Digitális Témahét: a 11. évfolyam számára a pénzügyi tudatosság és a kiberbiztonság pont abban az életszakaszban jön, amikor elkezdenek önálló bankszámlával, bankkártyával rendelkezni. A fiatalok szivacsként gyűjtik magukba az infokommunikációs eszközök alkalmazásának rutinját. De mi a helyzet az idősebb generációkkal?! Hogyan tudnak a diákok segíteni szüleiknek, nagyszüleiknek a csalókkal szemben az internetes bankolás világában?

Projektterv: "Kiberpajzs a zsebemben"

Célcsoport: 11.a és 11.b osztály

Időtartam: 5 tanóra (tantárgyközi projekt)

Központi téma: Adathalászat elleni védekezés és biztonságos digitális bankolás.

---

1. NAT Kapcsolódási pontok és Kompetenciafejlesztés

- **Digitális kompetencia:** Biztonság (személyes adatok védelme, kockázatok felismerése), Problémamegoldás (technikai zavarok és veszélyhelyzetek kezelése). A mesterséges intelligencia etikus alkalmazása a tanulási folyamatban.
- **Matematikai, gondolkodási kompetencia:** Kombinatorikai készségek fejlesztése, algoritmus alapú gondolkodás.
- **Anyanyelvi kommunikáció:** Kritikai szövegértés, érveléstechnika, különböző stílusrétegek felismerése.
- **Állampolgári kompetencia:** Felelősségvállalás, jogkövető magatartás, áldozatvédelem.
- **Személyes és társas kapcsolati kompetencia:** Generációk közötti hídépítés, segítő attitűd (empátia az idősebbek felé).

---

2. Tantárgyi kapcsolatok és felépítés

I. Matematika (1 óra): A biztonság számokban

- **Téma:** Jelszóbiztonság és kombinatorika. (kombinatív gondolkodás)
- **Tevékenység:** A Gamma PPT alapján a hallgatók elemzik a jelszóerősséget. Hány lehetőség van? Fókuszban a kombinatorika. Milyen egy erős jelszó? 6 vagy 8 karakter, csak kisbetűk vagy a jelszó tartalmazzon speciális karaktereket is?
- **Matematikai háttér:** Ismétléses variációk kiszámítása.
- **Eszköz:** Gamma prezentáció. Internetes keresés számítógépen és telefonon.

II. Magyar nyelv és irodalom (1 óra): A manipuláció nyelve

- **Téma:** Adathalász e-mail elemzése. (kritikai szövegértés)
- **Tevékenység:** A Gemini által generált e-mail boncolása. A diákoknak meg kell találniuk a

"red flag"-eket: sürgető hangnem, helyesírási hibák, gyanús feladó, maszkolt linkek.
- **Szituációs játék:** Hogyan magyarázzuk el a nagymamának érthetően, de nem leereszkedően, hogy miért ne kattintson? (Stílusgyakorlat).

III. Informatika / Rendészet (2 óra): A védelem technikai és jogi bástyái

- **Informatikai fókusz:** Hogyan működik a titkosítás? (HTTPS, kétfaktoros azonosítás – 2FA). A biztonságos böngészés alapjai. (kombinatív gondolkodás, algoritmikus gondolkodás)
- **Rendészeti fókusz:** Mi a teendő, ha megtörtént a baj? A feljelentés menete, a banki protokoll (kártyaletiltás), és a kiberbűnözés jogi következményei.
- **Szemléltetés:** Digitális tábla. Power point bemutató.

IV. Osztályfőnöki óra (1 óra): Digitális szakadék és reflexió

- **Téma:** Generációs különbségek és társadalmi felelősség. (empátia, felelősségteljes gondolkodás)
- **Tevékenység:** "Digitális útmutató" készítése: plakát készítése csoportmunkában mesterséges intelligencia segítségével. „*Hogyan ismerhető fel egy adathalász üzenet?”*

Zárás: A projekt tapasztalatainak, tanulságainak összegzése.

---

3. Értékelés és kimenet

A projekt végén a diákok készítenek az új ismeretek, tapasztalatok alapján egy ***"Prevenciós plakátot"***, amit megosztanak az iskola Diákönkormányzat közösségi oldalán és elküldhetnek szüleiknek, nagyszüleiknek. A projekt egy-egy darab 100 %-os érdemjeggyel értékelhető magyar nyelv és irodalom, matematika és szakmai tantárgyakból. A kiemelkedő aktivitás további osztályzatokkal jutalmazható tantárgyanként 50 %-os súlyozással.

Melléklet

A mesterséges intelligencia segítségével generált adathalász üzenet:

Tárgy: Sürgös Figyelmeztetés: Fiókja felfüggesztésre került !!

Tisztelt Ügyfél!

Értesitjük önt, hogy a rendszerünk biztonsági hiba észlelt az ön online banki fiókja kapcsán. Az ön biztonsága érdekében ideiglenesen korlátoztuk a kifizetések és átutalások.

Ahhoz, hogy ne veszítse el a hozzáférést a pénzéhez, kérjük, végezze el a hitelesitési folyamat azonnal. Ha nem teszi meg 24 órán belül, a számláját véglegesen lezárjuk.

Kérjük kövesse az alábbi lépéseket:

1. Kattintson a lenti biztonságos linkre.
2. Adja meg a bankkártya száma, a lejárati dátumot és a biztonsági kód (CVV).
3. Erősítse meg a személyes adatok: anyja neve, lakcím és születési dátum.

Kattintson ide a frissítéshez: [http://biztonsagos-bank-belepes-hu-99.xyz/bejelentkezes]

Kérjük, ne válaszoljon erre az emailre, mert ez egy automata rendszer generált.

Köszönjük a türelmét és együttműködését.

Üdvözlettel,

A Központi Banki Biztonság Csoport

„Az ön pénze, a mi dolgunk!”

Ez egy remek kezdeményezés a Digitális Témahétre!

A kiberbiztonsági tudatosság alapja, hogy felismerjük azokat az apró, gyanús jeleket, amelyek felett egy sietős hétköznapon átsiklanánk.

A promptnak megfelelően összeállítottam egy szándékosan rossz magyarsággal megírt, klasszikus adathalász (phishing) mintát, amelyet elemzésre használhattok.

Elemzési szempontok a diákok számára:

A projekt során az alábbi hibákra érdemes felhívni a figyelmet:

- **Helyesírási hibák:** Hiányzó ékezetek (pl. *Sürgös*, *értesitjük*, *hitelesitési*), elütések és furcsa központozás (kettős felkiáltójel).
- **Magyartalan megfogalmazás:** A Google Fordítóra jellemző nyelvtani hibák (pl. *„a rendszerünk biztonsági hiba észlelt”*, *„személyes adatok: anyja neve”*).
- **Sürgető hangvétel:** A "24 órán belüli lezárás" tipikus pszichológiai nyomásgyakorlás, hogy a felhasználó ne gondolkodjon, csak cselekedjen.
- **Gyanús link:** A domain név (xyz végződés, furcsa kötőjelek) egyértelműen jelzi, hogy nem a hivatalos banki oldalon járunk.
- **Túlzott adatkérés:** Egy bank **soha** nem kéri el emailben a bankkártya CVV kódját vagy a teljes személyes adatsort egy linkre kattintva.