TÁJÉKOZTATÓ
jelszavukat e-mailben kiadó felhasználók számára

Az SzSzK szabályzatának II./13 .§ (1) bekezdése kimondja, hogy a számla (account) nem átruházható. Jelszavának továbbadása a számla megosztásának minősül.

Mik ezek a levelek amiket kapott?
A kéretlen levelek egy fajtája a phising vagy adathalász levél. Ezekben a felhasználó hozzáférési adatait próbálják megszerezni. Az ilyen levelekben vagy azt kérik hogy azokra válaszolva adják meg loginnevüket és jelszavukat, vagy egy az e-mailben szereplő linket kell meglátogatni, ahol loginnévvel és jelszóval kell belépni.

Miért akarják megszerezni a jelszavakat?
A leggyakoribb hogy a hozzáférést kéretlen reklám levelek küldésére, vagy további adathalász levelek küldésére szeretnék felhasználni, de előfordulhat az is hogy személyes vagy üzleti titkokat akarnak megszerezni.

Hogyan ismerhető fel hogy egy ilyen levél adathalász e-mail, vagy valódi?
A feladó sokszor nem helyi, azaz semmi köze az egyetemhez, a válaszcím sokszor egészen más mint a feladó címe. Sokszor pongyola, vagy hemzseg a helyesírási hibáktól. Aláírásként általában valamilyen nem is létező egység, vagy személyten „admin“ vagy hasonló szerepel. A linkben megadott hosztnév nem .pte.hu -ra végződik, stb... de a legegyszerűbben a következő szempontot figyelembe véve ismerhetők fel ezek a levelek: **MIND HAMIS!** A számítóközpont sosem kér e-mailben jelszót, és sosem küld linket olyan oldalakra ahol kötelezően be kéne lépni a „gammás“ loginnév-jelszó párossal.

„Nincs semmi titkos/fontos a levelezésemben, nem történt tragédia.“
Ez a - sajnos tipikus - felhasználói hozzáállás a hozzá nem értésből fakad. Lássuk milyen károk érhetik a felhasználót, illetve karunkat egy ilyen eset kapcsán:

- *a támadók hozzáférnek a felhasználó minden tárolt leveléhez, és címjegyzékéhez.*
A nincs semmi titkos/fontos a levelezésemben állítás lehet, hogy a felhasználó részéről akár igaz is, de nem biztos, hogy a mások által írt leveleket a küldő sem értékeli bizalmasként, előfordulhat hogy kiszivárgásuk zavarja őket. Ha valóban semmi fontos nincs a levelezésében, javasoljuk a felesleges mailbox megszűntetését.
A címjegyzékben szereplő e-mail címek, illetve a különböző mappákban álló levelek feladói, címzettjei számíthatnak rá hogy bekerülnek a spammerek különböző adatbázisaiba, mint létező - élő e-mail címek, így egyre több kéretlen levelet fognak kapni.

- *a támadók nagy mennyiségű kéretlen reklámlevelet, vagy adathalász leveleket küldenek a felhasználó nevében.*
A felhasználó később szembetalálhatja magát azzal, hogy e-mail partnerei nem kapják meg leveleit, vagy azok rendszeresen a spam mappájukba kerülnek.
Sok esetben a kiküldött levélmennyiség eléri azt a szintet hogy a feladó szerver bekerül egyes internetes tiltó listákba, aminek hatására a gép több e-mail rendszerbe nem képes levelet küldeni. Ebben az esetben már nem csak a felhasználót, hanem - mivel ezek a tiltó listák rendszerint IP címekre vonatkoznak - karunkat is, és a gamma.ttk.pte.hu-t használók mindegyikét is kár éri. Az efféle blokkolások manapság egy-egy nem megérkező e-mail miatt akár milliós pályázatok elbukását is eredményezhetik, vagy - hogy egy még gyakoribb példát hozzunk fel - kérdésessé tehetnek akár érdemjegyeket is, ha beadandók emiatt nem érkeznek meg egy oktatóhoz. Ugyanígy hatással lehet ez persze pl. a TO-val történő e-mailes ügyintézésre is. Az ilyen tiltó listákról lekerülni sokszor heteket is igénybe vehet, és minél többször szerepelünk rajtuk, lekerülni annál nehezebb. A rendszeres szereplésünk ezeken a listákon aláássa egyetemünk, és karunk hírnevét is.

- *a támadók bármit megtehetnek a levelezésünkkel.*
Előfordul, hogy a támadók átirányítják a levelezésünket, és így el is tűnhetnek azok a levelek, amiket nekünk írtak a feltörés ideje alatt.
Szintén gyakori, hogy - mivel a spammerek e-mail cím listái ritkán tökéletesek - a sok visszapattanó levél miatt elfogy a hely, és a spammerek viszavonhatatlanul törölnek olyan leveleket, vagy akár egész mappákat, amelyek számunkra fontosak voltak.

- *a támadók visszaélhetnek a hozzáféréssel.*
A felhasználót megszemélyesítve obszcén leveleket küldhetnek az illető nevében, dolgozók esetében akár utasításokat adhatnak ki nevükben. Sok fórum és közösségi oldal jelszava is megszerezhető, ha hozzáférnek az e-mailünkhöz amivel regisztráltunk, mivel sikertelen belépés esetén új jelszót, vagy jelszó visszaállító linket kaphatnak a spammerek e-mailben.

- *a támadók úgy érzik, olyan felhasználói bázist találtak akiktől könnyű megszerezni jelszavukat.*
Ennek hatására egyre több és több adathalász e-mail fog érkezni mindenkihez a karon.

- *a számítóközpont - amennyiben a naplókból, tiltólisták logjaiból, vagy bejelentés alapján tudomására jut, hogy jelszava kiszivárgott - blokkolhatja hozzáférését.*
Ilyen esetekben általában nem tudjuk a felhasználót informálni erről, hiszen levelezéséhez éppen a zárolás miatt nem fér hozzá. Ez kellemetlenséggel járhat, főként, hogy a zárolás feloldásához, illetve új jelszó kiadásához hitelt érdemlően igazolnia kell magát a számítóközpont felé, személyes megjelenéssel, illetve arcképes igazolvánnyal.

Mire számítson, mire figyeljen miután visszakapta jelszavát?
- Legyen az eddiginél szkeptikusabb az e-mailekkel szemben. Vegye figyelembe, hogy a feladó hamisítható, és hogy a számítóközpont egyáltalán nem szokott körleveleket írni. Egy sikeres betörés után nagyobb mennyiségben számíthat a paypal vagy banki leveleknek látszó átverésekre is.
- Ellenőrizze átirányítási beállításait, nem kapnak-e a betörők továbbra is másolatot bejövő levelezéséről.
- Nézze át tárolt leveleit, nem hiányoznak-e mappák - minél korábban jelzi hiányukat, annál nagyobb az esély rá, hogy egy korábbi állapotot vissza tudunk másolni mentéseinkből.
- Változtasson jelszót azokban a rendszerekben ahol az itteni levelezésével megegyező jelszót adott meg, vagy amelyek e-mailben küldték el jelszavát.
- Ellenőrizze, hogy be tud-e jelentkezni azokba a rendszerekbe amelyekben kontaktként itteni e-mail címét adta meg.