Co-funded by the
Erasmus+ Programme
of the European Union

INOVATÍVNE VZDELÁVACIE NÁSTROJE

VIRIBUS UNITIS

FUNDACJA ROZWOJU REGIONALNEGO

TÉMA: „BEZPEČNOSŤ V SIETI”

Tomasz Zacłona

Monika Makowiecka

I. Odôvodnenie výberu témy

Vedomosti o hrozbách na internete a spôsoboch, ako im zabrániť, sú v súčasnosti jedným z najdôležitejších problémov súvisiacich s používaním počítača. V dnešných časoch je internet nevyhnutnou súčasťou každodenného života.

Vlastnenie antivírusového programu v svojom počítači, notebooku, či telefóne sa určite oplatí a odporúča. A to z jednoduchého dôvodu: antivírusový program zničí väčšiu časť vírusov: malware, trojských koní a iných hrozieb, ktoré číhajú na každého užívateľa internetu v sieti.

II. Všeobecné vzdelávacie ciele

- Dať žiakom šancu, aby sa oboznámili s hrozbami, ktoré na nich číhajú pri používaní internetu a počítača.
- Dôležitým prvkom témy je tiež naučiť sa, ako čeliť existujúcim hrozbám.

III. Tematický rozsah hodín

1. Bezpečnosť v sieti
2. Ktoré témy súvisia s bezpečnosťou v sieti?
3. Hrozby na internete
4. Čo je to antivírus?
5. Spôsoby, ako byť na internete v bezpečí
6. Cvičenia

IV.Metódy vedenia hodín

1) Miniprednáška (na základe prezentácie)
2) Ilustračné materiály – interaktívny film
3) Práca pod vedením
4) Práca v skupine

1. Bezpečnosť v sieti

Pojem „bezpečnosť v sieti" sa týka každej činnosti, cieľom ktorej je chrániť použiteľnosť a integritu údajov na našom počítači.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

- Bezpečnosť mobilných zariadení
- Bezpečnosť aplikácií
- Kontrola prístupu
- Antivírusový softvér
- Zabezpečenie úniku údajov
- Zabezpečenie e-mailu
- Brány firewall

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Bezpečnosť mobilných zariadení

Kybernetické útoky sa čoraz viac zameriavajú na mobilné zariadenia – nie je na tom nič zvláštne, vzhľadom na ich rastúcu popularitu.

Uchovávajú naše osobne údaje, sú prepojené so sociálnymi sieťami, webovými stránkami a bankami.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Bezpečnosť aplikácie

Akýkoľvek softvér, ktorý používate a ktorý je pripojený k Vašej sieti, by mal byť chránený.

Myslite tiež na to, že aplikácie môžu obsahovať chyby v zabezpečení, ktoré môžu útočníci využiť na prienik do Vašej siete.

Nebojte sa, existujú ochranné aplikácie, ktoré tieto medzery vyplnia.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Kontrola prístupu

POZOR! Nie každý užívateľ by mal mať prístup k Vašej sieti!

Aby ste znížili riziko neoprávneného vstupu, je potrebné kontrolovať každého užívateľa a každé zariadenia.

Neautorizované zariadenie je možné odmietnuť alebo vpustiť len s obmedzeným prístupom.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Antivírusový softvér

Počítačové vírusy, červy a trójske kone, čiže špionážne softvéry útočia na našu sieť alebo na naše zariadenia a infikujú ich činnosť.

Antivírusové programy by mali vyhľadávať a bojovať proti škodlivým aplikáciám a okrem toho sledovať infikované súbory, aby našli anomálie alebo diaľkovo ovládaný škodlivý softvér.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Prevencia úniku údajov

Firmy a združenia musia uchovávať citlivé informácie v bezpečí a zabrániť, aby ich mohli zdieľať pracovníci.

Také technológie ako Data Loss Prevention (DLP) brania prenosu citlivých údajov.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Bezpečnosť e-mailov

Brány elektronickej pošty sú miestom, kde dochádza k najväčšiemu narušenia bezpečnosti.

Útočníci využívajú osobné informácie a sofistikované taktiky na klamanie a infikovanie príjemcu. Bezpečnostné e-mailové aplikácie blokujú prichádzajúce útoky a kontrolujú aj odchádzajúce e-maily.

2. Ktoré témy súvisia s bezpečnosťou v sieti?

Brány firewall

Brány firewall sú bariéry, ktoré staviame medzi našou dôveryhodnou sieťou a vonkajšou sieťou, takou ako internet.

Určujú zásady filtrovania. Firewall môže byť softvérový, hardvérový a existujú aj hybridné riešenia.

3. Hrozby na internete

- Kybernetická šikanovanie
- Závislosť
- Nebezpečné obsahy(šikanovanie)
- Porušenie zákona
- Krádež osobných údajov
- Vlámania do počítača
- Technické hrozby(vírusy)
- Krádež citlivých informácií

3. Hrozby na internete

Kybernetické šikanovanie

Je to vlastne kybernetická hrozba.

Medzi také činnosti napríklad patrí: nadávanie, zastrašovanie, alebo ponižovanie niekoho na internete. Príkladom kybernetického šikanovania je aj to, že niekomu urobíte fotografiu a potom ju bez jeho súhlasu uverejníte a posielate ďalej.

3. Hrozby na internete

Závislosť

Počas využívania internetu si musíte uvedomiť hrozby, ktoré na Vás číhajú.

Jednou z nich je aj závislosť na internete, ktorá sa môže týkať aj Vás.

3. Hrozby na internete

Nebezpečný obsah

Veľká časť obsahu dostupná na internete je násilná a má negatívny vplyv na psychiku, predovšetkým mladého užívateľa.

3. Hrozby na internete

Porušenie zákona

Dávajte si pozor na stránky, ktoré ponúkajú výhru za malý poplatok alebo Vás informujú, že Vás vylosovali a vyhrali ste milión dolárov!

Je to trik!

3. Hrozby na internete

Krádež osobných údajov

Je mnoho stránok, ktoré sa snažia neoprávnene získať Vaše údaje. Napríklad si pýtajú heslo do vášho elektronického bankovníctva.

Vlámanie sa do počítača

Toto je jedna z najbežnejších hrozieb.

Myslíte si, že ak máte počítač doma a dom má dobré dvere a spoľahlivý zámok, tak sa Vám nikto do počítača nevláme?

Omyl!

Všetko sa deje na diaľku!

3. Hrozby na internete

Technické hrozby (vírusy)

Pri používaní počítača s prístupom na internet, sme vystavený nebezpečenstvu tzv. vírusov, čiže programov, ktoré sú určené na to, aby poškodili Váš počítač.

Tieto vírusy môžu vymazať údaje, vypnúť počítač, prehrávať nežiadúce zvuky, spomaliť počítač, kradnúť informácie, ktoré sa nachádzajú na disku.

3. Hrozby na internete

Technické hrozby (vírusy)

Medzi nebezpečné vírusy patrí trójsky kôň, ktorý sleduje Vaše aktivity a umožňuje ovládať váš počítač inými osobami.

Druhým, rovnako populárnym vírusom je tzv. červ, čiže program, ktorý tvorí svoje vlastné kópie. Jeho činnosťou dochádza ku zmenšovaniu miesta na disku, ktoré môžete využiť pre svoje potreby.

Phishing dôverných informácií

Internet o Vás vie viac, než si myslíte, stačí, že sleduje stránky, ktoré ste navštívili. Stačí, že prestanete byť v strehu!

3. Hrozby na internete

Myslite na to, že:

- Príliš časté využívanie internetu môže spôsobiť to, že od neho budete závislý.
- Nainštalujte si na Váš počítač antivírusový program.
- Používajte ťažko uhádnuteľné heslá.
- Kvôli hrozbám na internete buďte opatrný a neuvádzajte o sebe všetky informácie a neposielajte svoje fotky.
- Počas prezerania internetových stránok sa môžete stretnúť s tým, že sa Vás bude snažiť niekto kontaktovať, kto sa bude vydávať za niekoho iného.

4. Čo je to antivírus

Antivírusový program preoseje väčšinou vírusov, červov, trójskych koní a iných hrozieb, ktoré číhajú na každého užívateľa internetu v sieti.

Dobrý antivírusový program je istým nárazníkom medzi hrozbami a každodennou prácou.

4. Čo je to antivírus

Nielen vírusy predstavujú neustálu hrozbu, veľkú škodu môžu spôsobiť aj útoky hackerov.

Pred týmito hrozbami chráni firewall. Bohužiaľ nie všetky antivírusové programy disponujú takým modulom a prenechávajú túto úlohu systémovému nástroju Windows.

4. Čo je to antivírus?

Najväčším zdrojom útokov sa stávajú sociálne siete, z ktorých mimoriadnu hrozbu predstavuje práve Facebook. Najväčšou hrozbou pre užívateľov sú stránky, ktoré sa vydávajú za stránky bánk a také, ktoré dokážu zachytiť čísla bankových účtov, kariet, kreditných kariet alebo číslo PIN.

Bezplatné programy Vás nechránia! Neverte tomu, že si stačí stiahnuť program, ktorý Vám odporúčal sused a všetko bude zabezpečené.

5. Spôsoby, ako byť na internete v bezpečí

- **Heslá, heslá, heslá!** – to je Vaše základné a najdôležitejšie zabezpečenie. V tomto prípade si to nesnažte uľahčiť a neuvádzajte všade jedno a to isté heslo, napríklad dátum narodenia alebo meno svojho štvornohého priateľa. Silné heslo je lepšie zabezpečenie.
- **Pri klikaní na odkazy buďte opatrný** – bežným spôsobom, ako napadnúť súkromie a vytiahnuť údaje je zasielanie emailov, ktoré obsahujú zvláštne prílohy alebo odkazy, na ktoré je potrebné kliknúť. Tak zvaný phishing. Neexistuje jeden stopercentný spôsob na ochranu. Najlepšie je jednoducho dávať pozor a nikdy ich neotvárať.

5. Spôsoby na zachovanie bezpečnosti v sieti

- **Šifrovanie súborov na disku –** disk Vášho počítača obsahuje množstvo cenných informácií a údajov o Vás. Aby boli toto údaje dobre zabezpečené, je potrebné šifrovanie.
- **Dvojstupňové overenie-** Tam, kde je potrebné overenie, napríklad pri internetových platbách, je nevyhnutné dvojstupňové overenie. Čiže okrem prihlásenia sa na danú stránku, si nastavte napríklad kód, ktorý dostanete smskou.
- **Virtual Private Network -** VPN je riešenie, ktoré umožňuje bezpečný prenos dát bez zobrazenia polohy.

5. Spôsoby na zachovanie bezpečnosti v sieti

- **Režim inkognito –** Výber tohto režimu umožňuje nezapisovať históriu prehľadávača a nezobrazuje polohu.
- **DuckDuckGo** – je to názov internetového vyhľadávača, ktorá oveľa lepšie ako Google chráni údaje užívateľov. Má však jednu nevýhodu, jeho výsledky nie sú také precízne.
- **Šifrovacie komunikátory-** Radi veľa píšete a práve cez internet komunikujete so známymi? V takomto prípade využite komunikátor, ktorý šifruje posielané texty.
- **Odhlásenie sa a používanie pseudonymov –** Vždy po ukončení práce by ste sa mali odhlásiť z danej stránky a počítača. Týka sa to tiež používania pseudonymov, ktoré neumožňujú jednoduchú identifikáciu osoby a uvádzania čo najmenej informácií o sebe.

6. Praktické cvičenia

Ďakujem za pozornosť