Domande e risposte

Che cos'è Card Security e chi vi si cela dietro?
Card Security è un'iniziativa di prevenzione su scala nazionale pensata per proteggere la popolazione dalle frodi con carte di debito e di credito. Card Security si rivolge alla popolazione con campagne mirate, tramite i social media, il sito web card-security.ch, reportage e canali d'informazione dei partner interessati. Il lavoro di prevenzione è incentrato sulla sensibilizzazione e sulle attuali tipologie di frodi e sulla comunicazione di regole comportamentali da adottare nell'uso delle carte di debito e di credito. Anche gli specialisti della polizia e degli istituti finanziari possono ottenere informazioni approfondite in merito sulla piattaforma.

Mittente di Card Security è la polizia. L'iniziativa è sostenuta dall'associazione Card Security, il cui comitato direttivo si compone di rappresentanti delle società emittenti carte di pagamento e della polizia. L'iniziativa è frutto di un'ampia collaborazione tra la polizia, le società emittenti carte di pagamento e le banche.

Perché serve Card Security?
Le frodi con carte di credito o di debito aumentano ogni anno del 10-20 per cento. Card Security è il punto di contatto centrale della polizia per tutte le domande inerenti all'abuso delle carte di pagamento. Card Security riunisce il know-how di vari esperti della polizia, degli istituti finanziari e delle società emittenti carte di pagamento. Sul sito web card-security.ch le e i titolari di carte, la polizia e i dipendenti delle banche possono trovare informazioni approfondite sulle più recenti frodi ai danni delle carte di pagamento e su tutte le misure di prevenzione.

Card Security si rivolge anche agli specialisti e alle specialiste. Sul sito web card-security.ch i corpi di polizia e le banche trovano le attuali campagne, materiali informativi e articoli aggiornati sull'argomento.

«LINDA protegge dal phishing!» – Che cosa s'intende?
La campagna 2026 di Card Security ha per motto «LINDA protegge dal phishing!» LINDA è una pescatrice e ogni lettera del suo nome è sinonimo di una frase promemoria con la quale è possibile impedire il phishing:

L = Link e allegati: non fidarti mai
I = Idee e contenuti: controllali prima
N = Neutralità: fai attenzione!
D = Domanda urgente: occhio!
A = Autore del messaggio: verificalo sempre

L'acronimo LINDA aiuta le e i titolari di carte di pagamento, ricordando loro le principali norme di comportamento quando usano carte di debito e di credito, e contribuisce a evitare casi di phishing.

A chi è rivolta la piattaforma Card Security?
È rivolta alla vasta popolazione, in particolare alle e ai titolari di carte di debito e di credito. Inoltre, la piattaforma offre numerose informazioni utili per i professionisti della polizia e degli istituti finanziari.

Le frodi con carte di pagamento sono aumentate negli ultimi anni?
In passato le frodi con carte di pagamento venivano perpetrate soprattutto presso i terminali di pagamento e i bancomat. Questi cosiddetti casi di skimming sono diminuiti sensibilmente. Oggi le frodi con carte di pagamento si verificano nella maggior parte dei casi online. Le frodi di questo tipo aumentano ogni anno del 10-20 per cento.

Quali sono le frodi più frequenti in rete?
La maggior parte delle frodi con carte di pagamento in rete iniziano con il phishing. Manipolando astutamente le proprie vittime, i malfattori le inducono a trasmettere codici PIN, codici SMS, numeri CVC/CVV o password. Ciò avviene p. es. attraverso siti web o codici QR fasulli, link presenti in e-mail, telefonate o messaggi brevi (SMS, WhatsApp, servizi di messaggistica istantanea ecc.). Con questi dati i malfattori riescono poi facilmente a rubare il denaro alle loro vittime.

Come possono le vittime dimostrare di non essere cadute nella trappola del phishing?
È difficile. Spesso le vittime non si ricordano neanche più di avere ricevuto un'e-mail di phishing e di aver lasciato i propri dati personali in un sito contraffatto. Nella maggior parte dei casi passa infatti molto tempo tra l'acquisizione dei dati e le transazioni fraudolente.

Perché le banche non assumono la responsabilità o mostrano più correntezza nei casi di frode?
La responsabilità è disciplinata nei contratti stipulati tra la banca e i suoi clienti. In caso di controversia, la questione della responsabilità va chiarita in sede giudiziaria. Si può però supporre che la banca non risponde se la vittima della frode ha violato l'obbligo di diligenza.

È sensato sporgere denuncia contro ignoti?
Sì. I truffatori che si muovono in Internet lasciano tracce che possono essere seguite. A seconda della tattica di dissimulazione adottata, tuttavia, è difficile arrivare ai malfattori. Per questo è importante sporgere denuncia alla polizia. Solo in tal modo la polizia è in grado di accedere a elementi importanti per le indagini e di riconoscere anche la portata della minaccia.

Solo se la polizia (in qualità di organo di perseguimento penale) ha un quadro completo della situazione può avviare misure transfrontaliere. Questo rafforza anche gli sforzi di prevenzione, poiché consente di acquisire nuove conoscenze.

A seconda della procedura seguita dai truffatori, risulta tuttavia difficile scoprire dov'è finito il denaro. Spesso vengono impiegati i cosiddetti money mule (riciclatori di denaro) che agiscono in Paesi che pongono la polizia di fronte a enormi sfide o che si avvalgono di servizi anonimizzati per dissimulare le tracce.

È forse più sicuro pagare con denaro contante?
Il contante sta perdendo sempre più importanza. Spesso non è possibile neppure più pagare in contanti. È quindi ancora più importante che i titolari di carte di pagamento si tutelino il più possibile quando utilizzano carte di credito o di debito e adottino i pochi consigli di prevenzione. La stragrande maggioranza delle frodi con carte di pagamento può essere evitata attenendosi a tali consigli.

I consigli di prevenzione sono riassunti sulla piattaforma di prevenzione card-security.ch/it/proteggi-le-tue-carte/.

Cosa posso fare per tutelarmi dalle frodi con carte di pagamento?
LINDA protegge dal phishing!

L = Link e allegati: non fidarti mai
I = Idee e contenuti: controllali prima
N = Neutralità: fai attenzione!
D = Domanda urgente: occhio!
A = Autore del messaggio: verificalo sempre