TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Phishing

Come individuare e-mail, chiamate e messaggi sospetti e come gestirli adeguatamente

Il phishing è un tentativo di accedere a informazioni sensibili come codici delle carte di credito, password e informazioni sui conti attraverso siti web, e-mail, telefonate e sms apparentemente innocui. Scoprite come individuare i tentativi di furto di informazioni e di frode e come gestirli.

Attenzione al phishing – come proteggervi

Diffidate dei contatti non richiesti

Fate attenzione alle comunicazioni inattese, siano esse e-mail, chiamate telefoniche o fax, in apparenza provenienti da banche, società fornitrici di carte di credito o aziende online presso le quali avete un account. Non divulgate mai informazioni confidenziali se non siete sicuri di chi sia il mittente / l'interlocutore o quale sia il motivo della richiesta. Se siete in dubbio riguardo a una comunicazione inviata a nome di TopCard, la preghiamo di informarci.

Se un'e-mail vi sembra sospetta non cliccate sui link e non scaricate gli allegati

A volte può essere difficile distinguere tra un'e-mail vera e un tentativo di phishing. Un indirizzo del mittente insolito, errori di ortografia ed elementi strani come il tono del messaggio, i disclaimer e i logo devono mettervi in guardia. Se avete dubbi sull'autenticità del messaggio non cliccate sui link e non aprite gli eventuali allegati.

Visitate soltanto siti web affidabili

L'indirizzo di un sito web sicuro inizia con https://. Registrate i siti web che visitate di frequente nella vostra lista dei favoriti. Non inserite mai dati confidenziali in formulari elettronici se non siete sicuri della legittimità del sito. Tenete inoltre presente che TopCard non invia messaggi con link a pagine di login come ad esempio E-Banking e non vi chiederà mai il vostro numero di contratto E-Banking o il vostro PIN.

TOPCARD

TopCard Service AG
Flughofstrasse 35
8152 Glattbrugg

www.topcard.ch

Ignorate le e-mail relative a presunti movimenti insoliti sul conto

Le e-mail di phishing sono spesso concepite per destare la vostra curiosità, mettervi in agitazione o sotto pressione in modo che clicchiate su un link o apriate un allegato. È molto improbabile che un'organizzazione legittima vi contatti tramite posta elettronica per informarvi in merito a pagamenti sospetti o bonifici dal vostro conto. Cancellate questo genere di messaggi e vuotate il cestino del programma. Pensate a utilizzare filtri antispam per bloccare questi messaggi in futuro.

Aggiornate il vostro software

Per una protezione ottimale accertatevi regolarmente che il vostro sofware antivirus sia aggiornato. Utilizzate eventualmente filtri antispam e applicazioni «antiphishing» per proteggervi da potenziali rischi di phishing su siti web e nelle e-mail.