



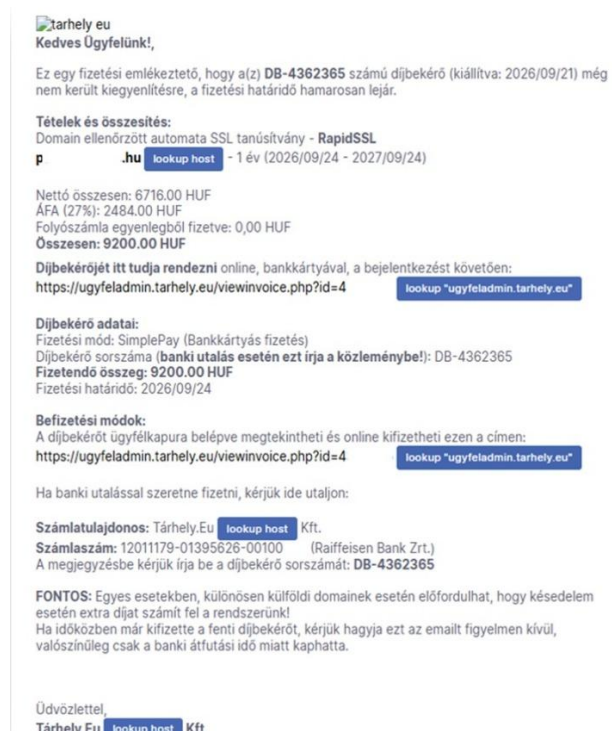
Riasztás

a Tárhely.Eu nevében küldött adathalász kampány kapcsán

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a Tárhely.Eu tárhelyszolgáltató nevében küldött adathalász kampány kapcsán. A beérkezett bejelentések alapján ismeretlen elkövetők a Tárhely.Eu névvel visszaélve fizetési felszólításokat küldenek különböző vállalkozások részére.

A levélben foglaltak szerint a címzett vállalkozásnak valamely szolgáltatás, például egy SSL-tanúsítvány megújítása kapcsán kiegyenlíthetetlen díjbekérője van, amelynek fizetési határideje néhány napon belül lejár (1. ábra).



1. ábra: A csaló levél, fizetési emlékeztető egy SSL-tanúsítvány díjbekérőjéről

A levélben látható link az ügyfeladmin valódi címét mutatja (ugyfeladmin.tarhely.eu), a hivatkozásra való kattintás után azonban máshová irányítja a felhasználót. A link valójában a SendGrid címére mutat (2. ábra).





```
hxxps[://]u115278589[.]ct[.]sendgrid[.]net/ls/click?upn=u001[.]fInagUB5D9uhjHt3nq30hboN-2F6hrR9Qw-  
2FHZd9Ns7Y9BDp0VPPrRABPQ83hp6iKUbPnc7X89wX23tA-2B-  
2FFz605vk0YRG75vSEbk0eAkVn8X5UFn1GRPDT6rYkSuNJAX0gQLtvFwDw6t6MCAnNRB4K6T0YYip1fmRDwcDXC3ND7Xsj00iSsqxpEF1euVKzjUvtiz8ew_F58  
0SZ0Q15wHeH4DtZSDZ0TDjJTsKwPt9iv4BgBMhu5DtG03xBuSHKmA0f1dYfmsevu1E04mg5VC1w5EbKMCJW7SHlWAQtGEGPzeWGBsJteR5sBsK5JP-  
2Bc6arG7ge7XZQDNa30kUb0itedwFy0NtEddGZvmHT5hr8ywwE-2F1-2BJzY8dj8xjNGBFtsZr0mTUEU9ufvEkIiuPjMT2vmGWhfpjw-3D-3D
```

2. ábra: A levélben lévő link valódi címe, egy SendGrid kattintáskövető link

A SendGrid egy legitim, széles körben használt e-mail-küldő szolgáltatás, amely a rajta keresztül küldött levelekben elhelyezett linkeket automatikusan a saját kattintáskövető címére írja át, majd onnan továbbírányít egy előre meghatározott címre.

A csalók ezt használják ki, két okból:

- a SendGrid jó hírneve miatt a levél könnyebben átjut a spamszűrőkön, és a linkellenőrzők is gyakran csak a SendGrid címét látják,
- a valódi célcím kódolva van, így a levélből nem derül ki, hová vezet a link.

A levelek egy SendGrid-ügyfélfiókon keresztül kerülnek kiküldésre. Ezt a fiókot a csalók valószínűleg feltörték, vagy kifejezetten erre a célra hozták létre. A levélben egy láthatatlan követőkép is van, ezért a csalók azt is látják, ki nyitotta meg a levelet.

```
hxxps[://]ugyfeladmin-tarhely-eu[.]hu/tarhely/tarhely/web/log[.]php?  
searchvalue=Z684084071HU&token=5a5f12b43ac7c7c3bee7e46b8c06ff07756e94da
```

3. ábra: Az átirányítás végcélja, a hamis ügyféladmin oldal címe

Az átirányítás után a címzett egy hamis ügyfélportálra kerül (3. ábra), amely első ránézésre megtévesztően hasonlít a valódi ügyféladmin oldalára (4. ábra). Itt a felület bejelentkezést kér, illetve a megadott fizetési lehetőségek közül csak a bankkártyás fizetést engedi kiválasztani, így a csalók megszerezhetik az ügyféladmin jelszavát és bankkártya adatait (5. ábra).





NEMZETI
KIBERBIZTONSÁGI
INTÉZET

TLP: CLEAR
Szabadon terjeszthető!

The screenshot shows a web browser window with the URL <https://ugyfeladmin-tarhely.eu>. The page title is "ÜgyfélAdmin" and the subtitle is "Tárhely.Eu admin rendszere". The main heading is "Áttekintés és megrendelés". Below this, there is a table showing the order details:

Tételek vagy kiegészítők	Ár vagy díjazás
RapidSSL Szekuritás	6716.00 HUF
SSL Tanúsítványok	
+ SSL telepítési szolgáltatás: Nem szükséges, az admin felületen magán végzem el	

Below the table, there is a section for "Kuponkód alkalmazása" and "Bevezető kód". A green button labeled "Küldje megrendelést" is visible. Below this, there is a "Megrendelés áttekintése" section with a table showing the order summary:

Részletek	Ár
Részösszeg	6716.00 HUF
AFA @ 27.00%	2484.00 HUF
Mindösszesen	9200.00 HUF

The total amount is 9200.00 HUF. A green button labeled "Megrendelési oldal" is visible. A "Segítség" button is also present.

4. ábra: A hamis ügyfélportál megrendelés-áttekintő oldala

The screenshot shows a web browser window with the URL <https://ugyfeladmin-tarhely.eu>. The page title is "SimplePay" and the subtitle is "Fizetési módok". The main heading is "Fizetési módok". Below this, there is a section for "Tárhely.Eu Kft." and "RapidSSL". The order summary is shown:

Tételek vagy kiegészítők	Ár vagy díjazás
RapidSSL Szekuritás	6716.00 HUF
SSL Tanúsítványok	
AFA @ 27.00%	2484.00 HUF
Mindösszesen	9200.00 HUF

Below the table, there is a section for "Fizetési módok". A green button labeled "Fizetés bankkártyával" is visible. A "Segítség" button is also present.

5. ábra: A hamis fizetési oldal, amely bankkártya adatokat kér



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



+36-1-336-4833



csirt@nki.gov.hu

TLP: CLEAR
Szabadon terjeszthető!



A csalásra utaló jelek:

- A feladó nem a Tárhely.Eu. A megjelenített név „Tárhely.Eu Ügyfélszolgálat”, de a tényleges e-mail cím nem a szolgáltató domainjéről való.
- A linkek nem oda mutatnak, ahová az olvasható szöveg sugallja. Ha a kurzort kattintás nélkül a linken lebegtetjük, látszik, hogy nem az ugyfeladmin.tarhely.eu-ra, hanem egy SendGrid-címre visz.
- A bankszámlaszám nem a Tárhely.Eu-é. A levélben egy másik bank, egy másik tárhelycég számlaszáma szerepel. Ez valószínűleg egy másik szolgáltató ellopott levélsablonjából maradt benne. A Tárhely.Eu hivatalos számlaszáma a tarhely.eu kapcsolati oldalán található.
- Hibás a számítás. Az ÁFA nem 27%-kal van kiszámolva, hanem kb. 37%-kal. A számokat utólag igazították egy előre kitalált végösszeghez.
- Formai hibák vannak benne, például kettős írásjel és felesleges szóközök.
- Sürget: rövid, pár napos határidőt ad, és késedelmi díjjal fenyeget.

Javasolt intézkedések:

- Ne kattintson a levélben lévő linkekre, és ne utaljon a megadott számlaszámra.
- Ha kétsége van, az ügyféladmint webcímének kézzel történő begépelésével nyissa meg (ugyfeladmin.tarhely.eu), és ott ellenőrizze, van-e valóban kifizetetlen tétele. Ennél még biztonságosabb, ha az eredeti címet korábban már könyvjelzőként elmentette, és onnan nyitja meg.
- Ha már rákattintott a linkre és megadta az adatait: azonnal változtassa meg az ügyféladmin-fiók jelszavát, valamint minden más fiókban is, ahol ugyanezt a jelszót használta. Ha bankkártyaadatokat is megadott, haladéktalanul tiltsa le a kártyát a bankjánál.





NEMZETI
KIBERBIZTONSÁGI
INTÉZET

TLP: CLEAR

Szabadon terjeszthető!

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

Nemzetbiztonsági Szakszolgálat

Nemzeti Kiberbiztonsági Intézet

Telefon: +36-1-336-4833

Incidensbejelentés: csirt@nki.gov.hu

TLP: CLEAR

Szabadon terjeszthető!



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



+36-1-336-4833



csirt@nki.gov.hu