Anti-phishing document

Număr tot mai mare de escrocherii: fiți vigilenți!

Având în vedere numărul tot mai mare de escrocherii ale unor companii și persoane rău intenționate, vă recomandăm să fiți mai vigilenți.
Vă reamintim că Olkypay și KyPay nu oferă spre vânzare credite, acțiuni sau alte investiții financiare.
În niciun caz nu trebuie să divulgați codurile sau datele de identificare KyPay sau Olkypay.

Care sunt fraudele frecvente?

De obicei, escrocii încearcă să vândă acțiuni prin intermediul e-mail-ului sau prin telefon, pretinzând că reprezintă o neobancă sau o instituție de plată, precum a noastră.

Ce este phishing-ul?

Această tehnică de înșelăciune urmărește să colecteze informații personale și confidențiale prin e-mail (detalii de conectare, numărul cardului bancar etc.) și să determine victimele să efectueze o tranzacție financiară.

Ce este vishing-ul?

Vishing-ul este o metodă de phishing prin telefon, care are ca scop, de asemenea, să extorcheze de la victime date financiare ori de securitate confidențiale sau chiar să le determine să efectueze un transfer de bani. Escrocii își contactează victimele prin intermediul telefonului pretinzând că sunt angajați ai companiei.

Cum să depistați frauda? Care sunt cele mai bune practici?

Recunoașterea unui e-mail fraudulos

Atunci când primiți un e-mail care pretinde a fi din partea KyPay sau Olkypay, vă oferim câteva idei pentru a vă ajuta să faceți diferența între o comunicare legitimă și o tentativă de phishing.

1. Adresa de e-mail a expeditorului este adresa obișnuită KyPay sau Olkypay?

Escrocii folosesc de obicei o adresă apropiată de cea legitimă. Asigurați-vă că verificați adresa expeditorului (numele și adresa de e-mail).

2. E-mail-ul vă este destinat dvs. personal?

Verificați dacă, conținutul e-mail-ului este personalizat sau dacă începe cu un mesaj de tipul "Stimate client". Un alt criteriu este acela că, dacă adresa dvs. de e-mail nu apare ca destinatar, înseamnă că mesajul nu vă este adresat personal și a fost trimis în cadrul unui mailing în masă.

3. Conținutul e-mail-ului pare obișnuit din punct de vedere al formei și conținutului?

Adresa de e-mail a expeditorului utilizează numele organizației sau al societății a cărei identitate este uzurpată, dar conține adesea anomalii (neconcordanțe în ceea ce privește logo-ul, întinderea logo-ului, erori tipografice, greșeli de ortografie, formatare etc.). Acest lucru ar trebui să vă determine să fiți precauți.

Acest tip de e-mail invită, în general, victimele să răspundă într-o perioadă scurtă de timp. E-mail-ul poate conține fie un link către un website fraudulos care seamănă foarte mult cu site-ul oficial al companiei, fie un atașament. Nu faceți clic pe link-uri fără a verifica originea acestora și nu deschideți atașamentele dintr-un e-mail suspect, pentru a evita să oferiți informații escrocilor și să vă infectați calculatorul cu un virus.

Rămâneți în alertă atunci când sunteți sunați

Nu uitați că numărul care vă apare pe telefon poate fi fals. Nu efectuați transferuri de bani și nu vă furnizați niciodată prin telefon codul de identificare bancară, PIN-ul sau orice alt cod de securitate.
Nici o persoană care pretinde că este angajat al companiei noastre sau al unuia dintre furnizorii noștri de servicii, nu are permisiunea de a vă contacta pentru a vă solicita date de conectare sau informații bancare, precum numele de utilizator sau parola.

Ce să faceți în cazul în care aveți îndoieli?

În cazul în care aveți îndoieli cu privire la legitimitatea unui e-mail sau a unui apel telefonic, vă rugăm, nu ezitați să ne contactați folosind următorul formular: https://support.olkypay.com/?_locale=ro.