Správa o činnosti pedagogického klubu

Prioritná os:	Vzdelávanie
Špecifický cieľ:	1.2.1 Zvýšiť kvalitu odborného vzdelávania a prípravy reflektujúc potreby trhu práce
Prijímateľ:	Stredná priemyselná škola technická, Komenského 5, 085 42 Bardejov
Názov projektu:	**Inovujeme a vzdelávame pre prax**
Kód ITMS projektu:	**312011Z527**
Názov pedagogického klubu:	**14b Klub učiteľov FG**
Dátum stretnutia pedagogického klubu	14.06.2022
Miesto stretnutia pedagogického klubu	Stredná priemyselná škola technická, Komenského 5, 085 42 Bardejov
Meno koordinátora pedagogického klubu	Mgr. Dana Janečková
Odkaz na webové sídlo zverejnenej správy	https://iavpp.spsbj.sk

Téma stretnutia:

Komunikácia s bankou osobným, písomným a elektronickým spôsobom

Rámcový program stretnutia: Problémy a východiská

Kľúčové slová:

- Banka a jej základné princípy
- Elektronické bankovníctvo
- Implementácia pojmov - finančný sprostredkovateľ, poradca, hypotekárny poradca, elektronické komunikácia,

HLAVNÉ BODY, TÉMY STRETNUTIA, ZHRNUTIE PRIEBEHU STRETNUTIA:

1) Oboznámenie členov s aktuálnym programom:
   a) Východzí dokument - Národný štandard finančnej gramotnosti verzie 1.2
   b) Aktivity, metódy a formy podporujúce upevnenie používaných pojmov z Finančnej gramotnosti
2) Zhodnotenie práce klubu za minulý mesiac
3) Analýza komunikácie s bankou

Na základe osobných skúseností zistiť využívanie elektronickej komunikácie s bankou
Na základe všeobecného prehľadu zistiť možnosti komunikácií s bankou a bankovými subjektmi

Krátka anotácia:

Témou stretnutia bola príprava otvorenej hodiny, v rámci ktorej by sa spracovala téma z oblasti finančnej gramotnosti - Komunikácia s bankou osobným, písomným a elektronickým spôsobom. Pri napĺňaní programu stretnutia členovia vychádzali okrem metodiky a základných zásad vyučovacieho procesu aj z Metodiky pre zapracovania a aplikácie tém finančnej gramotnosti do školských vzdelávacích programov stredných škôl a dlhodobej analýzy finančného trhu. Výber témy vychádzal z aktuálnej národohospodárskej situácie.

V priebehu stretnutia sa vychádzalo z materiálov Európskej centrálnej banky https://www.ecb.europa.eu/ecb/orga/transparency/html/eb-communications-guidelines.sk.html, jej organizácie, transparentnosti, štatistík, zo štatistík z predchádzajúcich rokov, ktoré porovnávali intenzitu komunikácie bánk na SVK - https://www.2muse.sk/sk/blog/komunikacia-bank-v-roku-2018, elektronického bankovníctva a vysvetlenia pojmov s ním spojených - https://totalmoney.sk/slovnik/E/elektronicke-bankovnictvo/, a porovnania bežných účtov a balíkov služieb v jednotlivých bankách - https://totalmoney.sk/bezne-ucty, a vlastnej tvorby.

1. **Úvod**

   V úvode sme si vysvetlili základne pojmy, ekonomické pojmy, potreby a statky, rozdelenie bánk v systéme NBS a ECB.

2. **Výber témy**

   Bol závislý od aktuálnej situácie komunikácie s bankou mladých ľudí (študenti od 16 - 23r.) dospelých a seniorov.

3. **Zoznámenie sa s Kódexom bankovej etiky**

Elektronické bankovníctvo a jeho rozdelenie

Forma bankovníctva, pri ktorej nedochádza k priamemu kontaktu medzi bankou a klientom a pri ktorej sú zároveň ako komunikačný nástroj využívané moderné telekomunikačné technológie (internet, mobilné telefóny, pevné linky, faxy). Identifikácia klienta je zabezpečovaná zadaním mena, hesla, rodného čísla, PIN kódu, údajov z GRID karty a pod. Prostredníctvom elektronického bankovníctva je možné realizovať pasívne operácie, poskytujúce všeobecné informácie napr. o zostatku na účte, kurzové lístky a pod., alebo aktívne operácie, umožňujúce disponovať s prostriedkami uloženými na účte klienta.

V ponuke služieb v oblasti elektronického bankovníctva sú:

Internet banking – komunikácia klienta s bankou prostredníctvom internetu, pričom

môže byť buď pasívny alebo aktívny.

Demo verzie Internet bankingu v jednotlivých bankách nájdete v časti Viac o bežných účtoch - elektronické bankovníctvo.

Mobil banking – všeobecný termín používaný pre realizáciu pasívnych alebo aktívnych bankových operácií prostredníctvom mobilného telefónu. Pod mobil banking spadá SMS banking, WAP banking, GSM banking, SIM Toolkit banking a pod.

SMS banking – komunikácia klienta s bankou cez SMS správy, ktorá môže byť buď pasívna (informatívna) alebo aktívna (realizácia aktívnych operácií s prostriedkami uloženými na účte klienta).

Home banking - služba, ktorá umožňuje komunikáciu medzi klientom a bankou prostredníctvom prepojenia osobného počítača klienta, ktorý je vybavený špeciálnym softwarom (aplikáciou) banky.

Telephone banking (telefón banking) – služba umožňujúca klientovi komunikovať s bankou prostredníctvom telefónneho aparátu s tónovou voľbou, možnosťou spojenia s hlasovým informačným systémom alebo s operátom.

GSM banking – umožňujúci pasívne alebo aktívne operácia s účtom prostredníctvom GSM mobilnej siete. V GSM bankingu môže prebiehať komunikácia medzi klientom a bankou formou zašifrovaných alebo nezašifrovaných textových správ, WAPu alebo JAVA. V prípade zašifrovaných textových správ sa využíva napr. technológia SIM Toolkit, pri ktorej sa do mobilného telefónu vloží špeciálna SIM Toolkit karta s nahratou bankovou aplikáciou, ktorá zabezpečí odoslanie zašifrovaných správ a odšifrovanie prijatých správ. V prípade nezašifrovaných SMS správ je možné využiť všetky druhy SIM kariet. Komunikácia s bankou je potom založená na princípe odosielania a prijímania klasických krátkych textových správ, pričom bezpečnosť je postavená buď len na zadaní PIN kódu ku konkrétnej SIM karte alebo využití tzv. autentizačných kalkulátorov.

Mail banking – zasielanie mailových správ o operáciách na bežnom účte na e-mail klienta.

WAP banking - využitie mobilného telefónu s možnosťou pripojenia na internet prostredníctvom aplikácie WAP s následným realizovaním aktívnych alebo pasívnych operácií cez WAP.

Komunikácia:

Táto časť stretnutia bola vedená s prihliadnutím a využitím bakalárskej práce z katedry financií

a bankovníctva Bankového inštitútu vysokej školy Praha - https://is.ambis.cz/th/jfluo/BP_Misulova_Jana.pdf

http://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2018/05-2018/05_biatec5_sedliakova.pdf

Bezpečnosť na internete:

Aké sú najčastejšie hrozby na internete?

Hrozby internetu zasahujú do mnohých oblastí. Krádež peňazí a osobných údajov je pritom najčastejším, no nie jediným cieľom kybernetických útočníkov.

Poznať treba najmä phishing a smishing, napríklad e-mailom, ktorých cieľom je získať bankové detaily a zneužiť ich (**Phishingový test – https://safelab.sk/phishingovy-test/start,** https://www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html).
Na uvedených stránkach nájdete testy, ktorými si žiaci môžu overiť, ako správne postupovať pri podobných emailoch, ktoré si môžu nájsť v svojej schránke.

Túto aktivitu je vhodné zaradiť v úvode hodiny, následne vysvetliť , či upresniť už známe pojmy, s ktorými sa bežne v médiách žiaci stretávajú a korekciu ich nesprávnych riešení osvojiť si potrebné postupy smerujúce k bezpečnému používaniu internetových bankových produktov.

Ďalším veľmi bežným útokom na Slovensku sú podvodné telefonáty. Útočníci sa tvária ako polícia či zamestnanci banky, čo pôsobí veľmi dôveryhodne, a snažia sa od vás vymámiť citlivé údaje.

Tieto útoky sú zamerané najmä na dospelých, ktorí vlastnia bankové účty. Nebezpečenstvo však číha aj na deti, ktoré majú prístupy alebo platobné karty. Časté sú napríklad útoky v hrách. Internetový podvodník dieťaťu sľúbi znásobenie virtuálnych peňazí v hre a vypýta si od neho prístupy do hry. Následne vybieli skutočný účet cez pridanú kartu.

Bezpečnosť pri online platbách a transakciách

Rýchlemu technologickému pokroku sa musia prispôsobiť aj bezpečnostné opatrenia. Dnes je potrebné každú platbu na internete potvrdiť, no aj napriek tomu môžete jednoducho prísť o peniaze.

Odporúčanie:

- **Vždy si dôkladne preverte, koľko peňazí a kam posielate**. Nikdy neobchádzajte oficiálne spôsoby platby pre prísľub zľavy alebo zisku.
- **Nastavte si v telefóne notifikácie o všetkých platbách,** ktoré si v prípade zneužitia môžete všimnúť, keď už bude neskoro.
- Udržujte si **základný prehľad** o svojich financiách a kontrolu nad nimi.

Ako nakupovať na internete bezpečne

Buďte obozretní pri nakupovaní z neznámeho obchodu alebo pri príliš výhodných ponukách. Na stránke predajcu by mali byť vždy uvedené kontaktné údaje a názov spoločnosti, ktorý si môžete overiť v obchodnom registri. **Spoľahlivým ukazovateľom sú aj reálne skúsenosti ľudí, ideálne tých, ktorých poznáte**. Ak je recenzií na konkrétny obchod málo, majte na pamäti, že recenzie na webe môžu byť aj vymyslené, resp. podhodené útočníkom. Pomôže vám i zoznam rizikových e-shopov na stránke Slovenskej obchodnej inšpekcie.

https://www.tatrabanka.sk/predigitalnubezpecnost/test-digitalnej-bezpecnosti/

Najdôležitejšie bezpečnostné pravidlá #predigitalnubezpecnost
Pre elektronické bankovníctvo:

1. Vždy si dobre skontrolujte adresu na prihlásenie sa do Internet bankingu.

- Pri prihlasovaní sa do Internet bankingu si vždy prekontrolujte URL adresu danej banky. Všímajte si, či je uvedená presne, bez vložených znakov či slov navyše, a či neobsahuje preklepy.
- Internet banking nevyhľadávajte cez vyhľadávače, keďže medzi prvými vyhľadanými sa môže nachádzať platená reklama podvodníkov, ktorá vás presunie na falošnú stránku podobnú tej pravej.
- Využívať môžete aj prihlasovanie sa cez odkaz, ktorý ste si uložili medzi svojimi obľúbenými stránkami.
- Prihlásenie sa do Internet bankingu môžete zrealizovať aj bezpečným presmerovaním z oficiálnej stránky banky.

2. Banka od vás nikdy nepýta citlivé údaje, prihlasovacie kódy ani údaje o karte prostredníctvom komunikácie cez e-mail, SMS alebo četovacie služby.

- V prípade, že od vás niekto pýta akékoľvek prihlasovacie údaje do Internet bankingu alebo mobilnej aplikácie, kódy z Karty a Čítačky danej banky alebo číslo karty, zamyslite sa, či to je skutočne vaša banka. Porozmýšľajte, kto to od vás žiada, prečo to robí a čo tým chce získať.
- Nenechajte sa nalákať a ani nekonajte pod nátlakom. Radšej si zavolajte do banky a preverte danú situáciu.

3. Realizujte iba také nákupy, registrácie a platby, ktoré chcete uskutočniť na základe vlastnej iniciatívy.

- Všímajte si podozrivé znaky mailov a správ v četovacích službách, ktoré vás nabádajú na platbu, prevzatie výhry, podozrivo výhodnú kúpu či príspevok na dobročinné účely. Takéto správy sú často odoslané zo zvláštnych e-mailových adries, obsahujú gramatické nepresnosti alebo sú podozrivo naliehavé či apelujúce na vykonanie pre vás neobvyklej aktivity.
- Všímajte si, či od vás tretia strana nechce detaily, ktoré pri vykonávaní podobných akcií nie sú potrebné a ktoré bežne nikomu neposkytujete.
- Na prevzatie výhry určite nie je potrebné uvádzať číslo svojej karty alebo iné bankové údaje.

Pre platby kartou na internete:

1. Údaje z platobnej karty, ako i kód na potvrdenie platby (tzv. 3D Secure kód) používajte vždy len na potvrdenie konkrétnej platby kartou, ktorú vy sami práve realizujete.

- Ak od vás niekto žiada číslo karty, exspiráciu, CVV a potvrdzovací kód, aby vám napríklad mohol poslať peniaze, je to určite podvodník. Ak ste mu už údaje z platobnej karty poskytli, bezodkladne ju zablokujte.
- Ani banka od vás nikdy nevyžaduje potvrdenie prijatej platby na váš účet bezpečnostným kódom.
- Pri platbách kartou na internete používajte jednorazové číslo karty, ktoré si jednoducho vygenerujete v mobilnej aplikácii príslušnej banky, a to pre každý nákup zvlášť.

2. Pri potvrdzovaní platieb kartou cez internet si vždy dôsledne skontrolujte presnú sumu a názov obchodníka.

- Ak ste boli pri platbe na webovej stránke vyzvaný na prepísanie bezpečnostného kódu zaslaného do SMS, aplikácie alebo Internet bankingu, banka vám v správe vždy uvedie

presnú sumu a názov obchodníka, u ktorého realizujete nákup. Čítajte pozorne, akú správu vám banka poslala a všímajte si aj desatinné čiarky uvedené v sume.
- V prípade, že sa názov obchodníka alebo iné údaje v autorizačnej správe nezhodujú s tým, čo je uvedené na webovej stránke, a nepoužili ste jednorazovú platobnú kartu, odporúčame bezodkladnú blokáciu karty.

3. Bezpečnostný kód určený na aktiváciu služby Apple Pay alebo Google Pay nikdy nezadávajte na žiadnej webovej stránke, telefonicky ani do žiadnej aplikácie podobnej platobnej bráne. Obchodník ho na spracovanie platby nepotrebuje a nemá dôvod žiadať ho od vás.
- Ak bezpečnostný kód od vás žiada ktokoľvek na účel pripísania platby alebo overenia transakcie, je to vždy podvodník. Ak ste mu už platobné údaje poskytli, kartu bezodkladne zablokujte.
- Bezpečnostný kód určený na aktiváciu služby Apple Pay alebo Google Pay, ktorý vám bol zaslaný do mobilnej aplikácie alebo Internet bankingu, použite výlučne iba v situácii, keď si vedome pridávate novú platobnú kartu do elektronickej peňaženky alebo si aktivujete túto službu (aplikáciu) na novom zariadení.
- Pridanie platobnej karty do aplikácie Google Pay/Apple Pay iniciujte vždy radšej priamo z mobilnej aplikácie príslušnej banka.

ZÁVERY A ODPORÚČANIA:

1. Odporúčame, aby sa členovia klubu, ktorí sa v rámci tejto témy vzdelávali, kládli dôraz na zvýšenú bezpečnosť pri komunikácií.

2. Pri tvorbe aktivít v rámci vyučovania vychádzajúcich z kladenia otázok, by učitelia mali brať na vedomie potrebu tvorby otázky:
- s dôrazom na aktívne zapojenie študentov,
- s dôrazom na kritické myslenie,
- na aktuality v oblasti bezpečnosti na internete.

Vypracoval (meno, priezvisko)	Mgr. Dana Janečková
Dátum	15.06.2022
Podpis	
Schválil (meno, priezvisko)	Ing. Jaroslav Bujda
Dátum	15.06.2022
Podpis	

Koordinátorka klubu učiteľov Finančnej gramotnosti vypracovala zápisnicu na základe podkladov k danej téme stretnutia podľa schváleného plánu.

Príloha 1: Prezenčná listina zo stretnutia pedagogického klubu
Príloha 2: Test bezpečnosti pri platbách na internete