Truffe online: attenti al falso sito della Geox

Attenzione all'ennesimo tentativo di truffa online che questa volta sfruttava un falso sito internet nel quale si pubblicizzava la vendita, a prezzi irrisori, di articoli del marchio di scarpe e abbigliamento Geox.

Il sito truffaldino "geoxoutlet.online", utilizzava logo e informazioni del tutto simili a quelli che compaiono sui canali ufficiali dell'azienda, inducendo gli utenti a fare acquisti online nella convinzione di trovarsi su uno store outlet ufficiale della società, la quale ha comunicato che si tratta di un sito falso.

Quando acquistate online fatelo con molta attenzione e seguite i consigli della Polizia postale:

utilizzate software e browser completi e aggiornati, installando sui vostri dispositivi un antivirus aggiornato all'ultima versione;

attenzione al prezzo, non sempre il più basso è un buon affare, e diffidate dei siti che propongono articoli a prezzi irrisori perché potrebbero nascondere una truffa;

date la preferenza a siti certificati o ufficiali, verificando sempre la presenza di certificati di sicurezza quali TRUST e VERIFIED / VeriSign Trusted che permettono di validare l'affidabilità del sito;

prima di completare l'acquisto verificate che il sito sia fornito di riferimenti quali un numero di partiva Iva, un numero di telefono fisso, un indirizzo fisico e ulteriori dati per contattare l'azienda. Un sito privo di tali dati probabilmente non vuole essere rintracciabile e potrebbe avere qualcosa da nascondere. I dati fiscali sono facilmente verificabili sul sito istituzionale dell'Agenzia delle entrate;

fate una ricerca sull'attendibilità del sito attraverso i motori di ricerca, forum o sui social, analizzando commenti e feedback di altri acquirenti;

per i pagamenti utilizzate soprattutto carte di credito ricaricabili;

per completare una transazione d'acquisto sono indispensabili pochi dati come numero e scadenza della carta e indirizzo per la spedizione della merce, se un venditore chiede ulteriori dati probabilmente vuole assumere informazioni personali (numero del conto, Pin o password) che non dovete divulgare;

la presenza del lucchetto chiuso in fondo alla pagina o di "https" nella barra degli indirizzi sono ulteriori conferme sulla riservatezza dei dati inseriti nel sito e della presenza di un protocollo di tutela dell'utente, ovvero i dati sono criptati e non condivisi;

non cadete nella rete del phishing o dello smishing attraverso i quali i cybertruffatori, utilizzando mail o sms contraffatti, richiedono di cliccare su un link al fine di raggiungere una pagina web trappola simile a quella originale, con lo scopo di rubare i vostri dati sensibili.

29/05/2020