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	Obchodná akadémia, Kapušianska 2, 071 01 Michalovce
4. Názov projektu	Prepojenie stredoškolského vzdelávania s praxou
5. Kód projektu ITMS2014+	312011AGS3
6. Názov pedagogického klubu	Pedagogický klub pre IKT zručnosti
7. Dátum stretnutia pedagogického klubu	22. jún 2021
8. Miesto stretnutia pedagogického klubu	Obchodná akadémia Michalovce
9. Meno koordinátora pedagogického klubu	Ing. Katarína Hovanová
10. Odkaz na webové sídlo zverejnenej správy	www.oami.sk

11. **Manažérske zhrnutie:**
krátka anotácia, kľúčové slová

2. polrok /téma č.12

Téma stretnutia č. 12
Základné zásady bezpečnosti na internete

Rámcový program stretnutia
Ako sa správať na internete - výmeny skúseností a best practice z vlastnej vyučovacej činnosti.

Kľúčové slová
- počítačová bezpečnosť, bezpečnostná chyba, malware, patch, aktualizácia, firewal, port, červ, trójsky kôň, spyware, keylogger, adware, antivírus, hoax, spam, sociálne inžinierstvo, sociotechnika, phishing, pharming

Krátka anotácia

- Úplne zabezpečiť počítač pred útočníkmi alebo škodlivými prvkami je takmer nemožné. Každý používateľ by sa mal preto snažiť, aby bola cesta útočníka alebo škodlivých prvkov čo najviac sťažená.

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

Hlavné body témy stretnutia – Bezpečnosť a riziká na internete

Prvým predpokladom bezpečného využívania počítača je nepochybne dodržiavanie pravidiel uvedených v etickom kódexe používateľa a v desatore bezpečnosti na internete. Bezpečný počítač by nemal obsahovať žiadny nežiaduci softvér a nemal by byť napadnuteľný po pripojení na internet. Počítačovú bezpečnosť môžeme charakterizovať ako odhaľovanie a eliminovanie rizík spojených s používaním počítača. Okrem ochrany pred neoprávnenou manipuláciou s údajmi v počítači ide aj o ochranu pred neoprávnenou manipuláciou so zariadeniami počítača, ochranu pri komunikácii a prenose údajov, ži inému zneužitiu počítača používateľa a jeho údajov. Používateľ môže stratiť svoje údaje viacerými spôsobmi. Ide o hrozby:

- Prírodné a fyzické (živelné pohromy)
- Technické (poruchy počítačov, počítačových sietí, nosičov údajov)
- Technologické (poruchy spôsobené programami, ako sú vírusy, malware, trójske kone)
- Ľudské (hekeri, teroristi, špionáže, zamestnanci firmy a pod.)

Z týchto hrozieb sú najvýznamnejšie hrozby technologické a ľudské. V operačných systémoch a aplikačnom softvéri sa stále objavujú možnosti , ako môže byť vďaka ich nedokonalostiam zneužitý počítač používateľa rôznymi spôsobmi. Tieto možnosti označujeme ako bezpečnostné chyby. Softvér, ktorý predstavuje pre používateľa hrozbu označujeme ako škodlivý softvér alebo malware. Ide o súhrnné pomenovanie pre vírusy, červy, trójske kone, adware, spyware a pod. tieto programy sa v súčasnosti šíria prostredníctvom internetu a trvá len veľmi krátky čas, kým tvorcovia týchto hrozieb využijú bezpečnostné chyby v počítačoch používateľov. V momente, keď je opísaná nejaká bezpečnostná chyba, je reakciou tvorcov operačných systémov vytvorenie opravy (záplaty, patch), ktorá túto chybu v operačnom systéme používateľa odstráni. Podmienkou je, aby používateľ túto opravu pridal do svojho počítača. Urobí tak, keď svoj operačný systém včas aktualizuje. Ďalším nástrojom ochrany v počítači je firewall, ktorý vytvára akúsi ochrannú hrádzu medzi počítačom používateľa potenciálne škodlivým obsahom na internete. Služby na sieti, ktoré využíva používateľ sa spájajú s počítačom cez rôzne porty (brány). Firewal kontroluje, čo sa na jednotlivých portoch deje, a povoľuje komunikáciu, ktorú vyžiada alebo povolí používateľ počítača.

Ďalším škodlivým programom je počítačový vírus. Ide o program , ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných programov, alebo súborov. Tak ako biologický vírus, aj počítačový vírus potrebuje na svoje rozširovanie hostiteľa. Podľa cieľ infekcie môžeme hovoriť o vírusoch:

-programových – svoj kód umiestňujú do tela iných programov a aktivujú sa ich spustením,

- makrovírusoch – sú vo forme makier, ktoré napádajú priamo dokumenty najčastejšie používaných programov (napr. textový editor)

- bootovacích – napádajú v počítači bootovacie sektory diskov a spúšťajú sa tak pri načítaní operačného systému.

Ďalšou skupinou škodlivého softvéru sú červy, ktoré nepotrebujú na svoje fungovanie hostiteľský program a dokážu sa rozšíriť za veľmi krátky čas prostredníctvom počítačovej siete. Osobitnou skupinou je program nazývaný Trójsky kôň, ktorý navodzuje dojem užitočnosti. Svoju činnosť však v skutočnosti nemusí vykonávať, ale na pozadí vykonáva deštrukčnú činnosť. Vzhľadom zapadá do bežného užívateľného prostredia.

Ďalšími škodlivými programami sú spyware, ktoré sledujú činnosť používateľa počítača a informujú o tom útočníka, adwaere, ktorý sleduje činnosť používateľa a na základe toho mu posiela reklamu. Jednou z efektívnych možností ochrany pred vírusmi je používanie antivírusového programu, ktorý sa štandardne spúšťa pri štarte systému. . Je však nutná jeho ustavičná aktualizácia.

Priebeh stretnutia

Učitelia sa stretli v odbornej učebni, kde podpísali prezenčnú listinu. Stretnutie sa uskutočnilo v priaznivej a tvorivej klíme. Učitelia si vymenili skúsenosti ,zo zabezpečovania počítača a hrozieb, ktoré sa šíria v súvislosti ako škodlivý softvér na internete. Pomenovali jednotlivé príčiny hrozieb na internete a zároveň zhodnotili ich praktický význam. Zhodli sa, že najväčšie nebezpečenstvo pochádza z technologických a ľudských hrozieb. Definovali čo je to škodlivý softvér a pomenovali techniku opráv pri vzniku bezpečnostnej chyby. Vyzdvihli význam použitia automatickej aktualizácie operačného systému. Objasnili si pojem firewall a porta zhodnotili ich praktický význam pre bezpečnosť. V ďalšej časti podrobne charakterizovali počítačový vírus ako škodlivý program, jeho vlastnosti, spôsob šírenia a rozdelenie vírusov podľa cieľa infekcie. Charakterizovali škodlivý softvér červ, Trójsky kôň, Spyware a adware aj so zreteľom na ich praktický dopad na používateľa. Konštatovali, že najlepšou ochranou je zakúpenie a inštalácia antivírusového programu, jeho ustavičná aktualizácia. Vymenovali všetky nástroje prevencie proti škodlivým programom a to aktualizácia, zváženie návštevy podozrivých webov, zváženie registrácie na podozrivých weboch, sťahovanie programov z podozrivých webov, pozornosť pri sťahovaní neznámych príloh, bezpečné odhlasovania pri ukončení práce na počítači, zálohovanie údajov, blokovanie vyskakovacích okien, nastavenie ochrany osobných údajov, pravidelné mazanie vyrovnávacej pamäte, nastavovanie kontroly používateľských účtov a pod.

13. **Závery a odporúčania:**

Záver

Členovia pedagogického klubu pre IKT si vymieňali skúsenosti so zabezpečovania počítača a hrozieb, ktoré sa šíria na internete v súvislosti so škodlivým softvérom. Oboznámili sa s druhmi bezpečnostných hrozieb a s druhmi škodlivého softvéru. Podrobne si všímali rozdiely a spoločné črty škodlivého softvéru a mechanizmus ich šírenia v počítači. Diskutovali o úrovni aktuálne dostupného antivírusového programu , nevyhnutnosti jeho neustáleho aktualizovania a popisovali ďalšie možné spôsoby ochrany.

Odporúčania:
Na všetkých vyučovacích hodinách, na ktorých sa používa počítač a internet, poučiť žiakov o nutnosti zabezpečenia počítača, súborov pomocou kvalitného antivírusového programu a ďalších spôsobov ochrany..

14. Vypracoval (meno, priezvisko)	Ing. Katarína Hovanová
15. Dátum	22. 06. 2021

16. Podpis	
17. Schválil (meno, priezvisko)	Ing. Dana Kerekešová
18. Dátum	22. 06. 2021
19. Podpis	

Príloha:

Prezenčná listina zo stretnutia pedagogického klubu

Pokyny k vyplneniu Správy o činnosti pedagogického klubu:

Prijímateľ vypracuje správu ku každému stretnutiu pedagogického klubu samostatne. Prílohou správy je prezenčná listina účastníkov stretnutia pedagogického klubu.

1. V riadku Prioritná os – Vzdelávanie
2. V riadku špecifický cieľ – uvedie sa v zmysle zmluvy o poskytnutí nenávratného finančného príspevku (ďalej len "zmluva o NFP")
3. V riadku Prijímateľ - uvedie sa názov prijímateľa podľa zmluvy o poskytnutí nenávratného finančného príspevku
4. V riadku Názov projektu - uvedie sa úplný názov projektu podľa zmluvy NFP, nepoužíva sa skrátený názov projektu
5. V riadku Kód projektu ITMS2014+ - uvedie sa kód projektu podľa zmluvy NFP
6. V riadku Názov pedagogického klubu (ďalej aj „klub“) – uvedie sa názov klubu
7. V riadku Dátum stretnutia/zasadnutia klubu - uvedie sa aktuálny dátum stretnutia daného klubu učiteľov, ktorý je totožný s dátumom na prezenčnej listine
8. V riadku Miesto stretnutia pedagogického klubu - uvedie sa miesto stretnutia daného klubu učiteľov, ktorý je totožný s miestom konania na prezenčnej listine
9. V riadku Meno koordinátora pedagogického klubu – uvedie sa celé meno a priezvisko koordinátora klubu
10. V riadku Odkaz na webové sídlo zverejnenej správy – uvedie sa odkaz / link na webovú stránku, kde je správa zverejnená
11. V riadku Manažérske zhrnutie – uvedú sa kľúčové slová a stručné zhrnutie stretnutia klubu
12. V riadku Hlavné body, témy stretnutia, zhrnutie priebehu stretnutia - uvedú sa v bodoch hlavné témy, ktoré boli predmetom stretnutia. Zároveň sa stručne a výstižne popíše priebeh stretnutia klubu
13. V riadku Závery o odporúčania – uvedú sa závery a odporúčania k témam, ktoré boli predmetom stretnutia
14. V riadku Vypracoval – uvedie sa celé meno a priezvisko osoby, ktorá správu o činnosti vypracovala
15. V riadku Dátum – uvedie sa dátum vypracovania správy o činnosti
16. V riadku Podpis – osoba, ktorá správu o činnosti vypracovala sa vlastnoručne podpíše
17. V riadku Schválil - uvedie sa celé meno a priezvisko osoby, ktorá správu schválila (koordinátor klubu/vedúci klubu učiteľov)
18. V riadku Dátum – uvedie sa dátum schválenia správy o činnosti
19. V riadku Podpis – osoba, ktorá správu o činnosti schválila sa vlastnoručne podpíše.