CCN SERVIZI di PAGAMENTO SpA

Via Kennedy n. 5 - 42040 Campegine (RE)

CCN Servizi di Pagamento S.p.A a socio unico
Sede legale Via Kennedy n. 5 - 42040 Campegine (RE)
Istituto iscritto all'Albo degli Istituti di Pagamento tenuto da Banca d'Italia n. 36039.6 Codice ABI 36039.6
Iscritto al Registro Imprese di Reggio Emilia n. 02509150351
Codice fiscale n. 02509150351 Partita IVA n. 02509150351 Capitale sociale € 4.000.000,00 i.v.
Sito Internet www.ccnservizidipagamento.it Indirizzo di posta elettronica certificata ccnservizidipagamento@legalmail.it
Tel. 0522-905398 Fax 0522-905399 Email info@ccnservizidipagamento.it

COME MANTENERE AL SICURO IL PROPRIO CONTO DI PAGAMENTO

Le principali pratiche illegali per sottrarre denaro o informazioni sensibili sono messe in atto da malintenzionati che fingono di essere il tuo Istituto di Pagamento attraverso e-mail, SMS, chat e telefono. Per un utilizzo responsabile del tuo conto online e per aumentare la tua consapevolezza rispetto alle frodi bancarie, trovi qui un elenco di suggerimenti da mettere subito in pratica.

Diffida da chi ti chiede credenziali o PIN
Le informazioni e gli strumenti con cui accedi ai servizi dell'Istituto (password, utente ecc…) sono strettamente personali e vanno custoditi con cura. L'Istituto può contattarti telefonicamente o via email, ma non ti chiederà mai di fornire credenziali, dati sensibili o codici usa e getta (OTP).

Conserva le tue credenziali in sicurezza
Modifica periodicamente i codici di accesso alla tua area riservata e conservali/memorizzali in maniera sicura (non nel portafoglio!).

Non autorizzare operazioni sconosciute
Controlla regolarmente la movimentazione del conto per assicurarti che non vi siano operazioni sconosciute.

Non accedere all'Internet Banking direttamente da link all'interno di e-mail o sms
Digita tu stesso l'indirizzo web del sito. Le informazioni e gli strumenti con cui accedi ai servizi dell'Istituto (password, codici, ecc…) sono strettamente personali e vanno custoditi con cura. L'Istituto può contattarti telefonicamente o via email, ma non ti chiederà mai di effettuare bonifici dal tuo conto.

Attenzione al nome mittente
Il nome mittente presente nelle comunicazioni (sms o email) ed il numero chiamante, sono falsificabili. Ti ricordiamo che se un sms si accoda a messaggi autentici dell'Istituto non ne garantisce la veridicità; gli smartphone organizzano infatti le comunicazioni in base al mittente, senza valutarne l'affidabilità.

Chiama solo numeri ufficiali
Non chiamare numeri differenti da quelli ufficiali, soprattutto se ricevuti via sms.

FAI ATTENZIONE AL PHISHING VIA SMS

Lo smishing (o phishing tramite sms) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti.

Come funziona lo smishing?
I malintenzionati fanno leva sul timore legato ad un rischio incombente per convincerti ad abbassare il livello di prudenza e a reagire d'impulso. I messaggi di smishing invitano a compiere azioni (cliccare link, effettuare ricariche o bonifici) o fornire informazioni con urgenza, per non rischiare danni (es: blocco del conto o blocco della carta di credito) o sottrazioni di denaro. Di solito, inviano messaggi per chiedere alle vittime di:

- Cliccare un link che conduce ad un finto sito web in cui inserire dati personali, dati del conto di pagamento.

CCN Servizi di Pagamento S.p.A a socio unico
Sede legale Via Kennedy n. 5 - 42040 Campegine (RE)
Istituto iscritto all'Albo degli Istituti di Pagamento tenuto da Banca d'Italia n. 36039.6 Codice ABI 36039.6
Iscritto al Registro Imprese di Reggio Emilia n. 02509150351
Codice fiscale n. 02509150351 Partita IVA n. 02509150351 Capitale sociale € 4.000.000,00 i.v.
Sito Internet www.ccnservizidipagamento.it Indirizzo di posta elettronica certificata ccnservizidipagamento@legalmail.it
Tel. 0522-905398 Fax 0522-905399 Email info@ccnservizidipagamento.it

- Scaricare un allegato che può contenere programmi malevoli capaci di prendere il controllo dello pc/smartphone o accedere ai dati in esso contenuti.
- Rispondere ai messaggi ricevuti, inviando dati personali (il codice fiscale, il PIN dell'Internet banking, il codice usa e getta (OTP) da utilizzare per eseguire operazioni sul conto di pagamento.
- Chiamare un numero di telefono, dove poi un finto operatore o un sistema automatizzato chiede di fornire informazioni di vario tipo, compresi dati del conto di pagamento.

Come difendersi?

Per aiutarti a comprendere al meglio come riconoscere le situazioni di frode, abbiamo stilato una lista di regole che è bene tenere a mente.

- L'Istituto non invia sms con link che rimandano alla pagina di accesso; quindi, se ricevi un sms con un link, evita di inserire le tue credenziali.
- L'Istituto non chiama mai per chiedere PIN, PASSWORD o CODICI USA E GETTA (OTP).
- Il nome mittente presente nelle comunicazioni (sms o e-mail) ed il numero chiamante, sono falsificabili. Ti ricordiamo che, se un sms si accoda a messaggi autentici dell'Istituto non ne garantisce la veridicità; gli smartphone organizzano infatti le comunicazioni in base al mittente, senza valutarne l'affidabilità.
- Digita tu stesso l'indirizzo web relativo al sito dell'Istituto nella barra di navigazione e controlla che il nome del sito sia scritto correttamente.
- Non chiamare numeri differenti da quelli ufficiali, soprattutto se ricevuti via sms.

FAI ATTENZIONE AI TENTATIVI DI VISHING

Il termine "vishing" deriva dall'unione di due parole: "voice" e "phishing". Si tratta di una truffa telefonica usata per ingannare le persone ed ottenere informazioni sensibili, come dati riservati, finanziari o credenziali d'accesso.

Come funziona il vishing?

Il truffatore sfrutta tecniche di manipolazione emotiva (social engineering) e trucchi psicologici per convincerti a rivelare informazioni personali. Solitamente fa leva sull'urgenza della situazione, ad esempio un problema da risolvere, come un pagamento non riconosciuto, per sollecitare risposte rapide e immediate.

Come riconoscerlo?

- Il numero di telefono è sconosciuto oppure sembra un numero autentico (questo è possibile tramite il fenomeno dello spoofing), non ti fidare quindi se vedi il numero dell'Istituto, i truffatori riescono a contraffarlo.
- Chi chiama dice di appartenere ad un call center di un istituto di credito, di una società di software o di telecomunicazioni.
- Ti chiedono di trasferire denaro su un altro account a richiesta. L'Istituto non ti chiederà mai di farlo.

CCN Servizi di Pagamento S.p.A a socio unico
Sede legale Via Kennedy n. 5 - 42040 Campegine (RE)
Istituto iscritto all'Albo degli Istituti di Pagamento tenuto da Banca d'Italia n. 36039.6 Codice ABI 36039.6
Iscritto al Registro Imprese di Reggio Emilia n. 02509150351
Codice fiscale n. 02509150351 Partita IVA n. 02509150351 Capitale sociale € 4.000.000,00 i.v.
Sito Internet www.ccnservizidipagamento.it Indirizzo di posta elettronica certificata ccnservizidipagamento@legalmail.it
Tel. 0522-905398 Fax 0522-905399 Email info@ccnservizidipagamento.it

- L'interlocutore che ti ha telefonato ti chiede di fornire pin o password, di effettuare operazioni di pagamento per mettere al sicuro il tuo conto corrente oppure di scaricare un app sul telefono per controllare da remoto il dispositivo.
- I truffatori possono trovare le tue informazioni di base online (ad es. attraverso i social media). Non presumere che chi chiama sia autentico solo perché possiede questi dati.

Come evitarlo?

- Fai attenzione alle chiamate telefoniche indesiderate.
- Segnati il numero del chiamante e avvisalo che lo richiamerai.
- Per verificare l'identità, contatta direttamente l'Istituto.
- Ricorda quali informazioni personali non dovrai mai fornire e fidati solo delle tue chiamate in uscita.
- Se hai dubbi, interrompi la conversazione e contatta direttamente l'Istituto per assicurarti che si tratti di una procedura regolare.

FAI ATTENZIONE AI MALWARE

I malware sono software sviluppati per compromettere la sicurezza dei tuoi dati. Alcune tipologie di malware possono infettare il tuo dispositivo (PC/ Tablet/Smartphone) attraverso azioni che puoi compiere inconsapevolmente come aprire il file di un'e-mail sospetta o installare un programma scaricato da fonti non sicure.

Per tutelare la sicurezza dei tuoi dispositivi, ti consigliamo di:

- Scaricare sul tuo smartphone solo App da fonti sicure come Play Store o Apple Store.
- Proteggere i tuoi dispositivi con un buon antivirus e mantenerlo sempre aggiornato.
- Evitare di salvare le password sui tuoi dispositivi.
- Non aprire mai allegati e non cliccare su link provenienti da indirizzi sospetti o da persone che non conosci.
- Verificare accuratamente le e-mail contenenti un allegato anche se provenienti da una persona che conosci. Talvolta i computer infettati dei tuoi conoscenti possono inviare e-mail contenenti virus a loro insaputa.
- Prestare attenzione ai siti web a cui accedi: un vettore di infezione dei malware è l'accesso a siti "strani", legati ad esempio a pubblicità online dove viene avviato un download automatico o sfruttata una vulnerabilità per infettare il device.
- Installare adeguati software di protezione antivirus sui tuoi devices (pc, tablet, smartphone) e aggiornarli sempre.
- Accedi al tuo conto online soltanto dai tuoi dispositivi e da reti wifi personali. Le reti wifi pubbliche di hotel, bar, ristoranti o aeroporti sono assolutamente da evitare.