



Bonifici istantanei, nuove regole dal 9 ottobre: ecco le 6 frodi bancarie da evitare

Descrizione

(Adnkronos) â??

Cosa cambierÃ con la normativa sui bonifici istantanei prevista dal 9 ottobre e quali sono le truffe piÃ¹ diffuse? A chiarirlo l'Unione nazionale consumatori e CBI, hub per l'innovazione tecnologica e la digitalizzazione. Ogni giorno migliaia di italiani utilizzano i bonifici per pagamenti online, vendite su marketplace e transazioni commerciali. Ma dietro questa comoditÃ si nasconde un pericolo crescente: le truffe bonifico sono in costante aumento. I numeri parlano chiaro:â?le frodi sui pagamenti digitali hanno raggiunto livelli record, con perdite importanti per consumatori e aziende. Dalle vendite online false ai finti fornitori, dai messaggi phishing ai ceo fasulli, i truffatori hanno affinato tecniche sempre piÃ¹ sofisticate. La buona notizia? Dal 9 ottobre 2025 un nuovo servizio chiamato Vop (Verification of payee), verifica del beneficiario, rivoluzionerÃ la sicurezza dei bonifici istantanei. Il servizio Vop rappresenta il piÃ¹ importante aggiornamento per la sicurezza bancaria degli ultimi anni. La novitÃ piÃ¹ importante? Quando inserisci i dati per un bonifico, la banca verifica automaticamente se lâ??Iban appartiene davvero alla persona o azienda indicata. Ma intanto, ecco le 6 truffe bonifico piÃ¹ pericolose e come riconoscerle prima che sia troppo tardi. 1) Truffa vendita online: il bonifico che non câ??Ã. Come funziona:â?hai messo in vendita la tua vecchia bicicletta su un sito di annunci. Un potenziale acquirente si dice interessato e ti invia la prova di aver effettuato un bonifico. Ti chiede di spedire subito il prodotto perchÃ© ha fretta. Ma attenzione: il bonifico Ã solo ordinato, non eseguito. Il trucco:â?i truffatori sfruttano il fatto che i bonifici ordinari non sono immediati. Possono essere revocati entro il giorno lavorativo successivo se non câ??Ã copertura sul conto. Ricevi la conferma dellâ??ordine di pagamento, spediscei lâ??oggetto, ma poi il pagamento viene annullato. Come difendersi: mai spedire prima di aver ricevuto lâ??effettivo accredito sul conto; diffidare di acquirenti che premono per spedizioni immediate; verificare sempre che i soldi siano realmente disponibili sul proprio conto prima della consegna. 2) Frode fornitore: quando lâ??Iban cambia allâ??improvviso. Come funziona:â?ricevi una mail apparentemente dal tuo fornitore abituale che ti comunica un 'cambio delle coordinate bancarie' per i pagamenti futuri. Lâ??email sembra autentica, ha loghi e grafica ufficiali, ma Ã un falso. Il trucco:â?i criminali intercettano le comunicazioni tra te e il fornitore (spesso violando caselle email) e si inseriscono nella conversazione. Una volta effettuato il bonifico sul nuovo Iban, i soldi spariscono definitivamente. Come difendersi: verificare sempre telefonicamente i cambi di coordinate bancarie; non fidarsi mai di comunicazioni via email per modifiche agli Iban; controllare attentamente mittente e dettagli delle comunicazioni; utilizzare canali alternativi (telefono, contatto diretto) per confermare. 3)

Phishing bancario: le nuove tecniche dei truffatori. Come funziona: arriva un sms o un'email allarmante: 'operazione sospetta sul tuo conto, clicca qui per verificare'. Il link porta a un sito identico a quello della tua banca, inserisci le credenziali e hai appena dato le chiavi del tuo conto ai truffatori. Il trucco: i criminali creano copie perfette dei siti bancari. Una volta ottenute le credenziali, accedono al tuo conto e dispongono bonifici verso i loro conti. Come difendersi: mai cliccare link in sms o email bancarie sospette; accedere sempre digitando manualmente l'indirizzo della banca; e banche non chiedono mai credenziali via email o sms; verificare sempre l'URL del sito (deve iniziare con https://). 4) Falso rimborso: la truffa che svuota il conto. Come funziona: ti contattano spacciandosi per un'azienda, un ente pubblico o addirittura l'Agenzia delle Entrate. Ti dicono che hai diritto a un rimborso, ma per riceverlo devi prima pagare 'le spese di pratica' con un piccolo bonifico. Il trucco: il rimborso non esiste. Una volta inviato il bonifico per le spese, i truffatori spariscono. A volte chiedono anche dati personali per completare la pratica, che poi usano per altre truffe. Come difendersi: nessun ente chiede mai bonifici per erogare rimborsi; verificare sempre contattando direttamente l'ente coinvolto; diffidare di comunicazioni non richieste su presunti rimborsi; non fornire mai dati bancari per telefono. 5) Manomissione Iban: la truffa invisibile piÃ¹ pericolosa. Come funziona: questa Ã¨ forse la truffa piÃ¹ sofisticata. I criminali intercettano le tue comunicazioni email (tramite malware o violazioni) e modificano gli Iban nelle fatture o negli ordini di pagamento prima che ti arrivino. Il trucco: tu ricevi regolarmente la fattura del tuo fornitore, ma l'Iban Ã¨ stato modificato durante la trasmissione. Effettui il bonifico in buona fede, ma i soldi finiscono ai truffatori. Come difendersi: mantenere sempre aggiornato l'antivirus; verificare periodicamente gli Iban dei fornitori abituali; fare attenzione a 'improvvisi' cambi di coordinate; utilizzare sistemi di posta elettronica sicuri. 6) Business e-mail compromise: la frode del ceo che ruba milioni. C'Ã¨ poi una sesta truffa sempre piÃ¹ diffusa, che riguarda le aziende e ha provato a toccare anche noi di Unione nazionale consumatori. Come funziona: Ã¨ successo anche a noi. L'amministrazione di Unc ha ricevuto un'email dal nostro Presidente che chiedeva un bonifico per un'operazione urgente. A destare sospetti nell'incaricata, la cifra e soprattutto il tono troppo perentorio. Il trucco: i cybercriminali studiano l'organizzazione aziendale attraverso i social network e creano email false. Sfruttano la gerarchia aziendale e la paura del dipendente di contraddire il capo. Come difendersi: verificare sempre telefonicamente richieste inusuali di bonifici; nessuna operazione legittima richiede segretezza assoluta; stabilire procedure aziendali chiare per i pagamenti; ormare i dipendenti a riconoscere queste truffe.

Ecco le 5 regole essenziali per proteggere i propri pagamenti. 1) Diffida sempre dell'urgenza: i truffatori fanno leva sulla fretta per evitare che tu ragioni. 2) Verifica sempre con canali alternativi: se qualcosa ti sembra strano, controlla per telefono. 3) Non fidarti ciecamente delle email: anche quelle piÃ¹ convincenti possono essere false. 4) Tieni aggiornati i sistemi di sicurezza: antivirus e sistemi operativi sempre all'ultima versione. 5) Quando hai dubbi, aspetta: meglio perdere un'occasione che cadere in una truffa. economicawebinfo@adnkronos.com (Web Info)

Categoria

1. H24News

Tag

1. adnkronos
2. Ultimora

Data di creazione

Settembre 13, 2025

Autore

andreaperocchi_pdnrf3x8

default watermark