti misure.

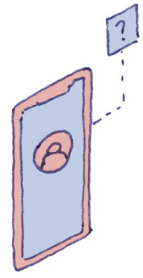
LA MIA CASELLA DI POSTA ELETTRONICA È STATA COMPROMESSA

- Recuperare l'accesso utilizzando le indicazioni del fornitore e cambiare immediatamente la password (facendo lo stesso anche per tutti gli altri conti che utilizzavano la stessa password)
- Informare conoscenti e contatti che tale indirizzo elettronico non è temporaneamente più affidabile
- Determinare eventuali irregolarità in base al contenuto della casella di posta elettronica (transazioni, informazioni confidenziali) e contattare le parti interessate
- Verificare o fare verificare la configurazione della casella di posta elettronica, in particolare per quanto concerne eventuali inoltri automatici dei messaggi impostati dai pirati informatici



HO RICEVUTO UNA RICHIESTA DI RISCATTO PER VIA ELETTRONICA

- Non pagare il riscatto
- Contattare immediatamente un esperto informatico



HO FORNITO INFORMAZIONI SENSIBILI PER TELEFONO A UNA PERSONA MALINTENZIONATA

- Modificare le password potenzialmente interessate
- Informare partner e conoscenti che potrebbero essere colpiti
- Bloccare il numero di telefono della persona malintenzionata e non rispondere più a successive chiamate

COME RICONOSCERE UN MESSAGGIO PROVENIENTE DA UN TRUFFATORE?

Non esistono metodi sicuri al 100%,
ma alcuni segnali di allarme dovrebbero attirare
l'attenzione degli utilizzatori.

È importante non fidarsi in particolare dei messaggi che:

- provengono da un indirizzo sconosciuto o insolito; occorre prestare attenzione soprattutto al fatto che un indirizzo falsificato può cercare di imitare quello di un contatto conosciuto;
- includono elementi sospetti, sembrano minacciosi o trasmettono una sensazione d'urgenza;
- contengono promesse vaghe o insperate;
- invitano ad aprire un documento allegato o a cliccare su un link per scoprire il contenuto completo del messaggio;
- non menzionano chiaramente il destinatario del messaggio e non provengono dall'indirizzo solitamente utilizzato dal mittente.

Se un messaggio presenta uno o più dei segnali di cui sopra, non è certo che si tratti di un messaggio fraudolento. Tuttavia, prima di trattare il messaggio, è opportuno adottare alcune precauzioni.

Pictet
Il Gruppo Pictet è diretto da sette soci, che ne sono al tempo stesso i titolari e si occupano direttamente della sua conduzione. I principi di successione nell'ambito del collegio dei soci e di trasmissione del capitale sono rimasti invariati dalla sua fondazione nel 1805. Il Gruppo si dedica in via esclusiva alla gestione dei patrimoni, alla gestione degli investimenti e all'asset servicing. Non concede crediti commerciali e non svolge attività di banca d'investimento. Con patrimoni in gestione o in amministrazione pari a CHF 544 miliardi al 30 giugno 2019, Pictet è oggi uno dei principali wealth manager e asset manager indipendenti in Europa.

Il Gruppo ha sede a Ginevra, dove le sue attività sono iniziate, e impiega più di 4300 collaboratori. Con 27 uffici a livello globale, è presente anche ad Amsterdam, Basilea, Barcellona, Bruxelles, Dubai, Francoforte, Hong Kong, Losanna, Londra, Lussemburgo, Madrid, Milano, Montreal, Monaco, Nassau, Osaka, Parigi, Roma, Singapore, Stoccarda, Taipei, Tel Aviv, Tokyo, Torino, Verona e Zurigo.

Realizzazione
Large Network

FSC
MIX
Paper
FSC® C002504

www.gruppo.pictet