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	Súkromná stredná odborná škola polytechnická DSA, Novozámocká 220, Nitra
4. Názov projektu	Prepojenie teórie s praxou – vzdelávanie 4.0
5. Kód projektu ITMS2014+	312011ACZ5
6. Názov pedagogického klubu	Finančná a matematická gramotnosť v bežnom živote – prierezové témy.
7. Dátum stretnutia pedagogického klubu	03.11.2021
8. Miesto stretnutia pedagogického klubu	SSOŠ polytechnická DSA, Novozámocká 220, Nitra
9. Meno koordinátora pedagogického klubu	Mgr. Mária Staňová
10. Odkaz na webové sídlo zverejnenej správy	https://sospnitra.edupage.org/

11. **Manažérske zhrnutie:**

Cieľom stretnutia nášho klubu bola tvorba námetov posilnenia bezpečnosti v oblasti finančnej gramotnosti, diskusia a modelovanie situácií z oblasti identifikácie bežných typov spotrebiteľských produktov a ohrozenia, ktoré prináša virtuálne prostredie. Spoločne sme na predmetnú tému diskutovali, zdieľali naše skúsenosti a na záver stretnutia sme tvorili pedagogické odporúčanie.

Kľúčové slová: spotrebiteľské podvody, online podvody, modelovanie situácie.

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

Hlavné body:

1. Prezentácia od koordinátora klubu.
2. Diskusia.
3. Výmena OPS – modelovanie situácie.
4. Záver.

Témy: Finančná a matematická gramotnosť, Prepojenie teórie s praxou.

Program stretnutia:

1. Multimediálna prezentácia – OPS v danej oblasti.
2. Diskusný kruh,
3. Spoločná debata – výmena pedagogických skúseností.
4. Záver a tvorba pedagogického odporúčania.

13. Závery a odporúčania:

Zhrnutie z diskusie – vedomosti a metódy:

Z prezentácie koordinátora klubu sme sa dozvedeli najnovšie informácie z oblasti bezpečnosti na internete pri realizácii finančných produktov, o ktorých budeme ďalej informovať žiakov.

Z prezentácie:

Falošné správy a dezinformácie v oblasti finančných produktov sú súčasťou nášho sveta tak dlho ako samotné správy. Niekedy môže ísť len o prostý žart, no v niektorých prípadoch predstavujú oveľa vážnejšie riziko.

Za najväčší zdroj šírenia dezinformácií sa považuje internet a sociálne médiá. Internet je síce svet plný neobmedzených možností, vďaka ktorému dnes máme na dosah ruky množstvo informácií s potenciálom spájať svet, ale možno ho veľmi jednoducho zneužiť na podvody v oblasti finančných produktov.

Malvér je skratkou pre anglický výraz „malicious software“, teda škodlivý softvér alebo škodlivý kód. Môže ním byť akýkoľvek kód, ktorého úlohou je napadnúť počítač, tablet alebo telefón (jednoducho akékoľvek zariadenie) a vykonať v ňom neželané zmeny. Napríklad vypnúť určité funkcie, prebrať kontrolu nad operačným systémom alebo z neho ukradnúť informácie.

Ransomvér

Ide o typ malvéru, ktorý po infiltrácii počítača uzamkne súbory používateľa. Používateľovi zabráni vo využívaní zariadenia a za odomknutie súborov pýta výkupné (zvyčajne v kryptomene). Dokáže vám nielen zamedziť prístup do operačného systému, ale aj zaheslovať vaše súbory a to niekedy nenávratne. Zaplatenie výkupného nezaručuje, že budú vaše údaje naozaj dešifrované.

Spyvér

Tento druh malvéru je známy ako sledovací škodlivý softvér, ktorý zhromažďuje informácie o obeti bez jej vedomia. Jeho primárnou funkciou je zhromažďovanie osobných informácií uložených v počítači či monitorovanie webových stránok, ktoré používateľ navštevuje, prípadne položiek, ktoré si zakúpi online.

Bankový malvér

Druh malvéru, ktorý sa zameriava na krádež finančných informácií obete. Ide najmä o čísla kreditných kariet, prístupy do bankových účtov, kryptopeňaženiek či iných služieb spojených s peniazmi alebo kryptomenami.

Password Stealer

Malvér, ktorý sa pokúša ukradnúť uložené používateľské mená či heslá. Je podobný spyvéru a bankovému malvéru, no zameriava sa výhradne na súbory a programy, ktoré by mohli obsahovať heslá.
Password stealer dovoľuje útočníkovi do infikovaného zariadenia nainštalovať ďalší škodlivý softvér, prípadne môže nasmerovať infikované zariadenie do škodlivého botnetu (teda siete ďalších infikovaných zariadení) na účely odosielania spamu alebo iných škodlivých aktiv

Po prezentácii sme sa zaoberali metódami, ktorými by sme žiakom tieto nebezpečné situácie čo najlepšie predstavili, nakoľko sa týkajú bežných spotrebiteľských produktov.
Efektívna metóda:
Hranie rolí je patrí medzi základné metódy využívajúce interakcie žiakov v procese učenia. To znamená, že na rozdiel od situačného modelovania hra na hranie rolí znamená väčšiu aktivitu a interakciu, zameranie sa na efektívne výsledky vzdelávania, ako aj určité psychologické závery učiteľa.

S pomocou hry na hranie rolí sa žiak ocitne v situácii, ktorá obsahuje rovnaký súbor obmedzení, nátlakov a motivácií, ktoré sa vyskytujú v reálnom svete v spolupráci s ostatnými účastníkmi procesu.
Vo vzdelávacom procese sú hry na hranie rolí zvyčajne založené na herných konštrukciách, to znamená, že úloha môže byť prezentovaná ako model, ako hra na hranie rolí a ako experiment.

Zhodli sme sa, že o uvedených skutočnostiach budeme žiakov informovať začlenením témy do didaktickej analýzy učiva v predmete, ktorý vyučujeme.

14. Vypracoval (meno, priezvisko)	Mgr. Mária Staňová
15. Dátum	03.11.2021
16. Podpis	
17. Schválil (meno, priezvisko)	Ing. Oľga Hodálová
18. Dátum	03.11.2021
19. Podpis	