Felhasználói informatikai biztonsági tudatosság oktatás

SOCIAL ENGINEERING

(Pszichológia manipuláció)

Készítette: Tóth Attila
Debreceni Egyetem
Információbiztonsági felelős

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

Tartalom

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 indokolttá 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 szerepköralapú 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 szerepköralapú 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**
   A modul célja
   A modul eredménye
   Mi is az a Social engineering
   Meggyőzési alapelvek
   Támadási technikák
   Technikai alapú social engineering 1.
   Adathalászat típusai
   Technikai alapú social engineering 2.
   Humán alapú social engineering 1.
   Humán alapú social engineering 2.
   Humán alapú social engineering 3.
   Humán alapú social engineering 4.
   Humán alapú social engineering 5.
   Gyakoroljunk!
   Veszélyek bemutatása
   Smishing (SMS adathalászat) 1.
   Smishing (SMS adathalászat) 2.
   Közösségi oldalak
   Személyiség felvétel
   Adathalászat példa
   Hogyan védd meg magad a pszichológiai manipulátoroktól?
   Összefoglalás

2. Képernyő quiz
   Oktatási téma visszaellenőrzés már a tananyag megtekintése során is történik, látványos megoldások alkalmazásával. A quizre kötelező választ adni, a továbblépés aktiváláshoz.

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

IV. Eszköz

A Debreceni Egyetem Moodle alapú eLearning oktató rendszere.

V. Eredmény

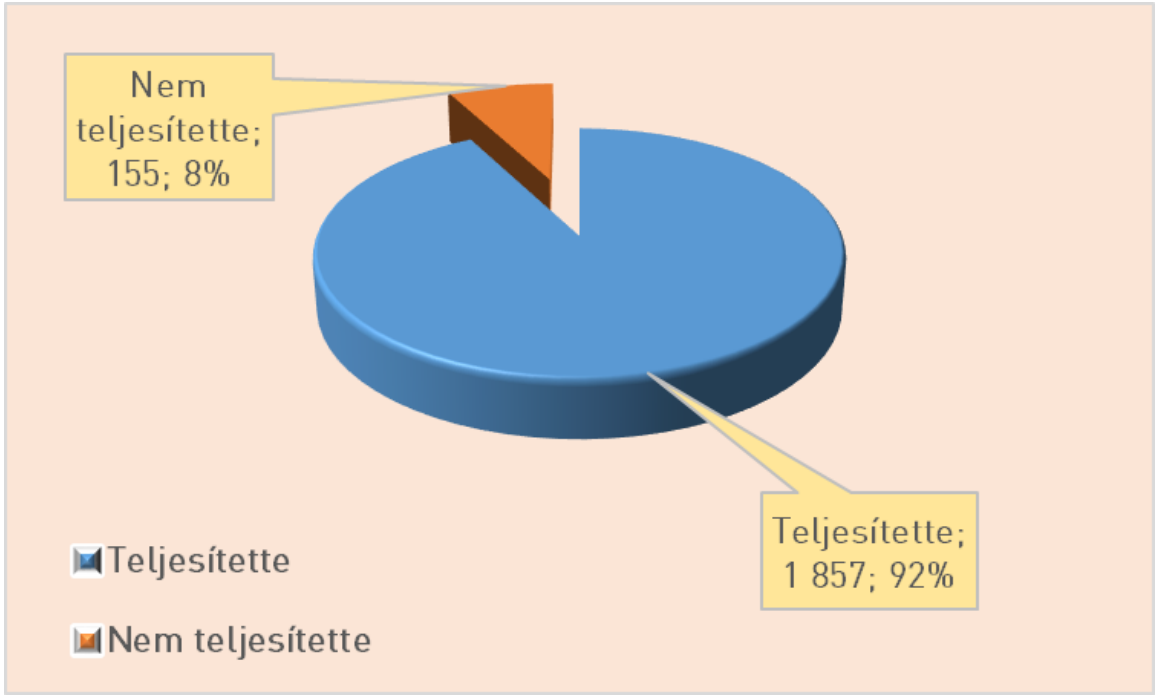
A „Bevezetés az IT biztonságba I." oktató kampány eredményének kiértékelése.

Összesítő statisztikai jelentés

Tananyag neve	Teljesítés csoportok	Elindította a tananyagot	Teljesítette	Százalék	Nem teljesítette	Százalék
Social engineering	Social engineering – oktatási anyag	2 012	1 857	92,30%	155	7,70%
	Tanúsítvány - Social engineering	2 012	1 595	79,27%	417	20,73%

Tananyag neve	Összes megnyitás	Teljesített	Százalék
Social engineering	2 012	1 595	79,27%

Teszt teljesítése (5/3) mutatói



VI. Értékelés

A „Social Engineering" oktatási kampány, minimális célt ért el, mivel a Debreceni Egyetem dolgozóinak információbiztonsági tudatosság viselkedését pozitiv irányba befolyásolni kívánó oktatása, az Egyetemi dolgozók egésze vonatkozásában, a kiírt határidőig, melynek dátuma, 2025. Január 31., kb. az összes munkavállalói létszám, egyötöde teljesítette.
Levont következtetésünk, hogy a munkaválalók többszöri felszólításra történő tananyag megtekintése, befolyásoló tényező lehet a kibertérből érkező napi támadások kezelésének hatékony megoldásában.
A tananyag teszt teljesítésének mutatói (92% igen, 8% 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 ismételjük meg.

Tudatos információbiztonságot sértő támadás megelőzése és kivédése nem történhet ösztönös viselkedés által, mivel a napjainkban összetett, kifinomult és mesterséges inteligenciával 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 biztonságtudatos-, pozitív hozzáálással történhet eredményesen.

A biztonsági tudatosság, az Egyetem kultúrájának része.
Olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják-, betartatják és másokkal is megismertetik azokat.

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