PÍSOMNÁ PRÍPRAVA NA VH

I.

Predmet: Informatika	**Škola:** Gymnázium Edity Steinovej
Ročník: 3.	**Vyučujúci:** Michal Puheim
Tematický celok: Internetové služby	**Dátum:** -
Téma: Bezpečnosť na internete	**Medzipredmetové vzťahy:** Náuka o spoločnosti
Typ vyuč. hodiny: základný (kombinovaný)	**Poradie vyuč. hodiny:** -

II.

Špecifické ciele vyuč. hodiny:	**kognitívne:** Porozumieť: Definovať hrozby na internete Aplikovať: Chrániť sa pred hrozbami na internete pomocou dostupných prostriedkov Aplikovať: Bezpečne používať internetové služby Aplikovať: Mať pod kontrolou prístup k svojim účtom a dátam
	afektívne: Vnímať: Uvedomiť si akým spôsobom môžeme byť na internete ohrození. Reagovať: Správať sa tak, aby sme ohrozenie minimalizovali.
	psychomotorické: žiadne

III.

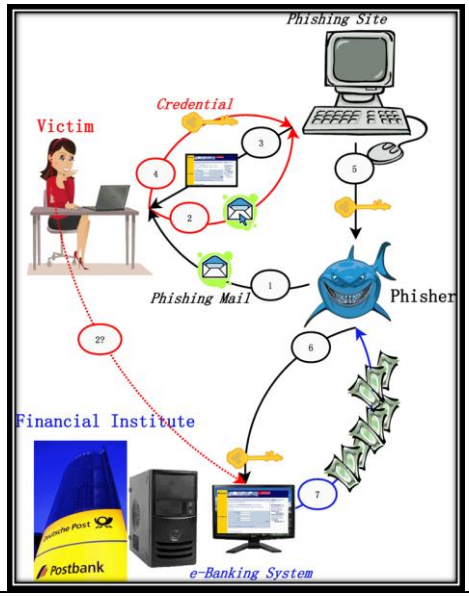
Priebeh VH a metodický postup:	**DZ**	**OFV**	**MDP**	**VM**		**min.**
				U	**Ž**	
1. Organizačná časť	5,7	frontálna	počítač, internet	vysvetľo-vanie	pozoro-vanie	2´
Pozdrav, predstavenie sa, evidencia dochádzky, zápis do elektronickej triednej knihy, oboznámenie žiakov s priebehom hodiny: *„Dobrý deň, žiaci. Na dnešnej hodine sa budeme venovať internetovej bezpečnosti, hrozbám, ktoré nás môžu prostredníctvom internetu ohroziť a aj tomu, ako im predchádzať.“*						
2. Oboznámenie Ž so ŠC VH a vstupná motivácia	1,2,3, 7	frontálna	elektronic-ká tabuľa, 2x PC	demonštrá-cia, vysvet-ľovanie, diskusia	pozoro-vanie, diskusia	8´
U demonštruje útok na počítač prostredníctvom vzdialeného prístupu: *Na úvod si ukážeme názorný príklad útoku na nedostatočne zabezpečený počítač.* U na žiackom PC spustí ľubovoľnú aplikáciu (napr. dokument v editore) *Predstavte si, že pracujete na svojom počítači, napr. na dôležitej záverečnej práci.* U z učiteľského počítača prostredníctvom vzdialeného prístupu prevezme kontrolu nad napadnutým počítačom *A zrazu vás operačný systém odhlási – a netušíte, čo sa deje.* U zobrazí spustenú aplikáciu z napadnutého počítača na elektronickej tabuli. *Pritom vašu prácu má už k dispozícii niekto iný.* U diskutuje so žiakmi na nasledujúce otázky: *Ako bolo možné sa k počítaču pripojiť?* *Prečo to bolo možné?* *Ako by podobný prístup mohol získať útočník?* U vysvetlí, aký postup použil pre pripojenie k počítaču: *Pripojenie vzdialenej plochy (remote desktop connection) – štandardná súčasť OS* *Znalosť IP adresy počítača (alebo jej uhádnutie)*						

Prístup do vnútra siete v učebni (prípadne verejná adresa) U vysvetlí, prečo bol prístup k počítaču možný: *Chýbajúce heslo používateľa „Študent“* *Povolenie prístupu cez vzdialenú plochu (ktorý je štandardne zakázaný)* *Nastavenie výnimky vo firewalle* U vysvetlí, ako by mohol útočník zmeniť nastavenie počítača tak, aby získal prístup: *Lenivosť používateľa – účet bez hesla* *Prienik do WIFI siete so slabým zabezpečením (napr. WEP), prípadne verejná IP adresa PC* *Spustenie skriptu, ktorý vypne v registroch OS príslušné zabezpečenie – použitím vírusu/malvéru* U oboznámi žiakov so ŠC VH: *2. Porozumieť: Definovať hrozby na internete* *3. Aplikovať: Chrániť sa pred hrozbami na internete pomocou dostupných prostriedkov* *3. Aplikovať: Bezpečne používať internetové služby* *3. Aplikovať: Mať pod kontrolou prístup k svojim účtom a dátam*						
3. Aktualizácia prv osvojeného učiva	4,5,6	frontálna, individuálna, skupinová	elektronic-ká tabuľa, počítač	pozoro-vanie, diskusia	samostat. práca, diskusia	5´
Pozrime sa, aké možnosti má útočník na umožnenie útoku na počítač. U zobrazí na snímke pojmy reprezentujúce rôzne druhy nevyžiadaného softvéru, ktorý môže narušiť zabezpečenie počítača, vrátane pojmov: *Vírus, Malware, Červ, Bot, Trojan, Hacker* U sa formou diskusie pýta Ž, či dané pojmy poznajú, prípadne, či vedia povedať, čo predstavujú: *Tieto pojmy určite už poznáte. Viete povedať čo približne znamenajú?* U registruje odpovede Ž, prípadné chybné odpovede poopraví. Ak niektorý pojem Ž nedokážu definovať, U nechá odpoveď otvorenú na vysvetlenie v nasledujúcom videu.						
4. Osvojovanie nového učiva	1,3,4, 5,8	frontálna, skupinová, individuálna	elektronic-ká tabuľa, počítače	demonš-trácia, diskusia	pozoro-vanie, diskusia	20´
U spustí video popisujúce uvedené hrozby: https://youtu.be/c34QwtYI40g Po zobrazení videa U spoločne so Ž dodefinuje všetky otvorené definície.						

U uvedie možnosti ochrany pred uvedenými hrozbami:
Demonštrovaná situácia môže pôsobiť znepokojujúco, avšak ako používatelia máme možnosti chrániť sa pred podobnou zmenou bezpečnostných nastavení počítača. Medzi základné formy ochrany patrí antivírus a firewall, ako aj pravidelne aktualizovaný operačný systém. Antivírus zamedzuje spusteniu nevyžiadaného softvéru a firewall jeho preniknutiu do počítača zo siete. Aktualizácie pomáhajú zaplátať prípadné bezpečnostné diery v architektúre operačného systému.
U diskutuje so Ž, či je uvedená ochrana dostatočná:
Otázka je, či je takáto ochrana dostatočná? Vieme spraviť ešte niečo, aby sme svoj počítač neohrozili?
U analyzuje výsledky diskusie, v prípade potreby uvedie dve základné pravidlá bezpečného správania:
Samozrejme, uvedené prostriedky nie sú postačujúce, dôležité je, aby sme sa ako používatelia správali rozumne, teda A) nenavštevovali neznáme a podozrivé stránky a B) neotvárali neznáme a podozrivé emaily. Je to dôležité hlavne preto, lebo antivírusové databázy nemusia nevyhnutne registrovať všetok nebezpečný softvér.

U prejde do ďalšej časti hodiny, teda bezpečnosti internetových služieb.
Zatiaľ sme sa rozprávali najmä o zabezpečení počítača ako takého, ale v súčasnosti používame stále viac rôzne internetové služby a preto je potrebné, aby sme si povedali niečo aj o bezpečnosti v tejto oblasti.

U uvedie a definuje pojem phishing:
V súčasnosti je jednou z najvážnejších hrozieb, tzv. phishing. Phishing je forma útoku ktorej cieľom je získať používateľské údaje potrebné pre prístup k internetovej službe, napr. sociálnej sieti, online hre alebo internet bankingu. Najčastejšie sa realizuje formou podvodnej stránky, ktorá navonok vyzerá rovnako, ako stránka napadnutej služby, ale v skutočnosti ju spravuje útočník.
U uvedie názorný príklad útoku pomocou schémy:
Podvodný email (1) pod zámienkou vyžiada od používateľa prihlásenie do služby, pričom používateľa odkáže na podvodnú stránku (2). Používateľ svojim prihlásením (3) odovzdá útočníkovi svoje prihlasovacie údaje (4, 5) a ten následne presmeruje používateľa na skutočnú stránku služby (6). Útočník prihlasovacie údaje následne zneužije, zvyčajne s cieľom svojho obohatenia (7).



U uvedie možnosti ochrany pred Phishingom:
Pred phishingom sa vieme chrániť najmä osobnou kontrolou URL navštevovanej webovej stránky. Pre pripojenie k stránke by sme mali použiť zabezpečený protokol HTTPS (HyperText Transfer Protocol Secured) a overiť si, či certifikát zabezpečenia webovej stránky je overený uznávanou autoritou (zvyčajne spoločnosťou, ktorá zabezpečuje antivírusové riešenia). Webové prehliadače nás o tejto skutočnosti upozorňujú (zeleným) zámkom pred URL danej stránky. Ak je zámok preškrtnutý alebo ak chýba, pravdepodobne ide o podvodnú stránku.
U uvedie dôležitosť ochrany prístupových údajov k internetovým službám:
V súvislosti s internetovými službami je dôležitá ochrana prístupových údajov. Základným predpokladom je v žiadnom prípade nikomu svoje prihlasovacie údaje neposielať. To platí aj pre komunikáciu s konkrétnou internetovou službou. Pamätajte, že žiadna služba nepotrebuje, aby jej používateľ posielal svoje prihlasovacie údaje, napr. prostredníctvom emailu. Služba vaše údaje pozná a vy ich máte zadávať iba na webovej stránke služby (prostredníctvom zabezpečeného pripojenia), nikdy nie inak. Ďalším pravidlom je vytvoriť dostatočne silné heslo, ktoré nebude možné jednoducho uhádnuť.
U uvedie dôležitosť silného hesla a spôsoby, akými je možné silu hesla odhadnúť:
Ako vypočítame silu hesla?
- Predpokladajme, že dĺžka hesla je n
- Ak použijeme len číslice pre uhádnutie existuje 10^n možností.
- Ak použijeme všetky písmená v abecede dostaneme 26^n možností (anglická abeceda), resp. 46^n možností (slovenská abeceda vrátane diakritiky).
- Ak použijeme všetky ASCII znaky (.,(){}[]+-/ atď.), dostaneme až 256^n možností.*
Ďalšou možnosťou je použiť na odhadnutie sily hesla internetovú službu, napr. http://www.passwordmeter.com/
(Pozor! Do danej služby nezadávajte vaše skutočné heslá, pretože služba nepoužíva zabezpečenie HTTPS!)
U zadá žiakom úlohu vypočítať silu uvedených hesiel a ich overenie v službe passwordmeter:
Pre nasledujúce heslá vypočítajte ich silu a overte ich aj v službe passwordmeter:
- 9857
- ahoj
- Zlomprst29
- 3bodky...
U uvedie možnosť ďalšej ochrany účtu pomocou dvojfaktorovej autentifikácie:
Okrem používateľského mena a hesla umožňujú mnohé informačné služby v súčasnosti aj použitie tzv. dvojfaktorovej autentifikácie, čo je dodatočná forma ochrany, kde používateľ pri každom prihlásení zadáva

okrem hesla aj dodatočný kód, ktorý je mu jednorazovo poslaný napr. prostredníctvom SMS alebo emailu. Ak sa bojíte o bezpečnosť svojho účtu, určite túto možnosť využívajte.
Na záver tejto časti hodiny U upozorní žiakov na potrebu kontroly prístupu k svojim účtom:
Internetové služby sú v súčasnosti navzájom prepojené, napr. Facebook môže mať prístup k vašim údajom na Google+, resp. ku kontaktom v mobile. Rovnako, keď ste pracovali so službou IFTTT, udelili ste jej prístup ku svojmu účtu. Ako používatelia môžete prístup rôznych aplikácií a služieb k vašim účtom kontrolovať prostredníctvom nastavenia účtu. Vo vlastnom záujme si tieto nastavenia pravidelne kontrolujte vo všetkých dôležitých internetových službách a v prípade, že v zozname uvidíte aplikácie, ktoré nepoznáte, zakážte im prístup.
U zobrazí na snímke prezentácie adresy smerujúce k nastaveniam prístupu pre najvýznamnejšie internetové služby.

5.upevňovanie a prehlbovanie nového učiva	2,5,6	frontálna, skupinová, individuálna	elektronic-ká tabuľa	pozorova-nie, rozprá-vanie, roz-hovor	samostat. práca, pozoro-vanie, rozhovor	14´

Samostatná práca Ž pri kontrole účtov používaných internetových služieb. U odpovedá na prípadné otázky žiakov.

Frontálna sumarizácia obsahu VH a kontrola naplnenia cieľov VH rozhovorom U so žiakmi:
Hrozby na internete:
- Malvér, vírusy, červy, hackeri...
Ochrana pred hrozbami:
- Antivírus, Firewall, (NAT) + nerobiť hlúposti
Bezpečne používať internetové služby
- certifikované HTTPS, silné heslo, 2-faktorová autentifikácia
Mať pod kontrolou prístup k svojim účtom a dátam
- obmedzením podozrivých aplikácií a služieb v nastaveniach účtu

6. Záverečná etapa	7	frontálna	-	rozprávanie	pozoro-vanie	1´
U zhrnie prebrané učivo, udelí pochvaly/napomenutia a pozdravom ukončí VH.						
Učebné zdroje: - Školská učebnica Informatiky, Internet						

Vysvetlivky: DZ (Didaktické zásady): **1.** systematickosti a sústavnosti; **2.** trvácnosti; **3.** vedeckosti; **4.** individuálneho prístupu; **5.** uvedomelosti a aktivity; **6.** názornosti; **7.** jednoty teórie a praxe, **8.** utvorenia optimálnych podmienok pre vyučovací proces, **9.** primeranosti, **10.** zamerania vyučovacieho procesu pre všestranný rozvoj osobností žiakov **11.** motivácie; **OFV** (Organizačné formy výučby): **a** - frontálna, **b** - skupinová, **c** - individuálna; **MDP** (Materiálne didaktické prostriedky); **VM** (Vyučovacie metódy); **U** (učiteľ); **Ž** (žiak)

IV. PRÍLOHY

- prezentácia (PowerPoint), formulár k písomke