Dietro i grandi numeri degli acquisti online ci sono in agguato anche le organizzazioni criminali di tutto il mondo pronte a inserirsi nelle transazioni o impegnate ad architettare truffe in cui sono numerosissime le vittime.

E proprio per arginare il fenomeno criminale che sta dietro al piatto ricco dell’e-Commerce che le polizie di tutto il mondo si sono unite e hanno attuato dei protocolli operativi per contrastare questa forma di criminalità senza confini.

Su questo fronte si è da poco conclusa l’operazione internazionale “e-Commerce Action 2018”, sostenuta da 28 Paesi dal 4 al 15 giugno 2018, con un centinaio di truffatori professionisti arrestati, responsabili di oltre 20 mila transazioni fraudolente con carte di credito compromesse, per un valore stimato di oltre 8 milioni di euro.

L’azione è stata coordinata dal Centro europeo per il Cyber Crime (EC3 European Cyber Crime Center) presso la sede di Europol all’Aia, che ha ricevuto la collaborazione diretta dei negozi di e-commerce, dei commercianti, delle società di logistica, di banche e dei gestori di carte di pagamento.

La Polizia postale e delle comunicazioni si è distinta in ambito internazionale per gli ottimi risultati conseguiti che hanno consentito di segnalare all’Autorità giudiziaria 35 persone di cui 11 finite agli arresti.

All’azione operativa fa seguito una campagna di prevenzione e sensibilizzazione, denominata #BuySafePaySafe con consigli e comportamenti da tenere per non cadere vittime di frodi.

I sistemi più comuni utilizzati dai cyber-criminali per commettere reati su internet sono il phishing, gli attacchi attraverso malware, la creazione di siti web clone e l’utilizzo di piattaforme di social media per commettere le truffe.

I social media vengono utilizzati per creare profili di vendita (negozi), pubblicizzare la merce, in genere offerta a metà prezzo o comunque a cifre molto vantaggiose, per carpire i dati finanziari delle ignare vittime. Successivamente, i truffatori effettuano gli acquisti – spesso molto costosi – con tali dati.

Altro sistema utilizzato è quello di “acquistare”, direttamente nel Dark web, i dati sensibili delle carte di pagamento, in precedenza sottratti magari con attacchi a banche dati attraverso malware o phishing.

Alla fine, oltre ai clienti che percepiscono il danno solo quando la merce non giunge a

destinazione o quando il corrispettivo viene addebitato, sono le banche e i commercianti a subire le perdite di questa attività criminale, che raggiunge i miliardi di euro in tutto il mondo, nel corso dell’anno.

Per saperne di più su uno shopping online sicuro, visitate la pagina dedicata al Commercio elettronico.