CASSA DI RISPARMIO
DI ORVIETO
Gruppo Mediocredito Centrale

ATTENZIONE
SE TI CHIEDONO PASSWORD, PIN, DATI PERSONALI
PROBABILMENTE
È UNA FRODE

PROTEGGITI DALLE FRODI BANCARIE ONLINE

La sicurezza dei clienti e la tutela del loro denaro sono aspetti essenziali e complementari, che Cassa di Risparmio di Orvieto affronta in diversi modi e con più strumenti.
Da un lato sono previste difese elettroniche sempre più sofisticate per salvaguardare le connessioni online, dall'altro sono stati attivati dispositivi che tengono al sicuro le filiali dai fenomeni di microcriminalità. Daresti a uno sconosciuto le tue chiavi di casa o il PIN del tuo Bancomat? Certamente no! Come nel mondo reale è meglio essere estremamente diffidenti e non consegnare i propri dati riservati senza conoscere l'identità di chi ce li sta chiedendo. È bene proteggere le proprie password di accesso all'Home Banking e al Mobile Banking, avere sempre cura del token che genera l'OTP (One Time Password) per effettuare le dispositive e più in generale conservare i dati per l'accesso a proprio uso esclusivo.

UTILIZZARE UNA PASSWORD EFFICACE ***

Una password sicura:
- Non deve contenere informazioni personali (es. nome e cognome, data di nascita, codice fiscale...).
- Non deve contenere sequenze di lettere o numeri (1234, abcd...).
- Non deve essere la stessa usata per altri servizi online (conto, email, siti...).
- Non deve essere salvata nel browser.

CONTROLLARE L'ACCESSO AL SITO DI HOME BANKING

- Controllare che nella barra dell'indirizzo compaia sempre la dicitura https://, che certifica l'ufficialità del sito.
- A conclusione della sessione sul sito di Home banking, utilizzare l'apposita funzione di Logout.

PROTEGGERE IL PROPRIO DISPOSITIVO DI ACCESSO

Occorre sempre avere cura dei propri dispositivi personali utilizzati per accedere alle applicazioni messe a disposizioni della Banca. Rientrano in questa categoria il computer desktop, notebook, tablet, smartphone, etc.

È importante effettuare sempre le seguenti attività:
- Installare e aggiornare il software di protezione antivirus e antispyware.
- Installare sempre gli aggiornamenti ufficiali del sistema operativo.
- Installare gli aggiornamenti e le patch di sicurezza del browser e delle applicazioni.
- Evitare di installare software da fonti non attendibili che potrebbero nascondere minacce o attacchi di tipo 'trojan', altrimenti i malintenzionati potrebbero prendere il controllo del dispositivo o carpire informazioni dal dispositivo stesso.

BANKING TROJAN

L'utilizzo di dispositivi non sicuri per accedere al servizio di Home Banking, può esporre il cliente al rischio di incorrere in cyber truffe sempre più sofisticate.
Nella fattispecie i "banking trojan" sono molto pericolosi in quanto non hanno un comportamento distruttivo da subito, la loro presenza nel computer della vittima può essere non rilevata per un periodo di tempo variabile se non è presente una valida soluzione antivirus.
È importante, quindi, accertarsi che nella barra dell'indirizzo del browser compaia sempre la dicitura https://, che certifica l'ufficialità del sito di home banking.

DISPOSIZIONI DI PAGAMENTO ATTRAVERSO IL CANALE DI HOME BANKING

Recentemente si è diffuso un malware che, in maniera silente, esegue il furto di credenziali utente, numeri di account e, infine, denaro da operazioni bancarie, mediante tecniche note come "man in the browser" e "web injection".
Tali malware, oltre a rubare dati all'utente, riescono a sostituire il codice IBAN durante un bonifico bancario; l'importo specificato dall'utente rimane inalterato, ma il malware modifica l'IBAN beneficiario e si intromette nelle comunicazioni tra l'utente e la banca, intercettando le credenziali e impartendo (o alterando) delle operazioni senza che l'utente possa accorgersene.
A tale scopo, nell'esecuzione di qualunque transazione, è necessario:
- Verificare che nella barra dell'indirizzo del browser compaia sempre la dicitura https://, che certifica l'ufficialità del sito di home banking;
- Verificare l'esattezza del codice IBAN prima di confermare una disposizione di pagamento (e.g. bonifico), e successivamente accertarsi che siano corretti i dati di riepilogo (IBAN e importo) nella lista delle disposizioni effettuate.

CONSIGLI UTILI

Di seguito sono elencati alcuni comportamenti caratteristici che permettono di individuare la presenza di malware di questo genere.
- Ricezione di **mail sospette**, con oggetti insoliti o contenuti ambigui;
- Il contenuto dell'allegato delle mail sospette è sicuramente la caratteristica più distintiva dei malware in oggetto. Di solito si tratta di un documento Office (e.g.: Word, Excel), che invita l'utente ad attivare le macro per visualizzare il contenuto del documento in modo corretto;
- **Rallentamento della navigazione** da parte del browser, in quanto è presente un maggior utilizzo della rete da parte del malware;
- Il fatto che si presenti una **schermata d'errore** immediatamente dopo il login o improvvisamente durante una sessione, deve far insospettire l'utente. In questo caso si consiglia immediatamente di prendere contatti con l'help desk o la propria filiale per verificare o revocare eventuali transazioni non autorizzate.

IL PHISHING

Il phishing è una frode informatica ideata allo scopo di rubare i dati personali di un utente (chiavi di accesso al servizio di home banking, numeri di carta di credito...).
È attuato attraverso false e-mail, apparentemente provenienti da una banca o da una società emittente carte di credito, composte utilizzando logo, nome e il layout tipico dell'azienda imitata.
Queste e-mail invitano il destinatario a collegarsi tramite un link a un sito Internet del tutto simile a quello della banca e a inserirvi le informazioni riservate, generalmente attraverso una finestra pop up che si apre dallo stesso link.

CRO non richiede mai, direttamente o tramite terzi, informazioni personali o codici di accesso ai servizi di internet banking.

Diffida delle mail che richiedono l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali.

È POSSIBILE RICONOSCERE LE TRUFFE VIA E-MAIL DA UNA SERIE DI DETTAGLI:

- non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici);
- fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente;
- non riportano una data di scadenza per l'invio delle informazioni.

Non rispondere mai a e-mail con richieste di questo tipo, cestinale subito ed eventualmente informa la Banca tramite il call center.

POCHI SEMPLICI ACCORGIMENTI PER EVITARE DI SUBIRE DI UNA FRODE BANCARIA

- **Non cliccare su link presenti in e-mail sospette**, potrebbero condurti a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser è visualizzato l'indirizzo corretto, non ti fidare: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del tuo browser un indirizzo diverso da quello nel quale realmente ti trovi.

- Quando inserisci dati riservati in una pagina web, assicurati che si tratti di una **pagina protetta**. Queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto.

- Diffida di **e-mail con indirizzi web molto lunghi**, contenenti caratteri inusuali come, in particolare, la @.

- **Controlla regolarmente gli estratti conto** del tuo conto corrente e delle carte di credito per assicurarti che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contatta la Banca e/o l'emittente della carta di credito.

- Diffida se improvvisamente cambia la modalità con la quale ti viene chiesto di inserire i tuoi codici di accesso all'home banking: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite **pop-up** (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contatta la Banca tramite il call center.

GLI ACQUISTI ONLINE

Effettuare transazioni, come pure vendere e acquistare su Internet, è ormai pratica molto frequente. A tutela dei propri clienti Cassa di Risparmio di Orvieto dispone dei seguenti sistemi di sicurezza:

TOKEN Hardware o Software

Sono dispositivi digitali altamente affidabili che consentono di operare online con estrema sicurezza. La Banca prevede che qualsiasi operazione dispositiva sia confermata da un OTP (One Time Password) generata appunto da uno di questi dispositivi (costi e informazioni come da Fogli informativi).
Nell'immagine viene riportato un dispositivo hardware (la tipologia del modello potrebbe differire in base alla disponibilità del modello). Il dispositivo software è installato insieme alla mobile app ed è utilizzato direttamente attraverso il proprio smartphone (occorre verificare la compatibilità del software del sistema operativo e del modello dello smartphone).

SERVIZIO 3D SECURE CARTA DI DEBITO MAESTRO

Il Servizio 3D Secure è il sistema creato per garantire la sicurezza delle transazioni sui siti degli esercenti convenzionati con il circuito internazionale Maestro. Per confermare il pagamento, il titolare della carta di pagamento dovrà, ove previsto, inserire il codice di sicurezza OTP ricevuto tramite SMS sul proprio cellulare o notifica push sul device abilitato e il codice di sicurezza Key6 registrato sul portale 3DS della Banca.

Costo del servizio: gratuito.

3 SEMPLICI REGOLE CHE SUGGERIAMO DI SEGUIRE IN OGNI CASO:

1. Verifica che il venditore sia un esercizio reale, meglio se conosciuto, e che il sito indichi tutti i suoi dati, compreso l'indirizzo.
2. Diffida degli accessi gratuiti a siti che richiedono i dati della carta di pagamento.
3. Evita di inserire il numero della carta in siti non protetti da sistemi di sicurezza internazionali.

ANCHE TU DEVI FARE LA TUA PARTE

La prevenzione è la migliore arma per difendersi dalle frodi bancarie online, di qualunque tipo.
I tuoi comportamenti sono determinanti.

- **TIENITI AGGIORNATO**
  I sistemi sono in continua evoluzione, perciò è importante tenersi informato sulle truffe più comuni.
- **NON ESSERE FRETTOLOSO**
  La prudenza non è mai troppa. Prenditi il tempo per fare dei controlli prima di rispondere a qualsiasi comunicazione.
- **PROTEGGI I TUOI DATI**
  Non fornire mai i tuoi dati personali (password, numeri di carta di credito, ecc.).

LA SICUREZZA IN BANCA

In linea con i più aggiornati standard di sicurezza, Cassa di Risparmio di Orvieto si avvale di dispositivi che limitano il maneggio del contante durante le operazioni di cassa in filiale, creando così minori occasioni di rapina.
In particolare, buona parte delle filiali utilizza le cosiddette casse **"cash in cash out"**, la cui caratteristica è di avere restrizioni nell'erogazione del denaro in uscita e nessuna per quello in entrata. In pratica le banconote vengono rese disponibili in modo automatico, per importi definiti e richiesti dal cassiere, con tempi di erogazione crescenti in relazione all'entità dell'importo. In questo modo **i cassieri non hanno alcuna giacenza di denaro**, e ovviamente **non hanno alcuna possibilità né di sbloccare né di aprire le casse.**