A JELSZÓ LEHET JÓ IS MEG HAM IS

KESZTHELYI András
egyetemi docens, Óbudai Egyetem Keleti Károly Gazdasági Kar
associate professor, Óbuda University Keleti Károly Faculty of Business and Management
email: Keszthelyi.Andras@kgk.uni-obuda.hu
ORCID: 0000-0002-8001-4888

ABSTRACT
PASSOWORD MAY BE EITHER GOOD OR FAKE

The role of passwords in the field of information security is of critical importance even today. One could think that there is nothing new in this field. Very unfortunately there have been obsessions or delusions related to passwords out in the wild which are dangerous. Sometimes these delusions and practices are taught and/or strengthened by famous institutions as well. In this paper I investigate some of them and prove their harmfulness hoping that someone will learn from it. These (and many other) worst practices are the basic source of this paper. They can be found anywhere and every time in our everyday life. This field has a side effect on university rankings as well. I'll show that there is (at least) one aspect in which Óbuda University is significantly better than the Stanford University.

Keywords: password, information security, university ranking
Kulcsszavak: jelszó, információbiztonság, egyetemi rangsor

1. Bevezetés

A jelen tanulmány kereteit (messze) meghaladja olyan alapfogalmak részletes körüljárása és bemutatása, mint pl. „rendszer", „környezet", „műveltség", „kultúra" stb. Axiómaként rögzített kiindulópont[1],[2] – Szücs Ervin és kollégái, hajdanvolt tanáraim nyomán --, hogy az ember egyrészt természeti lény, másodrészt társadalmi, harmadrészt pedig technikai, és ennek megfelelően kell vizsgálnunk természeti, társadalmi és technikai környezetét, ezeknek általános és specifikus szabályait, működését.

Az azóta eltelt évtizedekben az infokommunikációs technológiák olyan robbanásszerű fejlődésen mentek keresztül, ami olyannyira átalakítja mindennapi

1 Szücs Ervin: Rendszer és modell. Nemzeti Tankönykiadó, Budapest, 1996.

2 Endrei Walter – Makkai László – Nagy Dénes – Szücs Ervin: Ember és technika I. Tankönyvkiadó, Budapest, 1989.

életünket, hogy az analóg, fizikai, hagyományos értelemben vett világ mellett nyugodtan beszélhetünk virtuális világról is. Tekinthetnénk ez utóbbit a technikai környezetünk részének, de éppen azért, mert hatásai, befolyása, tőle való függésünk mértéke ekkora, indokolt önálló, immáron negyedik környezetünkként kezelni. A Nemzetközi Távközlési Egyesület (ITU) becslése szerint az internet teljes adatforgalma 2022-ben mintegy 5.291 EB (exabájt, 1018 byte) volt[3], erőteljesen, exponenciális ütemben növekvően. A digitális hálózatokon kezelt adatoknak nemcsak a mennyisége elképesztő, de az ezen adatoktól való függésünk mértéke is. Gondolatkísérlet: mi történne, ha péntek déltől rá következő hétfő reggel nyolcig nem lenne internet?

Negyedik környezetünknek, a virtuális világnak olyan sajátos jellemzői[4] is vannak, amelyek homlokegyenest ellentétesek a hagyományos világban megszokottakkal. Ezen sajátosságok alapja az a körülmény, hogy a digitális hálózatok virtuális világában bármiről (könyv, dal, film stb.) készíthetünk az eredetivel egyenértékű másolatot. Ennek időigénye és közvetlen költsége gyakorlatilag nulla. Ezen másolatokat pedig az internet bármely pontjára eljuttathatjuk gyakorlatilag nulla idő és költség fejében.

A biztonságnak (is) mindegyik környezetünkben megvannak a maga szabályai. Természeti környezetünkben főleg étkezés előtt kezet mosunk, hogy elkerüljünk egyes fertőző betegségeket. Társadalmi környezetünkben lemondunk az erőszak személyes alkalmazásáról, mert bízunk abban, hm, hogy a közrendet a mindenkori államhatalom fenntartja. Technikai környezetünkben is vannak a biztonságot közvetlenül érintő, befolyásoló szabályok, pl. a 10/2016. (IV. 5.) NGM rendelet a munkaeszközök és használatuk biztonsági és egészségügyi követelményeinek minimális szintjéről. A virtuális világban pedig a hozzáférés egyik kézenfekvő biztonsági eszköze a jelszó. A jelszavakat már sokszor és sokan próbálták temetni, mint idejétmúlt és problémás módszert. Figyelembe véve azonban azt a körülményt, hogy alkalmazásuk járulékos költséggel nem jár (mint a birtoklás alapú és biometrikus módszereknél), valamint kellő körültekintés esetén rendkívül biztonságosak lehetnek, biztosra vehetjük, hogy még sokáig velünk maradnak. Épp ezért kiemelt fontosságú, hogy tisztában legyünk a jelszóbiztonság legfontosabb tudnivalóival felhasználóként[5] és rendszerüze-

3 Facts and Figures 2023. https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-traffic/

4 Keszthelyi, A. (2015). Age of Cyber Crime and Culture of Security. In: Science Journal of Business and Management. Special Issue: The Role of Knowledge and Management's Tasks in the Companies. Vol. 3, No. 1-1, 2015, pp. 39-45. doi: 10.11648/j.sjbm.s.2015030101.17

5 Keszthelyi, A. (2013). About Passwords. Acta Polytechnica Hungarica 10 : 6 pp. 99-118. , 20 p. (2013)

meltetőként[6] is, de az információbiztonságot érintő auditok esetében is kiemelten vizsgálandó ez a terület.[7]

2. Jelszavak

A jó jelszó – könnyen belátható – megjegyezhető és mások által megtippelhetetlen. A megjegyezhetőséget mindenki – szubjektíve – a saját maga számára el tudja dönteni, a megtippelhetetlenség vizsgálatához pedig ismerni kell a jelszavas védelmek elleni támadási módszereket. Az a jelszó, ami kellően ellenálló a lehetséges támadásoknak, azt minősíthetjük megtippelhetetlennek.

A jelszavak megtippelésére irányuló módszerek a következők[8]:

A néhány száz leggyakoribb jelszó (asdfgh, 123456 stb.) kipróbálása. A következő szint, ha kapcsolat van a felhasználó személye és jelszava között (pl. születési dátuma, macskája neve), vagy formális kapcsolat van a felhasználói név és a jelszó között (admin – admin), illetve ha a felhasználói név és a jelszó között logikai kapcsolat van (JamesBond – 007). Ha ezen módszerek valamelyike eredményes (lehet), az a súlyos gondatlanság esete, azaz a közmondásos emberi tényező fontosságát támasztja alá[9].

Ha ezek nem vezettek eredményre, a támadó következő lehetősége a szótár alapú (offline) támadás egyszerű, ill. továbbfejlesztett változata, melynek során egy célprogram egyenként kipróbálja egy adott szólista minden elemét, esetleg ezek gyakori toldalékolt változatait (ablak, ..., zsiráf; ablak01, ..., ablak99 stb.). A hatékonyság növeléséhez jó támpont a napvilágra került jelszóadatbázisok szerkezeti elemzése.

Ha a felhasználó olyan jelszót választott, ami ezen módszerekkel eredményesen megtalálható, azt nehéz másképpen minősíteni, mint a könnyelmű gondatlanság esetét.

---

6 Tick, Andrea ; Szabó-Harka, Nikolett, Analysis of Information Security in a Corporate Environment – a Human Perspective, In: IEEE, Publ. (szerk.) IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics : SAMI 2024 : Proceedings, Danvers (MA), Amerikai Egyesült Államok : IEEE (2024) pp. 469-474. https://doi.org/10.1109/SAMI60510.2024.10432889

7 Tran, Nguen Bao Ngo ; Andrea, Tick , Cyber-security risks assessment by external auditors, Interdisciplinary Description of Complex Systems 19 : 3 pp. 375-390. (2021), https://doi.org/10.7906/indecs.19.3.3

8 Keszthelyi, A. (2013). About Passwords. In: ACTA POLYTECHNICA HUNGARICA 10 : 6 pp. 99-118. , 20 p. (2013)

9 Sámson, Norbert ; Tick, Andrea, Digital Defense: Investigating Human Aspects of Cybersecurity, In: Anikó, Szakál (szerk.) SACI 2024: 18th IEEE International Symposium on Applied Computational Intelligence and Informatics: Proceedings, Timisoara, Románia : IEEE (2024) pp. 525-532.

A legvégső eset a nyers erő alkalmazása, amikor az erre szakosított célprogram (John the Ripper, pl.) minden lehetséges karakterkombinációt egyenként végigpróbál. Ez a módszer egész biztos megtalálja a helyes jelszót, a kérdés csak az, hogy ez megtörténik-e a világegyetem vége előtt.

A „megtippelhetetlen" jelszót tehát valójában tehát az minősíti, hogy a nyers erős próbálkozásnak mennyi ideig tud ellenállni. A különbség nem a fél óra és a négy hónap között van, hanem az emberileg még felfogható (pár hónap, esetleg év) és már felfoghatatlan (a világegyetem becsült koránál több) időtartam között.

A törési időigény kiszámítása elvben igen egyszerű. Legyen KH a karakterhalmaz számossága, amelyből a jelszó egyes karakterei választhatók (pl. ASCII karakterek), legyen a jelszó legnagyobb hosszúsága H darab karakter. Ekkor a lehetséges különböző karakterkombinációk száma, KK így adódik:

$$KK=KH^H$$

(Mint ahogyan a négyjegyű pin-kód esetében KH=10, H=4, KK=10.000; 0000, ..., 9999.)

A törési sebességet (TS) próba/másodpercben tudjuk mérni, így az adódik, hogy adott paraméterek mellett a szükséges idő (SZI), ami alatt mindenképpen (azaz a legutolsó próbálkozással) megtalálja a támadó a jelszót:

$$SZI=KK/TS \text{ [másodperc]}$$

A törési (próbálkozási) sebesség függ az erre felhasználható hardver teljesítményétől, illetve az alkalmazott hash-függvény számításigényétől, egy adott esetben ez mintegy 350 milliárd próba/másodperc volt.[10],[11] Hogy a kvantumszámítógépek ezen a téren milyen változás hoznak, azt még nem tudjuk.

Ezen a ponton tudatosítani kell, hogy ha az alaphalmaz (KH) számosságát próbáljuk növelni, azaz a minél vegyesebb összetételt követeljük meg, akkor egyrészt a lehetséges kombinációszámot (KK) hatványfüggvény adja meg, és avval a problémával szembesülünk, hogy ezen alaphalmaz számossága csak erőst korlátozottan növelhető (l. szabvány billentyűzet). Ha viszont a jelszó hosszát növeljük, akkor a lehetséges kombinációszámot (KK) exponenciális függvény adja meg. Egy feltételezett, TS=1012 próba/mp találgatási sebességgel az alábbi időigények adódnak:

KH	H	SZI	
80	8	0,5	óra
100	8	3	óra
80	10	4	hónap
80	21	1020	év

1. táblázat: nyers erős törés időigénye

10 Update: New 25 GPU Monster Devours Passwords In Seconds. https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/, 2024.06.22.

11 New 25-GPU Monster Devours Strong Passwords In Minutes. https://acta.uni-obuda.hu/Keszthelyi_44.pdf, 2024.06.22.

3. Legrosszabb gyakorlatok

Gyakorlatilag mindenhol a jelszó vegyes összetételét követelik meg, mondhatni, hogy minimális hosszúság mellett, azaz a biztonság szempontjából nem állnak a helyzet magaslatán a különböző, általában nagyszámú ügyfelet kiszolgáló vállalatok.

„Az OTP Csoport Kelet-Közép-Európa meghatározó bankcsoportja. Tizenkét országban, 17 millió ügyfelet szolgálunk ki modern eszközökkel”[12]. A felhasznált eszközök lehetnek modernek, de a felhasználói jelszavakkal kapcsolatos elvárások nem teljesen szakszerűek. „Az új jelszó 6-8 karakterből állhat, és tartalmaznia kell számot, továbbá kis- és nagybetűt is. A jelszó csak számokat és betűket tartalmazhat. Ne használj egyéb írásjeleket, pl. ?, %, _, szóköz! Ne használj ékezetes betűket! Új jelszavadnak legalább 3 karakterben el kell térnie régi jelszavadtól.”[13]

Azt, hogy a jelszó nem lehet 8 karakternél hosszabb, a mai viszonyok között egyértelműen hibás szabálynak kell minősíteni. Az, hogy írásjeleket és ún. speciális karaktereket nem enged meg, indokolatlan korlátozás. Az pedig, hogy legalább 3 karakterben el kell térnie az előző jelszótól, azt az aggályt veti föl, hogy tárolják magukat a jelszavakat (is), nem csupán a jelszóból képzett ellenőrző összeget (hash, árnyékjelszó).

„Az Erste Bank Hungary 1997 óta tagja az osztrák Erste Groupnak, amely az első osztrák takarékpénztárként 1819-ben jött létre. 1997 óta a nemzetközi Erste Csoport Kelet-Európa egyik legnagyobb pénzügyi szolgáltatójává vált, mely 7 országban (Ausztria, Csehország, Szlovákia, Románia, Magyarország, Horvátország és Szerbia) közel 46 000 munkavállalójával 16,5 millió ügyfelet szolgál ki 2 900 fiókból álló hálózatában.”[14] Jelszószabályzatuk szerint „Az új jelszó 8-32 karakter hosszúságú legyen, valamint tartalmazzon kisbetűt, nagybetűt, számot és speciális karaktert is. Az alábbi speciális karakterek használata megengedett: !, %, /, =”[15]. A hosszúság, vagy legalábbis annak maximuma megnyugtató. A vegyes összetétel merev megkövetelése indokolatlan, de ehhez képest is a speciális karakterek önkényes korlátozása (a normál billentyűzetről elérhetőek közül) nem magyarázható.

Saját házam táján, az Óbudai Egyetem SAP-vel összekötött személyzeti ügyek portálján ezen szabályokat találjuk: „Új jelszó (Minimum 8 karakter, tartalmaznia kell kisbet... A jelszónak tartalmaznia kell számot! A jelszónak tartalmaznia kell nagybetűs karaktert! A jelszónak tartalmaznia kell speciális karaktert! A jelszónak

12 https://www.otpbank.hu/portal/hu/Rolunk, 2024.06.27.

13 Gyakran ismételt kérdések, Hozzáférés az internetbankhoz, Jelszó. https://www.otpbank.hu/portal/hu/OTPdirekt/Belepes, 2024.06.27.

14 Erste Bank Hungary Zrt. https://www.erstebank.hu/hu/ebh-nyito/bankunkrol/erste-bank-hungary-zrt, 2024.06.27.

15 Segítség a belépéshez, Milyen kell legyen a jelszó? https://www.erstebank.hu/hu/erstestore-help-hu/erstestore-help-default, 2024.06.27.

legalább 8 karakter hosszúnak kell lennie!”[16] A 8 karakter mint alsó méretkorlát kétszer is szerepel, viszont azt nem írja, hogy 16 karakternél nem lehet hosszabb, mert azt nem fogadja el. Ez utóbbi technikailag indokolatlan korlátozás.

Nemzetközi kitekintésben vegyük a Google-t, ami sokáig a csodált, osztályon felüli minőséget is jelentette. Bejelentkezés utáni jelszóváltoztatási kísérlet esetén[17] bőséges tájékoztatást kaphatunk a kellően biztonságos jelszó választásáról. „Legalább 8 karakterből kell állnia. Ne használjon olyan jelszót, amelyet más webhelyen is használ, és ne használjon túl nyilvánvaló szavakat, például háziállata nevét. (...) ne tartalmazzon személyes adatokat, például a születési dátumát vagy a telefonszámát. (...) Jelszava betűk, számok és szimbólumok bármilyen kombinációjából állhat (csak ASCII-karaktereket használhat). Ékezeteket és ékezetes karaktereket nem lehet használni. Nem használható olyan jelszó, amely: kifejezetten gyenge, például «jelszo123»; egyezik a fiók valamely korábbi jelszavával; szóközzel kezdődik vagy végződik.” Ezen előírásokkal teljes mértékben egyet lehet érteni. A további tanácsok azonban megkérdőjelezhetők: „Próbálja ki a következőket: dalszöveg vagy vers részlete; emlékezetes idézet filmből vagy beszédből; könyvrészlet; egy mondat, amelyet fontosnak tart”, ezen esetek ugyanis nagy valószínűséggel az adott személyhez kötődő lehetőségeket eredményeznek.

A doktori.hu nem ír ki semmilyen, jelszóval kapcsolatos elvárást. Pár évvel ezelőtti személyes élményem, hogy a jelszó módosításánál elfogadta a hosszú jelszót, viszont belépésnél csonkolt 16 karakterre, tehát nem lehetett belépni, jött az „elfelejtett jelszó” művelet.

Az Innovációs és Technológiai Minisztérium által meghirdetett OTKA pályázatok benyújtásához készült technikai útmutató[18] szerint „A jelszó legalább 7, de legfeljebb 12 karakteres legyen, tartalmaznia kell legalább 1 kisbetűt, 1 nagybetűt és két számjegyet”. A mérsékelten vegyes összetétel (nincs szó az ún. speciális karakterekről, írásjelekről) megkövetelése nem volna baj, de a 12 karakterben maximált hosszúság megint csak indokol(hat)atlan.

A Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézetének GYIK oldalán[19] található előírás szerint „A jelszónak tartalmaznia kell: legalább 10, de legfeljebb 20 karaktert; kis- és nagybetűket illetve legalább 1 számot; !, ?,

16 https://hrportal.uni-obuda.hu/#/home/security/change-password, 2024.06.27. Belépést követő jelszómódosítási kísérlet esetén olvasható az új jelszó megadására szolgáló űrlapon, a kisbetű(k)re vonatkozó előírást csak az idézett módon, csonkolva jeleníti meg az oldal.

17 https://myaccount.google.com/u/0/signinoptions/password?hl=hu&pli=1&rapt=AEjHL4OLZrbdEVL2mqV91bLKa0ikkX9M_p_gzj5hlWh-NVEinlWsWCWXict-N5CHazWce8tczNm984HCHs8y6Eb0hLEyaDXLjAi-6gYNAqEHVUpR7ykDlWJ8, 2024.06.22.

18 https://nkfih.gov.hu/download.php?docID=35394, 2024.06.27.

19 https://kti.uni-nke.hu/kozszolgalati-tovabbkepzesek/probono-rendszer-es-hasznalata/gyakori-kerdesek-tisztviseloknek, 2024.06.27.

#, $ karakterek közül 1 db-ot (speciális karakter). A jelszó nem tartalmazhat: ékezetes betűt; a fent felsorolt karaktereken kívül más speciális karaktert (pl: @, _, -); javasolt a nevek mellőzése". A hosszúságra vonatkozó elvárás elfogadható, bár érdekes kérdés lenne, hogy a 20 karakternyi felső korlátnak milyen szakmai oka lehet. Ezen túl azonban itt is a vegyes összetétel a hangsúlyos elvárás.

Alan H. Karp módszere nagyon sokáig megtalálható volt a HP valamelyik oldalán. Ez ma már nincs így, maga az eredeti cikke azonban megvan.[20] Ebben egy nagyon ötletes, kiváló módszert ismertet, ill. ennek a módszernek az általa készített segédprogramját adja közre. A módszer lényege, hogy könnyen megjegyezhető, egyszerű jelszavakból állít elő elegendően hosszú, véletlenszerűnek tűnő karaktersorozatot mint jelszót. Ennek során két bemenő adatot használ föl: az adott oldal nevét (pl. amazon.com), és egy, egyébként akár vállalhatatlanul egyszerű jelszót. A kettőt összefűzi, MD5 ellenőrző összeget készít belőle, azt base64 kódolással ASCII karakterekké alakítja, és levágja belőle a kívánt, a cikkben 12 karakternyi hosszt. Bejelentkezésnél a jelszó megadásánál a másolás-beillesztés egyszerű és gyors művelet, hasonlóképpen nem problémás a domain név és az egyszerű, rövid jelszó megadása. Egyetlen kifogás a módszer ellen a publikáció ténye, mert ha egy támadó csak megsejti, hogy a célszemély ezt az eljárást alkalmazza, akkor fogja a leggyakoribb, legtipikusabb jelszavakat, és azokat próbálgatja végig az adott oldalon az adott felhasználó nevében. A legvalószínűbb száz jelszó feltűnés nélkül kipróbálható online, véges idő alatt, és jó eséllyel még sikeres is lehet.

Az Óbudai Egyetem Jelszómódosítás oldalán[21] azt az előírást találjuk, hogy a jelszó „Minimum 8 karakter, legyen bene kis és nagybetű és szám is!" A mai világban teljesen elfogadható, normál, szokványos felhasználást feltételezve.

A példák sorában a legérdekesebb, egyben legproblémásabb a Stanford Egyetem. Az egyetemi hálózat jelszószabályzata[22] különbséget tesz a felhasználói jelszó hosszának függvényében. Ha a jelszó 8-11 karakter, kis- és nagybetűket, számjegyeket és speciális karaktereket is kell tartalmaznia. Ha 12-15 karakter, akkor legalább kis- és nagybetűk és számok kell legyenek benne. 16-19 karakternyi hossz esetén elegendőek a (kis és nagy) betűk, 20 karakter és annál hosszabb jelszó esetében nincs megkötés. Kiegészítő szabályok, hogy a jelszó nem lehet szótári alapszó, és csak az amerikai billentyűzetről közvetlenül beírható karaktereket tartalmazhat.

Az eddig felsorolt példákból ez a leginkább szakszerű.

A probléma a Tájékoztató a jelszókövetelményekről (Password requirements quick guide) c. oldalukon[23] található. Azt javasolják, hogy a kellően hosszú, de

20 Karp, Alan H. (2003). Site-Specific Passwords. Approved for External Publication. https://www.labs.hpe.com/techreports/2002/HPL-2002-39R1.pdf, 2024.06.27.

21 https://io.uni-obuda.hu/jelszomodositas-e-mail-office-365, 2024.06.27.

22 https://uit.stanford.edu/service/accounts/passwords, 2024.06.27.

23 https://uit.stanford.edu/service/accounts/passwords/quickguide, 2024.06.27.

mégis megjegyezhető jelszót úgy válasszon a jámbor felhasználó, hogy fogjon négy véletlenszerű alapszót (a konkrét példában: orange, eagle, key, shoe – narancs, sas, kulcs. cipő), fűzze össze, és van egy jól vizualizálható, elegendően hosszú, a konkrét példában 21 karakter hosszú jelszava. Ennek becsült törési ideje 1020 év, ami beláthatatlan, sőt felfoghatatlan időtartam.

A probléma azonban az, hogy ebben az esetben számolhatunk másképpen is. Figyelembe véve, hogy a tippet tartalmazó ábra 2014 áprilisi alkönyvtárból van linkelve, vélelmezhető, hogy legalább tíz éve ott virít a Stanford honlapján. Feltételezhető tehát, hogy számos felhasználó követhette ezt a javaslatot jelszava megválasztásánál. Ha a kb. 80 karakteres alaphalmazból összerakott 20+ hosszúságú jelszó teljesen reménytelen törése helyett egy – mondjuk – kétezer szavas alapszótárból választott négy szó minden lehetséges kombinációját próbáljuk végig, a fenti számításban feltételezett törési sebességet véve alapul mintegy 16 másodperc adódik. Ami hihetetlenül gyengének számít.

4. Következtetések

A jó jelszóval szemben támasztandó elsődleges követelmény a hosszúság. Kiegészítő követelmény, hogy a jelszóra vagy annak értelmes részeire a keresők (mint pl. a Google) egyetlen találatot se adjanak – ez utóbbival a fő probléma, hogy komoly tétre menő helyzetben nem lehet kipróbálni.

Általánosítható az a tapasztalat, hogy a régi szabályokat érdemes újragondolni és megvizsgálni, hogy még mindig helytállóak-e, dacára a közben eltelt időnek. Az a szabály, ami teljes mértékben helytálló volt tíz-húsz-harminc éve, nem biztos, hogy az időközben megváltozhatott körülmények között is helytálló marad.

A konkrét példa arra is rámutat, hogy az egyetemi rangsorok összeállítása is vet föl problémákat, legelsősorban is azt, hogy erősen problémásnak tűnik összetett, bonyolult jelenségeket skalárral mérni eleve problémás, és hogy a rangsor erősen függ a vizsgálati szempontrendszertől. Például a jelszóbiztonság szempontjából az Óbudai Egyetem két nagyságrenddel jobb, mind a Stanford (kb. fél óra és 16 másodperc).

5. Köszönetnyilvánítás

Köszönet illeti a Stanford Egyetemet, a hivatkozott honlapjuk nélkül ez a cikk nem készült volna el. És külön köszönettel adózom néhai kedves tanárom, Földi Tivadar emlékének, Tőle tanultam azt is, hogy a régi szabályokat időnként érdemes újragondolni.

FELHASZNÁLT IRODALOM / REFERENCES

Szücs E. (1996): Rendszer és modell. Nemzeti Tankönykiadó, Budapest

Endrei W. – Makkai L. – Nagy D. – Szücs E. (1989): Ember és technika I. Tankönyvkiadó, Budapest

Facts and Figures (2023): https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-traffic/

Keszthelyi, A. (2015): Age of Cyber Crime and Culture of Security. In: Science Journal of Business and Management. Special Issue: The Role of Knowledge and Management's Tasks in the Companies. Vol. 3, No. 1-1, 2015, pp. 39-45. doi: 10.11648/j.sjbm.s.2015030101.17

Keszthelyi, A. (2013): About Passwords. Acta Polytechnica Hungarica 10 : 6 pp. 99-118. , 20 p. (2013)

Tick, A. – Szabó-Harka, N.: Analysis of Information Security in a Corporate Environment – a Human Perspective, In: IEEE, Publ. (szerk.) IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics : SAMI 2024 : Proceedings, Danvers (MA), Amerikai Egyesült Államok : IEEE (2024) pp. 469-474. https://doi.org/10.1109/SAMI60510.2024.10432889

Tran, N. – Tick, A. (2021): Cyber-security risks assessment by external auditors, Interdisciplinary Description of Complex Systems 19 : 3 pp. 375-390. (2021), https://doi.org/10.7906/indecs.19.3.3

Sámson, N. – Tick, A. (2024): Digital Defense: Investigating Human Aspects of Cybersecurity, In: Anikó, Szakál (szerk.) SACI 2024: 18th IEEE International Symposium on Applied Computational Intelligence and Informatics: Proceedings, Timisoara, Románia : IEEE (2024) pp. 525-532.

New 25 GPU Monster Devours Passwords In Seconds (2012): https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/, 2024.06.22.

Az OTP Csoportról: https://www.otpbank.hu/portal/hu/Rolunk, 2024.06.27.

Gyakran ismételt kérdések, Hozzáférés az internetbankhoz, Jelszó: https://www.otpbank.hu/portal/hu/OTPdirekt/Belepes, 2024.06.27.

Erste Bank Hungary Zrt.: https://www.erstebank.hu/hu/ebh-nyito/bankunkrol/erste-bank-hungary-zrt, 2024.06.27.

Segítség a belépéshez, Milyen kell legyen a jelszó?: https://www.erstebank.hu/hu/erstestore-help-hu/erstestore-help-default, 2024.06.27.

https://hrportal.uni-obuda.hu/#/home/security/change-password, 2024.06.27. Belépést követő jelszómódosítási kísérlet esetén olvasható az új jelszó megadására szolgáló űrlapon, a kisbetű(k)re vonatkozó előírást csak az idézett módon, csonkolva jeleníti meg az oldal.

Jelszó: https://myaccount.google.com/u/0/signinoptions/password?hl=hu&pli=1&rapt=AEjHL4OLZrbdEVL2mqV91bLKa0ikkX9M_p_gzj5hlWh-NVEinlWsWCWXictN5CHazWce8tczNm984HCHs8y6Eb0hLEyaDXLjAi-6gYNAqEHVUpR7ykDlWJ8, 2024.06.22.

Technikai útmutató: https://nkfih.gov.hu/download.php?docID=35394, 2024.06.27.

Mire kell figyelnem az új jelszó megadásakor?: https://kti.uni-nke.hu/kozszolgalati-tovabbkepzesek/probono-rendszer-es-hasznalata/gyakori-kerdesek-tisztviseloknek, 2024.06.27.

Karp, A. H. (2003): Site-Specific Passwords. Approved for External Publication. https://www.labs.hpe.com/techreports/2002/HPL-2002-39R1.pdf, 2024.06.27.

Jelszómódosítás - E-mail, Office 365: https://io.uni-obuda.hu/jelszomodositas-e-mail-office-365, 2024.06.27.

Accounts and Passwords: https://uit.stanford.edu/service/accounts/passwords, 2024.06.27.

Password Requirements Quick Guide: https://uit.stanford.edu/service/accounts/passwords/quickguide, 2024.06.27.