MEDIOBANCA
PRIVATE BANKING

ISTRUZIONI TECNICHE e NORME DI SICUREZZA COMPORTAMENTALE

MEDIOBANCA
PRIVATE BANKING

Sommario

ISTRUZIONI TECNICHE

Al fine di garantire sicurezza e affidabilità al suo conto presso il nostro istituto, La preghiamo di prestare attenzione alle istruzioni tecniche di utilizzo che le sono state fornire in fase di sottoscrizione del Contratto Online Banking e alle seguenti misure di sicurezza comportamentale.

Le raccomandiamo di tenere custoditi separatamente e con massima cura la user e la password e di non comunicarle a terzi.

Le ricordiamo che la password in suo possesso non verrà richiesta per nessun motivo dal nostro istituto, dal suo Private Banker ovvero dal Servizio Help Desk.

Per qualsiasi dubbio o necessità la preghiamo di far riferimento al suo Private Banker, alla filiale della Banca stessa oppure di contattare il Servizio Help Desk al numero verde 800 403203 raggiungibile da un numero fisso o mobile (dall'estero contattare 0131 1923160) che provvederà al blocco dello stesso.

Il servizio è attivo dal lunedì al venerdì dalle 8 alle 22. Il sabato dalle 8 alle 14.

MEDIOBANCA
PRIVATE BANKING

NORME DI SICUREZZA COMPORTAMENTALE

PROTEGGERE SEMPRE LA PROPRIA IDENTITA' DIGITALE

Come proteggere la propria identità digitale

Per proteggere la propria identità digitale, è sufficiente seguire alcune semplici raccomandazioni:

- Utilizzare un indirizzo e-mail diverso per ogni contesto (ad esempio per i conti bancari, per gli account aziendali, per le newsletter...). In questo modo le comunicazioni di un certo tipo, ad esempio quelle bancarie, arriveranno sempre e solo su una specifica mail. Pertanto, nel caso ricevesse strane mail da parte della banca su altri account mail, saprà subito che si tratta molto probabilmente di tentativi di frode.
- Se le vengono richiesti dei dati sensibili via mail o al telefono, faccia attenzione e non si fidi. Generalmente le società non fanno queste richieste: non bisogna fornire dunque alcun dato, interrompere la comunicazione nel caso sia una telefonata e mettersi in contatto con la società tramite i canali ufficiali che trova sul loro sito web. Molto probabilmente scoprirà che era un tentativo di truffa per avere i suoi codici.
- Non utilizzare mai informazioni personali facilmente accessibili per creare una password. Inserire il proprio nome e cognome, il numero di telefono, l'indirizzo, il nome del figlio o del cane o altre informazioni simili, potrebbe far sì che qualcuno riesca ad impossessarsi di queste informazioni e accedere facilmente ai suoi servizi.
- Non utilizzare la stessa password per più servizi. Se usa una password sempre uguale, qualora riuscissero a rubarla, potrebbero poi accedere a tutti i suoi servizi.
- Infine, quando deve scegliere la sua password, le consigliamo di pensare a frasi o a diverse parole che ricorderà facilmente e utilizzare solo le prime lettere di queste parole. Aggiungere poi una combinazione di numeri e caratteri speciali, in tal modo la password risulterà facile da ricordare ma molto complessa e difficilmente indovinabile.

SALVARE LA PROPRIA IDENTITA' DIGITALE IN MODO SICURO

Dove salvare i propri dati personali in modo sicuro

Oltre a rendere la propria identità digitale difficile da indovinare e intercettare, deve ricordarsi di proteggerla anche quando la salva sui suoi dispositivi.

Per salvarla in modo sicuro, è necessario:

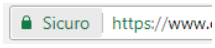
- Salvare i dati relativi alla propria identità digitale solo se necessario
- Salvare i dati solo su dispositivi sicuri (ad es, non salvare le tue password su un file di testo in una chiavetta USB che tiene in borsa o sul suo Smartphone)
- Rimuovere tutti i dati che non utilizza più dai dispostivi
- Creare un duplicato (backup) dei suoi dati, meglio su un disco rigido esterno riposto al sicuro, oppure custodirli su servizi in "Cloud" che garantiscano la sicurezza dei suoi dati. In questo modo potrà recuperare le informazioni senza esporle a malintenzionati.

UTILIZZARE I SERVIZI ONLINE IN MODO SICURO

Come comportarsi quando si utilizza un servizio online

Ogni volta che usa un servizio online tramite la sua identità digitale, è fondamentale seguire queste semplici regole.

- Disabilitare il salvataggio automatico delle password: è un'abitudine rischiosa perché se il dispositivo che usa è in condivisione o se, ad esempio al lavoro, lo dimentica acceso e non bloccato, qualsiasi persona potrebbe usare le password già memorizzate per accedere ai suoi servizi
- Quando ha finito di usare un servizio online, si assicuri sempre di effettuare il "logout" dal suo account in modo che nessuna persona che usi la sua postazione dopo di lei (o che passi di lì) possa vedere o utilizzare il servizio con il suo account

- Se deve usare un servizio online critico (come l'accesso al suo conto corrente) si ricordi di:
    - Non utilizzare mai dispositivi condivisi! Non accedere quindi da postazioni presenti in luoghi pubblici o computer / smartphone di amici , potrebbero infatti essere compromessi senza che nessuno lo sappia e rubarle la sua identità digitale.
    - Non utilizzare mai reti internet non protette come le reti Wireless accessibili da tutti. Queste reti non garantiscono il corretto livello di sicurezza e potrebbero esserci connessi utenti malintenzionati che cercano di rubare i dati delle persone connesse.
    - Verificare sempre di essere su un sito web sicuro. Può facilmente identificarlo controllando se all'inizio della barra degli indirizzi c'è la dicitura 

    - Digitare sempre con cura l'indirizzo del servizio e non cercarlo sui motori di ricerca, così sarà sicuro di non essere rimandato a siti illeciti che potrebbero diffondere contenuti malevoli o sembrare identici ai siti veri e richiederti le credenziali di accesso al servizio rubandole i codici

UTILIZZARE SEMPRE UN AMBIENTE DI LAVORO SICURO

Rendere sicuri i suoi dispositivi

I suoi dispositivi personali come computer e smartphone, le permettono di usare la sua identità digitale in tutto il mondo virtuale; si assicuri che siano adeguatamente protetti altrimenti la sua identità digitale sarà sempre a rischio. In particolare si ricordi di:

- Aggiornare periodicamente il sistema operativo dei suoi dispositivi installando tutte le patch di sicurezza per proteggere il suo dispositivo dalle minacce più recenti.
- Proteggere i suoi dispositivi da minacce come Virus e Malware tramite l'installazione di programma conosciuto di anti-virus/ anti-malware ed

eseguire scansioni periodiche per rilevare la presenza di eventuale software malevolo.

- Installare un firewall personale sul dispositivo per proteggerlo da attacchi diretti, in tal modo eventuali malintenzionati non potranno cercare di accedere da remoto al suo dispositivo.
- Spegnere sempre il suo computer quando non lo usa; infatti lasciandolo in modalità "standby" e connesso alla rete si espone ad accessi non autorizzati che potrebbero portare al furto dei suoi dati.
- Non lasciare i suoi dispositivi personali in mano a terze persone, nemmeno se opportunamente bloccati. Potrebbero provare ad accederci indovinando le credenziali e, nel caso ci riuscissero, avrebbero accesso completo alle sue informazioni riservate.
- Prima di smaltire un vecchio dispositivo che non usa più, si assicuri di rendere illeggibili le informazioni al suo interno. Può farlo tramite procedura magnetica o software dedicato se si tratta di un computer, altrimenti per gli Smartphone basta eseguire un reset di fabbrica (ovvero il ripristino alle condizioni iniziali)
- Eliminare sempre le e-mail provenienti da fonti sconosciute senza aprirle ed evitare di scaricare file da un sito web di cui non si fida completamente. Inoltre stia attento ai "pop-up" e agli annunci casuali perché potrebbe ritrovarsi il dispositivo infetto e mettere a rischio la sua identità digitale.

Quando utilizza servizi online critici, stia attento a chi le siede vicino in luoghi pubblici o sui mezzi di trasporto. Alcune persone potrebbero cercare di leggere informazioni sul suo schermo recuperando dati sensibili (ad es. le password inserite o la sua liquidità sul conto economico)

MANTENERE SICURO IL SUO SMARTPHONE

Utilizzare in modo sicuro le App sul suo smartphone

Come è necessario prestare attenzione ai software che installa sul computer, è altrettanto importante che fare attenzione alle APP che installa sul suo Smartphone.

Si ricordi di:

- Non installare applicazioni provenienti da Store non ufficiali: su Market non ufficiali si trovano molte App illecite che, una volta installate sul suo dispositivo, lo compromettono intercettando le sue informazioni personali (credenziali, servizi utilizzati e persino la posizione del GPS).
- Controllare sempre le impostazioni di privacy che vengono richieste dalle APP che installa: configurarle in modo da condividere la quantità minima di dati possibile.
- Disabilitare il caricamento automatico dei suoi dati sul Cloud; potrebbe ritrovarsi senza saperlo ad avere le sue credenziali su server remoti non controllabili ed esporsi a rischi.
- Se utilizza dispositivi in condivisione con minorenni, utilizzi i "filtri di contenuti" in modo che non possono inavvertitamente scaricare applicazioni che contengano contenuti inappropriati o dannosi che metterebbero a rischio i suoi dati.

PROTEZIONE DEI DATI A SEGUITO DI UNA VIOLAZIONE

Come procedere in caso di furto della propria identità digitale

Se si accorge che le hanno rubato la sua identità digitale, è fondamentale che proceda subito a modificare i dati che le hanno sottratto.

Ad esempio:

- Se hanno fatto accesso alla sua e-mail, cambi subito la password di accesso e, se possibile, attivi un doppio fattore di autenticazione

- Se hanno fatto accesso a servizi dispositivi o con dati sensibili (come ad esempio il conto bancario), contatti immediatamente il gestore del servizio per:
    - Bloccare i codici rubati
    - Bloccare eventuali strumenti di pagamento (es carte di debito/credito)
    - Verificare gli ultimi movimenti svolti sul servizio online e gli ultimi accessi
    - Bloccare eventuali transazioni svolte illecitamente dal suo conto
    - Se le hanno sottratto il computer o lo smartphone contenenti credenziali e dati sensibili (o hanno fatto accesso a servizi su cui li avevi salvati), li modifichi quanto prima per evitare che ne vengano in possesso e li utilizzino per attività fraudolente.

Come procedere in caso di violazione di chi gestisce il servizio online

Se viene informato di una possibile violazione del servizio online che utilizza, prima di effettuare qualsiasi attività di modifica dei tuoi codici, è opportuno:

- contattare il gestore del servizio (ad es la Banca oppure il suo Private Banker) per verificare la correttezza delle informazioni reperite
- seguire le indicazioni fornite dal gestore del servizio (es cambio password, blocco e riemissione della carta, etc)

Diffidare sempre delle mail o degli SMS che la informano di violazioni informatiche e consigliano di cambiare immediatamente i tuoi codici tramite un link fornito nel messaggio: probabilmente sono messaggi falsi finalizzati a rubarle la sua identità digitale.

FRODI INFORMATICHE DA MALWARE

Cos'è il Malware?

Il malware è un software malevolo creato con lo scopo di danneggiare o eseguire azioni non autorizzate sul computer su cui viene eseguito.

Come avviene una frode da malware?

I malware vengono solitamente distribuiti attraverso siti compromessi, mail di spam e scambio di file infetti.

Una volta che il computer viene infettato, il malware si attiva quando l'utente accede a determinati siti web come la casella di posta elettronica, l'HomeBanking, siti di acquisto online, etc al fine di intercettare i dati sensibili come codici di accesso, codici dispositivi, codici di carte di credito etc..

In alcuni casi il malware non si limita a rubare i codici digitati dall'utente in fase di utilizzo (es: in fase di accesso all'Online Banking) ma interagisce e mostra all'utente delle finte pagine web con la stessa grafica del sito al fine di richiedere ulteriori informazioni solitamente non richieste dal sito lecito (es i codici delle carte di credito)

Come si evitano le frodi da malware?

E' necessario:

- Mantenere aggiornato il proprio dispositivo (computer e Smartphone) all'ultima versione software disponibile ed installare tutte le patch di sicurezza fornite dal venditore;
- Installare software antimalware sui propri dispositivi e mantenerli sempre aggiornati;
- Diffidare da qualunque mail sospetta che invita ad aprire link o allegati contenuti al suo interno;
- Verificare sempre l'attendibilità dei siti web su cui si accede, diffidando di siti con una grafica anomala o scritti in italiano non corretto;
- Diffidare dai siti web che richiedono dati mai chiesti in precedenza (ad es il sito della banca che chiede i codici della carta di credito);

- Non scaricare e installare programmi e App da Store non ufficiali.

Nel caso in cui ritenga di avere un dispositivo infetto da malware, è sempre necessario contattare il gestore del servizio e bloccare i propri codici.

PHISHING

Cos'è il Phishing?

Il "Phishing" è un sistema di truffa via e-mail, sms o telefono volto a sottrarre ai titolari di un Conto i propri dati e le credenziali di accesso. Si tratta di messaggi che imitano quelli ufficiali della Banca ma che, in realtà, inducono l'utente a rilasciare le proprie informazioni che vengono poi utilizzate per tentativi di frode.

Come funziona il Phishing?

Il Titolare del Conto riceve una richiesta formulata come se fosse inviata dalla Banca, motivata dalla scusa di verificare i suoi dati per il ripristino di servizi che sarebbero stati bloccati in via cautelativa. Queste richieste spesso contengono minacce di sospensione del servizio laddove non vengano seguite le procedure richieste. Cliccando sulla e-mail di Phishing si atterra su una pagina web molto simile a quella della Banca dove viene richiesto di inserire le proprie credenziali di accesso, i dati riguardanti le Carte o altre informazioni riservate.

Come si evita il Phishing?

- Diffidare di qualunque richiesta di dati personali o credenziali di accesso, informazioni relative al Conto o alla Carta, che arrivi via e-mail, sms, telefono.
  Mediobanca ha una politica sulla sicurezza molto rigorosa: non richiede mai tali informazioni via e-mail o telefono, né opera con numeri telefonici diversi da quelli pubblicati sul sito web ufficiale.
- Collegarsi al sito di Mediobanca Private Banking scrivendo l'indirizzo web www.mediobancapb.com direttamente nella barra di navigazione.
- Non cliccare mai su collegamenti presenti su una e-mail, che potrebbero condurre a siti contraffatti, magari del tutto analoghi all'originale.
- Diffidare di qualsiasi messaggio (posta elettronica, pop-up, ecc.) che inviti a scaricare programmi o documenti dei quali si ignorano provenienza e attendibilità.
- Fare attenzione a eventuali anomalie rispetto alle abituali modalità con cui viene richiesto l'inserimento dei dati personali ai fini dell'accesso ai servizi.
- Prestare attenzione ad eventuali falsi siti web controllando il link nel proprio browser.

Per qualsiasi dubbio o bisogno di chiarimento riguardo a comunicazioni di Mediobanca che sembrassero sospette la preghiamo di contattare subito il Servizio Help Desk al numero verde **800 403203** raggiungibile da un numero fisso o mobile (dall'estero contattare **0131 1923160**) che provvederà al blocco dello stesso.

Il servizio è attivo dal lunedì al venerdì dalle 8 alle 22. Il sabato dalle 8 alle 14.