CERT-RO: O noua campanie de phishing vizeaza clientii serviciului OLX România

Centrul National de Raspuns la Incidente de Securitate Cibernetica (CERT-RO) avertizeaza în legatura cu o noua campanie de phishing care vizeaza clientii serviciului OLX România.

Conform avertizarii postate pe site-ul institutiei, echipa CERT-RO a primit în ultimul timp numeroase notificari cu privire la incidente de securitate cibernetica de tip frauda, propagate prin intermediul serviciului OLX si prin WhatsApp.

"Atacatorii contacteaza un utilizator care a publicat un anunt de vânzare a unui produs pe OLX, se declara interesati de achizitie, apoi sustin ca au efectuat plata. Dar, pentru încasarea sumei corespondente ar fi necesara accesarea unui link si introducerea datelor cardului pe care ar trebui virata suma. Desigur, este vorba despre o capcana, atacatorii sistând orice conversatie dupa ce primesc datele de card, iar victimelor li se extrag bani din cont", explica expertii CERT-RO.

Potrivit acestora, utilizatorii serviciului OLX care pun spre vânzare anumite produse sunt contactati direct de potentiali cumparatori. La scurt timp, folosind un anumit pretext, clientul fals muta conversatia de pe OLX pe un alt canal de comunicare, de regula WhatsApp.

"De cele mai multe ori, mesajele primite au o exprimare ciudata, desi sunt în limba româna. Este un semn ca acel text ar putea fi fost tradus cu un instrument disponibil gratis online. Greselile gramaticale sau repetitia unor termeni în cadrul aceleiasi propozitii pot fi astfel de indicii, asa ca analizati cu atentie informatiile, înainte de clic", semnaleaza specialistii în securitate cibernetica.

Urmatorul pas pe care atacatorii îl fac este informarea potentialelor victime ca produsul a fost deja achitat. Acestia genereaza un link fals unde vânzatorilor li se cer datele cardului, inclusiv codul CVV/CVC, sub pretextul de a fi facuta plata pentru produsul tranzactionat. Acel link duce catre o pagina de phishing, prin care infractorii cibernetici încearca sa colecteze datele de card ale utilizatorilor.

"Cum ne dam seama de acest lucru? Desi acea pagina web foloseste identitatea vizuala a brandului OLX, în realitate, daca analizam denumirea domeniului din link-ul transmis (.xyz), putem observa ca nu mai suntem pe site-ul oficial, ci pe un site malitios. În plus, singurul moment în care OLX cere introducerea datelor cardului este cel în care se cumpara serviciile OLX de publicare sau de promovare a anunturilor", subliniaza expertii CERT-RO.

Acestia mentioneaza ca în momentul în care utilizatorul introduce datele de card pe astfel de site-uri de phishing, acestea intra automat în posesia atacatorilor, care au din acel moment posibilitatea de extrage bani de pe acel card.

"Desigur, orice conversatie se opreste, dupa acel moment, iar vânzatorii au surpriza nu doar ca nu le-au intrat banii în cont, ci chiar ca le-au fost extrasi ilicit anumite sume de pe card. În ultimele zile, echipa CERT-RO a fost notificata de faptul ca atacatorii folosesc si alte identitati vizuale pentru site-urile de pishing, de regula ale unor companii cu reputatie în România. Un exemplu ar fi FanCurier", adauga ei.

În acest context, CERT-RO recomanda: analizati cu atentie si validati informatia primita, înainte de a face clic pe link-uri sau atasamente din surse necunoscute! De ce ati oferi cuiva datele complete de card, cu codul de validare al tranzactiilor (CVV)? Oricine are acces la aceste date poate folosi cardul pentru a face plati. În plus, puteti scana astfel de link-uri suspicioase cu anumite instrumente disponibile gratis online (ex: VirusTotal), daca nu aveti o solutie de securitate instalata pe dispozitiv, pentru a evita infectarea cu malware sau astfel de tentative de phishing.

De asemenea, se recomanda atentie la exprimarea interlocutorilor în scris, precum si la corectitudinea gramaticala

a textului, deoarece, de multe ori, atacatorii nu sunt de origine româna si se folosesc de instrumente automate de traducere a textului pentru a se conversa cu potentialele victime în limba lor nativa.

"În cazul în care ati cazut în aceasta capcana, este vital sa va adresati cât mai repede bancii emitente a cardului, pentru a bloca cardul si eventuale tranzactii ilicite din cont. Ulterior, daca ati suferit pagube materiale, va trebui sa depuneti o plângere la cea mai apropiata sectie de Politie, pentru a deschide o investigatie în acest sens", mai recomanda specialistii Centrului National de Raspuns la Incidente de Securitate Cibernetica.