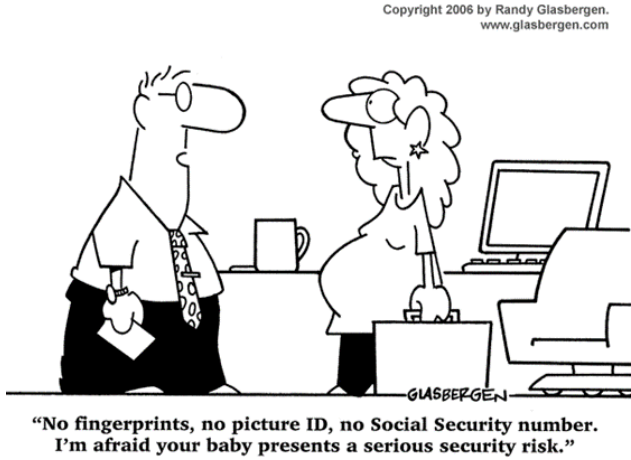
MagiCom
BUDAPEST LONDON

„Információvédelem menedzselése”
XCIV. Szakmai Fórum
Budapest, 2021. január 20.

Jelszómenedzsment kihívások egy radikálisan megváltozott környezetben avagy a COVID és a távmunka hatása a biztonságos jelszókezelésre

Dr. Tarján Gábor

Áttekintő tartalom



- Miben más ez az új világ (jelszómenedzsment szempontból)?
  - A COVID-19 hatása az információbiztonságra
  - Mi történik a jelszavakkal a home office-ban
- Egy jelszavakkal kapcsolatos felmérés eredményei
- Egy jelszómenedzsment rendszer általában (és mit várunk el tőle?)
- A jelszómenedzsmenttel kapcsolatos elvárások a szabványok világában és előírások világában
  - nemzetközi szabványokban
  - és a hazai előírásokban
- Egy jelszómenedzsment rendszer működése a gyakorlatban

A COVID-19 hatása az információbiztonságra

- „A COVID-19 a valaha volt legnagyobb kiberbiztonsági fenyegetés.”

https://www.passcamp.com/blog/password-manager-for-business-response-to-covid-19/

- „A COVID krízis alatt a jelszavak extrém módon sérülékenyekké váltak a kibertámadásokkal szemben. Egy kutatás azt mutatja, hogy a jelszavak elleni támadások masszív 667 %-kal nőttek.”

https://www.teampassword.com/blog/covid-password-management-technologies

- Az elsődleges célpont az egészségügy és a banki rendszerek.

https://www.passcamp.com/blog/covid-19-reveals-weak-areas-in-password-management-system/

Mi történik a home office-ban a jelszavakkal?

- *Employees might not change their passwords as frequently as they would in the office. Home devices might not utilize password "time out" technologies or other security features.* – Nem cserélik elég gyakran a jelszavakat!
- *Employees might use passwords that aren't strong enough. Passwords might not contain enough characters, upper and lower case letters, numbers, etc.* – Nem elég erős jelszavakat használnak!
- *Employees might use computer systems or mobile devices with security vulnerabilities or without proper protection.* – Nem védett vagy sérülékeny eszközöket használnak.
- *Managers aren't around to encourage employees to strengthen password security.* – A menedzserek nem erőltetik, hogy a munkatársak szigorúbb jelszóbiztonságot alkalmazzanak.

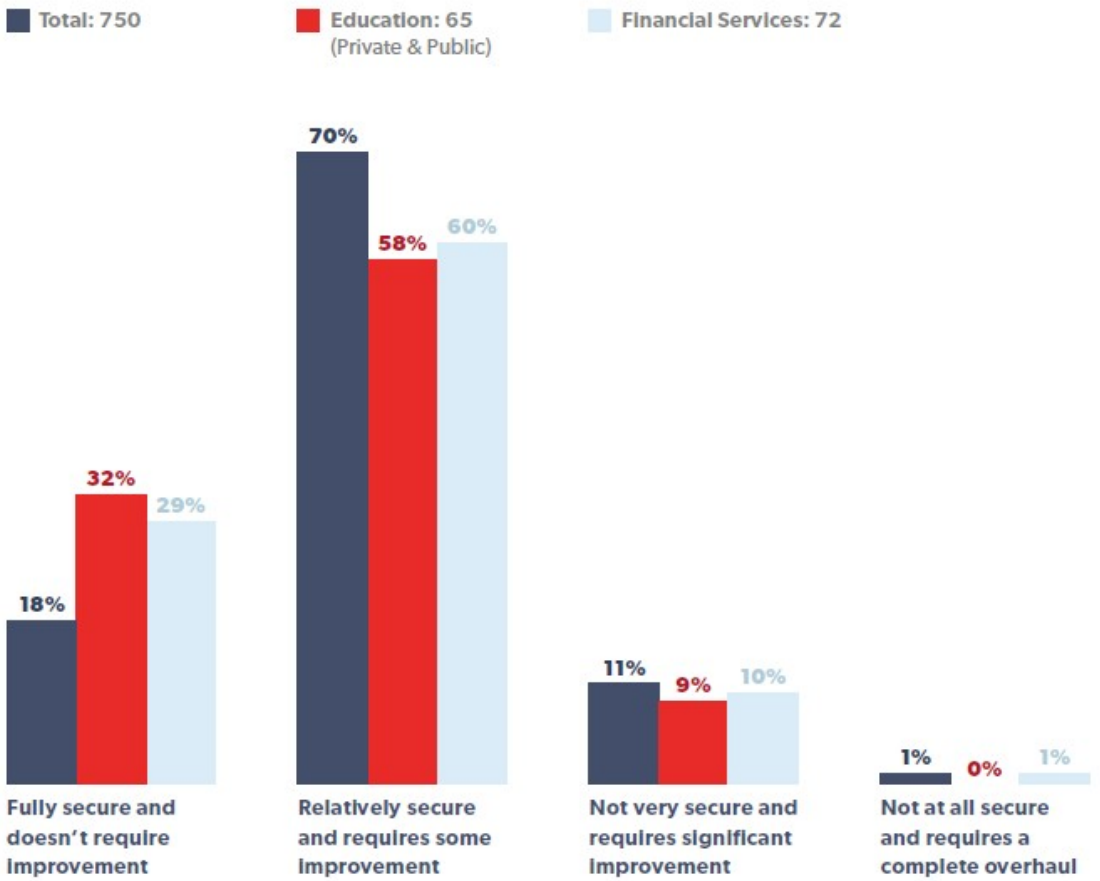
https://www.teampassword.com/blog/covid-password-management-technologies

Részletek egy felmérésből

- LogMeIn partnership / partnerség
- LastPass product and manged service provider (L1 és L2)
- 750 IT és biztonsági szakértő
- szervezetek 250 – 3,000 fő között
- UK, France, Germany, Australia, Singapore, US
- Pénzügyi szolgáltatások, IT, oktatás

https://www.lastpass.com/solutions/passwordless-access/from-passwords-to-passwordless

PERCEIVED SECURITY OF CURRENT IDENTITY AND ACCESS MANAGEMENT SOLUTION(S)



TIME SPENT MANAGING PASSWORDS EACH WEEK

3 HOURS
Singapore

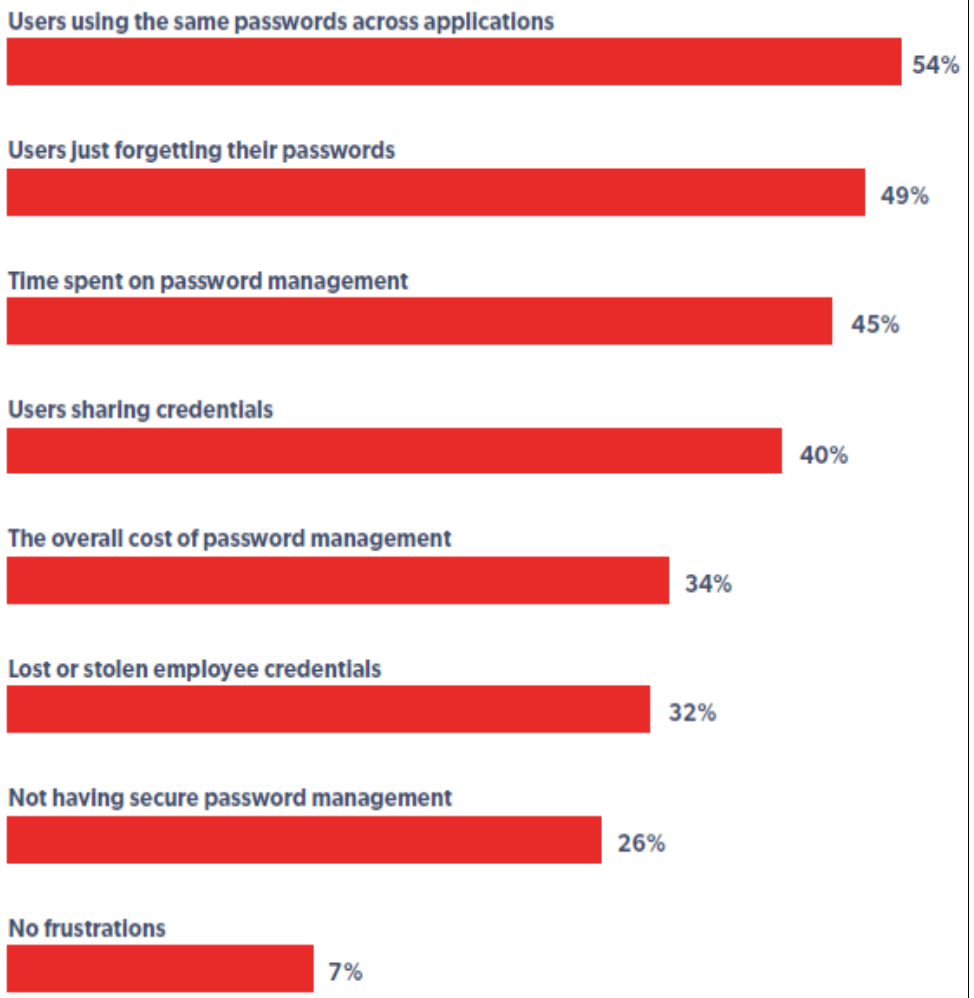
4 HOURS
United Kingdom
France
Australia

5 HOURS
Germany

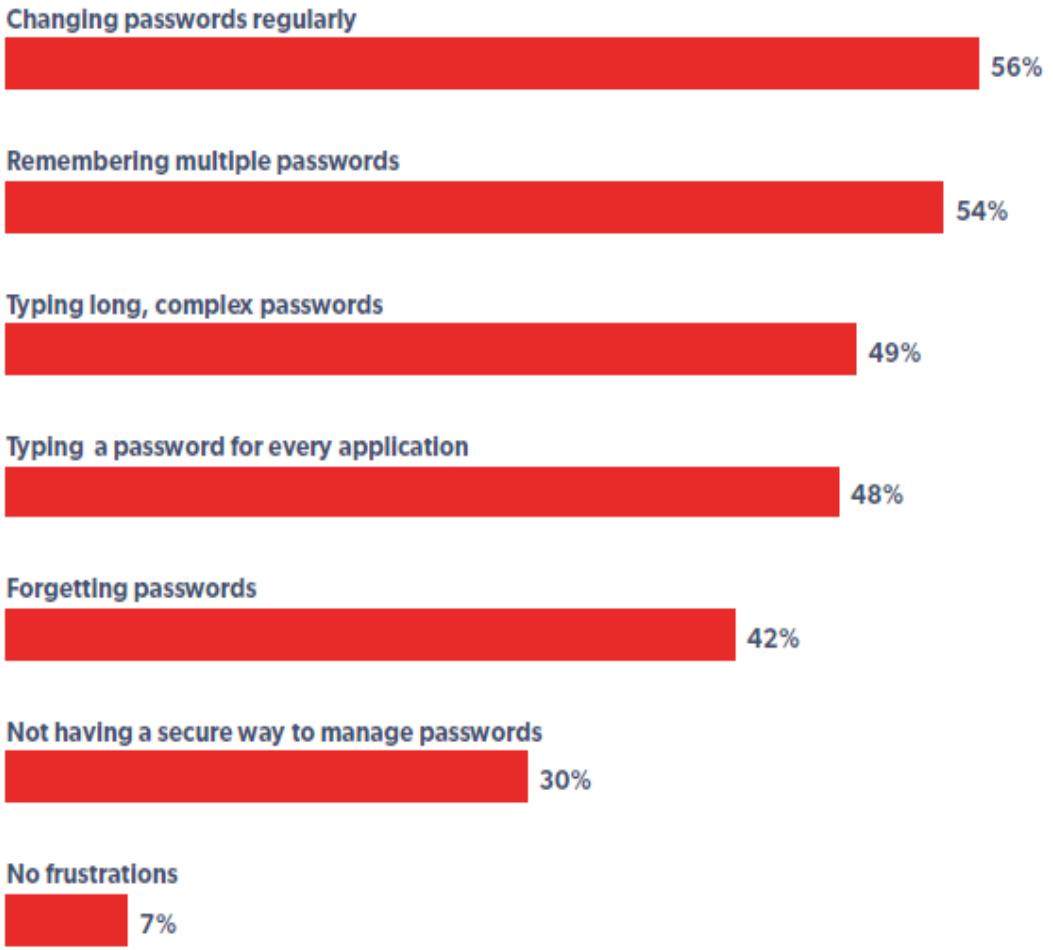
6 HOURS
United States

Weekly time spent managing users' password and log in information has increased 25% since 2019.

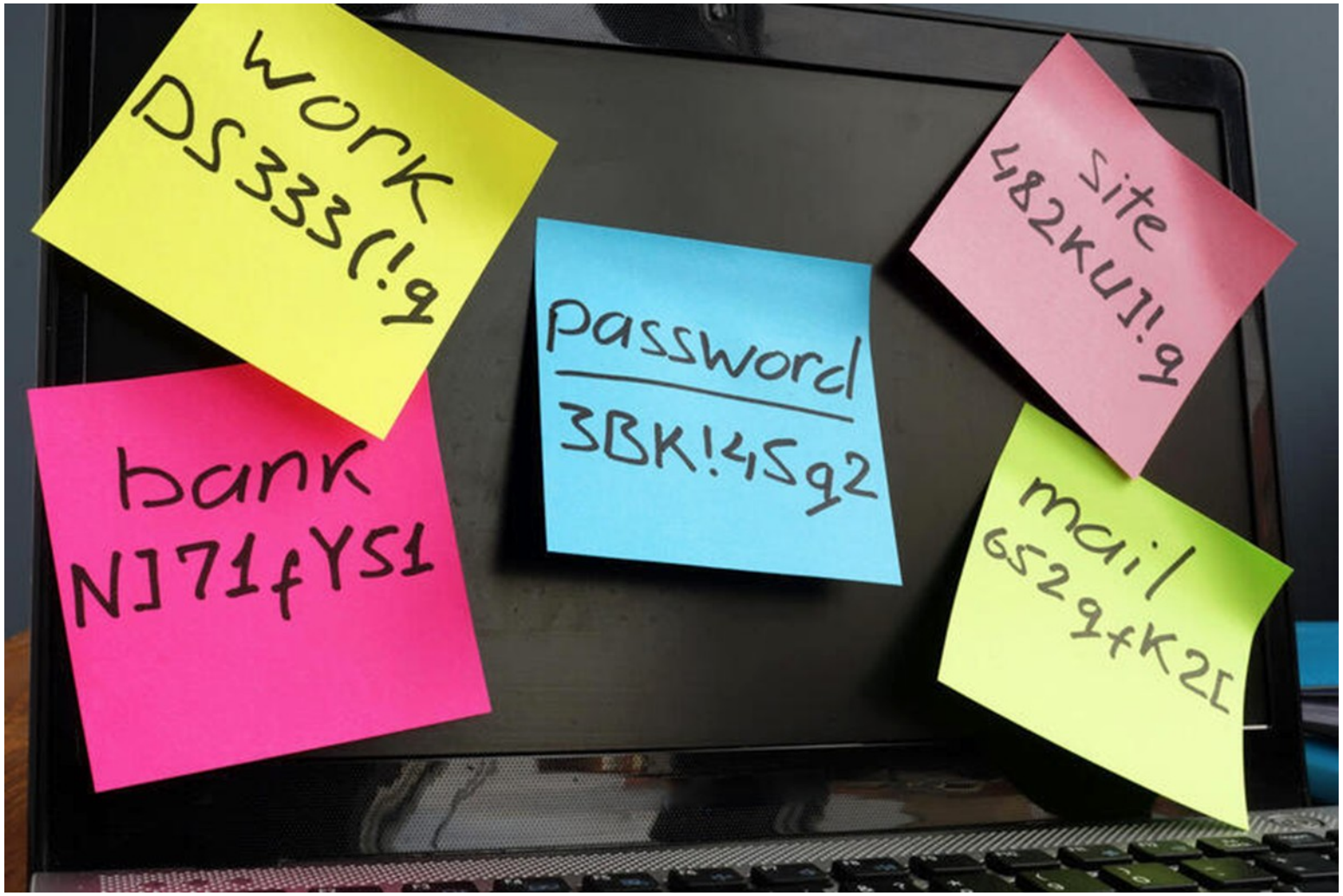
IT DEPARTMENT PASSWORD CHALLENGES



EMPLOYEE PASSWORD CHALLENGES



Mi ez?


work
DS333(!9
password
3BK!45q2
site
482KU1!9
bank
N171fY51
mail
652q+K2L

Mit várunk el általában egy jelszómenedzsment rendszertől?

- Biztonságos széf-architektúra / Secure vault architecture (End-to-End Encryption, Zero Knowledge Proof, Secure Authentication)
- Biztonságos adatmegosztás / Secure data sharing (secure password sharing, Guest feature, Multi-tier sharing)
- Időmegtakarítás / Time-saving features
- Kétfaktoros authentikáció / Two-factor Authentication – to add a second level of security to all employees' accounts.
- Mobil applikáció és böngésző kiterjesztés / Mobile App and Browser Extension – for even more efficient work of your team, no matter where they work – in an office, in a co-working space, at home, or on the beach.
- Naplózás képessége / History Log – to strengthen control of the company's data. If an employee shares or edits your password, you will get informed about it immediately.

https://www.passcamp.com/blog/password-manager-for-business-response-to-covid-19/

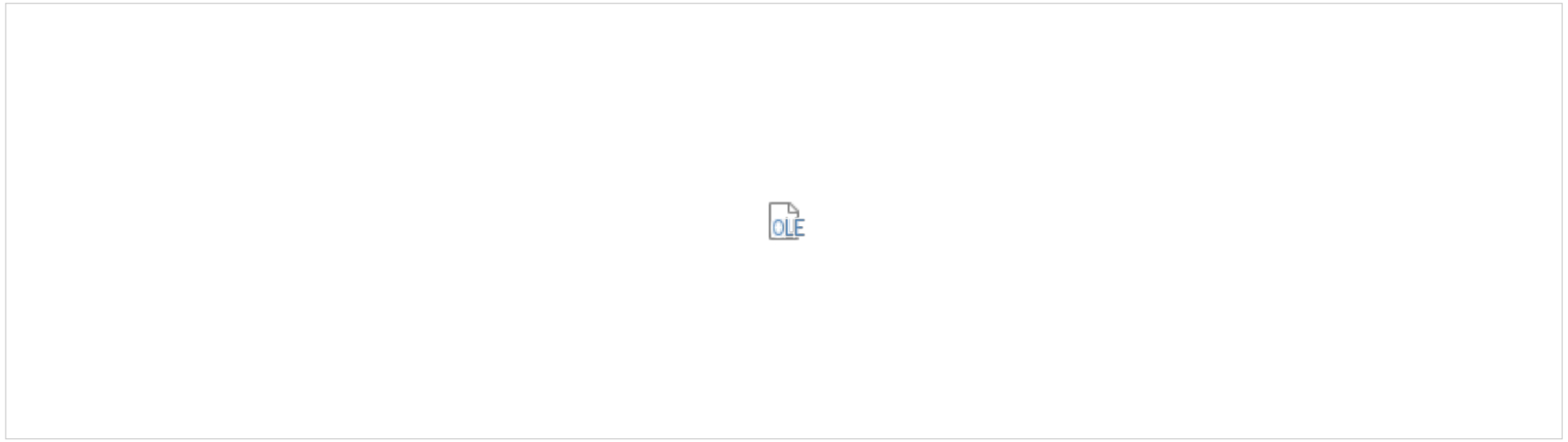
Mit mond a jó öreg ISO 27001:2013 („A” melléklet)?

A.9.4.2 *Biztonságos bejelentkezési eljárások*	Ahol azt a hozzáférés-szabályozási szabályzat megköveteli, a rendszerekhez és alkalmazásokhoz való hozzáférést egy biztonságos bejelentkezési eljárással kell szabályozni.

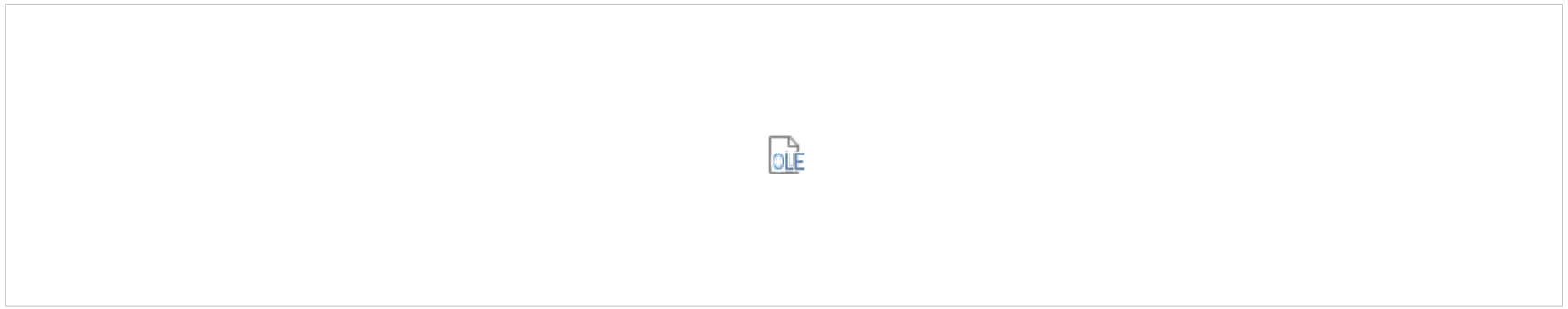
A.9.4.3 *Jelszó menedzsment rendszer*	A jelszó menedzsment rendszer legyen interaktív és biztosítson jó minőségű jelszavakat.

Mit mond a TISAX (v 5.0.2)?

2.1.4 Control question, requirements (must), requirements (should)



4.1.2 Control question, requirements (must), requirements (should)



Mit mond a jelszavakról az MNB 12/2020. (XI.6.) számú távmunka ajánlása?

20. a) a távoli hozzáféréshez használt eszközöket a távoli felhasználó ne hagyja őrizetlenül, rövidebb távollét esetén is zárja le a képernyőt vagy kapcsolja be a jelszóval ellátott képernyővédőt;

20. d) a távmunka során a távoli felhasználó saját otthoni WiFi hálózatának biztonságosabbá tételére (WiFi router alapértelmezett adminisztrátori jelszavának megváltoztatása és a tűzfal biztonságos beállítása, WiFi hálózathoz való csatlakozás csak jelszóval történhessen megfelelő titkosítás mellett, WEP és WPS tiltás stb.);

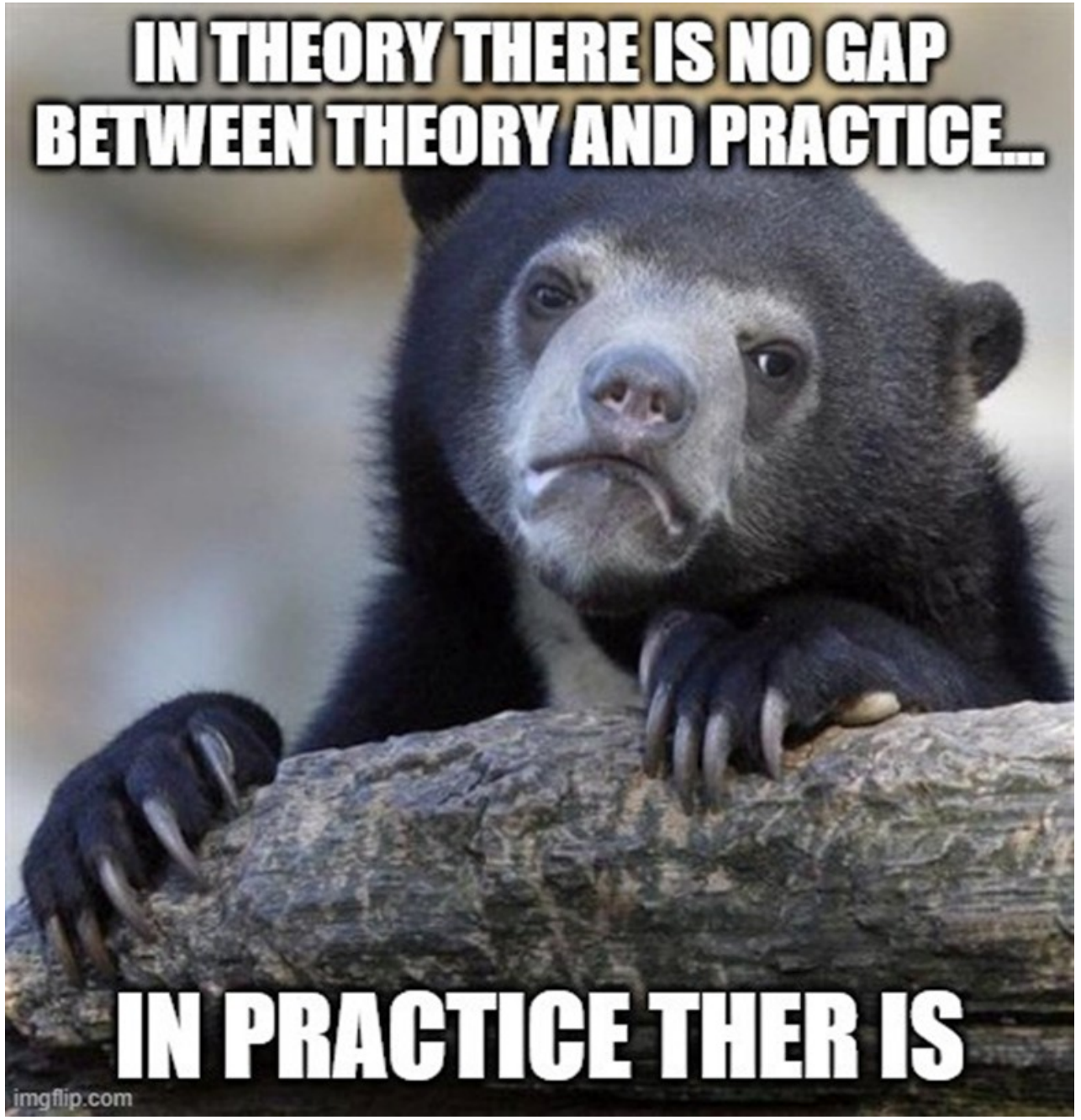
26. Az MNB a távoli hozzáférés során az intézmény részéről elvárja:
f) azt, hogy a távmunkához használt jelszavak erőssége és összetettsége érje el vagy haladja meg az intézmény belső hálózatához való hozzáférésre vonatkozó követelményeket;

20. i) az intézmény hálózatához és az alkalmazásaihoz szükséges jelszavakat a távoli felhasználó ne használja a magánügyek intézésénél;

12.f) az okoseszközökön tárolt adatok megfelelő titkosítással, azonosítási móddal, jelszavakkal történő védelmét;

Egy lehetséges megoldás – LastPass Enterprise

- 81 %, 191 (250), 2005, 27001…
- Központi adminisztráció / Central admin control (dashboard!)
- Felhasználói könyvtárak integrációja / User directory integration (automate onboarding and offboarding, group management
- Biztonságos és kényelmes jelszómegosztás / Secure and convenient password sharing (collaborative teams)
- Részletes biztonsági jelentés / Detailed security reports (compliance – audit)
- Több mint 100 féle szabály beállításának lehetősége / 100+ security policies (enforce best practices)
- Általános hozzáférés / Universal access (office, home, on the road)
- Egyszeri bejelentkezés / Single Sign-On (user experience!)
- Kétfaktoros authentikáció / Two factor authentication


IN THEORY THERE IS NO GAP
BETWEEN THEORY AND PRACTICE...
IN PRACTICE THER IS
imgflip.com

MagiCom
BUDAPEST LONDON

Köszönjük a figyelmet!

Ha érdeklik a részletek, lépjen kapcsolatba velünk!

www.magicom.hu

Dr. Tarján Gábor

+36-20-5027775

gabor.tarjan@magicom.com