Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti
Die Stimme der VerbraucherInnen
La voce dei consumatori

Centro Tutela Consumatori Utenti

Via Dodiciville 2
39100 Bolzano
Tel. 0471 975597
info@verbraucherzentrale.it

Scena del crimine: lo smartphone

Mer 13/10/2021 - 11:10

Truffatori a “pesca” di dati con sms o e-mail truffaldine
Da conti e carte spariscono importi a 4 zeri

Lo spazio digitale offre infinite possibilità – ma infinite paiono anche le attività criminali che vi si sviluppano. Nelle ultime settimane al Centro Tutela Consumatori Utenti (CTCU) sono pervenute le chiamate di molti consumatori, alcuni dubbiosi su messaggi che hanno ricevuto sui propri cellulari, altri disperati per importi, fino a 5.000 euro, purtroppo spariti da carte o conti.

Il tutto prende il via con un, all’apparenza innocuo, SMS: il prestatore di servizi finanziari (o così pare) comunica che vi sono dei problemi con la carta, il conto, l’account, e prega di eseguire un login ad un link dato, per ovviare al problema.

La pagina che si apre pare poi del tutto autentica, e si serve anche di una connessione sicura attraverso https – ma chi controlla con estrema attenzione nota che l’indirizzo non è quello usuale. Ma chi di noi se ne accorgerebbe, soprattutto quando si ha fretta di fare il login, visto che ci è stato segnalato un problema da risolvere urgentemente con la carta o il conto?

Purtroppo a quel punto il danno può già essersi concretato – i dati di accesso sono stati “pescati”, ed i truffatori hanno avuto accesso alla carta o al conto. Con l’entrata in vigore della nuova direttiva sui servizi di pagamento (PSD2), che ha imposto un’autenticazione al login in due passi, questi problemi si pensavano superati – ma al CTCU si registra un aumento dei casi di truffa, e non una diminuzione (vedasi anche ultimi comunicati al riguardo).

Il rimedio è quindi uno solo: mantenere la calma, ed eseguire tutte le operazioni affidandovi anche al buonsenso. Se volete contattare il prestatore di servizi, utilizzate sempre i riferimenti che trovate sull’estratto conto oppure sul sito ufficiale dello stesso.

Alcuni consigli:
Gli istituti bancari e le aziende serie non richiedono mai password, numeri di carte di credito o altre in-

formazioni personali; non vi chiedono inoltre mai di andare su un determinato sito e inserire i dati di login. Se ricevete un simile invito, diffidate!
Quando eseguite il login, digitate l'indirizzo web a mano, ed usate l'indirizzo ufficiale – non cliccate sui link contenuti in messaggi oppure e-mail (se fosse troppo faticoso digitare l'indirizzo ad ogni login, si può posizionare un "segnalibro" digitale alla prima visita).
Nel caso vi venga richiesto di inoltrare o comunicare delle password ad utilizzo unico (le cd. OTP, che arrivano ad es. per SMS sul cellulare), devono squillare tutti i campanelli d'allarme: queste password sono destinate esclusivamente a voi!

In caso di dubbi, contattate il vero prestatore di servizi per ogni più opportuna verifica. Anche il Centro Tutela Consumatori Utenti e la Polizia Postale possono aiutarvi.

Maggiori informazioni e consigli per proteggervi dal "phishing" le trovate anche al seguente link: https://www.kaspersky.it/blog/phishing-ten-tips/6913/

Nel caso ci si dovesse accorgere di operazione bancarie fraudolente a valere sul proprio conto o su quello della propria carta di credito, la procedura da seguire è sempre la stessa:

- blocco immediato della carta o del conto;
- presentazione di una denuncia-querela alla più vicina stazione di pubblica sicurezza (Polizia, Carabinieri);
- invio di un reclamo scritto all'emittente la carta o alla propria banca, con la precisazione di disconoscere le operazioni fraudolente rilevate sull'estratto conto e con richiesta di riaccredito immediato delle relative somme sottratte;
- a fronte di una risposta negativa o di una non risposta da parte dell'intermediario nei 60 gg. Successivi al reclamo, l'utente ha la possibilità di inoltrare successivamente un ricorso all'Arbitro Bancario Finanziario (ABF – www.arbitrobancariofinanziario.it) che provvederà ad esaminare il caso e a fornire una decisione in merito.