Emittente:
Cassa Centrale Banca - Credito Cooperativo del Nord Est Società per Azioni
Sede sociale e Direzione generale in via Segantini n. 5, 38122, Trento (Italia)
Tel.: +39.0461.313111, fax: +39.0461.313119, e-mail: info@cassacentrale.it
Capitale sociale sottoscritto € 140.400.000,00 interamente versato
Società iscritta all'albo delle Banche – Cod. ABI 03599
Iscr. Reg. imprese di Trento, Cod. Fisc. e P.IVA 00232480228
Aderente al Fondo di Garanzia dei Depositanti del Credito Cooperativo e al Fondo Nazionale di Garanzia
Appartenente al Gruppo bancario Cassa Centrale Banca n. 20026
Società soggetta all'attività di direzione e coordinamento di Centrale Finanziaria del Nord Est S.p.A.

SCHEDA INFORMATIVA SULLA SICUREZZA DEI PAGAMENTI IN INTERNET

Il presente documento riporta le informazioni principali legate alla sicurezza del servizio di pagamento via Internet e alcuni dei principali suggerimenti sull'utilizzo sicuro e consapevole del servizio "Carte Prepagate". La tua Banca sarà sempre a disposizione per approfondimenti e ulteriori informazioni riguardanti questi aspetti; sono inoltre disponibili contenuti aggiornati sulla sicurezza nell'area clienti del sito ***www.carteprepagate.cc***.

1. REQUISITI TECNOLOGICI

Collegamento via Internet

Per poter usufruire del servizio è necessario disporre di un collegamento alla rete Internet tramite un ISP – Internet Service Provider a scelta (le spese di collegamento telefonico sono a carico del chiamante).

Dispositivi (requisiti hardware)

Per accedere al servizio è sufficiente disporre di dispositivi connessi alla rete Internet (personal computer, smartphone, …).

Requisiti Software

Il servizio è fruibile attraverso l'utilizzo di sistemi operativi e browser supportati. Per un utilizzo sicuro, si suggerisce di dotarsi di un software antivirus, costantemente aggiornato e installato sul dispositivo. Per approfondimenti e consigli per un utilizzo efficace dell'antivirus, si faccia riferimento al documento "Sicurezza e Frodi - Alcune regole per un uso corretto delle carte" pubblicato tra i documenti informativi dell'area clienti del sito ***www.carteprepagate.cc***.

2. SICUREZZA ON-LINE

Per proteggersi da frodi, accessi e modifiche non autorizzate ai dati sensibili di pagamento, sono implementati opportuni presidi di sicurezza tramite misure tecnologiche (ad esempio tramite l'utilizzo di crittografia) e procedure per garantire il controllo accessi e la tracciatura delle attività.

Sicurezza del canale di comunicazione

Per tutti gli scambi di dati sensibili di pagamento via Internet, è garantita la sicurezza dei canali di comunicazione tra le parti coinvolte grazie a:

- Misure di crittografia end to end per tutta la durata della sessione;
- Tecniche di cifratura robuste e ampiamente riconosciute.

Verifica del protocollo

Controllare che l'URL della pagina Internet inizi con ***https://www.carteprepagate.cc*** in particolare, la presenza dell'intestazione "https" indica che la navigazione sta avvenendo su un canale cifrato e quindi sicuro. Il sito dispone di un certificato emesso da una Certification Authority riconosciuta e accreditata internazionalmente.

Emittente:
Cassa Centrale Banca - Credito Cooperativo del Nord Est Società per Azioni
Sede sociale e Direzione generale in via Segantini n. 5, 38122, Trento (Italia)
Tel.: +39.0461.313111, fax: +39.0461.313119, e-mail: info@cassacentrale.it
Capitale sociale sottoscritto € 140.400.000,00 interamente versato
Società iscritta all'albo delle Banche – Cod. ABI 03599
Iscr. Reg. imprese di Trento, Cod. Fisc. e P.IVA 00232480228
Aderente al Fondo di Garanzia dei Depositanti del Credito Cooperativo e al Fondo Nazionale di Garanzia
Appartenente al Gruppo bancario Cassa Centrale Banca n. 20026
Società soggetta all'attività di direzione e coordinamento di Centrale Finanziaria del Nord Est S.p.A.

Misure di identificazione dell'utente

L'inoltro dei pagamenti via Internet, così come l'accesso ai dati sensibili relativi ai pagamenti in Internet (dati che possono potenzialmente essere utilizzati per perpetrare una frode) sono protetti da un sistema di "strong customer authentication", attraverso l'utilizzo, in aggiunta alla verifica di nome utente e password, dell'apposito strumento di sicurezza fornito dalla Banca e richiesto al momento della conferma dell'operazione.

Mobile OTP

Il funzionamento di tale strumento prevede che il Cliente riceva un messaggio (tramite canale SMS o tramite apposita applicazione di sicurezza) sul numero di cellulare fornito dal Cliente, ogniqualvolta si renda necessario l'inserimento del codice OTP - one time password. Il messaggio conterrà il codice OTP che il Cliente dovrà inserire per autorizzare l'operazione.

Raccomandazioni per l'utilizzo sicuro del proprio dispositivo mobile

- Proteggere sempre l'accesso al dispositivo mediante PIN.
- Nel caso di utilizzo del browser del dispositivo mobile evitare di memorizzare le credenziali di accesso.
- Nel caso di furto o smarrimento del dispositivo mobile contattare il proprio operatore telefonico per il blocco della SIM.

Procedura di inoltro e autorizzazione operazioni di pagamento

Il sevizio prevede le seguenti fasi operative per l'invio alla propria Banca della disposizione di pagamento:

1. Inserimento dati della disposizione;
2. Verifica dei dati della disposizione;
3. Autorizzazione tramite lo strumento di sicurezza;
4. Feedback di conferma di inoltro della disposizione alla Banca.

3. ULTERIORI MISURE DI SICUREZZA

Per aumentare il livello di sicurezza delle operazioni effettuate tramite Internet, sono applicate o messe a diposizione del Cliente ulteriori misure di sicurezza.

Requisiti di autenticazione

Per aumentare il livello di sicurezza nella fase di autenticazione è definito un limite massimo di cinque tentativi falliti di login o di autenticazione; al superamento di tale limite l'accesso al servizio è bloccato. Nell'utilizzo del servizio tramite APP, il Cliente può impostare in autonomia un "accesso facilitato" per l'accesso all'applicazione stessa che comunque garantisce gli standard di sicurezza richiesti per i servizi di pagamento in Internet.

Minuti di inattività (controllo automatico sull'attività di una postazione)

Al fine di prevenire utilizzi fraudolenti, nel caso in cui un'utenza connessa rimanga inattiva per un determinato lasso di tempo, il sistema provvede a disconnetterla automaticamente.

Limiti Operativi impostati dalla Banca

Per maggiore sicurezza alcune funzionalità dispositive di pagamento hanno dei limiti (es: massimali giornalieri, mensili) impostati dalla Banca. Superato tale limite, il sistema impedisce l'invio di ulteriori disposizioni nel periodo.

Limiti Operativi impostati dal Cliente

Il Cliente può provvedere autonomamente a ridurre, secondo necessità, i limiti operativi impostati dalla Banca, fino all'azzeramento del limite stesso (con conseguente indisponibilità dei servizi che ad esso fanno riferimento) sia da sito che da APP.

Emittente:
Cassa Centrale Banca - Credito Cooperativo del Nord Est Società per Azioni
Sede sociale e Direzione generale in via Segantini n. 5, 38122, Trento (Italia)
Tel.: +39.0461.313111, fax: +39.0461.313119, e-mail: info@cassacentrale.it
Capitale sociale sottoscritto € 140.400.000,00 interamente versato
Società iscritta all'albo delle Banche – Cod. ABI 03599
Iscr. Reg. imprese di Trento, Cod. Fisc. e P.IVA 00232480228
Aderente al Fondo di Garanzia dei Depositanti del Credito Cooperativo e al Fondo Nazionale di Garanzia
Appartenente al Gruppo bancario Cassa Centrale Banca n. 20026
Società soggetta all'attività di direzione e coordinamento di Centrale Finanziaria del Nord Est S.p.A.

Messaggi di Alert

Il Cliente ha la facoltà di richiedere l'attivazione del servizio di Alert (tramite canale SMS, notifica in APP o e-mail), che lo avvisa quando vengono effettuate disposizioni di pagamento (operazioni di pagamento, bonifici SCT, ecc.). Inoltre il Cliente ha la possibilità di attivare la ricezione degli Alert in occasione di ogni accesso al sito e APP con la propria utenza e nei casi di modifica delle impostazioni personali e di sicurezza.

4. CONSIGLI PER LA SICUREZZA

I personal computer, gli smartphone e tutti i dispositivi utilizzati per l'accesso ad Internet sono strumenti sofisticati. É importante conoscere i comportamenti corretti da seguire in tema di sicurezza online per evitare un utilizzo irresponsabile.
La posta elettronica che giunge da indirizzi sospetti o che richiede di seguire link anomali, i programmi che invitano a scaricare documenti sospetti o che provengono da fonti inattese possono veicolare contenuti dannosi. Non verranno mai richieste credenziali o informazioni personali al di fuori del sito ***www.carteprepagate.cc***.

Al fine di presidiare la navigazione nel web ai massimi livelli è necessario installare dei software di protezione (ad esempio un antivirus e un Firewall) e mantenere sempre aggiornato il proprio sistema operativo e tutti i programmi installati. É importante effettuare delle scansioni periodiche con l'antivirus installato sul pc per verificare la presenza di eventuali Virus o Trojan.

Navigare con intelligenza

Le frodi sono sempre in agguato ma basta un minimo di attenzione per evitarle. É sempre consigliato digitare gli indirizzi web direttamente nella barra di navigazione, controllando in anticipo la destinazione del link. Per eventuali dubbi è possibile verificare il certificato del sito cliccando due volte sull'icona del lucchetto.

Variare frequentemente la password di accesso

È consigliabile scegliere una password "forte", che contenga almeno un carattere delle seguenti categorie: lettere maiuscole, lettere minuscole e numeri. Si sconsiglia fortemente di salvare i propri codici di autenticazione (codice utente e password) in un file localizzato nel computer o nel browser utilizzato.

Massimo controllo del conto online

Visualizzare regolarmente i movimenti dei propri rapporti è buona norma per mantenere un controllo costante sulla propria operatività.

Aggiornamento recapiti

Il numero di telefono cellulare e l'indirizzo email del Cliente sono elementi fondamentali per la gestione della sicurezza; si consiglia al Cliente di tenerli costantemente aggiornati e di comunicare ogni loro variazione alla Banca.

Servizio Assistenza

È possibile segnalare eventuali tentativi di frode direttamente dal form d'assistenza messo a disposizione sul sito ***www.carteprepagate.cc***, oppure contattando direttamente la tua Banca.

5. FRODI CLASSICHE ON-LINE

La posta elettronica è lo strumento principale utilizzato per le frodi online. Spacciandosi per la Banca, i truffatori potrebbero richiedere i dati personali facendo leva sulla buona fede del Cliente. Ecco alcuni semplici consigli per evitare di incorrere in queste truffe: una su tutte, il cosiddetto Phishing.

Emittente:
Cassa Centrale Banca - Credito Cooperativo del Nord Est Società per Azioni
Sede sociale e Direzione generale in via Segantini n. 5, 38122, Trento (Italia)
Tel.: +39.0461.313111, fax: +39.0461.313119, e-mail: info@cassacentrale.it
Capitale sociale sottoscritto € 140.400.000,00 interamente versato
Società iscritta all'albo delle Banche – Cod. ABI 03599
Iscr. Reg. imprese di Trento, Cod. Fisc. e P.IVA 00232480228
Aderente al Fondo di Garanzia dei Depositanti del Credito Cooperativo e al Fondo Nazionale di Garanzia
Appartenente al Gruppo bancario Cassa Centrale Banca n. 20026
Società soggetta all'attività di direzione e coordinamento di Centrale Finanziaria del Nord Est S.p.A.

Phishing: cos'è e come funziona?

Tradizionalmente il mezzo principale per cadere in una truffa è la posta elettronica. La minaccia maggiore che incombe sugli utenti online è la pratica chiamata Phishing, termine inglese che nel caso delle frodi online assume il significato di "spillare dati sensibili": lo scopo dei truffatori è quello di conoscere le informazioni personali degli utenti legittimi.

E-mail falsa

Nessuna Banca richiederà mai per posta elettronica le credenziali di accesso. Le e-mail contraffatte hanno lo scopo di indurre gli utenti ad adottare comportamenti non sicuri simulando con una grafica simile all'originale, una comunicazione ufficiale.

Link al sito contraffatto

Lo scopo della e-mail fraudolenta è quello di appropriarsi delle credenziali di accesso, allarmando il Cliente con avvisi di particolari problemi verificatisi, quali presunti controlli di sicurezza o aggiornamenti. In questo modo, si induce l'utente a cliccare su un link presente nella e-mail che dovrebbe condurlo alla presunta pagina di autenticazione del sito www.carteprepagate.cc. In realtà il sito non è che una copia fittizia dell'originale: pertanto, accedendovi e digitando codice utenza e password si consegnano direttamente i dati nelle mani del truffatore.

Cosa si può fare?

Cadere nella truffa è solo frutto di disattenzione. L'indirizzo del sito è sempre www.carteprepagate.cc. Di seguito alcune regole base di buona condotta:

- La posta elettronica che giunge da indirizzi sospetti e richiede di seguire link anomali va trattata con attenzione;
- Non saranno mai richieste credenziali o informazioni personali da un canale diverso da www.carteprepagate.cc;
- Accedere al sito solo direttamente dalla barra degli indirizzi senza seguire link esterni; cliccare su link presenti nelle e-mail sospette è una pratica potenzialmente pericolosa.

6. NUOVE MINACCE ON-LINE

Le credenziali di accesso e la password sono merce preziosa per i malintenzionati: infatti, è molto più facile rubare queste informazioni che violare i sistemi di sicurezza. Prevenire questi nuovi tentativi di frode è più facile se si conosce il loro funzionamento.

Come funzionano?

I tentativi di frode più moderni cercano di sfruttare la disattenzione e la buona fede del Cliente; in questi casi non si punta a violare i sistemi, che sono di per sé estremamente difficili da aggirare, ma si cerca piuttosto di ingannare gli utenti per farsi consegnare le credenziali di accesso e le password di conferma delle disposizioni.

Furto delle credenziali

Un Trojan è un programma che opera sul dispositivo dell'utente per conto di un malintenzionato, detto Hacker. Grazie al Trojan, l'Hacker richiede o memorizza le credenziali di accesso, la password dispositiva (codice OTP) utilizzando questi dati per accedere al sito e mettere in atto una frode.

Cosa si può fare?

Diffidare quindi da ogni richiesta di password che venga proposta in modalità diverse rispetto a quelle usuali di www.carteprepagate.cc. Per segnalare una di queste anomalie è importante non fornire le credenziali, terminare la navigazione e comunicare l'accaduto all'assistenza carte prepagate o alla tua Banca.

Emittente:
Cassa Centrale Banca - Credito Cooperativo del Nord Est Società per Azioni
Sede sociale e Direzione generale in via Segantini n. 5, 38122, Trento (Italia)
Tel.: +39.0461.313111, fax: +39.0461.313119, e-mail: info@cassacentrale.it
Capitale sociale sottoscritto € 140.400.000,00 interamente versato
Società iscritta all'albo delle Banche – Cod. ABI 03599
Iscr. Reg. imprese di Trento, Cod. Fisc. e P.IVA 00232480228
Aderente al Fondo di Garanzia dei Depositanti del Credito Cooperativo e al Fondo Nazionale di Garanzia
Appartenente al Gruppo bancario Cassa Centrale Banca n. 20026
Società soggetta all'attività di direzione e coordinamento di Centrale Finanziaria del Nord Est S.p.A.

7. GLOSSARIO

Lista dei termini più utili per usare correttamente i servizi via Internet.

Antivirus Si tratta di un programma che riesce a rilevare ed eliminare il Malware presente in un PC. Un antivirus ricerca all'interno della memoria del PC delle particolari sequenze di dati che denotano la presenza di Malware, dette "firme"; per questo l'antivirus è efficace solo se costantemente aggiornato alle firme più recenti.

Firewall Un Firewall è un componente, hardware o software, che filtra il traffico di rete che fluisce tra un PC e Internet; applicando particolari regole di sicurezza, il Firewall scarta eventuali dati che non rispettano i parametri di sicurezza.

Hacker Persona che mira ad entrare in computer o reti informatiche altrui per motivi di lucro o anche per un semplice senso di sfida.

Keylogging Un Keylogger è un software che riesce a intercettare tutto ciò che viene digitato dalla tastiera di un certo computer. Può essere utilizzato per scopi malevoli in quanto permette all'Hacker di ritrovare le informazioni relative a nome utente e password digitati dall'utente. L'Hacker può successivamente sfruttare le legittime credenziali dell'utente per frodare l'utente stesso.

Malware Con Malware si intende un software creato per arrecare danno al computer su cui viene eseguito, all'utente del computer o ad un obiettivo esterno. Sono esempi di Malware i Virus e i Trojan. Il Malware viene sfruttato dall'Hacker malintenzionato per ricavare denaro tramite frodi online, con l'aiuto o meno di eventuali Money Mules.

Phishing Si intende con Phishing il furto di credenziali ottenuto tramite tecniche di ingegneria sociale. Scopo del furto di identità è quello di accedere alle informazioni personali del truffato e sottrargli denaro tramite transazioni online. La truffa viene portata avanti mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli che imitano la grafica dei siti istituzionali, portando il truffato a rivelare informazioni personali.

Spam Come Spam vengono definiti tutti quei messaggi di posta elettronica recapitati nella nostra casella di posta che non sono stati direttamente "sollecitati", e che potremmo definire anche come insieme di posta indesiderata. Lo Spam rappresenta un vettore per truffe e raggiri di diversa natura, soprattutto furti di identità, che si sono evoluti fino a trasformarsi in altre forme di minacce quali ad esempio il Phishing.

Trojan Si tratta di Malware distribuiti in modo fraudolento. Simili a Virus, si attivano all'arrivo di determinati segnali dall'esterno detti trigger. Sono software riconfigurabili dall'esterno ed adattabili.

Virus Un Virus è un tipo di Malware che è in grado, una volta eseguito, di infettare dei file e di riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. Solitamente un Virus danneggia direttamente solo il software della macchina colpita.