



Felhasználói informatikai biztonsági tudatosság oktatás

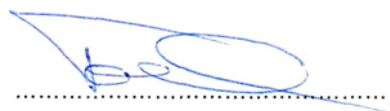
BEVEZETÉS AZ IT BIZTONSÁGBA (2. RÉSZ)

IT Biztonság tudatosság II.

Magyar nyelvű felhasználók részére

IT security awareness II.

Angol nyelvű felhasználók részére



Készítette: Tóth Attila
Debreceni Egyetem
Információbiztonsági felelős

Kelt: D e b r e c e n, 2025. Február 03.

Tartalom

I. Ok.....	3
II. Cél.....	5
III. Módszer.....	5
IV. Eszköz	6
V. Eredmény.....	6
VI. Értékelés.....	9

I. Ok

Releváns kivonat, a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról, 7_2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről, végrehajtási rendeletből.

3.2. Biztonságtudatossági képzés

3.2. A szervezet:

3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is):

3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal.

3.2.1.2. Amennyiben az EIR-ben bekövetkezett változások ezt indokoltá teszik, vagy a szervezet által meghatározott események ezt megkövetelik.

3.2.2. Meghatározza azokat a technikákat, melyeket a rendszer felhasználók biztonságtudatosságának növelése érdekében alkalmaz.

3.2.3. Frissíti a képzési és tudatossági tananyagot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe

3.3. Biztonságtudatossági képzés – Gyakorlati feladatok

3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.

3.4. Biztonságtudatossági képzés – Belső fenyegetés

3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.

3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés

3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére.

3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés

3.6. A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére

3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések

3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.

3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet

3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről és

3.8.2. alkalmazza az aktuális kiberbiztonsági fenyegetési információkat a rendszerüzemeltetésben.

3.9. Szerepkör alapú biztonsági képzés

3.9. A szervezet:

3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak:

3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel.

3.9.1.2. Amikor az EIR-ben bekövetkezett változás azt szükségessé teszi.

3.9.2. Frissíti a szerepkör alapú képzés tartalmát a szervezet által meghatározott rendszerességgel és a szervezet által meghatározott események bekövetkezését követően.

3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepkör alapú biztonsági képzésekbe

3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések

3.10. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.

3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések

3.11. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.

3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok

3.12. A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.

3.13. A biztonsági képzésre vonatkozó dokumentációk

3.13. A szervezet:

3.13.1. Dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket, ideértve az általános információbiztonsági tudatossági képzéseket és a speciális szerepkör alapú információbiztonsági

képzéseket.

3.13.2. Meghatározott ideig megőrzi a képzésről készült dokumentumokat.

3.14. Képzés eredményeiről való visszajelzés

3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.

II. Cél

A Debreceni Egyetem munkatársainak informatikai tudatossági szintjének emelése, fenntartása, időszerű hacker támadási trendek és azok elhárítását célzó információk átadása.

III. Módszer

Az oktatási folyamat leírása.

1. Vizuális felületek
2. "Képernyő quiz"
3. Teszt

1. Vizuális felületek

1. LECKE - TISZTA ASZTAL SZABÁLY
2. LECKE - JELSZÓ BIZTONSÁG
3. LECKE - BIZTONSÁGOS INTERNET HASZNÁLAT
3. LECKE - BIZTONSÁGOS INTERNET HASZNÁLAT / TIPPEK
Nagyon figyelj és tudatosan dönts, amikor linker kattintasz!
Legyél válogatós a letöltésekkel!
Letöltés, csak megbízható forrásokból
Mindig ellenőrizd a felkeresett webhely nevét (URL-jét)
Ne nyiss meg semmit, amiben nem bízol teljesen!
Nézd meg a fájlkiterjesztést!
Ne add meg mindenhol az e-mail címed!
Legyél óvatos, nyilvános számítógépek használatakor!
Lehetőség szerint, titkos webhelyeket használj!
Ellenőrizd, hogy biztonságos-e az internet kapcsolatod!
Vidd az egered a weblap linkje fölé!
4. LECKE - MOBIL ESZKÖZÖK VÉDELME
TARTSD A SZOFTVEREID FRISSEN
TÖRÖLD AZOKAT AZ ALKALMAZÁSOKAT, AMELYEKRE NINCS SZÜKSÉGED
KEZELD BIZTONSÁGOSAN KÉSZÜLÉKEID

AKTIVÁLD A NYOMKÖVETÉST
ENGEDÉLYEZD AZ AUTOMATIKUS KÉPERNYŐZÁRÁST
GYEREKEKNEK NE ENGEDD, HOGY HASZNÁLJÁK MOBIL
KÉSZÜLÉKED

5. LECKE - A KÖZÖSSÉGI OLDALAK BIZTONSÁGOS HASZNÁLATA
SPAM

SEO Támadások

Híresség, barát személyazonosság lopás

Phishing/Adathalászat

Alkalmazások és widgetek

4. LECKE - A KÖZÖSSÉGI OLDALAK BIZTONSÁGOS HASZNÁLATA / TIPPEK

Kétszer gondolt át, mielőtt megosztasz valamint. Az internet nem felejt.

Ne ossz meg kényes információkat!

Tudd, mit kell tenned, ha zaklatás él!

Legyél óvatos, amikor a munkádról vagy munkáltatódról beszélsz!

Kerüld a jelszavak újra felhasználását!

Figyeld, a kapcsolataid számát!

Használj különböző profilképeket a közösségi média fiókjaidban!

Használd az adatvédelmi és biztonsági beállításokat.

6. LECKE - BIZTONSÁGI INCIDENS

Ne várj - azonnal jelentsd az esetet!

Tudod, hihez fordulj?

Ne próbáld meg, egyedül megoldani a problémát!

Ne vonj be senki!

2. Képernyő quiz

Oktatási téma visszaellenőrzés már a tananyag megtekintése során is történik, látványos megoldások alkalmazásával. A quizre kötelező választ adni, a továbblépés aktiváláshoz. A jó és hibás választások szövegkibontó magyarázata megjelenik a tanuló számára.

3. Teszt

Random feltett 5 kérdésre, 3 helyes válasz, az elfogadott teljesítés.

IV. Eszköz

A Debreceni Egyetem Moodle alapú eLearning oktató rendszere.

V. Eredmény

A „Bevezetés az IT biztonságba II.” oktató kampány eredményének kiértékelése.

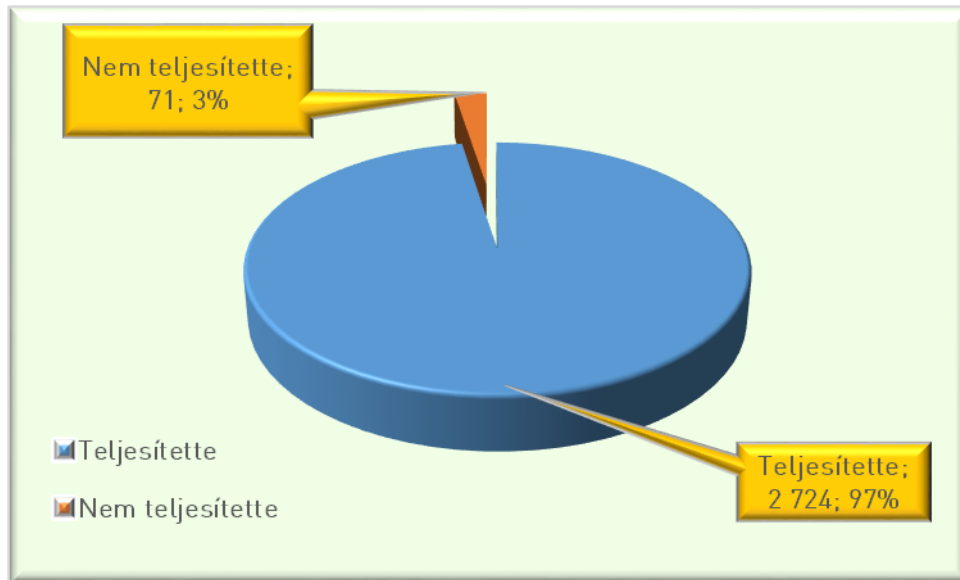
Összesítő statisztikai jelentés

Tananyag neve	Teljesítés csoportok	Elindította a tananyagot	Teljesítette	Százalék	Nem teljesítette	Százalék
Informatikai biztonsági tudatosság II.	Informatikai biztonsági tudatosság II.	2 795	2 754	98,53%	41	1,47%
	Tudásellenőrző teszt - Informatikai biztonsági tudatosság II.	2 795	2 724	97,46%	71	2,54%
	Tanúsítvány - Informatikai biztonsági tudatosság II.	2 795	2 446	87,51%	349	12,49%
IT security awareness II. (Angol nyelvű)	Informatikai biztonsági tudatosság II.	123	94	76,42%	29	23,58%
	Tudásellenőrző teszt - Informatikai biztonsági tudatosság II.	123	78	63,41%	45	36,59%
	Tanúsítvány - Informatikai biztonsági tudatosság II.	123	11	8,94%	112	91,06%

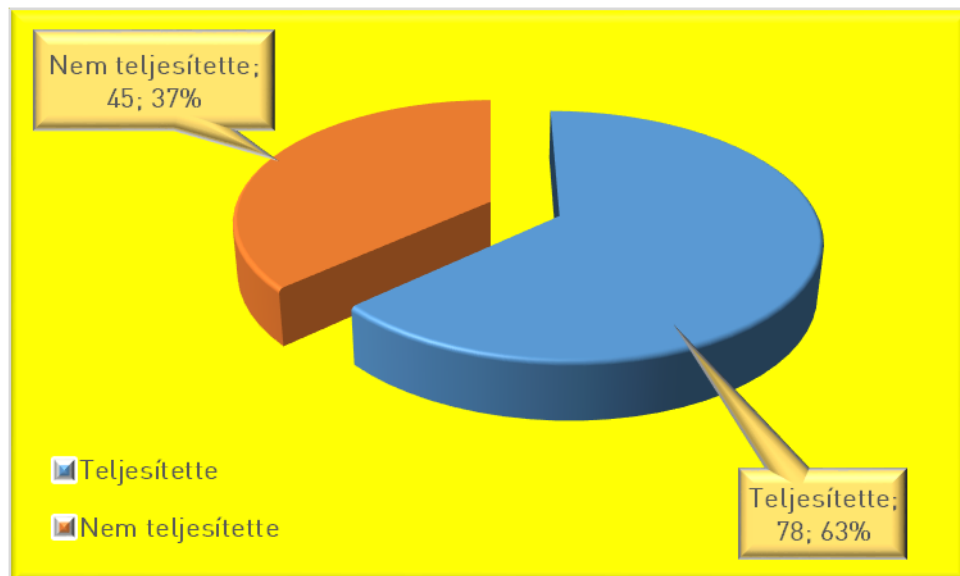
Tananyag neve	Összes megnyitás	Teljesített	Százalék
Informatikai biztonsági tudatosság II.	2 795	2 724	97,46%
IT security awareness II. (Angol nyelvű)	123	78	63,41%

Teszt teljesítése (5/3) mutatói

Magyar nyelvű tananyag



Angol nyelvű tananyag



VI. Értékelés

A „Bevezetés az IT biztonságba II.” oktatási kampány részben érte el a célját, mivel a Debreceni Egyetem dolgozóinak információbiztonsági tudatosság viselkedését pozitív irányba befolyásolni kívánó oktatása, az Egyetemi dolgozók egésze vonatkozásában, a kiírt határidőig, melynek dátuma, 2025. Január 31., kb. az összes munkavállalói létszám, egyharmada teljesítette.

Levont következtetésünk, hogy a munkavállalók többszöri felszólításra történő tananyag megtekintése, befolyásoló tényező lehet a kibertérből érkező napi támadások kezelésének hatékony megoldásában.

A tananyag teszt teljesítésének mutatói (97% igen, 3% nem) pozitívnak értékelhető, mivel kedvező azoknak a száma, akiket újra értesíteni szükséges a tananyag sikeres elvégzése érdekében.

A tananyag utógondozása folyamatos, és része a 2025. évi oktatási tervnek is. Teljesítésére, ismétlődő felkéréseket küldünk azon felhasználók részére, akik még nem nyitották meg a tananyagot. Statisztikai lekérdezéseinket ciklikusan, havonta ismétljük meg.

Tudatos információbiztonságot sértő támadás megelőzése és kivédése nem történhet ösztönös viselkedés által, mivel a napjainkban összetett, kifinomult és mesterséges intelligenciával támogatott fejlett kiberbűnözés egy lépéssel előtte halad a védelemnek.

Egy IT bölcselet szerint az informatikai problémák legnagyobb része a billentyűzet és a szék között van.

Az informatikai védelem leggyengébb láncszeme, „AZ EMBER”

- Szakképzetlenség
- Szakszerűtlen üzemeltetés
- Szakszerűtlen karbantartás
- Szándékos károkozás (bosszúállás)
- Eltulajdonítás
- Megvesztegetés
- Szabálytalan kezelés
- Figyelmetlenség, nem odafigyelés
- Hozzáférési előírások tudatos megsértése
- Jóhiszeműség

Ezek kezelése csak biztonság tudatos-, pozitív hozzáállással történhet eredményesen.

A biztonsági tudatosság, az Egyetem kultúrájának része.

Olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségéből elismerik a biztonsági intézkedések jogosságát, betartják-, betartatják és másokkal is megismertetik azokat.

Összegzés: A cél, a nem biztonság tudatos viselkedések minimalizása, hogy kiberbűnözők csaló módszerekkel megszerzett adatok birtokában semmilyen módon ne tudjanak az egyetemi infrastruktúrához, információs rendszereihez hozzáférni. A biztonság tudatosság erősítése, célzott és általános biztonság tudatossági oktatások biztosítása folyamatos tevékenység kell, hogy legyen, amit az Informatikai Biztonsági Központ biztosítani fog.