Kenyeres Attila Zoltán – Szűts Zoltán

Az adathalászat (phishing) fogalmi definiálása és főbb nyelvi jelei

Kivonat

A tanulmány nyelvészeti szempontból közelíti meg társadalmunk egyik kirívóan káros jelenségét, az adathalászatot. Az adathalászat (nemzetközi szóhasználatban: phishing) a kiberbűnözés egyik fajtája, amely az utóbbi években az infokommunikációs és digitális technológia fejlődésével világszerte jelentős anyagi károkat okoz a társadalom sok tagja számára. A leegyszerűsített definíció szerint a phishing a felhasználók érzékeny személyes adatainak (például bankkártyaadatok) interneten keresztül, pszichológiai manipulációs technikák segítségével történő kicsalása, általában anyagi haszonszerzés céljából. Ide tartoznak a felhasználó eszközeire trükkös csalással feltelepített rosszindulatú szoftverek is, amelyekkel ugyancsak érzékeny, személyes adatokat szerezhetnek meg az elkövetők. A tágabb fogalmi meghatározás szerint a phishing körébe tartoznak azon rosszindulatú aktivitások is, amelyek szintén pszichológiai manipulációval vagy egyéb csalás révén közvetlen pénzátutalásra veszik rá a gyanútlan felhasználókat. Ezenfelül a phishing egyéb alkategóriái is léteznek a felhasznált platform alapján: ilyen a telefonon keresztüli adatlopás, a vishing (voice-phishing) vagy az SMS-ben történő adatlopás, a smishing (SMS-phishing). A jelen tanulmány célja egy átfogó teoretikai keret felvázolása a phishing relációjában annak érdekében, hogy a nyelvészeti megközelítésünket megalapozzuk, ezért röviden áttekintjük a phishing történelmi előzményeit, majd összegezzük a jelenség szűkebb és tágabb definícióit a releváns nemzetközi szakirodalom alapján, illetve azt is meghatározzuk, mely aktivitások nem sorolhatók az adathalászat körébe. Ezt követően sorra vesszük a stratégiai (szándékosan alkalmazott) és nem stratégiai nyelvi eszközöket, az úgynevezett „szivárgó nyelvi jeleket", amelyek a phishing jelenlétére utalnak.

Kulcsszavak: adathalászat, phishing, nyelvi jelek, lingvisztika

Történelmi előzmények – az offline adathalászat

Az internet nemcsak a tudás terjedésének biztosít szinte végtelen platformot, hanem a félrevezetésnek is, köztük az álhíreknek (Balázs 2023a: 11; Kenyeres–Szűts 2024), illetve az olyan illegális aktivitásoknak is, amelyek a kiberbűnözés területébe sorolhatók. Ide tartozik az adathalászat – angolul phishing – is, amely arra a kísérletre utal, amikor: 1. az áldozatot pszichológiai manipuláció segítségével ráveszik arra, hogy rákattintson egy olyan link-

re (Parekh et al. 2018), amelyen keresztül adathalász weboldalra kerül, ahol megadja a csalók által kívánt információkat (Saberi et al. 2007), rendszerint érzékeny/személyes adatokat; 2. arra veszik rá a felhasználót, hogy tudtán kívül rosszindulatú szoftvert telepítsen az eszközére, amelynek segítségével ugyancsak érzékeny adatokat lopnak el tőle (Baslyman–Chiasson 2016; Canfield et al. 2016; Milletary 2005; Kirda–Kruegel 2006). Több szerző is említi, hogy a trükkös adatlopás nem új jelenség, alapja minden esetben a pszichológiai manipuláció (nemzetközi szakirodalomban: social engineering), amely már a számítógép és az internet előtt is létezett (Volkamer et al. 2017; Abroshan et al. 2021). Az internet elterjedése előtt a bűnözők többek közt telefonon keresztül, szóban adták ki magukat megbízható ügynököknek, hogy érzékeny, személyes információkat szerezzenek, így az ő tevékenységük tekinthető a phishing egyik közvetlen előzményének (Milletary 2005; Basit et al. 2021). A számtalan megtévesztő aktivitás közül az adathalászat is átkerült a fizikai világból a digitális platformokra (Bustio-Martínez et al. 2024). A phishing tehát egy évszázadok óta alkalmazott bizalmi, hatékony kommunikáción és meggyőzésen alapuló csalás modern, digitális változata: a személyes előnyök megszerzése érdekében történő megtévesztés (Volkamer et al. 2017). A pszichológiai manipulációt alkalmazó offline csalási formák ma is léteznek, párhuzamosan az online phishinggel, sok esetben egymással interkonnektivitásban állva.

A phishing kifejezés eredete

Az adathalászat szó eredetére többfajta magyarázat is olvasható a nemzetközi szakirodalomban, mindegyik megegyezik abban, hogy a szó alapját az angol „halászat", azaz „fishing" képezi. Az egyik értelmezés szerint a „phishing" kifejezés a „password" (jelszó) és a „fishing" (halászat) szavak összerántásából jött létre, arra utalva, hogy a csalók a felhasználók jelszóit próbálják meg „elhalászni" különféle trükkökkel (Wright et al. 2016). Mások szerint a szó az internetes adathalász támadások telefonos előzményeiből származik, amelyet „phone phreaking"-nek neveztek, a „fishing" kifejezés „f" betűjét emiatt cserélték le „ph"-ra (Basit et al. 2021). Egy másik magyarázat szerint pedig az angol „website phishing" kifejezésből származik, amely szintén a „fishing" szó egyik variációja (Parekh et al. 2018). Összességében tehát interneten történő adathalász tevékenységre utal a szójátékként is értelmezhető „phishing" kifejezés. A szakirodalomban egyetértés van abban, hogy a „phishing" szó az 1990-es évek közepén jelent meg először nyilvánosan, amikor a csalók az internetszolgáltatói (ISP) fiókadatok megszerzésére hasz-

nálták a módszert (Milletary 2005). Az első írásbeli megjelenés pontos dátumát illetően azonban már megoszlanak a források. Wright és társai szerint a kifejezést írásban nyilvánosan először egy Koceilah Rekouche nevű hacker használta 1995-ben az America Online (AOL) internetszolgáltató cég online felületén (Wright et al. 2016). Mások szerint a kifejezést 1996-ban alkották meg (Chaudhry et al. 2016; Parekh et al. 2018) olyan hackerek, akik az AOL-felhasználók jelszóit csalták ki (Parekh et al. 2018). Volkamer és társai adatai szerint először 1996. január 2-án használták a „phishing" szót írásban a bizalmi alapú csalások digitális változatára (Volkamer et al. 2017). A már kifejezetten internetes felületen történő adathalászatra vonatkozó „phishing" kifejezés tehát először az 1990-es évek közepén jelent meg dokumentálható módon a nyilvános kommunikációban.

Definiálási kísérletek: szűkebb és tágabb kategóriák

Az általunk feltárt nemzetközi szakirodalom a phishing egy szűkebb és egy tágabb definíciójával dolgozik. A szűkebb definíció szerint a phishing kizárólag internetes adatlopásra vonatkozik, a tágabb definíció már ide sorolja azokat a módszereket is, amikor közvetlen pénzátutalásra veszik rá a felhasználót.

A témát kutatók egy része az internetes bűnözés (kiberbűnözés) relációjában tárgyalja a fogalmat. Balázs rámutatott arra, hogy a digitális közeg táptalajt adhat az online bűnözésnek, és elősegíthet olyan jellegű visszaéléseket, mint a spam vagy a hackelés (Balázs 2023b). Az online bűnözés egyik formája a phishing is, amely bűnügyi tevékenységként, adatlopásként definiálva a személyes adatok interneten keresztül történő ellopását jelenti pénzügyi csalás elkövetése céljából (Milletary 2005). A kibertámadások általánosságban digitális platformokon történő rosszindulatú kísérletek, amelyek célja a bizalmas szervezeti vagy személyes adatokat tartalmazó rendszerek feltörése vagy ilyen jellegű adatok ellopása (Basit et al. 2021). Az adathalászat ennek megfelelően az internetes bűncselekmények egyik ága, a kiberbűnözés egyik formája (Chou et al. 2004; Saberi et al. 2007; Chaudhry et al. 2016; Parekh et al. 2018), amely során érzékeny személyes adatok (például jelszavak, hitelkártyaadatok) átadására késztetik a gyanútlan felhasználókat online megtévesztés útján, rosszindulatú szándékkal (Parsons et al. 2013; Harrison et al. 2016; Baltuttis–Teubner 2024; Yang et al. 2022). A sikeres phishing során tehát ellopják a felhasználók érzékeny adatait (Kirda–Kruegel 2006), így ez *„*egyfajta személyazonosság-lopás, amely bizalmas adatokat próbál ellopni, például online bankszámla-információkat*"* (Saberi et al. 2007: 311).

A phishing másik formája, amikor közvetett módon, valamilyen alkalmazás vagy szoftver közbeiktatásával „man-in-the-middle" módszerrel lopják

el a felhasználók adatait (Milletary 2005; Kirda–Kruegel 2006). Ennek során megfelelő kommunikációs módszerekkel arra veszik rá az áldozatot, hogy tudtán kívül valamilyen rosszindulatú szoftvert telepítsen a gépére, mobiltelefonjára, amelyek a weboldalakkal folytatott kommunikációt figyelik, és különféle érzékeny információkat gyűjtenek be (Milletary 2005; Chaudhry et al. 2016; Volkamer et al. 2017).

A tágabb meghatározás szerint az adathalászat fogalma kibővült, és az elektronikus pénzügyi bűncselekmények szélesebb körét is magába foglalja (Milletary 2005). Ilyen lehet az, amikor adatok helyett közvetlenül pénz átutalását kérik a csalók. Erre példa, amikor a közösségi hálózatokon valakinek a barátait, családtagjait értesítik arról, hogy az illető bajban van, és gyorsan pénzre van szüksége (Hong 2012; Chaudhry et al. 2016). Ilyenkor azonnali pénzátutalást kérnek, nem adatokat. De az áldozat elérhetőségei ebben az esetben is származhatnak adatlopásból, ebben az értelemben tehát végső soron itt is phishingről van szó.

Ugyancsak tágabb meghatározás szerint sorolhatók a phishing fogalomkörébe azok a módszerek, amikor meghamisított cikkekben, illetve deepfake videókban ismert személyek (pl. Elon Musk vagy egy ország gazdasági minisztere) ajánlanak nem létező befektetéseket. Hiszen ebben az esetben is közvetlen pénzutalás történik, viszont egyben adatlopás is, valamint szintén a pszichológiai manipuláció (csábító jutalom lebegtetése), illetve a technológiai eszközök (deepfake videók, webes cikkek készítése) kombinációja történik.

Ugyanakkor a kizárólag technikai módszerekkel, például az alkalmazások és/vagy a hálózati biztonsági eszközök sebezhetőségeinek kihasználásával végrehajtott adatlopás (Abroshan et al. 2021) nem tartozik a klasszikus phishing kategóriájába, hiszen ez esetben nem a felhasználót célozza meg a támadás, hanem a gépet, a felhasználóval nem történik kommunikáció, és nem alkalmaznak pszichológiai manipulációt sem. Viszont a rendszerek feltörését lehetővé tévő adatok már származhatnak a megtévesztésen alapuló phishing tevékenységből. Itt szerepet játszhat az úgynevezett kontextustudatos adathalászat: a támadó ekkor úgy nyeri el az áldozatok bizalmát, hogy nyilvános adatbázisokból minél több információt szerez róla. Például a vásárlási preferenciáiról (az eBay-en nyilvánosan elérhető adatokból), a fiókvezető bankjáról (például a böngészőből kinyert adatok révén) vagy az anya leánykori nevéről, amelyek a törvény által kötelezően nyilvánosságra hozott adatokból is kinyerhetők. A közösségi média segítségével további adatok is szerezhetők az egyénekről (Jagatic et al. 2007), ahogyan képek is, amelyek ugyancsak felhasználhatók különféle visszaélésekre.

Szemantikai támadás és pszichológiai manipuláció (social engineering)

Az adathalász kísérletek tehát nem a gépeket, hanem a felhasználót, az embert veszik célba, így a szemantikai támadások körébe sorolhatók. Downs és társai a számítógépes biztonsági támadásokat fizikai, szintaktikai és szemantikai típusokba sorolják. A fizikai támadások a számítógépes hálózatok infrastruktúráját fizikailag rombolják le, míg a szintaktikai támadások a szoftvereket teszik tönkre. Ezzel szemben a szemantikai támadások a számítógépet használó embert veszik célba. Nem a rendszer sebezhetőségét használják ki, hanem azt, ahogyan a felhasználó a számítógépekkel kapcsolatba lép, vagy ahogyan az onnan származó üzeneteket értelmezi (Downs et al. 2006). Az adathalászat tehát nem közvetlenül a digitális technológiai rendszereket, hanem a rendszereket használó embereket támadja (Hong 2012), a felhasználókat, az emberi ítélőképességet tekinti a rendszer sebezhető pontjának, ezért őket veszi célba (Canfield et al. 2016; Chaudhry et al. 2016; Bustio-Martínez et al. 2024). A csalók az emberi kognitív és viselkedési tulajdonságokat használhatják fel a trükkjeik megtervezéséhez és az áldozatok megtévesztéséhez (Abroshan et al. 2021). Ebben az értelmezési keretben tehát a phishing szemantikai támadási forma (Downs et al. 2006; Zhang et al. 2006; Liu et al. 2011), amely a szoftver sebezhetőségei helyett az emberi sebezhetőségre épít (Zhang et al. 2006). Az adathalászat ennek megfelelően „folyamatos szemantikai támadás, amely az áldozatokat arra készteti, hogy érzékeny információkat osszanak meg akaratlanul*”* (Liu et al. 2011: 1). Az adathalászat szemantikai támadásként interpretálva azt használja ki, hogy az emberek milyen jelentést tulajdonítanak a tartalomnak, tehát arra építenek, hogy az emberek általában elhiszik, amit látnak és hallanak. Ezért az adathalász e-maileket szándékosan készítik úgy, hogy megtévesszék a felhasználókat (Wash 2020).

A megtévesztés érdekében pedig a pszichológiai manipuláció (a nemzetközi szakirodalomban: social engineering) eszközeit alkalmazzák az elkövetők. Így érik el, hogy a csalók online felületére jusson az áldozat, ahol megadja a személyes adatait. „Az online adathalászat egyfajta social engineering, amelynek során a bűnözők a felhasználókat érzékeny információk felfedésére veszik rá” (Baslyman–Chiasson 2016: 1). A phishing során tehát minden esetben valamilyen pszichológiai trükköt használnak az emberek megtévesztésére és a bizalmuk megszerzésére, hasonlóan ahhoz, ahogyan az offline világban is teszik azt a csalók (Abroshan et al. 2021). A pszichológiai manipuláció részeként a támadó egy megbízható harmadik félnek adja ki magát, és így próbál érzékeny információkat kicsalni az áldozattól (Jagatic et al. 2007; Saberi et al. 2007). A pszichológiai manipuláció közvetítésére minden esetben valamilyen digitális platformot használnak, így a phishing végső soron

a pszichológiai manipuláció (social engineering) és a technológiai eszközök (pl. egy hamisított weboldalon található webes űrlap) kombinációja annak érdekében, hogy rávegyék a felhasználókat érzékeny információk átadására (Kirda–Kruegel 2006; Chaudhry et al. 2016; Basit et al. 2021; Abroshan et al. 2021; Baltuttis–Teubner 2024; Singh et al. 2024; Yang et al. 2022). Elsősorban a meggyőzés alapelveit alkalmazzák a felhasználók megtévesztésére (Bustio-Martínez et al. 2024). Az adathalászok által alkalmazott pszichológiai manipulációs módszereket az 1. táblázat foglalja össze az általunk feltárt nemzetközi szakirodalom alapján.

1. táblázat: Az adathalász próbálkozások során használt pszichológiai manipulációs módszerek

Módszer	**Példa**	**Említés**
Kíváncsiságra, tájékozódási igényre építés	Egy friss/szenzációs hírt ígérő videó.	Chaudry et al. 2016
	Világsztár intim fotóját ígérő linkek.	Hong 2012
Előzetes meggyőződésre, hiedelmekre építés	Hit abban, hogy az üzenetküldő megbízható.	Volkamer et al. 2017
Félelemkeltés, ijesztgetés	Rájuk ijeszt, félelmet kelt, szorongást kelt.	Hong 2012; Wash 2020; Volkamer et al. 2017
	Arról értesít, hogy feltörték a bankszámlát, vagy illetéktelenek megpróbáltak bejelentkezni a bankfiókba.	Sheng et al. 2010; Wu et al. 2006; Wu et al. 2006; Chaudry et al. 2016; Sheng et al. 2010
	Fióklezárásra figyelmeztet.	Harrison et al. 2016; Milletary 2005
	Figyelmeztetést küld, fenyeget.	Downs et al. 2006; Parsons et al. 2013; Jagatic et al. 2007; Chou et al. 2004; Sheng et al. 2010
Empátia felkeltése	Egy barát bajban van, gyorsan pénzre van szüksége.	Hong 2012
	Barátnak, rokonnak sürgősen pénzre van szüksége, természeti tragédia áldozatainak sürgősen pénz kell.	Chaudry et al. 2016
	Adakozásra hív fel természeti katasztrófa áldozatai javára.	Furnell 2007; Baslyman–Chiasson 2016
	Segítséget kér.	Baslyman–Chiasson 2016

Sürgetés	Sürgősen kell a pénz egy barátnak, rokonnak.	Hong 2012; Chaudry et al. 2016
	Sürgetés általánosságban.	Downs et al. 2006; Parsons et al. 2013; Abroshan et al. 2021; Milletary 2005; Baslyman–Chiasson 2016; Volkamer et al. 2017
	Az üzenet stílusa (pl. hogy a nyelvezet erőteljes, sürgős válaszra ösztönzött).	Furnell 2007
	Azt sugallják, hogy az ajánlat korlátozott (pl. korlátozott idő áll rendelkezésre a válaszadásra, vagy korlátozott számú hely áll rendelkezésre egy kurzuson).	Butavicius et al. 2016
Az emberi kapzsiságra és a gyors meggazdagodás vágyára építés	Mesés vagyon megszerzésében segítséget kérő, úgynevezett „nigériai herceg"-típusú csalások vagy banki kérdőív kitöltése pénzjutalomért cserébe.	Hong 2012
	Örökséget/üzletet ajánlanak.	Baslyman–Chiasson 2016
	Jutalmat ígér, árut/pénzt kínál, „nigériai herceg-típusú" csalások	Harrison et al. 2016; Milletary 2005; Baslyman–Chiasson 2016
	Pénzvisszatérítési igény benyújtására lehetőség – le kell tölteni fájlt hozzá, pénznyeremény igényléséhez kér személyes információkat.	Furnell 2007
	Vonzó tárgy az e-mailben.	Abroshan et al. 2021
A bizalom felkeltése megbízható szervezet nevével visszaélve	Hamisított weblapok, e-mailek megbízható cégek nevében.	Milletary 2005; Chou et al. 2004; Saberi et al. 2007; Hong 2012; Abroshan et al. 2021; Canfield et al. 2016; Butavicius et al. 2016; Kirda-Kruegel 2006; Wu et al. 2006; Downs et al. 2006; Zhang et al. 2007; Volkamer et al. 2017

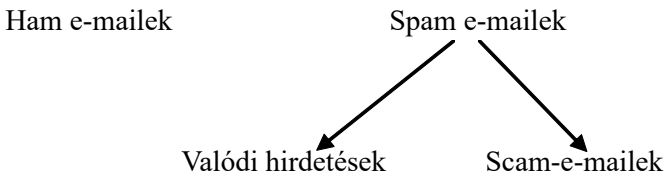
Bizalom keltése adatok útján	Kontextustudatos adathalászat révén szerzett adatok közlése az üzenetben.	Jagatic et al. 2007
	A címzettre vonatkozó adatok jelenléte (pl. a pontos név vagy bankszámlaszám).	Furnell 2007
Bizalom keltése másokra való utalással	Utalás másokra, akik hasonlóan cselekedtek: gyakran a társaik már megtették ezt a lépést (pl. „Több mint 1000 diák fog külföldön tanulni 2014-ben. Te is köztük leszel?")	Butavicius et al. 2016
	Ismert, megbízható személyre (pl. sztárokra) történő utalás, visszaélés az ő nevükkel.	Abroshan et al. 2021; Chaudry et al. 2016; Volkamer et al. 2017
Bizalom keltése figyelmeztetéssel	Félrevezető figyelmeztetések pl. arról, hogy ne kattintson e-mail-linkekre a megbízhatóság látszatát keltve.	Chaudry et al. 2016

Forrás: saját szerkesztés

Az 1. táblázatból kiolvasható, hogy a csalók jellemzően hét pszichológiai manipulációs módszert alkalmaznak a phishing esetében: 1. Kíváncsiságra, tájékozódási igényre építés; 2. Előzetes meggyőződésre, hiedelmekre építés; 3. Félelemkeltés, ijesztgetés; 4. Az empátia felkeltése; 5. Sürgetés; 6. Az emberi kapzsiságra és a gyors meggazdagodás vágyára építés; 7. Bizalomkeltés (megbízható szervezet nevével visszaélve, adatok útján, másokra való utalással, figyelmeztetéssel).

Az adathalászat elemei és lépései: a csali, a horog és a kapás

A horgászathoz hasonlóan az adathalászat is három fő lépésből áll: a virtuális csali (lure) kivetése, a horog (hook) alkalmazása, végül a kapás (catch) (Chaudhry et al. 2016). A csali sok esetben egy úgynevezett scam e-mail, ami végül egy adathalász webhelyre vezeti az áldozatot (Parekh et al. 2018). Saberi és társai az e-maileket három kategóriába osztották: a hamek, a spamek és a scamek (vö. 1. ábra).



1. ábra. Az e-mailek típusai
(Forrás: saját szerkesztés Saberi et al. 2007 alapján)

A ham kategóriába a felhasználók közötti mindennapos üzenetváltások tartoznak, míg a spamet sok esetben levélszemétnek is nevezik, ezzel utalva a marketing vagy hirdetési célú e-mailekre, amelyeket közel azonos tartalommal küldenek ki tömeges mennyiségben. A scamek a spam e-mailek alcsoportját képezik. A scam már kifejezetten illegális cél érdekében próbálja megtéveszteni a felhasználókat, ezért nagyon intellektuális módon alakítják ki (Saberi et al. 2007), kifejezetten azzal a céllal, hogy becsapják a felhasználót (Canfield et al. 2016). Ehhez a már említett pszichológiai manipuláció eszközeit felhasználva az adathalász scam e-mailek „olyasvalaminek adják ki magukat, amik valójában nem, hogy az e-mail címzettjét rávegyék valamilyen cselekedetre, amit normál esetben nem tenne meg" (Wash 2020: 1). Például, hogy rákkattintson egy olyan linkre, amely külsőre egy létező és megbízható áruház, pénzintézet, vagy egyéb cég oldalának néz ki, vizuálisan szinte teljesen megegyezik azzal, de valójában csalók oldala (Canfield et al. 2016; Volkamer et al. 2017; Wang et al. 2024), és ott megadja a személyes adatait. Léteznek bankok nevében kérdőív kitöltésére vonatkozó ajánlatok is, amelyek pénzjutalmat ígérnek a számlainformációk megadásáért, vagy szállodai jutalomklubok nevében írt e-mailek, amelyekben hotelfoglalás ürügyén kérik a felhasználók hitelkártyaadatait (Milletary 2005). A scam e-mailek pedig tartalmazzák a horogra mutató linket, amivel eljutunk az adathalászat második fázisához: a horog (hook) egy olyan weboldal, amely egy megbízható, legális szervezet (például egy pénzintézet) honlapját másolja le, amelynek az áldozat hajlandó bizalmas információkat kiadni. Az itt megadott adatok nem a megbízhatónak tartott szervezethez, hanem a csalókhoz érkeznek. Hogy a csalást leplezzék, a scam e-mailben elhelyezett link gyakran egy elmaszkírozott URL (Chaudhry et al. 2016). Az elmaszkírozás azt jelenti, hogy a felhasználó nem a tényleges URL-t látja, hanem egy megbízható szervezetét, de a link valójában a csalók honlapjára visz. Ugyanez a technika működik az adathalász e-mailek feladója esetében is, amikor a címzett nem a valódi feladó e-mail-címét látja, hanem egy létező, megbízható szervezet vagy személy hivatalos címe jelenik meg. Azonban a kurzort a feladó e-mail-címére görgetve a böngésző általában kiírja a valódi feladó

e-mail-címét. Így ez egy működő technika lehet az e-mail tényleges feladójának detektálására. A phishing harmadik fázisa a kapás, amikor az adathalászhoz befutnak az információk, és azokat saját céljaira felhasználja (Chaudhry et al. 2016). Ennek egyik módja lehet, amikor azt pénzzé teszi (Hong 2012), hamisított profilt hozhat létre, amelyekkel különböző tranzakciókat hajt végre, vagy felvehet pénzt az áldozat internetes bankszámlájáról (Saberi et al. 2007; Abroshan et al. 2021), de ipari vezérlőrendszer, illetve okosrepülőterek elleni támadásokra is felhasználhatók a csalással megszerzett adatok (Abroshan et al. 2021).

Terjedési módozatok

A tradicionális online adathalászat során a csalók kezdetben e-mailt használnak arra, hogy egy megbízhatónak és legitimnek tűnő, de valójában a támadók által ellenőrzött rosszindulatú webhelyre mutató linket küldjenek ki (Parsons et al. 2013; Harrison et al. 2016; Chaudhry et al. 2016; Kirda–Kruegel 2006; Wang et al. 2012; Yan et al. 2024; Baltuttis–Teubner 2024). Azóta elterjedt az SMS, az azonnali üzenetküldés (chat) alkalmazása, a közösségi média üzenőfalain, illetve közvetlen üzenetküldő felületein keresztüli továbbítási forma alkalmazása (Chaudhry et al. 2016; Parekh et al. 2018; Hong 2012; Kirda–Kruegel 2006; Lahti et al. 2024), a weboldalakon megjelenő bannerhirdetések (Chaudhry et al. 2016), a hangüzenetek, valamint a többszereplős online játékok is felületet jelentenek az adathalászatra (Chaudhry et al. 2016; Basit et al. 2021; Hong 2012; Baslyman–Chiasson 2016). Egy tipikus támadási mód, amikor a közösségi média csevegőfelületein egy vírus üzeneteket küld az áldozat ismerőseinek, amelyben arra ösztönzi őket, hogy látogassanak el egy rosszindulatú programokat tartalmazó webhelyre (Hong 2012).

A phishing altípusai

Spear phishing: a bűnözők egy része a tömeges e-mail-üzenetek küldéséről áttért egy továbbfejlesztett változatra, a szelektívebb, személyre szabott, úgynevezett „spear phishing” támadási módokra. Az elnevezés a lándzsával (spear) történő halfogásra utal, jelezvén, hogy itt nem tömeges „halászat” történik, hanem kifejezetten, célzottan egy-egy „halat” céloz meg az elkövető. Az általános megfogalmazású és nagyszámú címzettnek kiküldött hagyományos phishing üzenetekkel szemben a spear phishing e-maileket kifejezetten egy személynek vagy egy kisebb csoportnak készítik és küldik ki (Butavicius et al. 2016; Wash 2020). Ilyen csoport lehet egy cég alkalmazotti közössége,

akik számára a személyes adatok miatt ezek a hamis e-mailek úgy tűnnek, mintha a saját foglalkoztatójuktól származnának (Downs et al. 2006; Wang et al. 2012). A hitelesség megteremtése érdekében ezek az üzenetek már releváns, személyes és kontextuális információkat tartalmaznak az egyes áldozatok becsapására, például az egyénekről és a munkáltató szervezeteikről szerzett speciális ismereteket. Hong említi, hogy egy katonai személyzetet célzó spear phishing támadás tartalmazhat egy meghívót egy létező tábornok nyugdíjazási partijára, arra kérve a címzetteket, hogy egy linkre kattintva erősítsék meg, hogy részt vesznek rajta. Azok az emberek, akik nem dőlnének be egy személytelen adathalász üzenetnek, ebben az esetben a kontextus miatt áldozatul eshetnek (Hong 2012). A személyreszabottság különösen veszélyes lehet, például látszólag a főnöktől érkező üzenet vagy egy olyan folyóirat nevében kapott, névre szóló e-mail esetében, amelyre a felhasználó valóban előfizetett (Wright et al. 2016). Jagatic és társai kimutatták, hogy az emberek 4,5-szer nagyobb valószínűséggel dőlnek be egy látszólag már meglévő kapcsolatról, ismert címről érkező adathalász üzenetnek, mint az általános adathalász próbálkozásoknak (Jagatic et al. 2007). Downs és társai szerint ezek a spear phishing támadások hatékonyabbak lehetnek, mint a nem személyre szabott adathalász próbálkozások (Downs et al. 2006). A spear phishing egyfajta „kétlépcsős phishing", hiszen kutatómunka előzi meg, amely során a támadó összegyűjti azokat az adatokat, amelyek révén eléri, hogy az üzenete személyre szabott és hiteles legyen. Chaudry és társai szerint a spear phishing során a támadó előbb felkutatja a potenciális áldozatokat és annak körülményeit, amelyre a közösségi média is alkalmas lehet. Majd az adatok ismeretében és azokat felhasználva küld olyan üzenetet, amely úgy tűnik, hogy legitim forrásból származik (Chaudhry et al. 2016). Az adatgyűjtés a már említett kontextustudatos adathalászat révén is megvalósulhat (Jagatic et al. 2007). A spear phishing során elsősorban a szöveges üzeneteken van a lényeg: a szöveges meggyőzésre alapul, kevésbé jellemzőek a pénzügyi adathalászatnál előforduló vizuális jelek (Wang et al. 2012).

Whale phising: a spear phishing egy továbbfejlesztett változata, amely egy „nagy hal", vagyis „bálna" (whale) ellen, tehát magas rangú személyek ellen irányul. Ilyenek lehetnek a vállalati vezetők vagy kormányzati tisztviselők (Chaudhry et al. 2016). Ezek a célpontok jellemzően nagyobb hozzáféréssel rendelkeznek az érzékeny vállalati információkhoz, és szélesebb jogkörük van a fiókokhoz. Az egyik első dokumentált leírás 2008-ból származik, amikor több amerikai vállalat vezérigazgatójának hamis idézést küldtek egy olyan csatolmánnyal együtt, amely megnyitáskor rosszindulatú programot telepített (Hong 2012). Ez a technika is kétlépcsős, ez is

kontextustudatos adathalászaton alapul, tehát a csalók előre összegyűjtenek minél több információt, amelyek hihetővé teszik az üzenetet. Ilyenek lehetnek a címzett személyes vagy üzleti érdekeivel kapcsolatos információk (Butavicius et al. 2016).

Angler phishing: ez a csalási forma is személyre szabott. Ennek során a csalók a közösségi médiában megjelenő ügyfélpanaszokat figyelik, és az érintett szolgáltató cég nevében írnak rá a panasztevőre, megoldást kínálva a problémájára, például kártérítés kifizetését ígérve. A folyamat során pedig érzékeny személyes adatokat (elsősorban bankszámlaadatokat) csalnak ki (Siddhesh Vijay et al. 2022; O'Hagan 2018).

Egyéb altípusok: vishing: hang alapján, telefonon történő adathalászat (voice over phishing) (Parekh et al. 2018); smishing: SMS-en keresztüli adathalászat (SMS phishing) (Zieliński 2024; Parekh et al. 2018); mishing: mobiltelefonos adathalászat (mobile phishing) (Parekh et al. 2018).

A 2. táblázatban összefoglaltuk az általunk feltárt szakirodalom alapján a phishing jellemzőit.

2. táblázat: A phishing jellemzői az általunk feltárt szakirodalom alapján

A phishing jellemzői	Említések
A megtévesztés jellemzői	
Pszichológiai manipulációt (social engineering) és egyéb megtévesztő trükköket alkalmaznak.	Milletary 2005; Wright et al. 2016; Basit et al. 2021; Jagatic et al. 2007; Kirda-Kruegel 2006; Saberi et al. 2007; Hong 2012; Chaudry et al. 2016; Parekh et al. 2018; Abroshan et al. 2021; Baslyman–Chiasson 2016; Parsons et al. 2013; Harrison et al. 2016; Canfield et al. 2016; Butavicius et al. 2016; Yang et al. 2022; Downs et al. 2006; Baltuttis–Teubner 2024; Singh et al. 2024
Valamilyen ürüggyel cselekvésre veszik rá a felhasználót (pl. adategyeztetés, számlainformációk hitelesítése, kérdőív kitöltése, személyes adatok frissítése).	Milletary 2005; Kirda-Kruegel 2006; Furnell 2007; Wash 2020
Biztonsági frissítési csomag letöltésére hív fel.	Furnell 2007

Megbízható féltől származónak kinéző, de hamis e-mailt alkalmaznak.	Milletary 2005; Chou et al. 2004; Saberi et al. 2007; Hong 2012; Abroshan et al. 2021; Canfield et al. 2016; Butavicius et al. 2016; Kirda-Kruegel 2006; Wu et al. 2006; Downs et al. 2006; Zhang et al. 2007; Volkamer et al. 2017
Megbízható, legitim félnek adják ki magukat a csalók (social engineering része).	Jagatic et al. 2007; Saberi et al. 2007; Butavicius et al. 2016; Downs et al. 2006
Az üzenet linket tartalmaz, amely a csalók weblapjára mutat, ahol adatokat kell megadni.	Volkamer et al. 2017; Basit et al. 2021; Milletary 2005; Saberi et al. 2007; Chaudry et al. 2016; Parekh et al. 2018; Baslyman–Chiasson 2016; Canfield et al. 2016; Harrison et al. 2016; Wu et al. 2006; Downs et al. 2006; Wash 2020
Valódinak, legitimnek álcázott, de hamis weblapot használnak.	Volkamer et al. 2017; Basit et al. 2021; Milletary 2005; Chou et al. 2004; Kirda-Kruegel 2006; Dhamija et al. 2006; Saberi et al. 2007; Liu et al. 2011; Chaudry et al. 2016; Parekh et al. 2018; Canfield et al. 2016; Parsons et al. 2013; Harrison et al. 2016; Hong 2012; Kirda-Kruegel 2006; Yang et al. 2022; Wu et al. 2006; Downs et al. 2006; Zhang et al. 2007
Valamilyen csalit használnak az elkövetők.	Parekh et al. 2018
Rosszindulatú csatolmány, rosszindulatú programot telepítenek a felhasználó eszközére.	Milletary 2005; Hong 2012; Chaudry et al. 2016; Canfield et al. 2016; Butavicius et al. 2016; Kirda-Kruegel 2006; Wu et al. 2006; Abroshan et al. 2021; Wash 2020
Közvetlenül pénzküldésre is felszólíthat.	Chaudry et al. 2016; Hong 2012; Downs et al. 2006
Mellékletre kattintást kér	Baslyman–Chiasson 2016; Canfield et al. 2016; Abroshan et al. 2021
Szokatlan, várakozásokkal ellentétes, nem tipikus üzenet a vélt feladótól.	Canfield et al. 2016; Wash 2020
Ráveszik a felhasználót valamire, amit amúgy nem tenne meg.	Liu et al. 2011; Wash 2020; Hong 2012; Chaudry et al. 2016; Butavicius et al. 2016

A phishing céljai	
Pénzügyi csalásra használják.	Milletary 2005; Baslyman–Chiasson 2016
Személyazonosság ellopására használják.	Milletary 2005; Kirda-Kruegel 2006; Saberi et al. 2007; Baslyman–Chiasson 2016
Érzékeny, bizalmas személyes/céges adatok ellopására irányuló kísérlet.	Milletary 2005; Basit et al. 2021; Wright et al. 2016; Chou et al. 2004; Jagatic et al. 2007; Kirda-Kruegel 2006; Saberi et al. 2007; Liu et al. 2011; Chaudry et al. 2016; Parekh et al. 2018; Abroshan et al. 2021; Baslyman–Chiasson 2016; Parsons et al. 2013; Harrison et al. 2016; Canfield et al. 2016; Butavicius et al. 2016; Kirda-Kruegel 2006; Wang et al. 2012; Downs et al. 2006; Zhang et al. 2007; Wu et al. 2006
Jelszavakat/fiókadatokat próbálnak megszerezni.	Wright et al. 2016; Basit et al. 2021; Canfield et al. 2016; Kirda-Kruegel 2006; Downs et al. 2006; Zhang et al. 2007; Wright et al. 2016; Wash 2020
Bankkártyaadatokat, pénzügyi információkat próbálnak megszerezni.	Basit et al. 2021; Chaudry et al. 2016; Parekh et al. 2018; Downs et al. 2006; Zhang et al. 2007; Wu et al. 2006
Társadalombiztosítási adatokat próbálnak megszerezni.	Chaudry et al. 2016; Downs et al. 2006; Zhang et al. 2007
A phishing üzenet terjesztési platformjai	
E-mail-üzenetben terjed.	Volkamer et al. 2017; Parekh et al. 2018; Basit et al. 2021; Milletary 2005; Chou et al. 2004; Saberi et al. 2007; Hong 2012; Chaudry et al. 2016; Parekh et al. 2018; Abroshan et al. 2021; Baslyman–Chiasson 2016; Butavicius et al. 2016; Parsons et al. 2013; Harrison et al. 2016; Kirda-Kruegel 2006; Wu et al. 2006; Wang et al. 2012
Chatüzenetben terjed.	Parekh et al. 2018; Chaudry et al. 2016; Kirda-Kruegel 2006
Közösségi hálózatokon, üzenőfalon keresztül terjed.	Basit et al. 2021; Chaudry et al. 2016; Baslyman – Chiasson 2016; Lahti et al. 2024

SMS-ben is érkezhet (smishing).	Hong 2012; Chaudry et al. 2016; Parekh et al. 2018; Baslyman–Chiasson 2016
Többszereplős online játékokban is érkezhet.	Hong 2012; Chaudry et al. 2016; Baslyman–Chiasson 2016
Hangüzenetben is érkezhet (voice over phishing)	Chaudry et al. 2016; Parekh et al. 2018; Baslyman–Chiasson 2016
Bannerhirdetésben is terjeszthető.	Chaudry et al. 2016

Forrás: saját szerkesztés

Amint a 2. táblázatból látható, a phishing sokféle célból és sokféle módszerrel történhet, változatos platformokon. A lényeg mindig a pszichológiai manipuláció és valamilyen technológiai eszköz alkalmazásán van, amelyeket a felhasználó érzékeny, személyes adatainak kinyerése érdekében alkalmaznak. Fontos közös pont, hogy mindig van valamilyen link, amire kattintani kell, ez jelenti a platformot az adatok ellopására. Kivéve azokat a módszereket, amikor rosszindulatú mellékletet kell letöltenie a felhasználónak, mert ebben az esetben az alkalmazás küldi az adatokat. A phishing végső célja szinte mindig anyagi természetű, tehát a csalók pénzhez szeretnének jutni. A csalók mindig trükkösek, azonban a felhasználók számára jó hír, hogy mindig vannak olyan vizuális és nyelvi jelek, amelyek ismeretében az adathalász próbálkozások tetten érhetőek. A következőkben ezekre a nyelvi jelekre koncentrálunk.

Nyelvi jelek a digitális platformokon történő adathalászat esetében

A különböző csalások – akár offline térben, akár online eszközök segítségével történnek –, így az adathalászat esetében is minden esetben megjelennek azok a nyelvi jelzések, amelyek hazugságra és trükközésre utalnak. Emiatt fontos vizsgálni a csalási kísérletekben megjelenő lingvisztikai jelzéseket. Az interneten terjedő adathalászat nyelvi aspektusból történő elemzése során figyelembe kell venni azt, hogy az informatika átalakította a nyelvhasználatot, új létmódokat létrehozva, amelyeket Balázs összefoglalóan számítógépes kommunikációnak vagy CMC-kommunikációnak (computer-mediated communication) nevez (Balázs 2015). A számítógép vezérelte digitális/elektronikus kultúra retorikája pedig az úgynevezett e-retorika körébe sorolható. Ennek alapján a különféle digitális platformokon (SMS-ben, e-mailben, chaten, közösségi médiában, fórumokon, kommentekben) megjelenő szövegek beletartoznak az e-retorika fő kommunikációs funkcióiba (Balázs 2003, 2004, 2005, 2006, 2007, 2010, 2011). Ezek alapján a fenti platformokon ter-

jedő adathalász kísérletek szövegei is beleérthetők. Az infokommunikációs technológiák alapján létrejött e-retorika megduplázta a nyelvi létmódokat (az írást és a beszédet), és kialakította ezek alternánsait, a másodlagos írásbeliséget és szóbeliséget (Balázs 2015). A másodlagos írásbeliség általános (orto)grafikus jellemzői közé tartoznak a helyesírástól eltérő formák (például a folyamatos kis- vagy nagybetűs írás, egybeírás, betűk és írásjelek többszörözése) (Balázs 2010), amelyek megjelenése kimutatható az adathalász próbálkozások szövegeiben is.

Stratégiai és nem stratégiai nyelvi jelzések a hazugságra építők esetében

A hazugságra és trükközésre utaló nyelvi jelzések felderítéséhez fontos megvizsgálni a hazudozók érzelmeire és kogníciójára vonatkozó lingvisztikai jelzéseket, amelyeknek két fő típusa létezik: a stratégiai (tudatosan alkalmazott) és a nem stratégiai (nem tudatosan használt) nyelvi jelzések csoportja.

A nem stratégiai nyelvi jelzések általában kevés tudatossággal keletkeznek, inkább ösztönösek, nehéz őket kontrollálni még akkor is, ha az egyén erősen motivált erre (Toma–Hancock 2012). Ide tartoznak a funkciószavak (például a tartalom nélküli mondatrészek, névmások, prepozíciók, kötőszavak és segédigék), valamint a tartalmi szavak: például az érzelmi kifejezések (Chung–Pennebaker 2007).

Ezzel szemben a stratégiai nyelvi jelzéseket a pszichológiai manipuláció részeként tudatosan alkalmazzák a csalók. Részben azért, hogy hiteles, megbízható forrásnak mutassák magukat, részben azért, hogy kikapcsolják a racionális döntéshozatalt, és az érzelmi döntéshozatal felé mozdítsák a felhasználót. Az egyik ilyen stratégiai jel az adathalász e-mail szövegének a hossza. Ezek az e-mailek általában rövidek (Workman 2008), így ugyanis könnyebb elkerülni az ellentmondásokat és kezelni az információt (Toma–Hancock 2012). Jellemző a sürgősségre utaló jelzések alkalmazása (Butavicius et al. 2022; Workman 2008), olyan szavakat használva, mint a „határidő", vagy „közelgő számlazárás", valamint a fenyegetettség érzését felkeltő szavak használata, mint a „figyelmeztetés" vagy „igénylés nélkül maradt adó-visszatérítés". A fenyegetettség érzékelése az egyik fontos indikátora a pszichológiai manipuláció sikerének (Workman 2008). A félelmet keltő adathalász támadások visszatérően fenyegetnek azzal, hogy a fiókot hamarosan bezárják, vagy azt sugallják, hogy az veszélybe került (Toma–Hancock 2012). Das és társai egészségügyi témában végzett kísérlete szerint egy fenyegető vagy félelmet felkeltő elem elhelyezése az üzenet fokozottabb elfogadásához vezet az információfeldolgozásra gyakorolt sajátos hatása révén (Das et al. 2003). Az adathalászok célja, hogy

ezekkel a kifejezésekkel a racionális döntéshozatal helyett érzelmi reakciókat keltve a felhasználókat gyors döntésekre késztessék, amelyek során nagy esélyel figyelmen kívül hagyják a csalásra utaló jeleket (Vishwanath et al. 2011; Harrison et al. 2016). A félelemkeltés mellett a phishing üzenetek másik bevett pszichológiai manipulációs módszere, amikor a felhasználókat jutalomalapú üzenetekkel próbálják meggyőzni, valami értékes árut vagy pénzösszeget felajánlva. Erre példa az úgynevezett „nigériai herceg"-típusú átverés, amelyben több millió dollár értékű, Nigériából származó bankszámlán fekvő pénzösszeg jelentős százalékát ígérik, cserébe a segítségért a pénz Nigériából való kivitelében (Harrison et al. 2016)

A megtévesztő kommunikáció kiszivárgó nyelvi jelei

A hazugság aktusával együtt járó negatív érzelmek nyelvi szinten is kifejeződnek, úgynevezett „kiszivárgó jelek" (leakage cues) formájában, amelyek a csalók szándékaitól függetlenül felfedik megtévesztő eredetüket. A kiszivárgó jeleket elsőként Ekman és Friesen írta le a személyes, nem verbális kommunikáció relációjában. Ezeket olyan testmozgások és arckifejezések bizonyos típusaiként definiálták, amelyek „megszöktek" a megtévesztésre irányuló erőfeszítések közül (Ekman–Friesen 1969). Ugyanakkor a csak szöveges üzenetekből hiányzik az arckifejezés, a gesztusok, a testtartás és a távolságtartás, így ebben az esetben maga a szöveg az egyetlen forrás, amelyből következtethetünk annak hitelességére. A megtévesztés felderítésére a nyelvi információk szisztematikus elemzésére van szükség, meg kell vizsgálni a nyelvi alapú jelzéseket, amelyek a szövegegység(ek)ben található nyelvi információkkal kapcsolatosak: a szavakat, kifejezéseket, mondatokat, illetve a teljes üzenetet (Zhou et al. 2004).

A hazudozók valódi lelkiállapotára utaló, kiszivárgó nyelvi jel lehet a történetük elmeséléshez használt nyelvi stílus. A sikeres hazugsághoz előbb egy igaznak tűnő történetet kell kreálni, majd nyelvi manipuláció révén olyan stílusban kell előadni, hogy az őszintének tűnjön. A nyelvi stílus jelei a névmáshasználat, az érzelmi tónusú szavak, valamint a kognitív munkát jelző elöljárószavak és kötőszavak használata. Newman és társai szakirodalmi elemzésükben a megtévesztő kommunikáció következő nyelvi jeleit találták: 1. Kevesebb egyes szám első személyű névmás (pl. én, nekem, nekem) használata. 2. Kevesebb harmadik személyű névmás (pl. ő, ők) alkalmazása. 3. Több negatív érzelmi szó (pl. gyűlölet, harag, ellenség) használata. 4. Kevesebb kizáró szó (pl. de, kivéve, anélkül) alkalmazása. 5. Több mozgásige (pl. jár, mozog, megy) használata (Newman et al. 2003). Zhou és társainak kutatása szerint a csaló üzenetek kevésbé közvetlen nyelvezetet alkalmaz-

tak, inkább informális hangvételűek voltak, kevesebb írásjelet alkalmaztak, ugyanakkor érzelmesebb nyelvezetet használtak (Zhou et al. 2004).

Kiszivárgó nyelvi jelek a számítógép közvetítette üzenetek, így az adathalászat esetében is léteznek. Ilyen például a használt nyelv helyessége a társkereső profilok hitelességének megítélésekor (Toma–Hancock 2012), vagy a csaló szándékkal írt e-mailekben megjelenő tipográfiai hibák (Zhou et al. 2004). Az adathalász e-mailek tipikus kiszivárgási jelei a tipográfiai, nyelvtani és helyesírási hibák, amelyek azt jelzik, hogy az e-mailt valójában nem egy hivatalos szervezet/személy írta (Toma–Hancock 2012; Zhou et al. 2004; Harrison et al. 2016; Butavicius et al. 2022; Parsons et al. 2016).

3. táblázat: Stratégiai és nem stratégiai nyelvi eszközök az adathalász próbálkozások esetén

Nyelvi eszközök	Példák	Említések
Stratégiai nyelvi eszközök az e-mail-címben és az URL-ben	Homográfia: a nyelvi karakterek vizuális hasonlóságára épülő csalás (pl. a bankofthevvest.com bankofthewest.com helyett)	Hong 2012
	Megbízható cég nevének szerepeltetése az URL-ben, de nem a hivatalos címe (pl. tv2.hu helyett tv2-friss.com)	Wu et al. 2006; Volkamer et al. 2017; Downs et al. 2006; Jakobsson et al. 2007; Canfield et al. 2016; Furnell 2007; Milletary 2005; Baslyman–Chiasson 2016; Chou et al. 2004; Wash 2020; Basit et al. 2021; Volkamer et al. 2017; Sheng et al. 2010
	Elmaszkírozott URL (rákattintás után nem a kijelzett címre visz)	Wu et al. 2006; Kirda-Kruegel 2006; Furnell 2007
	Meghamisított e-mail-cím: megbízható cégre utal, de nem az (pl. pluszbetűt tartalmaz, eltérő végződésű, mint a hivatalos)	Downs et al. 2006; Bayl-Smith et al. 2020 Bayl-Smith et al. 2020; Furnell 2007; Wash 2020
	Elmaszkírozott e-mail-cím (nem a valódi feladó e-mail-címe jelenik meg, hanem egy megbízható szervezeté)	Kirda-Kruegel 2006; Volkamer et al. 2017

Stratégiai nyelvi eszközök a szövegben	Nem létező szervezet/ intézmény említése	Chou et al. 2004
	Sürgősségre utaló jelzők alkalmazása (pl. „határidő", „közelgő"	Workman 2008; Butavicius et al. 2022
	Rövid szövegek készítése (minél kevesebb lehetőséget hagyni a félreértésre, hibákra)	Workman 2008; Toma and Hancock 2012
	Félelmet keltő, fenyegetettség érzését keltő szavak használata	Das et al. 2003; Workman 2008; Toma and Hancock 2012
	Jutalmat ígérő szavak használata	Harrison et al. 2016
Nem stratégiai nyelvi eszközök, kiszivárgó nyelvi jelek	Nyelvtani/helyesírási hibák, tipográfiai hibák, félregépelések	Downs et al. 2006; Canfield et al. 2016; Furnell 2007; Baslyman–Chiasson 2016; Chou et al. 2004; Wash 2020; Volkamer et al. 2017; Parsons et al. 2016; Vishwanath et al. 2011; Bayl-Smith et al. 2020; Harrison et al. 2016; Parsons et al. 2016; Butavicius et al. 2022
	HTTP a HTTPS helyett az URL-ben	Chou et al. 2004; Dhamija et al. 2006
	Általános/személytelen megszólítás	Parsons et al. 2013; Sheng et al. 2010; Butavicius et al. 2022
	Helytelen nyelvezet: szokatlan (akár nevetséges) megszólítás/ elköszönés (pl. az adott országban másképp használják)	Wash 2020
	Hibás karakterek megjelenése (pl. ékezetek nélkül)	Milletary 2005
	Szokatlan tördelés, bekezdések, más betűtípus, mint ami megszokott	Wash 2020

Forrás: saját készítés

A 3. táblázat alapján elmondható, hogy az adathalász próbálkozások esetében is jól beazonosíthatók azok a stratégiai és nem stratégiai nyelvi jelek, amelyek visszatérően jellemzik az ilyen csalási kísérleteket. A stratégiai nyelvi jeleket két külön kategóriába tudtuk sorolni: az egyik csoportot kifejezetten a szövegben tudatosan alkalmazott, nyelvi megtévesztő elemek jelentik, a másikat az üzenet célbajuttatását jelentő platform (jellemzően e-mail) és az adatok ellopására szolgáló felületre mutató link relációjában alkalmazott nyelvi jelek alkotják. Ez utóbbiakat nem minden esetben lehet egyértelműen a stratégiai nyelvi jelek közé sorolni, ezek ugyanis egyúttal kiszivárgó nyelvi jelek is. Ugyanakkor a nem szándékosan megjelenő nyelvi jelek (pl. a helyesírási hibák, a helytelen nyelvtani szerkezetek, az ékezethibák, a félregépelések egyértelműen a nem szándékos, stratégiai nyelvi jelek körébe sorolhatók, és mint ilyenek, egyúttal automatikusan kiszivárgó nyelvi jelek is, amelyek alapján beazonosítható a csalási kísérlet.

Az általunk feltárt szakirodalom minimálisan foglalkozik azzal, milyen jelek szerepelnek a valós, hivatalos, becsületes szándékú üzenetekben, amelyeket nem csalók készítettek. A néhány említést, amelyet találtunk, a 4. táblázatban foglaltuk össze.

4. táblázat: Az üzenet valódiságára utaló jelek

Az üzenet valódiságára utaló jelek	Említések
Nem szerepel link az üzenetben.	Downs et al. 2006
Ha az üzenet tartalmaz linket, az valóban a magát mutató, megbízható harmadik fél hivatalos weblapjára visz.	Downs et al. 2006; Sheng et al. 2010
Az üzenet feladója ismert, és ellenőrizhető módon valóban az, akinek mutatja magát.	Downs et al. 2006
Az üzenetben létező, valós adatokra, tényekre utalnak (pl. egy munkahellyel kapcsolatban).	Downs et al. 2006
Az üzenet névre szóló megszólítást alkalmaz, személyre szól.	Downs et al. 2006; Butavicius et al. 2022
Professzionális, nyelvtanilag helyes nyelvezetet használ, ahogyan azt a hatósági jogkörrel rendelkező szervezetek (pl. a rendőrség vagy az adóhivatal) teszik.	Butavicius et al. 2022
Az üzenet nem kér jelszót vagy egyéb érzékeny személyes adatokat.	Downs et al. 2006
Nincs fenyegetés, sürgetés akkor sem, ha valamilyen problémára hívja fel a figyelmet.	Sheng et al. 2010

Forrás: saját szerkesztés

Összességében elmondható, hogy nyelvi szempontok alapján azok az üzenetek tekinthetők nagy eséllyel valódinak, amelyek nem tartalmazzák a 3. táblázatban szereplő jeleket. Ugyanakkor ez sem ennyire egyértelmű, hiszen bárkivel előfordulhat, hogy félregépel egy szót az üzenetben, illetve egy szolgáltatótól érkező hivatalos e-mail is tartalmazhat linket, amire kattintva számlát kell befizetni. Eközben egy adathalász üzenet is lehet nyelvtanilag tökéletes és kiváló helyesírású. Emiatt minden egyes üzenet szövegét egyenként kell lingvisztikai és vizuális elemzés alá vetni, több vizuális nyelvi jelet egyszerre kell megfigyelni, illetve egyéb külső körülményt is mérlegelni. De általánosságban elmondható, hogy ha az üzenetben nem látjuk a pszichológiai manipulációra utaló jeleket, ha nem történik érzelemkeltés (ijesztgetés vagy csábító dolog ígérete), ha nincs link, amire kattintani kell, ha nem váratlan és szokatlan az üzenet felbukkanása, ha minél több valós, ellenőrizhető adatot tartalmaz, ha nincs elmaszkírozott URL vagy e-mail-cím, ezekben nincsen elírás és/vagy szokatlan végződés, akkor nagyobb eséllyel minősíthető valódinak az adott üzenet.

Összegzés

Az adathalászat, különösen a phishing technikák vizsgálata alapján világossá válik, hogy ez a kiberbűnözési forma rendkívül kifinomult pszichológiai és nyelvi manipulációkra épül, amelyek célja a felhasználók érzékeny adatainak megszerzése. A digitális világban a social engineering technikák új dimenzióba léptek, amelyben az elkövetők a bizalomépítés és a megtévesztés komplex hálóját szövik, hogy kihasználják az emberek kognitív és érzelmi sebezhetőségét.

A jelen tanulmány rámutatott, hogy az adathalász technikák szoros kapcsolatban állnak a klasszikus megtévesztési módszerekkel, és ezek napjainkban az online platformokon keresztül öltöttek új formát. A vizsgálatok feltárták, hogy az adathalász támadások nem csupán az áldozat technikai tájékozatlanságát célozzák meg, hanem kihasználják az emberi döntéshozatal és érzelmi reakciók gyenge pontjait is. A támadók által alkalmazott módszerek, mint a sürgetés, a félelemkeltés, az empátia kiváltása vagy a jutalom ígérete mind hozzájárulnak ahhoz, hogy a felhasználók könnyen áldozatul essenek.

Az itt közreadott kutatásból kiderült, hogy a nyelvi elemek különösen fontos szerepet játszanak a phishing támadások sikerességében. Az adathalász üzenetekben megfigyelhető stratégiai nyelvi eszközök – például a sürgető hangnem, a bizalomkeltő szervezetekre való hivatkozás, valamint a vizuális hasonlóságokra építő homográfok – mind arra irányulnak, hogy az áldoza-

tokat a pszichológiai manipuláció révén cselekvésre ösztönözzék. Emellett az úgynevezett kiszivárgó nyelvi jelek, mint a helyesírási és nyelvtani hibák további nyomokat szolgáltatnak az ilyen típusú üzenetek felismeréséhez.

Összefoglalva: az adathalászat elleni védekezés kulcsfontosságú eleme az edukáció és a felhasználók tudatosságának növelése. Az embereknek meg kell tanulniuk felismerni azokat a nyelvi és kommunikációs mintákat, amelyek a phishing támadások jellemzői, és tudatosítaniuk kell, hogy ezek az üzenetek gyakran érzelmi reakciókat kiváltva igyekeznek manipulálni őket. Az adathalászat elleni hatékony küzdelem érdekében elengedhetetlen, hogy a nyelvészeti és pszichológiai elemzések által feltárt mintákat széles körben megismertessük a társadalommal, hiszen csak így csökkenthető a jövőbeli támadások sikeressége.

Szakirodalom

Abroshan, Hossein – Devos, Jan – Poels, Geert – Laermans, Eric 2021. Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* 9/44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Balázs Géza 2003. „Minden házfalat cseréljetek sms-falra!" Sms-fal mint elektronikus graffiti. *Magyar Nyelvőr* 144–59.

Balázs Géza 2004. Választási sms-ek folklorisztikai-szövegtani vizsgálata. *Magyar Nyelvőr* 36–53.

Balázs Géza 2005. Az új média új műfaja, az sms-hír – nyelvészeti megközelítésben. *Magyar Nyelvőr* 129–50.

Balázs Géza 2006. Az sms-folklór – a minimálfolklór nyelvi képe. I. rész. *Magyar Nyelvőr* 439–56.

Balázs Géza 2007. Az sms-folklór – a minimálfolklór nyelvi képe. II. rész. *Magyar Nyelvőr* 48–62.

Balázs Géza 2010. Az új médiumok retorikája. *ME.DOK Média-Történet-Kommunikáció* 4/5–16.

Balázs Géza 2015. Netfolklór – intermedialitás és terjedés. *Replika* 1–2/171–85.

Balázs Géza 2023a. *Újmédia-kislexikon.* IKU. Budapest. (IKU-Tár 22.)

Balázs Géza 2023b. *Az internet népe. Internet – társadalom – kultúra – nyelv. A kulturális és a tervezett evolúció határán*. Ludovika Egyetemi Kiadó. Budapest.

Baltuttis, Dennik – Teubner, Tim 2024. Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. *Computers & Security* 144/1–25. https://doi.org/10.1016/j.cose.2024.103940.

Basit, Abdul – Zafar, Maham – Liu, Xuan – Javed, Abdul Rehman – Jalil, Zunera – Kifayat, Kashif 2021. A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication systems* 1/139–54. https://doi.org/10.1007/s11235-020-00733-2

Baslyman, Malak – Chiasson, Sonia 2016. „Smells Phishy?": An educational game about online phishing scams. *2016 APWG Symposium on Electronic Crime Research, eCrime 2016, Toronto, ON, Canada, June 1–3, 2016.* IEEE, 1–11.

Bayl-Smith, Piers – Sturman, Daniel – Wiggins, Mark 2020. Cue Utilization, Phishing Feature and Phishing Email Detection. In: Bernhard, Matthew – Bracciali, Andrea – Camp, L. Jean – Matsuo, Shin'ichiro – Maurushat, Alana – Rønne, Peter B. – Sala, Massimiliano (eds.): *Financial Cryptography and Data Security*. Springer International. Cham, Switzerland. 56–70.

Bustio-Martínez, Lázaro – Herrera-Semenets, Vitali – García-Mendoza, Juan Luis – Álvarez-Carmona, Miguel Ángel – González-Ordiano, Jorge Ángel – Zúñiga-Morales, Luis et al. 2024. Uncovering phishing attacks using principles of persuasion analysis. *Journal of Network and Computer Alications* 230/1–15. https://doi.org/10.1016/j.jnca.2024.103964

Butavicius, Marcus – Parsons, Kathryn – Pattinson, Malcolm – McCormac, Agata 2016. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. In: *Australasian Conference on Information Systems 2015*. Adelaide, Australia. 1–10. https://doi.org/10.48550/arXiv.1606.00887

Butavicius, Marcus – Taib, Ronnie – Han, Simon J. 2022. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security* 123/1–10. https://doi.org/10.1016/j.cose.2022.102937

Canfield, Casey Inez – Fischhoff, Baruch – Davis, Alex 2016. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human factors* 8/1158–72. https://doi.org/10.1177/0018720816665025

Chaudhry, Junaid Ahsenali – Chaudhry, Shafique Ahmad – Rittenhouse, Robert G. 2016. Phishing Attacks and Defenses. *International Journal of Security and Its Applications* 1/247–56. https://doi.org/10.14257/ijsia.2016.10.1.23

Chou, Neil – Ledesma, Robert – Teraguchi, Yuka – Mitchell, John C. 2004. Client-side defense against web-based identity theft. In: *Proceedings of the Network and Distributed System Security Symposium, NDSS 2004,* The Internet Society. San Diego, California, USA. https://crypto.stanford.edu/SpoofGuard/webspoof.pdf (Letöltés: 2024. 07. 14.)

Chung, Cindy K. – Pennebaker, James 2007. The Psychological Functions of Function Words. Fiedler, Klaus (ed.): *Social communication. Frontiers of social psycholog.* Psychology Press, New York, USA. 343–59.

Das, Enny H. H. J. – Wit, John B. F. de – Stroebe, Wolfgang 2003. Fear appeals motivate acceptance of action recommendations: evidence for a positive bias in the processing of persuasive messages. *Personality & social psychology bulletin* 5/650–64. https://doi.org/10.1177/0146167203029005009

Dhamija, Rachna – Tygar, J. D. – Hearst, Marti 2006. Why phishing works. In: Grinter, Rebecca – Rodden, Thomas – Aoki, Paul – Cutrell, Ed – Jeffries, Robin – Olson, Gary (eds.): *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Conference on Human Factors in Computing Systems. Montréal Québec Canada, 22 04 2006 - 27 04 2006. Association for

Computing Machinery, New York, NY. USA. 581–90. https://escholarship.org/content/qt9dd9v9vd/qt9dd9v9vd.pdf (Letöltés: 2024. 07. 14.)

Downs, Julie S. – Holbrook, Mandy B. – Cranor, Lorrie Faith 2006. Decision strategies and susceptibility to phishing. In: Cranor, Lorrie Faith (ed.): *Proceedings of the second symposium on Usable privacy and security - SOUPS '06. the second symposium.* Pittsburgh, Pennsylvania, 2006. 07. 12. 2006. 07. 14. ACM Press. New York, USA 1–12. https://kilthub.cmu.edu/articles/journal_contribution/Decision_Strategies_and_Susceptibility_to_Phishing/6621860/files/12118340.pdf (Letöltés: 2024. 07. 14.)

Ekman, P. – Friesen, W. V. 1969. Nonverbal leakage and clues to deception. *Psychiatry* 32. 1/88–106. https://doi.org/10.1080/00332747.1969.11023575

Furnell, Steven 2007. Phishing: can we spot the signs? *Computer Fraud & Security* 3/10–5. https://doi.org/10.1016/S1361-372307.70035-0

Harrison, Brynne – Svetieva, Elena – Vishwanath, Arun 2016. Individual processing of phishing emails. *Online Information Review* 2/265–281. https://doi.org/10.1108/OIR-04-2015-0106

Hong, Jason 2012. The state of phishing attacks. *Communications of the ACM* 101/74–81. https://doi.org/10.1145/2063176.2063197

Jagatic, Tom N. – Johnson, Nathaniel A. – Jakobsson, Markus – Menczer, Filio 2007. Social phishing. *Communications of the ACM* 10/94–100. https://doi.org/10.1145/1290958.1290968

Kenyeres Attila Zoltán – Szűts Zoltán 2024. Az álhírek (fake news) definíciós kísérletei és nyelvi jelei. *Magyar Nyelvőr* 203–35. https://doi.org/10.38143/Nyr.2024.2.203

Kirda, E. – Kruegel, C. 2006. Protecting Users against Phishing Attacks. *The Computer Journal* 5/554–61. https://doi.org/10.1093/comjnl/bxh169

Lahti, Henri – Kokkonen, Marja – Hietajärvi, Lauri – Lyyra, Nelli – Paakkari, Leena 2024. Social media threats and health among adolescents: evidence from the health behaviour in school-aged children study. *Child and adolescent psychiatry and mental health* 18/1–17. https://doi.org/10.1186/s13034-024-00754-8

Liu, Gang – Xiang, Guang – Pendleton, Bryan A. – Hong, Jason I. – Liu, Wenyin 2011. Smartening the crowds: Computational Techniques for Improving Human Verification to Fight Phishing Scams. In: *SOUPS 2011 - Proceedings of the 7th Symposium on Usable Privacy and Security.* 7th Symposium on Usable Privacy and Security, SOUPS 2011, Pittsburgh, PA, United States, 20/07/11. https://dl.acm.org/doi/abs/10.1145/2078827.2078838 (Letöltés: 2024. 07. 14.)

Milletary, Jason 2005. *Technical Trends in Phishing Attacks*. Carnegie Mellon University. https://insights.sei.cmu.edu/library/technical-trends-in-phishing-attacks/ (Letöltés: 2024. 07. 14.)

Newman, Matthew L. – Pennebaker, James W. – Berry, Diane S. – Richards, Jane M. 2003. Lying words: predicting deception from linguistic styles. *Personality & social psychology bulletin* 5/665–75. https://doi.org/10.1177/0146167203029005010

O'Hagan, Louise 2018. Angler phishing: Criminality in social media. In: Cunnane, Vincent – Corcoran, Niall (eds.): *Proceedings of the 5th European Conference on Social Media*, *ECSM 2018.* Limerick Institute of Technology. Ireland. 190–7.

Parekh, Shraddha – Parikh, Dhwanil – Kotak, Srushti – Sankhe, Smita 2018. A New Method for Detection of Phishing Websites: URL Detection. In: *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. Coimbatore. India. 949–52. https://doi.org/10.1109/ICICCT.2018.8473085

Parsons, Kathryn – Butavicius, Marcus – Pattinson, Malcolm – Calic, Dragana – McCormac, Agata – Jerram, Cate 2016. Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? In: *Australasian Conference on Information Systems 2015*. Adelaide. Australia. 1–10. https://doi.org/10.48550/arXiv.1605.04717

Parsons, Kathryn – McCormac, Agata – Pattinson, Malcolm – Butavicius, Marcus – Jerram, Cate 2013. Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In: Janczewski, Lech J. – Wolfe, Henry B. – Shenoi, Sujeet (eds.): *Security and Privacy Protection in Information Processing Systems*. [IFIP Advances in Information and Communication Technology Vol.405.] Springer. Berlin Heidelberg. 366–78.

Saberi, Alireza – Vahidi, Mojtaba – Bidgoli, Behrouz Minaei 2007. Learn to Detect Phishing Scams Using Learning and Ensemble Methods. In: *2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops*. IEEE. 311–4. https://doi.org/10.1109/WI-IATW.2007.79

Sheng, Steve – Holbrook, Mandy – Kumaraguru, Ponnurangam – Cranor, Lorrie Faith – Downs, Julie 2010. Who falls for phish? In: Mynatt, Elizabeth – Fitzpatrick, Geraldine – Hudson, Scott – Edwards, Keith – Rodden, Tom Rodden (eds.): *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta Georgia USA, 10 04 2010 – 15 04 2010. ACM. New York, NY. USA. 373–82. https://doi.org/10.1145/1753326.1753383

Siddhesh Vijay, Jain – Kulkarni, Kaustubh – Arya, Arti 2022. Metaheuristic Optimization of Neural Networks for Phishing Detection. In: *2022 3rd International Conference for Emerging Technology INCET*. Belgaum. India. 2022. 05. 27. – 2022. 05. 29: IEEE. 1–5. https://doi.org/10.1109/INCET54531.2022.9824203

Singh, Tejveer – Kumar, Manoj – Kumar, Santosh 2024. Walkthrough phishing detection techniques. *Computers and Electrical Engineering* 118/1–15. https://doi.org/10.1016/j.compeleceng.2024.109374

Toma, Catalina L. – Hancock, Jeffrey T. 2012. What Lies Beneath: The Linguistic Traces of Deception in Online Dating Profiles. *Journal of Communication* 1/78–97. https://doi.org/10.1111/j.1460-2466.2011.01619.x

Vishwanath, Arun – Herath, Tejaswini – Chen, Rui – Wang, Jingguo – Rao, H. Raghav 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* 3/576–86. https://doi.org/10.1016/j.dss.2011.03.002

Volkamer, Melanie – Renaud, Karen – Reinheimer, Benjamin – Kunz, Alexandra 2017. User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & Security* 71/100–13. https://doi.org/10.1016/j.cose.2017.02.004

Wang, Jingguo – Herath, Tejaswini – Chen, Rui – Vishwanath, Arun – Rao, H. Raghav 2012. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication* 4/345–62. https://doi.org/10.1109/TPC.2012.2208392

Wang, Mengli – Song, Lipeng – Li, Luyang – Zhu, Yuhui – Li, Jing 2024. Phishing webpage detection based on global and local visual similarity. *Expert Systems with Alications* 252/1–13. https://doi.org/10.1016/j.eswa.2024.124120

Wash, Rick 2020. How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-Computer Interaction* CSCW2/1–28. https://doi.org/10.1145/3415231

Workman, Michael 2008. A test of interventions for security threats from social engineering. *Information Management & Computer Security* 5/463–83. https://doi.org/10.1108/09685220810920549

Wright, Adam – Aaron, Skye – Bates, David W. 2016: The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *Journal of general internal medicine* 10/1115–8. https://doi.org/10.1007/s11606-016-3741-z

Wu, Min – Miller, Robert C. – Garfinkel, Simson L. 2006. Do security toolbars actually prevent phishing attacks? In: Grinter, Rebecca – Rodden, Thomas – Aoki, Paul – Cutrell, Ed – Jeffries, Robin – Olson, Gary (eds.): *CHI '06: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Conference on Human Factors in Computing Systems. Montréal Québec, Canada 22 04 2006 – 27 04 2006. Association for Computing Machinery. New York, NY. USA. 601–10. https://doi.org/10.1145/1124772.1124863

Yan, Chuyi – Han, Xueying – Zhu, Yan – Du, Dan – Lu, Zhigang – Liu, Yuling 2024. Phishing behavior detection on different blockchains via adversarial domain adaptation. *Cybersecurity* 7/1–22. https://doi.org/10.1186/s42400-024-00237-5

Yang, Rundong – Zheng, Kangfeng – Wu, Bin – Di Li – Wang, Zhe – Wang, Xiujuan 2022. Predicting User Susceptibility to Phishing Based on Multidimensional Features. *Computational intelligence and neuroscience* 2022/1–11. https://doi.org/10.1155/2022/7058972

Zhang, Yue – Egelman, Serge – Cranor, Lorrie – Hong, Jason 2006. Phinding Phish: Evaluating Anti-phishing Tools. Carnegie Mellon University. Pittsburgh, Pennsylvania. https://lorrie.cranor.org/pubs/ndss-phish-tools-final.pdf (Letöltés: 2024. 07. 14.)

Zhou, Lina – Burgoon, Judee K. – Nunamaker, Jay F. – Twitchell, Doug 2004. Automating Linguistics-Based Cues for Detecting Deception in Text-Based Asynchronous Computer-Mediated Communications. *Group Decision and Negotiation* 1/81–106. https://doi.org/10.1023/B:GRUP.0000011944.62889.6f

Zieliński, Sebastian 2024. Evolving Threats, Emerging Laws: Poland's 2023 Answer to the Smishing Challenge. *Computer Law & Security Review* 9/1–18. https://doi.org/10.1016/j.clsr.2024.106013

Kenyeres Attila Zoltán
egyetemi adjunktus
Eszterházy Károly Katolikus Egyetem
E-mail: kenyeres.attila.zoltan@uni-eszterhazy.hu
https://orcid.org/0009-0009-5745-0073

Szűts Zoltán
egyetemi tanár
Eszterházy Károly Katolikus Egyetem
E-mail: szuts.zoltan@uni-eszterhazy.hu
https://orcid.org/0000-0001-8539-670X

Abstract

Kenyeres, Attila Zoltán – Szűts, Zoltán

Definition of Phishings and its Main Linguistic Signs

Phishing is a type of cybercrime that, in recent years, has caused significant financial damage to many members of society worldwide as a result of the development of information and digital technology. In its narrowest definition, phishing is the use of social engineering techniques to steal sensitive personal data (such as bank card details) from users via the Internet, usually for financial gain. It also includes malicious software installed on users' devices by trickery to obtain sensitive personal data. A broader definition of phishing includes malicious activities that also use social engineering or other fraud to induce unsuspecting users to transfer money directly. In addition, there are other sub-categories of phishing based on the platform used, such as voice-phishing (vishing), or SMS-phishing (smishing). The aim of this paper is to outline a comprehensive theoretical framework for phishing, by briefly reviewing the historical background of phishing, summarising the narrower and broader definitions of the phenomenon based on the relevant international literature, and identifying which activities do not fall within the scope of phishing. We will then discuss the strategic (intentionally used) and non-strategic linguistic devices, the so-called „leaky linguistic signals", which indicate the presence of phishing.

Keywords: phishing, language signals, linguistics