

Tájékoztatás

A GLS névvel és arculati elemeivel visszaélő adathalász támadásokról

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) tájékoztatót ad ki egy iMessage-en terjedő adathalász kampánnyal kapcsolatban, amely visszaél a GLS futárszolgálat névvel és arculati elemeivel, hogy személyes és bankkártya adatokat gyűjtsön.

Szervezetünkhöz több bejelentés érkezett, amelyek szerint a batijyrugetynah@email[.]com feladóról olyan SMS-üzeneteket küldtek, amelyek a hXXps[.]/glsexl[.]xyz/hu adathalász weboldalra mutató hivatkozást tartalmaztak, és egyúttal válaszüzenetet vártak. A linkre való kattintás egy GLS arculati elemeit felhasználó adathalász weboldalra irányít. Az oldalon több valós GLS link is elhelyezésre került, ezzel is növelve a hitelesség látszatát.

Az adathalászat első lépcsőjeként a felhasználó egy kapcsolati adatokat bekérő űrlappal találja magát szemben. Kitöltést követően egy 200 Ft-os szállítási díjra hivatkozva egy bankkártyás online fizetési felület jelenik meg, ahol valójában nem történik fizetés. A kitöltött személyes és bankkártya adatok az adathalásznak kerülnek továbbításra.

Az NBSZ NKI biztonsági javaslatok a következők:

- Javasolt elkerülni az SMS-ben érkezett hivatkozások megnyitását.
- Célszerű a feladót letiltani az Üzenetek (iMessage) alkalmazásban és spamként jelölni (Report Junk) azt.
- Ajánlott nem válaszolni az SMS-re, mert a válasz deaktiválhatja az iOS beépített adathalász védelmét.
- Javasolt bekapcsolni az ismeretlen feladók szűrését: Beállítások → Üzenetek → Ismeretlen feladók szűrése → BE
- Érdemes kikapcsolni az olvasási visszaigazolásokat: Beállítások → Üzenetek → Olvasási visszaigazolások küldése → KI
- Ajánlott bekapcsolni az Apple ID kétfaktoros hitelesítését.
- Célszerű erős, egyedi Apple ID jelszót használni.
- Javasolt az iOS rendszert naprakészen tartani.

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu