Utilizzo sicuro della ING Corporate Card

Introduzione

L'ING Corporate Card permette di effettuare pagamenti ad esempio per pernottamenti in hotel, congressi, biglietti aerei, ristoranti e taxi. La Corporate Card, tuttavia, offre molto di più.

Varie agenzie di viaggio, ad esempio, hanno optato per le prenotazioni con la praticità della Corporate Card. Sempre più persone utilizzano questa carta grazie alla sicurezza dei pagamenti (per affari).

Naturalmente tutti si aspettano che i loro pagamenti avvengano senza problemi. Questo documento fornisce informazioni su questo argomento. ING compie ogni sforzo per assicurare la sicurezza dei pagamenti. Ma non è sufficiente. Occorre che gli utenti rispettino alcune regole di base, per non dare alcuna possibilità ai criminali.

Questo opuscolo contiene una spiegazione di tali regole di base, consigli su come effettuare i pagamenti in sicurezza riconoscendo le frodi e un'illustrazione delle misure adottate da ING per garantire la massima sicurezza della Corporate Card. Sul retro è riportato un elenco di termini con una spiegazione dei concetti (internet) utilizzati in questo opuscolo.

Pratica e gratuita

Consigliamo di utilizzare l'ING Commercial Card app e il portale ING Commercial Card.
Ciò permette di controllare le transazioni, il conto corrente, le spese totali, il saldo e il limite rimanente. L'ING Commercial Card app si trova nell'Apple App Store e in Google Play (per Android).
Per trovare l'app digitare: ING Commercial Card app
Il portale ING Commercial Card si trova sul sito: www.ingcommercialcard.com

Denunciare direttamente le frodi

Chi è vittima di una frode con la Corporate Card è pregato di comunicarcelo immediatamente. In questo modo potremo aiutare chi è vittima di frodi, ora e in futuro. Siamo raggiungibili 24 ore su 24 e 7 giorni alla settimana, anche dall'estero e ai nostri numeri di accesso locali riportati sul retro.

Indice

1. Le cinque regole di base per un pagamento sicuro

Abbiamo definito le norme di sicurezza uniformi delle banche olandesi in cinque regole di base per l'uso della Corporate Card. In questo modo sono più facili da ricordare.

Regola di base 1: Proteggere i codici

Nessuno dà la chiave di casa a un passante qualunque. E neppure i codici di sicurezza della Carta. Occorre proteggerli in modo adeguato.

- **Ricordare i codici**
  Per i codici di sicurezza/le password, evitare di scegliere l'anno di nascita, il nome di un familiare o un altro codice facile da indovinare. Se si teme di dimenticarli, si possono annotare in modo che non siano decifrabili per le altre persone o come se fossero un rebus. Ad esempio, una frase con delle lettere maiuscole e dei codici ha un alto livello di sicurezza ed è facile da ricordare. Ad esempio: 'Meglio gli U2 della 6a di Beethoven!'. Se tutta la frase è troppo lunga, si possono prendere le iniziali di ogni parola: 'MgU2d6dB!'

- Una possibilità per ricordare il codice pin della Corporate Card è scegliere una parola per ciascuna cifra del codice, con un numero di lettere uguale alla cifra. Con le 4 parole si crea quindi una frase. Immaginiamo di avere il codice pin 9246. Si può ad esempio comporre questa frase: abbaiando (9) il (2) cane (4) arriva (6).

- **Non farsi vedere da nessuno**
  Evitare di farsi vedere da qualcuno mentre si inseriscono i codici. Si può ad esempio coprire la tastiera con il corpo o con la mano libera.

- **Non dare i codici a nessuno**
  Se qualcuno chiede i nostri codici di sicurezza o le nostre password, ad esempio per il portale Commercial Card, non bisogna darli a nessuno. I codici sono rigorosamente personali. Non si devono dare a nessuno, sapendo che i dipendenti di ING non chiedono mai i codici di protezione: né alla reception, né al telefono, né tramite e-mail, né su siti web o app diversi da quelli di ING e in nessun altro modo.

Regola di base 2: Custodire la Corporate Card

Il portafoglio non si lascia mai in giro. E quindi nemmeno la Corporate Card. La carta deve essere custodita correttamente.

- **Maneggiare la Corporate Card con attenzione**
  La Corporate Card è rigorosamente personale. Non la si deve quindi mai dare a nessuno. Non lasciare in giro la Corporate Card e dopo l'uso riporla subito in un luogo sicuro e noto. Occorre evitare che qualcuno sottragga la Corporate Card senza farsi notare.

  Si consiglia di non consegnare la Corporate Card ad esempio a un cameriere, ma di accompagnarlo al terminale di pagamento. Se è indispensabile consegnare a qualcuno la Corporate Card, accertarsi sempre che venga restituita.

  Si consiglia di controllare almeno una volta al giorno di avere ancora la Corporate Card. È un obbligo previsto anche dalle nostre condizioni.

- **Non lasciarsi distrarre**
  Evitare di lasciarsi distrarre durante l'uso della Corporate Card. Se non si presta attenzione, ad esempio, la Corporate Card potrebbe venire sostituita con una carta di credito dello stesso colore. Questo è il trucco dello scambio. Se si ha la sensazione che non sia sicuro utilizzare la Corporate Card, seguire il proprio istinto e riporla in un luogo sicuro.

- **Controllare periodicamente di non avere smarrito la Corporate Card**
  Se qualcuno ci ferma per la strada o ci urta mentre camminiamo, è consigliabile verificare che la Corporate Card non sia stata sottratta. Se non ci viene restituita dopo avere effettuato un pagamento, mettersi immediatamente in contatto con noi (24 ore su 24 e 7 giorni alla settimana) al numero +31 (0)10 428 95 81 o a uno dei nostri numeri di accesso locali (riportati sul retro).

Regola di base 3: Proteggere i dispositivi

La porta di casa si chiude sempre a chiave. Occorre fare lo stesso con i dispositivi che si utilizzano per effettuare transazioni online con la Corporate Card, come il telefono, il tablet, il PC e il laptop, che devono sempre essere protetti. In questo modo, i malintenzionati non hanno la possibilità di installare un software e ad esempio utilizzare un 'trojan' per prelevare dei dati personali, come quelli della Corporate Card.

- **Installare soltanto software legale e noto**
  Impostare il telefono in modo da non consentire l'accesso alle app provenienti da fonti sconosciute. Non effettuare 'Rooting' o 'jailbreaking' del telefono e scaricare le app soltanto dagli app store ufficiali. Installare soltanto software legale di cui si è controllata la provenienza. A questo scopo, andare sul sito web ufficiale del fornitore. In caso di offerta di un programma software sconosciuto, non scaricare immediatamente il programma, ma effettuare prima un controllo con l'antivirus.

- **Utilizzare la versione più recente dell'app e del sistema operativo**
  L'app Commercial Card e il sistema operativo del telefono, del tablet e del computer vengono continuamente aggiornati con tecniche di protezioni migliorate. Occorre quindi effettuare regolarmente gli aggiornamenti. Si consiglia di impostare gli aggiornamenti automatici.

- **Impostare un codice di accesso nei dispositivi**
  L'uso di un codice di accesso impedisce ad altre persone di accedere con facilità ai dati personali. Si consiglia di impostare codici di accesso non soltanto per i dati della Corporate Card, ma anche per i contatti, i messaggi e le foto.

- **Utilizzare un antivirus, un firewall e un anti-spyware**
  Per i pagamenti online con la Corporate Card si consiglia di utilizzare esclusivamente un PC o un computer portatile su cui sono installati un antivirus, un firewall e un anti-spyware. In questo modo si è protetti da virus e programmi indesiderati. Anche per i telefoni e i tablet esistono ora degli antivirus che offrono una maggiore protezione.

- **Proteggere il collegamento internet senza fili (wi-fi)**
  Non effettuare transazioni online con la Corporate Card se il collegamento internet non è protetto. Si consiglia quindi di proteggere il wi-fi con una password. Rivolgersi al provider internet per assistenza. Se si utilizza una rete wi-fi fuori casa, evitare di effettuare transazioni online con la Corporate Card.

Regola di base 4: Controllare i pagamenti e gli addebiti

È sempre opportuno controllare prima ciò che si paga esattamente e anche gli addebiti effettuati. A questo scopo si possono utilizzare il portale ING Commercial Card o la Commercial Card app. La Commercial Card app permette fra l'altro di vedere le transazioni in tempo reale.

- **Sapere ciò che si paga**
  Controllare che l'importo da pagare sia indicato correttamente sul display, oppure sullo scontrino (se ci si trova all'estero e occorre mettere la propria firma). Conservare la copia dello scontrino come promemoria. In questo modo rimane una prova nel caso in cui l'importo riportato sull'estratto della Corporate Card non sia corretto.

  Non rimanere sorpresi quando viene addebitato sulla Corporate Card l'importo pagato in una valuta estera.

- **Procedere nell'ordine giusto**
  Quando si effettua un acquisto online, inserire il numero di carta di credito, la data di scadenza e i codici di sicurezza soltanto quando si è certi dell'acquisto.

- **Controllare online gli addebiti**
  Controllare gli addebiti almeno una volta ogni due settimane. Si può così verificare che le transazioni siano corrette e comunicare direttamente gli eventuali abusi.

- **Denunciare tempestivamente i danni**
  Se si è subito un danno poiché non è stato possibile verificare subito gli estratti della Corporate Card, potrebbe essere necessario fornire una prova. In linea di principio, i danni dichiarati dopo che sono trascorsi trenta giorni dalla data dell'estratto non possono essere rimborsati.

Regola di base 5: Telefonare a ING in caso di dubbio

Se si sa o si sospetta di essere stati vittima di una frode, occorre comunicarlo direttamente a ING. In questo modo possiamo intervenire direttamente e prevenire gli eventuali danni. Ad esempio, facciamo eliminare i finti siti web per evitare che altri clienti subiscano delle frodi.

- **Telefonare subito**
  Se si sospetta una frode, si consiglia di telefonare immediatamente a ING, anche se la Corporate Card, la ING Commercial Card app o user ID del portale ING Commercial Card sono bloccati o se si è ricevuto un messaggio e-mail sospetto e qualcuno ha cercato di carpire i dati della Corporate Card.

- **Essere reperibili**
  In caso di transazioni sospette, è importante essere reperibili rapidamente, al telefono o tramite un sms. Se si desidera lasciare il numero di cellulare al nostro servizio clienti, telefonare al numero **+31 (0)10 428 9581 o a uno dei nostri numeri locali (riportati sul retro)**.

2. Riconoscere le frodi

Nonostante tutte le misure di sicurezza e l'uso prudente, non si può escludere il rischio di uso improprio della Corporate Card. Le informazioni seguenti aiutano a riconoscere i diversi tentativi.

Frodi tramite la Corporate Card

- **Skimming**
  Una forma nota di frode è lo skimming, la copia dei dati della carta di credito che si trovano sulla banda magnetica. Gli anni scorsi sono stati adottati diversi provvedimenti per prevenire lo skimming, grazie ai quali questo tipo di frode è sempre più raro.

- **Furto, scambio o manovre per distrarre**
  Accade ancora che le Corporate Card vengano scambiate o rubate e che i codici di sicurezza vengano visti mentre il titolare della carta li inserisce. Accade anche che le persone vengano distratte allo sportello automatico e che i criminali scappino con il denaro prelevato. Il trucco dei dieci euro è un esempio. Si viene distratti con una banconota da 10 euro in terra; nel frattempo, i criminali prendono rapidamente il denaro dallo sportello automatico.

  Queste forme di frode avvengono soprattutto nei negozi o agli sportelli automatici. Possono spiare il codice da dietro le spalle, mentre il titolare della carta lo digita o distrarlo in vari modi.

Frode tramite il computer

- **Phishing**
  Con il phishing, i malintenzionati 'pescano' i codici di sicurezza tramite un sms, un e-mail o un finto sito web. Si riceve un sms o un messaggio e-mail con la richiesta di fare clic su un link. Si arriva senza accorgerne su un finto sito web, ad esempio il portale ING Commercial Card, a cui viene richiesto di accedere con i codici di sicurezza. Non fare mai clic su link sospetti, ma eliminare subito il messaggio e-mail dalla casella di posta.

  I messaggi di phishing si riconoscono così:
  - Generalmente, il messaggio contiene una motivazione per agire con urgenza.
  - Viene richiesto di fare clic su un link. Si arriva senza accorgerne su un finto sito web, a cui viene richiesto di accedere con i codici di sicurezza.
  - Spesso il messaggio assomiglia a un messaggio della banca.

- **Malware**
  Il malware è software illecito con il quale i malintenzionati possono controllare a distanza il software su un computer di terzi per risalire ai dati di accesso. Il malware può essere installato con facilità su un computer senza antivirus e senza un buon firewall. Spesso ciò accade senza che il proprietario se ne accorda. Un noto esempio di software criminale è il 'trojan'.

  Il malware si riconosce così:
  - Qualche volta le pagine internet hanno un aspetto diverso da quello a cui si è abituati. Ad esempio vi è un campo in più per il numero di telefono.
  - Un computer infettato con malware è più lento e spesso si blocca.

Frode tramite il telefono

- **Phishing**
  Con il phishing, i malintenzionati 'pescano' anche telefonicamente i codici di sicurezza, come il codice pin della Corporate Card, i dati di accesso al portale ING Commercial Card o altri dati personali. Il phishing può avvenire anche tramite un sms, un messaggio e-mail o un finto sito web.

  Spesso i malintenzionati si fanno passare al telefono per qualcun altro, ad esempio un dipendente di ING o di una società informatica o di software. Raccontano una storia credibile, che generalmente richiede di agire subito. A questo punto chiedono i codici di sicurezza. Ricordiamo che i dipendenti di ING (o di altre aziende) non chiedono mai i codici di sicurezza.

  Non si è sicuri che la persona al telefono sia un dipendente di ING? In questo caso, si consiglia di chiedere il suo nome e di telefonarci **al numero stampato sul retro di questo opuscolo**.
  I dipendenti di ING comprendono perfettamente la questione e non avranno nulla in contrario.

  Esempi di finte telefonate:
  - Alcuni giorni dopo avere compilato i dati della carta di credito in un e-mail di phishing, la banca telefona affermando che c'è un problema con la Corporate Card. Se si seguono le istruzioni fornendo alcuni dati aggiuntivi per 'risolvere il problema', in seguito si constaterà che è stata compiuta una frode con la Corporate Card.
  - Qualcuno telefona affermando di essere un dipendente di una società informatica o di software, che chiede di andare su un sito web per installare un software.
  - Spesso sostiene che è necessario per la sicurezza del computer. Il software che si chiede di installare è un malware. Dopo averlo installato, i dati che vengono inseriti in seguito per le transazioni online con la Corporate Card diventano vulnerabili.
  - Una persona si presenta come dipendente di ING e afferma che vuole verificare i dati, ad esempio il nome utente e la password di portale ING Commercial Card.
  - I dipendenti di ING non lo chiedono mai. Non dare quindi i codici a nessuno.

3. Quali sono le misure adottate da ING?

Nella parte precedente abbiamo fornito numerosi consigli e suggerimenti per pagare in sicurezza. Naturalmente, anche ING fa in modo di garantire la sicurezza della Corporate Card, utilizzando varie tecniche visibili e invisibili.

Sicurezza della Corporate Card

- Il chip sulla Corporate Card e l'imboccatura per l'inserimento della carta nello sportello automatico prevengono lo skimming.

- Quando si effettua un pagamento con la Corporate Card, generalmente viene richiesto il codice pin in luogo della firma, poiché è più sicuro.

- Oltre al numero della Corporate Card, sul retro si trova anche il CVC (Card Validation Code, Codice di protezione della carta). Questo codice di tre cifre offre un controllo aggiuntivo.

Sicurezza al momento dei pagamenti

- **SMS Security Alert**
  Nelle transazioni a rischio, per le quali è opportuno effettuare verifiche aggiuntive, alcuni secondi dopo la transazione si riceve tramite SMS un 'Security Alert' (Avviso di protezione). Tramite questo SMS chiediamo di confermare la transazione. Se non è corretta, si prega di comunicarcelo immediatamente; in questo caso, la carta di credito può essere subito bloccata per evitare ulteriori abusi. Il messaggio SMS viene inviato dal numero: +44 78 60 04 74 44.
  - Se si tratta di un acquisto noto, si prega di rispondere come indicato nell'SMS. Non occorre fare nient'altro.
  - Se l'acquisto non è riconosciuto, si prega di rispondere come indicato nell'SMS. In questo caso, ING blocca immediatamente la Corporate Card e invia un secondo SMS contenente informazioni su come procedere.

  Questo servizio è gratuito per tutti i clienti in possesso di una Corporate Card. L'unica informazione che ci occorre è un numero di cellulare corretto. Si prega di telefonare al servizio clienti per verificare di avere fornito a ING il numero di cellulare.

  È importante sapere che se non si risponde all'SMS di protezione, ING non ha alcuna responsabilità in caso di frode. L'acquisto viene effettuato normalmente. A seconda della situazione, la carta può venire (temporaneamente) bloccata in seguito per un acquisto successivo.

- **Mastercard ID check**
  Gli acquisti online presso le aziende che partecipano a Mastercard ID check sono protetti dagli abusi sullo sfondo. In questo caso, viene visualizzato uno schermo con il testo 'Elabora'. Nella maggior parte dei casi, ING esegue tutti i controlli di sicurezza sullo sfondo, ma per alcune transazioni chiediamo di inserire un codice unico. Questo codice viene inviato tramite SMS. Per agevolare le cose, è importante che riceviamo il numero di telefono del titolare.

- **Blocco della Carta**
  Nelle situazioni (molto) sospette, ING può decidere di bloccare preventivamente la Corporate Card. In questo caso, l'utente viene informato prima possibile telefonicamente, tramite sms o per lettera. Se una transizione non va a buon fine, si prega di mettersi immediatamente in contatto con noi.

4. Cosa fare in caso di frode

ING compie ogni sforzo per evitare le frodi. Seguendo i consigli e le raccomandazioni riportati in questo opuscolo, i malintenzionati hanno poche probabilità di commettere delle frodi con la Corporate Card. Se si subisce una frode, saremo lieti di risolvere rapidamente il problema. Procedere come segue:

Denuncia delle frodi

- **Prima possibile**
  Segnalare telefonicamente prima possibile a ING la frode (sospetta). Si può telefonare 24 ore su 24 e 7 giorni alla settimana. Comunicarli in ogni caso entro 30 giorni dalla data dell'estratto (in formato digitale o cartaceo). Una segnalazione tempestiva ci permette di evitare nella maggior parte dei casi che l'importo venga incassato. Si evitano così conseguenze finanziarie impreviste per il titolare o l'azienda. Possiamo inoltre inviare subito una nuova Corporate Card.

- **Modulo per le frodi**
  Dopo la segnalazione telefonica inviamo telefonicamente un modulo per le frodi tramite posta o, se lo si desidera, tramite e-mail. Imponiamo la condizione di restituire il modulo entro 14 giorni. Più rapidamente si restituisce il modulo, più rapidamente è possibile sbrigare la frode. Talvolta potremmo avere bisogno di altre informazioni, poiché sono richieste dal negozio in cui si è verificato l'abuso.

- **Verbale**
  Se è stata commessa una frode con una Corporate Card smarrita, rubata, non ricevuta o non richiesta dal cliente, al modulo per le frodi occorre allegare il verbale di denuncia rilasciato dalla polizia.

Risarcimento dei danni

- **La nostra politica**
  Se il cliente non ha commesso alcun errore, la frode viene sempre risarcita. Nel corso della telefonata, il nostro addetto farà in modo che non venga addebitato nulla al cliente. In alcuni casi tuttavia (ad esempio se abbiamo già inviato l'ordine di incasso), non possiamo evitarlo. Esamineremo sempre la situazione previo accordo con il cliente, in modo da poter effettuare il rimborso prima possibile.

  Il rimborso diventerà definitivo in base alla dichiarazione scritta del cliente e alle nostre ricerche sull'uso improprio della Corporate Card. Lo comunicheremo per iscritto al cliente.

5. Definizioni

A

Anti-spyware
Un anti-spyware è un software per la protezione del computer, che impedisce l'installazione di programmi indesiderati tramite i quali si possono ottenere i dati dell'utente.

Antivirus
Un antivirus è uno degli strumenti che permettono di proteggere il computer. Questo software verifica che il computer non abbia virus e può eliminare i virus.

Attacco DDoS
Durante un attacco DDoS, un sito internet viene assalito con scambio di dati. Tale scambio di dati indesiderati viene bloccato dal firewall. Nel momento in cui lo scambio di dati indesiderato raggiunge dimensioni estreme, il firewall è così impegnato a bloccarlo che non lascia passare nemmeno i visitatori desiderati. ING adotta misure di sicurezza di livello molto elevato, mirate a distinguere gli scambi di dati indesiderati da quelli desiderati.

B

Blocco preventivo
Per proteggere i pagamenti, nelle situazioni sospette ING adotta subito dei provvedimenti. Per proteggere la Corporate Card possiamo bloccarla in modo preventivo, ad esempio se abbiamo il sospetto che sia stata copiata. In questo caso blocchiamo la carta di credito e cerchiamo di metterci immediatamente in contatto con l'utente.

Botnet
Una botnet è una rete di un grande numero di computer infettati da un Trojan o da un virus. In questo modo il computer diventa come un robot, in grado di lavorare in autonomia. I computer infettati possono essere dappertutto e qualunque computer può essere infettato. I malintenzionati possono quindi impartire a questi computer un unico ordine. I computer ad esempio vengono utilizzati per inviare e-mail di phishing o per carpire i dati della Corporate Card dell'utente.

Browser
Un browser è un programma del computer che permette di visitare i siti internet. I browser più noti sono Internet Explorer, Chrome, Firefox e Safari.

C

Chip EMV
Da alcuni anni, per la Corporate Card viene utilizzato il chip EMV, che permette ad esempio di effettuare pagamenti nei negozi con la Corporate Card utilizzando un codice pin. Il chip EMV è uno standard internazionale utilizzato in tutto il mondo. Il chip riduce le frodi con carte di credito nei negozi. Pertanto, la Corporate Card non viene più fatta passare nel lettore di bande magnetiche, ma viene inserita nel dispositivo di pagamento. Ciò permette la lettura del chip EMV

Codice di accesso
Sul computer o sul telefono/tablet è possibile impostare un codice che impedisce alle altre persone di utilizzare il dispositivo.

Commercial Card app
La ING Commercial Card app è l'app ufficiale per la Corporate Card e permette di verificare direttamente le transazioni degli ultimi 12 mesi. Si prega di scaricare l'app nell'Apple App Store o in Google Play (Android) facendo clic su 'ING Commercial Card app'.

Commercial Card portale
Con il portale ING Commercial Card è possibile recuperare gli estratti conto della Corporate Card in formato digitale fino a 12 mesi dopo. Gli estratti conto possono essere scaricati e memorizzati su un supporto digitale a piacere. In questo modo non occorre creare archivi in formato cartaceo.

Cookie
Un cookie è un piccolo file che viene installato da un sito web sul computer dell'utente per memorizzare il suo comportamento durante la navigazione. Molti negozi online utilizzano i cookie, in modo da disporre già dei dati dell'utente alla visita successiva.

Corriere di denaro
Un corriere di denaro mette a disposizione il suo conto corrente bancario per attività criminali. I criminali versano del denaro sul conto corrente bancario, quindi lo passano su altri conti o prelevano i contanti. In questo modo nascondono denaro rubato alla polizia e alla giustizia.

Criminali online
I criminali online commettono reati in internet. Ad esempio inviano messaggi e-mail con i quali chiedono i dati di accesso e/o i dati della carta di credito (phishing). I criminali online realizzano inoltre dei siti web molto simili al sito web di ING. Oppure cercano di prelevare i dati dal computer dell'utente tramite un virus che inviano con un altro programma (un cosiddetto Trojan).

CVC
CVC è l'abbreviazione di Card Validation Code. Si tratta di un codice di protezione a 3 cifre, riportato sul retro della Corporate Card, a destra del campo della firma. Questo codice può essere richiesto al momento del pagamento con la Corporate Card.

Cybercrime
Il cybercrime è la criminalità in internet. I criminali inviano dei messaggi e-mail nei quali richiedono i dati di accesso e/o i dati delle carte di credito (phishing) e creano dei siti web molto simili a quelli di ING. Cercano inoltre di prelevare i dati dal computer dell'utente tramite un virus che inviano con un altro programma (un cosiddetto Trojan).

E

Esperto di sicurezza
Disponiamo di un team di esperti di sicurezza che analizzano costantemente le transazioni e le operazioni sospette e intervengono quando è necessario. ING collabora attivamente con la polizia, con il governo e con altri enti come l'Associazione delle banche olandesi.

Estensione
Un'estensione è un'applicazione aggiuntiva per il browser che può essere scaricata dall'utente e che permette di aggiungere nuove funzioni al browser. Alcuni esempi sono Adobe Reader per la lettura di file pdf e Flash per la visualizzazione di video su YouTube.

F

False e-mail
Vedere la voce 'Phishing'

Firewall
Un firewall è uno degli strumenti che permettono di proteggere il computer. Questo software aiuta a impedire che altre persone accedano al computer dell'utente quando è collegato a internet o a una rete di computer. Un firewall controlla gli scambi in ingresso e in uscita su internet. In caso di scambio di dati sospetto, l'utente riceve un avviso.

Frode
Si possono subire frodi in diversi modi. Questo opuscolo è stato preparato per fornire informazioni sulle frodi.

Furto di identità
Un furto di identità significa che i criminali prelevano i dati personali e finanziari dell'utente e li utilizzano in modo improprio. Alcune abitudini automatiche, come gettare via con noncuranza le informazioni finanziarie, gli estratti della Corporate Card, una firma o una copia della carta d'identità possono agevolare questo tipo di frode. I criminali, tuttavia, prelevano i dati personali anche tramite phishing e social engineering. In seguito un criminale può ad esempio richiedere una carta di credito a nome dell'utente.

H

Henchman
Vedere 'Corriere di denaro'

I

Imboccatura
Un'imboccatura è un componente che si monta nella fessura in cui si introduce la carta di credito allo sportello automatico. L'imboccatura impedisce ai criminali di montare un lettore di carte di credito che copia i dati. La copia dei dati della carta di credito è detta skimming. L'imboccatura può variare da uno sportello automatico a un altro. Lo schermo dello sportello automatico visualizza l'imboccatura giusta.

J

Jailbreak
Per Jailbreak si intende l'aggiramento di una protezione del sistema operativo di un iPhone, di un iPod touch o di un iPad. In questo modo, la persona può ad esempio installare delle app non approvate da Apple. A seguito di un'operazione di questo tipo, il dispositivo è più esposto a virus e malware.

M

Malware
Per malware si intende un software maligno e/o nocivo. La parola è una contrazione dell'inglese 'malicious software' (software maligno). Il malware viene progettato appositamente per infiltrarsi in un computer senza che l'utente se ne accorga. Il malware, ad esempio, può infiltrarsi nel computer tramite un messaggio e-mail o un'immagine su un sito web.

Mastercard ID check
Vedere il capitolo 'Quali sono le misure adottate da ING?'

Money mule
Vedere 'Corriere di denaro'

N

NCSC
Nationaal Cyber Security Centrum. Cooperazione fra il governo e le aziende. Missione: il NCSC contribuisce a migliorare la difendibilità della società olandese nel dominio digitale e, con essa, a creare una società informatica sicura, aperta e stabile offrendo conoscenze e una prospettiva delle operazioni.

P

Phishing
Per phishing si intende la 'pesca' dei dati personali da parte di criminali con un unico obiettivo: prelevare informazioni sulla Corporate Card e utilizzarle per effettuare delle transazioni. Può avvenire tramite e-mail, telefono o un sito web. Ad esempio viene richiesto di fare clic su un link in un finto messaggio e-mail. Il messaggio assomiglia a un messaggio inviato da ING. Senza accorgersene, l'utente accede a un finto sito web in cui inserisce i dati della Corporate Card. Senza che se ne accorga, i criminali possono così effettuare delle operazioni con la Corporate Card.

R

Ransomware
Ransomware è un metodo di ricatto tramite malware. Ransomware è un programma che blocca il computer e chiede del denaro per 'liberarlo'. I pagamenti (ad esempio tramite la Corporate Card) non permettono di 'liberare' il computer, poiché i criminali vogliono impossessarsi del denaro.

Rilevamento
Per rilevamento si intende il rintracciamento di operazioni sospette. ING dispone di un team di esperti che si occupa quotidianamente della sicurezza dei pagamenti, analizzando costantemente le transazioni e le operazioni sospette e intervenendo quando necessario. ING collabora attivamente con la polizia, lo Stato e altri enti nazionali e internazionali. In questo modo è in grado di fornire informazioni rapidamente e con precisione.

Rooting
Per Rooting si intende l'aggiramento di una protezione del sistema operativo Android di un telefono o di un tablet. Eseguendo il rooting, la persona può ad esempio installare delle app non approvate per l'Android Market. A seguito di un'operazione di questo tipo, il dispositivo è più esposto a virus e malware.

S

Security Alert Service
Vedere il capitolo 'Quali sono le misure adottate da ING?'

Skimming
Per skimming si intende l'esecuzione di una copia dei dati della Corporate Card montando un lettore di carte di credito aggiuntivo nella fessura dello sportello automatico in cui si inserisce la carta di credito. I criminali rilevano quindi il pin personale e prelevano il denaro utilizzando i dati carpiti tramite skimming. Montando delle speciali imboccature nella fessura di inserimento delle carte di credito, ING cerca di prevenire il montaggio di lettori di carte di credito ad opera di criminali. Inoltre, incoraggiamo i responsabili a controllare periodicamente che i criminali non abbiano manomesso lo sportello automatico.

Sistema operativo
Un computer, un tablet o uno smartphone possono funzionare correttamente soltanto se vi è installato un software. Il software scritto affinché questi dispositivi funzionino correttamente è definito un sistema operativo.

Smishing
Lo smishing è il phishing tramite sms. Vedere la voce 'Phishing'

Social engineering
Con il social engineering, i criminali cercano di prelevare le informazioni riservate degli utenti. Sfruttano in modo improprio delle caratteristiche umane, come la curiosità, la fiducia, l'ingordigia, la paura e l'ignoranza. Il social engineering ha molte forme, dai falsi siti web, al phishing dei messaggi e-mail, alle conversazioni telefoniche, ai contatti personali alla porta. I criminali chiedono di eseguire determinate azioni, come compilare i dati personali, i codici di sicurezza o i dati della carta di credito, premere un pulsante o installare del malware.

Software antivirus
Vedere 'Antivirus'

Spyware
Lo spyware è un software che viene installato sul computer dell'utente (senza che questo se ne accorga). In questo modo è possibile prelevare i dati dell'utente e inviarli a terzi.

T

Trucco dei dieci euro
I criminali cercano di distrarre la persona che sta prelevando del denaro buttando in terra una banconota da dieci euro. Dicono alla persona che li ha persi e nel frattempo rubano il denaro prelevato dallo sportello automatico.

Trojan (o cavallo di Troia)
Trojan deriva da Trojan horse (cavallo di Troia). Un Trojan è un programma camuffato da file innocuo, che viene installato sul computer di terzi senza farsi notare, permettendo ai criminali di accedere a distanza a un computer di terzi, senza che questi se ne accorgano. Tramite i Trojan possono ad esempio risalire al nome utente e alla password per accedere a portale ING Commercial Card.

V

Virus
Un virus è una forma di software nocivo. I virus possono arrecare gravi danni al computer, cancellando le informazioni (riservate). Utilizzando un virus, inoltre, i criminali possono accedere al computer e prelevare il nome utente e la password.

Virus informatici
Vedere la voce 'Virus'

W

Password
Per eseguire operazioni bancarie sicure, è necessario avere una password sicura. Una password è sicura quando è impossibile da indovinare e da craccare. Si raccomanda quindi di utilizzare password sicure per tutti gli ambienti online.

Wi-Fi
Wi-Fi è l'abbreviazione in inglese di rete senza fili. La rete senza fili serve per accedere a internet.

Worm
Un worm cerca di diffondersi nelle reti e si sposta in modo automatico, come in una reazione a catena. Generalmente ciò avviene tramite gli indirizzi e-mail che si trovano su un computer infettato.

6. Numeri di telefono importanti

In caso di frode (sospetta), ci si può mettere in contatto con noi 24 ore su 24 e 7 giorni alla settimana al numero di telefono

+31 (0)10 428 95 81

o ai nostri numeri locali. Questi numeri si trovano sul sito

www.ingwb.com/cardcontact

Siamo sempre a disposizione del cliente!

PCM339 0918 © ING Bank N.V.

ING