Správa o činnosti pedagogického klubu

1. Prioritná os	Vzdelávanie
2. Špecifický cieľ	1.2.1 Zvýšiť kvalitu odborného vzdelávania a prípravy reflektujúc potreby trhu práce
3. Prijímateľ	SOŠ Jána Antonína Baťu, Námestie SNP 5, Partizánske.
4. Názov projektu	Zvyšujeme kvalitu vzdelávania a odbornej prípravy
5. Kód projektu ITMS2014+	312011Z792
6. Názov pedagogického klubu	Pedagogický klub finančnej gramotnosti v príprave na život – prierezové témy.
7. Dátum stretnutia pedagogického klubu	8. november 2021
8. Miesto stretnutia pedagogického klubu	Stredná odborná škola J. A. Baťu, Námestie SNP 5, Partizánske
9. Meno koordinátora pedagogického klubu	Ing. Ingrid Rigáňová
10. Odkaz na webové sídlo zverejnenej správy	https://sospe.edupage.org/text/?text=text/text19&subpage=5

11. **Manažérske zhrnutie:**

Cieľom stretnutia nášho klubu bola diskusia o metódach modelovania situácií pri rozvoji finančnej gramotnosti. Spoločne sme diskutovali o možnostiach identifikácie spotrebiteľských produktov vrátane online foriem predaja a zdieľali sme názory na aplikáciu inovatívnych metód pri rozvoj predmetných kompetencií. Na záver stretnutia sme tvorili odporúčanie.

Kľúčové slová: spotrebiteľské podvody, modelovanie situácií, finančná gramotnosť.

12. **Hlavné body, témy stretnutia, zhrnutie priebehu stretnutia:**

Hlavné body:

1. Práca s IKT- získavanie informácií.
2. Diskusia.
3. Výmena OPS.
4. Záver a tvorba odporúčania.

Témy: zvyšovanie kvality vzdelávania, rozvoj finančnej gramotnosti.

Program stretnutia:

1. Tvorba opisného výskumu- práca s IKT.
2. Diskusný kruh.
3. Spoločná výmena OPS – skladacie učenie.
4. Záver a tvorba pedagogického odporúčania.

13. Závery a odporúčania:

Zhrnutie z diskusie –bezpečne na internete a aplikácia situačných metód:

Téma Phishing

Je to podvodný pokus o získanie citlivých informácií používateľa a to napríklad používateľské meno, heslo alebo informácie o kreditných kartách. Ide zväčša o email, ktorý neobsahuje žiaden vírus, preto ho antivírus často neidentifikuje.

Princípy phishingu

Phishing je emailová alebo iná elektronická forma správy, ktorá obsahuje zväčša text, poprípade odkaz na webstránku.

Táto elektronická správa môže prísť od neznámej, ale dokonca aj od známej osoby. V tomto prípade je potrebné, aby ste rozlišovali medzi adresami užívateľov.

V prípade, že elektronická správa odkazuje na nejakú webovú lokalitu je potrebná zvýšená opatrnosť. V prípade phishingu ani daná webová lokalita nemusí obsahovať žiaden vírus a preto je opäť neidentifikovaná antivírusovým programom.

Metodika – bezpečne v online priestore – časť phishing:

Tipy ako odhaliť phishing

Neoprávnené získavanie údajov je obľúbenou formou počítačovej kriminality, pretože je veľmi efektívne. Kyberzločinci bývajú pri používaní e-mailov získavanie osobných údajov od ľudí často úspešní. Najlepšou ochranou je dostatočné povedomie a znalosť toho, na čo sa zamerať.

Pravopis a zlá gramatika. Útočníci sú často zo zahraničia a preto v prípade slovenčiny sú odosielané emaily plné gramatických chýb, nezvyčajn zvratov a zlého slovosledu. To isté však platí aj v prípade angličtiny. V poslednej dobe sa gramatika útočníkov zlepšuje a preto nie je možné spoliehať sa na tento jeden faktor.

Podozrivé prepojenia. Ak sa domnievate, že ide o podvodnú e-mailovú správu, neotvárajte žiadne prepojenia (odkazy), ktoré sú v nej zobrazené. Namiesto toho ukážte na prepojenie myšou, ale naň neklikajte, a skontrolujte, či sa adresa zhoduje s prepojením, ktoré je zadané v správe. V nasledujúcom príklade sa po podržaní myši na prepojení zobrazuje skutočná webová adresa v poli so žltým pozadím.

Mali by sme pamätať, že reťazec čísiel tvoriacich IP adresu rozhodne nevyzerá ako webová adresa nejakej spoločnosti.

Hrozby a nátlak. Tieto typy e-mailov navodzujú pocit nevyhnutného reagovania, aby sme čo najrýchlejšie odpovedali, vyplnili dotazník alebo vykonali akciu. Môžu obsahovať vyhlásenie, ako je napríklad „Musíte odpovedať do konca dnešného dňa“. Alebo sa v nich môže tvrdiť, že v prípade neodpovedania môžeme čeliť finančnému postihu, zablokovaniu účtu a pod.

Zmenené webové adresy. Forma podvodu, kde sa webové adresy iba podobajú názvom známych spoločností, ale sú mierne zmenené. Napríklad www.micorsoft.com či www.mircosoft.com.

Prehľad situačných metód vhodných pre predmetnú implementáciu:

Metódy konfliktných situácií

Žiakom je popísaná modelová situácia konfliktu autentifikácii platby falošným terminálom, inak povedané spor. Cieľom tejto metódy je analyzovať konanie týchto osôb a naučiť sa správne reagovať v podobných situáciách. Záverom by mali žiaci nájsť vhodnejšie riešenia tohto konfliktu a zhodnotiť správnosť reakcií účastníkov sporu.

Metóda incidentu

Učiteľ povie žiakom krátku správu, udalosť v nejakej situácii. Žiaci sa otázkami musia dopracovať k širším faktom o tejto udalosti, aby zistili príčiny problému a následne navrhli riešenie. Metódou pre tento typ úlohy je logická analýza rôznych faktov a informácií.

Uvedenú metodiku použijeme v rámci vlastného predmetu a zamerania.

14. Vypracoval (meno, priezvisko)	Ing. Ingrid Rigáňová
15. Dátum	30.11.2021
16. Podpis	
17. Schválil (meno, priezvisko)	Ing. Katarína Hartmannová, MBA
18. Dátum	30.11.2021
19. Podpis	