Interreg AUSTRIA–HUNGARY

Co-funded by the European Union

DigiUp NEXT
A COMPETENT BORDER REGION

PÁLYAORIENTÁCIÓS KONCEPCIÓ

KIBERBIZTONSÁGI SZAKÉRTŐ

Készült a DigiUp NEXT projekt keretében (2.3- tevékenység)

2026. március

A projekt az INTERREG VI-A Ausztria-Magyarország 2021-2027 program keretében valósul meg.

INHALTSVERZEICHNIS

BEVEZETÉS

A digitális átalakulás a gazdaság és az élet minden területét megváltoztatja, és a munka világának mélyreható átalakulásához vezet. A hagyományos szakmák folyamatosan átalakulnak vagy teljesen eltűnnek, miközben új munkaterületek – különösen az informatika területén – rendkívül gyorsan felértékelődnek. Ausztriában ma már szinte minden ágazat – az ipartól és közigazgatástól kezdve a kereskedelmen át egészen az egészségügyig – digitális infrastruktúrákra, automatizált folyamatokra és biztonságos informatikai rendszerekre támaszkodik.

Különösen dinamikusan fejlődő terület a **kiberbiztonság**. A vállalatok, hatóságok, iskolák és egészségügyi intézmények egyre intenzívebb digitalizációja miatt folyamatosan növekszik a digitális támadási felületek száma. Ezzel párhuzamosan Ausztriában is egyre több a kibertámadás. Az IT-biztonság területén dolgozó szakemberek ezért a **legfontosabb jövőbeli szakmák** közé tartoznak, és egyben **az informatikai ágazat legjobban fizetett és legsokoldalúbb karrierlehetőségeit kínálják**. A fiatalok körében végzett felmérések azt is mutatják, hogy a **pénzügyi biztonság és a vonzó fizetés** fontos szerepet játszik a pályaválasztás során.

A 13 és 16 év közötti fiatalok számára ezek a változások új perspektívákat nyitnak meg. Sokan már most érdeklődnek olyan digitális témák iránt, mint a programozás, a számítógépes biztonság, a gaming vagy a mesterséges intelligencia, ugyanakkor gyakran nem tudják, milyen szakmai lehetőségek kapcsolódnak ezekhez a területekhez, illetve hogyan néznek ki ezek a munkák a mindennapi gyakorlatban.

A **DigiUp Next projekt**, amely az **INTERREG VI-A Ausztria–Magyarország** együttműködési program keretében valósul meg, ezért azt a célt tűzte ki maga elé, hogy erősítse ennek a korosztálynak a digitális készségeit, valamint növelje az IT-szakmák vonzerejét. Ennek alapját egy empirikus kutatás képezi, amelyben mindkét országból összesen 1.200 tanuló vett részt. A felmérés feltárta, hogy a fiatalok milyen attitűdökkel rendelkeznek az IT-szakmákkal kapcsolatban, hogyan értékelik saját digitális kompetenciáikat, mekkora a továbbképzés iránti nyitottságuk, valamint milyen információforrásokat használnak a pályaorientáció során.

Az eredmények egyértelműen rámutatnak arra, hogy a digitális eszközök – különösen az okostelefon – központi szerepet töltenek be a fiatalok mindennapi életében. Emellett országspecifikus különbség is megfigyelhető volt: míg Magyarországon a fiatalok a digitális technológiákat inkább tanulási és iskolai folyamatok során használják, addig az osztrák fiatalok gyakrabban alkalmazzák a digitális eszközöket szabadidős és játékcélokra. Ugyanakkor továbbra is alacsony azoknak a fiataloknak az aránya, akik már dolgoznak olyan fejlettebb alkalmazásokkal, mint a robotika, a 3D-nyomtatás vagy a programozás. Ez egyértelmű fejlesztési igényre utal a digitális kompetenciák területén.

Éppen ebben az összefüggésben válik egyre fontosabbá a korszerű pályaorientációs intézkedések kidolgozása. A digitális átalakulás ugyanis ahhoz vezet, hogy a munkáról alkotott hagyományos elképzeléseket egyre inkább kiegészítik a hálózatba kapcsolt rendszerek, az algoritmusok, a felhőalapú megoldások és az adatvezérelt döntéshozatal. A fiatalok számára ez hozzáférést jelent a modern tanulási és munkakörnyezetekhez, a nemzetközi karrierlehetőségekhez, valamint ahhoz a lehetőséghez, hogy aktívan részt vegyenek az innováció alakításában.

Az IT-ágazat emellett különösen dinamikusan fejlődik: a programozási nyelvek, a biztonsági követelmények, az eszközök és az olyan technológiák, mint a mesterséges intelligencia, rendkívül gyors innovációs ciklusokban változnak. A fiataloknak ezért olyan pályaorientációra van szükségük, amely nemcsak technikai alapismereteket közvetít, hanem fejleszti a **problémamegoldó képesség**et, az **alkalmazkodókészség**et és az **egész életen át tartó tanulás** iránti nyitottságot is.

Jelen dokumentum keretében ezért 13–16 éves fiatalok számára készülnek IT-pályaorientációs tartalmak. Ennek részeként gyakorlatközpontú tananyagok és módszertanilag korszerű workshopkoncepciók jönnek létre, amelyek valósághű betekintést nyújtanak különböző IT-szakmákba – különösen a **kiberbiztonság** területére. A tartalmak a projekt korábbi tevékenységeire épülnek, többek között egy Serious Game eszközre, a fiatalok tudásszintjének és érdeklődésének elemzésére, valamint az osztrák–magyar határtérség vállalkozásainak kompetenciaigényét vizsgáló kutatásra.

Tanulási célok

A fiatalok …

- megértik, mit jelent a kiberbiztonság, és miért fontos.
- megismerik a kiberbiztonsági szakemberek tipikus feladatait.
- képesek felismerni az alapvető biztonsági kockázatokat (jelszavak, adathalászat/phishing, social engineering).
- egyszerű, játékos biztonsági elemzéseket végeznek.
- felismerik, hogy milyen erősségek és érdeklődési területek illenek ehhez a szakmához.

A SZAKMA – „KIBERBIZTONSÁGI SZAKEMBER“

Forrás: https://www.bic.at/berufsinformation.php?beruf=cyber-security-professional_m-w-d

A cyber security, vagyis kiberbiztonság a számítógépes rendszerek és hálózatok, adatbázisok, szerverrendszerek és más IT-infrastruktúrák védelmét jelenti a hardverek, szoftverek vagy elektronikus adatok ellopása, károsítása, illetve a rendszerek működésének megszakítása vagy eltérítése ellen. Célja a kibertámadások kockázatának csökkentése, valamint a rendszerek, hálózatok és adatok jogosulatlan felhasználásának megakadályozása.

A kiberbiztonsági szakemberek (nő/férfi/egyéb) olyan specializált informatikusok és IT-szakértők, akik vállalatok és szervezetek szervereinek, számítógépes hálózatainak, adatbázisainak és egyéb rendszereinek – különösen azok kiberbiztonságának – védelméért felelnek. Ügyfeleik közé például bankok és biztosítótársaságok, közintézmények, valamint minden olyan ágazat vállalkozásai tartoznak, amelyek nagy mennyiségű vagy érzékeny adatot kezelő IT-rendszereket működtetnek.

Az ebben a szakmában dolgozó szakemberek felelősek az IT-infrastruktúra biztonságáért, biztonsági szoftvereket és rendszereket vezetnek be és tartanak karban, valamint folyamatosan felügyelik és frissítik azok működését (például tűzfalak, vírusirtó programok, spam-szűrők). Azonosítják és kijavítják a biztonsági gyengeségeket, például adathalászati és hacker támadások szimulálásával. Emellett tanácsot adnak ügyfeleiknek az internetes bűnözéssel, online csalásokkal és kibertámadásokkal kapcsolatban, valamint arról, hogyan védhetők meg a vállalati számítógépes rendszerek és IT-infrastruktúrák ezekkel szemben.

A kiberbiztonsági szakemberek csapatban dolgoznak más IT-területek szakértőivel, például adatbázis-adminisztrátorokkal, hálózati rendszergazdákkal, webmesterekkel és felhőarchitektúrával foglalkozó szakemberekkel, továbbá kapcsolatot tartanak a vállalat különböző részlegeinek munkatársaival és vezetőivel.

Foglalkoztatási lehetőségek

- IT-vállalatok és üzleti tanácsadó cégek, adatközpontok
- Bankok és biztosítótársaságok

- Minden gazdasági ágazat vállalatai
- Olyan vállalatok és szervezetek, amelyek személyes adatokat kezelnek
- Szövetségek, szervezetek, érdekképviseletek
- Reklám és public relations területe
- Minisztériumok, hatóságok, közigazgatási intézmények

Képzési és képesítési utak (Ausztria)

A **kiberbiztonsági szakértő nem önálló szakma** vagy tanulószerződéses képzés, hanem **az informatika egyik specializációs és tevékenységi területe**. A belépés általában stabil IT-alapképzésen keresztül történik, amelyet később gyakorlati tapasztalatokkal és célzott biztonsági képzésekkel egészítenek ki.

Szakmai belépés szakmai képzésen keresztül

A kiberbiztonsághoz kapcsolódó tevékenységekbe való gyakorlatorientált belépés az alábbi **IT-szakmák**on keresztül lehetséges

- **Alkalmazásfejlesztés – Coding (szakmai képzés)**
  → Fő hangsúly: szoftrverfejlesztés, logikus gondolkodás, biztonságos programozás, hibakeresés
- **Információtechnológia – Rendszertechnika (szakmai képzés)**
- **Információtechnológia – Üzemeltetéstechnika (szakmai képzés)**

Ezek a képzések a kiberbiztonsághoz szükséges alapvető ismereteket nyújtják, többek között:

- hálózatok és szerverek
- operációs rendszerek
- IT-infrastruktúra
- alapvető IT-biztonsági intézkedések
- hibaelemzés és rendszerfelügyelet

Ezek **szilárd alap**ot biztosítanak a későbbi munkakörökhöz, például:

- IT-rendszeradminisztrátor biztonsági fókuszterülettel
- junior biztonsági elemző
- SOC-munkatárs (Security Operations Center)

Iskolai képzési utak

Alternatívaként vagy kiegészítésként iskolai IT-képzések is elérhetők:

- **Szakiskolák / középfokú szakképző intézmények (BMS / IT-szakiskolák)**

→ Alapismeretek informatika, hálózatok, adatbiztonság és rendszerüzemeltetés területén

- **Felsőbb műszaki tanintézetek (HTL)**

Szakterületek például:

  - Informatika
  - Információstechnológia

A HTL-ek elmélyült kompetenciákat nyújtanak az alábbi területeken:

- Hálózatbiztonság
- Szerver- és rendszerbiztonság
- A kiberbiztonság alapjai
- Biztonságos szoftver- és rendszerarchitektúrák

A HTL az egyik **leggyakoribb képzési út** a kiberbiztonsági szakmák felé.

Felsőfokú képzés

A kiberbiztonság területén magasabb szintű vagy specializált szerepkörökhöz:

- Szakfőiskolák (FH)

Például az alábbi szakokon:

  - Informatika
  - IT-biztonság
  - Rendszermérnök

- Szoftvermérnök

- Egyetemek

Például informatika vagy kapcsolódó műszaki képzések, különösen relevánsak az alábbi területeken:

- Biztonsági architektúrák
- Penetrációs tesztelés
- Kutatás és fejlesztés

Kiegészítő képesítések és tanúsítványok

A képzési úttól függetlenül a **specializációk és tanúsítványok** kiemelten fontosak:

- IT-biztonsági tanúsítványok (pl. CompTIA Security+)
- Hálózati tanúsítványok (pl. Network+, CCNA)
- Linux- és rendszeradminisztráció
- Felhőalapú és biztonsági tanúsítványok (AWS, Azure – biztonsági fókusz)

Ezek a tanúsítványok **gyakorlati biztonsági kompetenciák**at igazolnak, és különösen fontosak a munkáltatók számára.

Kiberbiztonsági szakértő – lehetséges képzési út

→ **Általános iskola**

→ **IT-szakmai képzés (alkalmazásfejlesztés vagy információtechnológia – rendszer-/üzemeltetéstechnika) vagy HTL**

→ Szakmai tapasztalat IT-rendszerek / hálózatok területén

→ **Biztonsági specializáció és tanúsítványok**

→ Munkavégzés **kiberbiztonsági szakértőkéntt**

Szakmai kompetenciák

Forrás: https://bis.ams.or.at/bis/beruf/593-Datensicherheitsexperte-expertin

- Operációs rendszerekkel kapcsolatos ismeretek (pl. Windows, Linux)
- Adatbiztonsági ismeretek (pl. adatbiztonsági koncepciók ismerete)
- Elektronikai ismeretek (pl. félvezető-technológiai ismeretek)
- IT-támogatási ismeretek (IT-biztonsági workshopok lebonyolítása)
- Menedzsmentismeretek (pl. adatvédelmi menedzsment)
- Hálózattechnikai ismeretek (pl. hálózatadminisztráció)
- Programozási nyelvek ismerete (pl. Java)
- Jogi ismeretek (pl. adatvédelmi törvény)
- Adatbázis-ismeretek

Mit csinál egy kiberbiztonsági szakértő?

- **Rendszerek és emberek védelme**
  - Számítógépek
  - Mobiltelefonok
  - Hálózatok
  - Cégek
  - Iskolák
  - Kórházak

- **Biztonsági rések felkutatása (de legálisan!)**
  - A penetrációs tesztelők ellenőrzik a rendszereket, mielőtt valódi hackerek találnák meg a gyenge pontokat.

- **Támadások felismerése és megállítása**
  - Ha egy vállalatnál valami gyanús történik, a kiberbiztonsági csapatok kiderítik:
    1. Ki hajtotta végre a támadást?
    2. Mit loptak el?
  - Hogyan lehet ezt a jövőben megelőzni?

- **Jelszókezelési szabályok, adatbiztonsági és védelmi intézkedések kidolgozása**

- **Munkatársak képzése**
  - Sok támadás emberi hibák miatt történik (pl. adathalászat / phishing). A kiberbiztonsági szakemberek megmutatják, hogyan lehet biztonságosan dolgozni.

WORKSHOP-BEVEZETÉSE– HACKER VAGY VÉDŐ?

Bevezetés

„Egy rövid helyzettel kezdünk:
Képzeljétek el… valaki megtalálja a telefonotokat az iskolaudvaron. A készülék nincs lezárva. Az illető nem ismer titeket. Mégis mindent láthat“

(Rövid szünet)

A telefonon ott vannak az üzeneteitek, fényképeitek, a tartózkodási helyetek, nyitva vannak az alkalmazások, talán még jelszavak is el vannak mentve.

Sokan azt gondolják: „Az én telefonom nem is olyan különleges.“

Pedig ma már szinte az egész életünk a digitális eszközeinken van.

→ A valós életből vett, fiatalok számára könnyen érthető példa

Kérdés a csoporthoz:

„Mi lenne a legfontosabb dolog, amit meg kellene védeni, ha valaki megtalálná a telefonotokat?“

Tipikus válaszok (ha senki nem válaszol, ezeket te is bedobhatod):

- Fotók
- Chatbeszélgetések
- Jelszavak
- Tartózkodási hely
- Közösségi média
- Játékok / felhasználói fiókok
- Online bank (ha van)
- Névjegyzék
- Jegyzetek

További kérdések, ha szükség van rájuk:

- Mit tehetne valaki az Instagram-fiókotokkal?”
- „Miért lenne probléma, ha valaki elolvasná az üzeneteiteket?”
- „Milyen gyorsan tudná valaki átvenni a személyazonosságotokat?”

A való életben vannak emberek, akik pontosan azon dolgoznak, hogy illetéktelenek ne férhessenek hozzá adatokhoz, eszközökhöz vagy információkhoz: Ezeket az embereket *kiberbiztonsági szakértő*knek nevezzük.

Ők számítógépeket, vállalatokat, alkalmazásokat és embereket védenek — mint egy biztonsági szolgálat, csak digitális formában.

BIZTONSÁGOS JELSZAVAK

Cél

A tanulók…

- megértik, miért fontosak az erős jelszavak.
- képesek megkülönböztetni a gyenge, közepes és erős jelszavakat.
- különböző nehézségi szintek szerint saját jelszavakat hoznak létre.
- megismerik a támadók tipikus módszereit (egyszerűen elmagyarázva).
- felismerik, hogyan kerülik el a kiberbiztonsági szakemberek a veszélyes jelszavakat.

Ezeken a weboldalakon ellenőrizhető a jelszavak erőssége. A második oldal azt is megmutatja, hogy a jelszó hányszor jelent meg már az interneten

https://checkdeinpasswort.de/

https://nordpass.com/de/secure-password/

Bevezetés

Az előadó tipikus rossz jelszavakat mutat:

- 123456
- password
- hallo123
- Születési dátum
- Háziállat neve + szám
- „qwertz“

Rövid kérdés a csoporthoz: **„Miért rosszak ezek a jelszavak?“**

Lehetséges válaszok, amelyeket a tréner kiemelhet:

- túl rövidek
- könnyen kitalálhatók

- gyakran használtak
- személyes információk
- szerepelnek a hacker által használt jelszólistákban

Fő rész – A „jelszó kihívás”

Feladat

Készítsetek három jelszót! Kérlek, ne valódi jelszavakat használjatok!
Egyszerűen találjátok ki őket!

- **Rossz jelszó**
    - rövid, egyszerű, könnyen kitalálható
    - pl. „nyúl08“, „1234“, „iskola12“
- **Közepes jelszó**
    - kreatívabb, de még kiszámítható
    - „Macska2024!“, „SziaMindenki12“
- **Erős jelszó**
    - legalább 12 karakter
    - nagy- és kisbetűk, számok és speciális karakterek keveréke
    - lehetőleg egy könnyen megjegyezhető mondat alapján

Példa:

- Mondat: „Minden pénteken 16 órakor focizok!“
- Jelszó: **Mp16Óf!**

Prezentáció és értékelés

Menet:

- Önként jelentkezők felolvasnak **1 jelszót** (bármelyiket).

- A csoport egy egyszerű skála alapján dönt:

Gyenge → könnyen kitalálható

Közepes → jobb, de feltörhető

Erős → nagyon nehéz feltörni

Mire figyeljen a csoport?

- hosszúság
- minták (1234, aaabbb)
- személyes adatok
- szótárban szereplő szavak
- speciális karakterek
- nagy- és kisbetűk használata
- véletlenszerűség

Szakmai input – Hogyan törik fel a hackerek a jelszavakat?

Brute Force támadás:

A számítógép minden lehetséges kombinációt kipróbál — másodpercenként akár milliókat.

Szótár alapú támadás:

A hackerek több millió gyakran használt jelszót tartalmazó listákat alkalmaznak.

Közösségi média:

A hackerek több millió gyakran használt jelszót tartalmazó listákat alkalmaznak:

születésnap, háziállat neve, kedvenc csapat stb., …

ADATHALÁSZAT

Célok

A fiatalok …

- felismerik az adathalász üzenetek tipikus jellemzőit
- megismernek 10–12 egyértelmű figyelmeztető jelet
- képesek megkülönböztetni a valódi és a hamis üzeneteket
- megértik, hogyan elemzik a támadásokat a kiberbiztonsági szakemberek
- megismerik, hogyan védhetik meg magukat a mindennapokban

Kérdés a csoporthoz:

„Ki kapott már közületek furcsa üzenetet — például egy linkkel?“

Ezután magyarázat:

A phishing (adathalászat) azt jelenti, hogy valaki megpróbál megtéveszteni titeket azért, hogy megszerezze az adataitokat, jelszavaitokat vagy a pénzeteket.

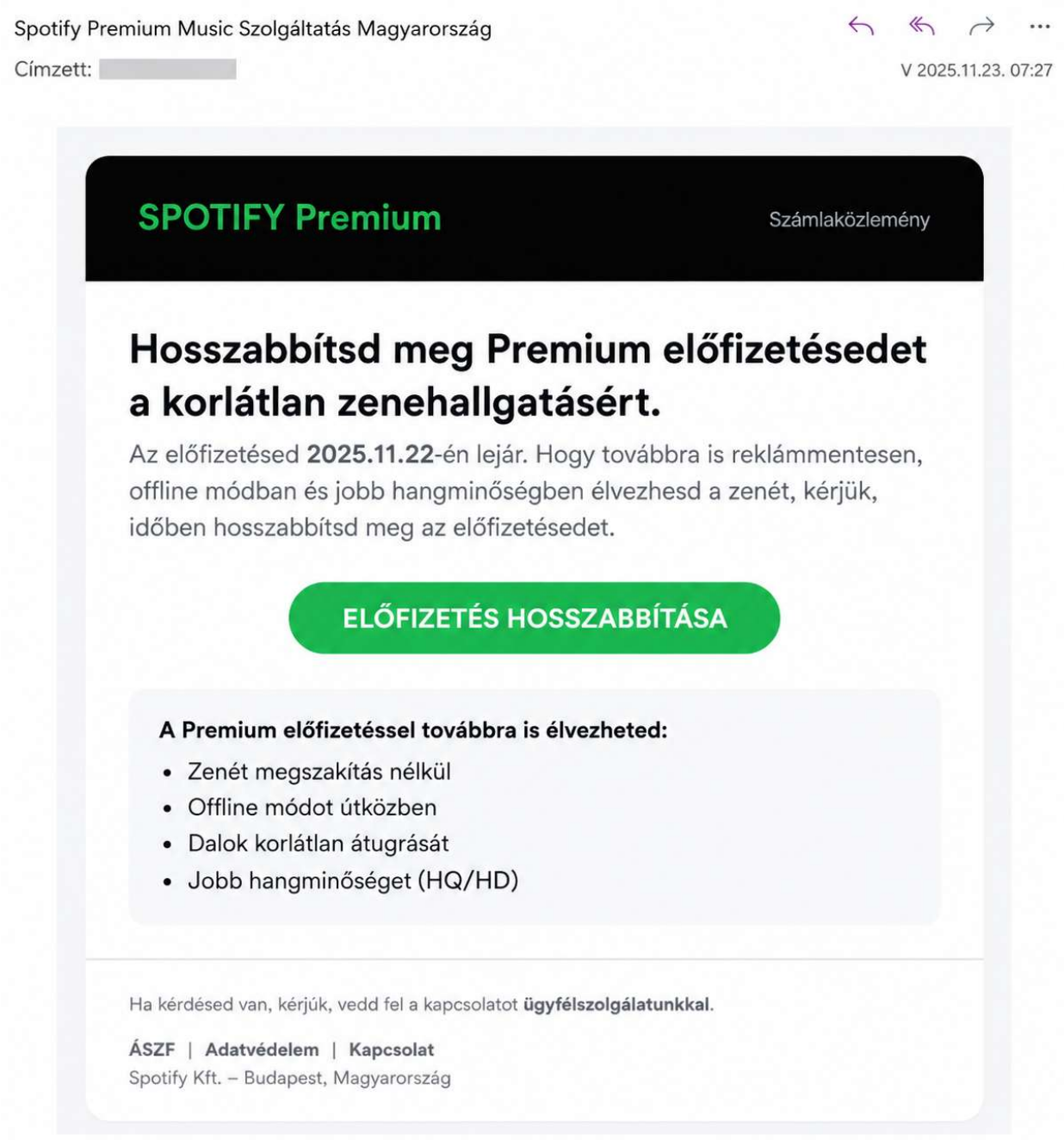
Ezt világszerte kiberbűnözők végzik — fiatalok ellen is.

A szó a „password” (jelszó) és a „fishing” (horgászat) szavakból származik.

Példák

1. Példa – Futárszolgálat

2. példa – Spotify



3. példa – E-mail

Az Ön e-mailje zárolva lett

Microsoft fiók csapat <privatemailcime@outlook.hu>

Tisztelt felhasználó!

Az Ön két beérkező e-mailje zárolásra került aktuális frissítés miatt az adatbázisunkban.

Annak érdekében, hogy ezeket az üzeneteket megkapja, kérjük, kattintson az alábbi linkre az azonossága megerősítéséhez, és várja meg a választ.

Kattintson ide az azonosításhoz

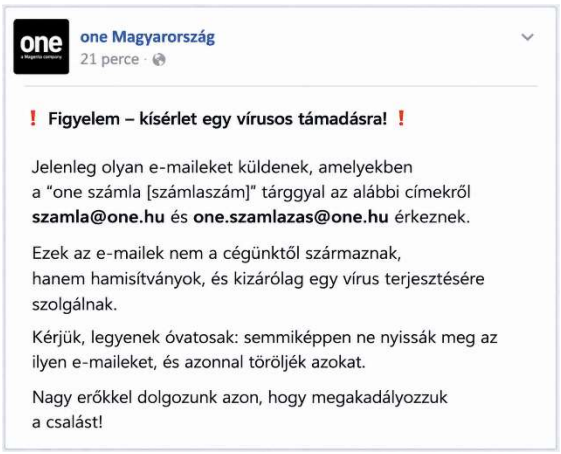
Az esetleges kellemetlenségekért elnézését kérjük, és köszönjük megértését.

Üdvözlettel
A Microsoft fiók csapata

4. példa– Nyereményjáték

5. példa – Hamis hír

6. példa – One vagy három SMS



A 10 legfontosabb figyelmeztető jel

- Szokatlan küldő
- Nyomásgyakorlás („Azonnal kattints!“)
- Meglepetés nyeremény
- Helyesírási hibák
- Ismeretlen link
- Üzenetek állítólagos barátoktól új telefonszámmal
- Idegen login oldalak
- Jelszavat azonnal módosítani kell
- Ismeretlentől származó mellékletek
- Érzelmekre ható trükkök (félelem, stressz, kíváncsiság)

Záró reflexió

Kérdések a csoporthoz:

„Melyik figyelmeztető jelet fogjátok biztosan megjegyezni?“

„Mit tanácsolnátok annak, aki ilyen üzenetet kap?“

„MENNYIRE FELTÖRHETŐ EGY ISKOLAI NAP?“

Mielőtt valódi kibertámadások történnek, szinte mindig vannak apró figyelmeztető jelek vagy kockázatos helyzetek. A kiberbiztonsági szakemberek elemzik ezeket a helyzeteket, és felmérik, mennyire veszélyesek.

Célok

A fiatalok…

- felismerik a biztonsági kockázatokat az iskolai és magánéletben.
- megtanulják megkülönböztetni az ártalmatlan és a veszélyes helyzeteket.
- kialakítanak egy alapvető biztonságtudatosságot.
- megértik, hogyan elemzik a valós kockázatokat a kiberbiztonsági szakemberek.
- fejlesztik a kritikus gondolkodást és a csapatkommunikációt

Csoportmunka - feladat

A fiatalok **2-4 fős csoportok**ban dolgoznak.

Minden csoport **6-8** iskolai vagy szabadidős **hétköznapi szituáció**t kap.

Minden szituációt a következők szerint értékelnek:

1. **Mennyire veszélyes?** (1–5)
2. **Miért?**
3. **Mi lenne a biztos megoldás?**

„A“ szituáció

Egy pendrive-ot találsz az iskolaudvaron.

→ Veszélyes (kártevő, adatlops)

„B“ szituáció

Egy barátod elkéri a hotspot-jelszavadat.

→ Közepesen veszélyes / veszélyes (megosztás, felelősség, visszaélés)

„C“ szituáció

Valaki odaszól neked: „Odaadod egy pillanatra a telefonodat? Meg kell néznem valamit a Google-ben.“

→ veszélyes (hozzáférés mindenhez)

„D“ szituáció

Instagram-üzenetet kapsz: „Nézd meg ezt a képet rólad 😳“ + Link

→ nagyon veszélyes (adathalászat, fiókfeltörés)

„E“ szituáció

Egy osztálytárs hangosan kimondja az iskolai WiFi-jelszót a folyosón.

→ Közepesen veszélyes (továbbadás, visszaélés)

„F“ szituáció

A számítógépterem jelszólistája nyitva fekszik a tanári számítógép mellett.

→ Nagyon veszélyes (hozzáférés minden rendszerhez)

„G“ szituáció

Telepítesz egy alkalmazást egy TikTok-videó alapján, mert „több lájkot kapsz vele”.

→ Veszélyes (csalás, kártevő)

„H“ szituáció

Egy e-mail azt állítja, hogy új házi feladat érhető el, és ehhez meg kell adni egy jelszót.

→ Nagyon veszélyes (iskolai adathalászat)

Csoportmunka - csoportszakasz

Minden csoport röviden bemutat **1–2 helyzet**et:

- saját értékelésüket
- saját megoldásukat

A tréner minden esetben kiegészíti:

- Mi lenne egy kiberbiztonsági szakember *professzionális álláspont*ja?
- Milyen valós veszélyek léteznek?
- Mi a legjobb eljárás ilyen helyzetben?

Nem szükséges minden helyzetet bemutatni — válasszátok ki a legérdekesebbeket.

VR ÉS AR TARTALMAK

VR tréning: Hibaanalízis egy IT-infrastruktúrában

A kiberbiztonság területén VR-szcenáriók alkalmazhatók az IT-biztonsági szakemberek tipikus feladatainak bemutatására.

Egy virtuális környezetben a tanulók például:

- szokatlan rendszerüzeneteket elemezhetnek
- lehetséges biztonsági problémákat azonosíthatnak
- egyszerű hibajavítási intézkedéseket hajthatnak végre

Ezek a szimulációk szemléltetik, hogy a kiberbiztonság nem csupán elméleti szabályokból áll, hanem szorosan kapcsolódik a technikai rendszerek elemzéséhez.

MELLÉKLET: „HOGYAN TÖRHETŐ FEL EGY ISKOLAI NAP?“

„A” szituáció *Egy pendrive-ot találsz az iskolaudvaron*	**„B” szituáció** *Egy barátod elkéri a hot-spot-jelszavadat*
„C” szituáció *Valaki kéri:* *„Odaadod egy pillanatra a telefonodat? Meg kell néz-nem valamit a Google-ben.“*	**„D” szituáció** *Instagram-üzenetet kapsz:* *„Nézd meg ezt a képet ró-lad 😂“ + Link*
„E” szituáció *Egy osztálytárs hangosan kimondja az iskolai WiFi-jelszót a folyosón*	**„F” szituáció** *A számítógépterem jelszó-listája nyitva fekszik a ta-nári számítógép mellett*
„G” szituáció *Telepítesz egy alkalma-zást egy TikTok-videó alapján, mert „több lájkot kapsz vele”.*	**„H” szituáció** *Egy e-mail azt állítja, hogy új házi feladat érhető el, és ehhez meg kell adni egy jelszót.*