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

INOVAČNÍ VZDĚLÁVACÍ NÁSTROJE

VIRIBUS UNITIS

FUNDACJA ROZWOJU REGIONALNEGO

Téma: „BEZPEČNOST V SÍTI”

Tomasz Zacłona

Monika Makowiecka

I. Opodstatnění volby tématu

Povědomí o nebezpečí na internetu a způsobech, jak mu předcházet, je v současné době klíčovou záležitostí při používání počítače. Internet je v dnešní době neodmyslitelnou součástí každodenního života.

Je dobré a doporučuje se mít ve svém počítači, notebooku, mobilu antivirový program. Příčina je prostá: antivirový program přefiltruje většinu virů, malwerů, trojských koní a jiných nebezpečí, která číhají na každého uživatele internetu.

II. Obecné cíle výuky

- Umožnění studentům seznámit se s nebezpečími spojenými s používáním počítače a internetu.
- Podstatnou součástí realizace tématu je také seznámení se se způsoby eliminace těchto nebezpěčí.

III. Tématický obsah výuky

1. Bezpečnost v síti
2. K jakým tématům se vztahuje bezpečnost v síti
3. Nebezpečí na internetu
4. Co je to antivirus
5. Způsoby, jak se chovat na internetu bezpečně
6. Cvičení

IV.Metody výuky

1) Mini přednáška (na základě prezentace)
2) Ilustrační materíály – interaktivní film
3) Práce pod vedením
4) Práce ve skupině

1. Bezpieczeństwo w sieci

Pojem „bezpečnost v síti” se vztahuje na každé jednání, které má za cíl chránit použitelnost a integritu údajů v našem počítači.

2. K jakým tématům se vztahuje bezpečnost v síti

- Bezpečnost mobilních zařízení
- Bezpečnost aplikací
- Kontrola přístupu
- Antivirové programy
- Předcházení úniku dat
- Bezpečnost mailů
- Bezpečnostní brány (ang. firewall)

2. K jakým tématům se vztahuje bezpečnost v síti

Bezpečnost mobilních zařízení

Kyberútoky jsou čím dál častěji mířeny proti mobilním zařízením – není se čemu divit, když vezmeme v potaz jejich rostoucí popularitu.

Obsahují naše soukromé údaje, jsou taky propojeny se sociálními sitěmi, servisy nebo bankami.

2. K jakým tématům se vztahuje bezpečnost v síti

Bezpečnost aplikací

Každý software, který používáš a který je napojený na tvou síť, by měl být chráněn.

Pamatuj na to, že aplikace mohou obsahovat mezery v zabezpečení, které můžou útočníci využít k infiltrování sítě.

Neboj se, existují ochranné aplikace, které ty mezery uzavřou.

2. K jakým tématům se vztahuje bezpečnost v síti

Kontrola přístupu

Pozor! Ne každý uživatel by měl mít přístup ke tvé síti!

Abys snížil riziko vniknutí nepovolané osoby, je třeba kontrolovat každého uživatele a každé zařízení.

Neautorizovaná zařízení mohou být odmítnuty nebo jim může být umožněn omezený přístup.

2. K jakým tématům se vztahuje bezpečnost v síti

Antivirový oprogram

Malware (zákeřný softwave) jako jsou viry, červi, trojské koně nebo spyware můžou zaútočit na naši síť nebo zařízení a narušit jejich fungování.

Antivirové programy mají vyhledávat a ničit zákeřné aplikace a také pozorovat narušené soubory, aby našly anomálie nebo dálkově řízený zákeřný software.

2. K jakým tématům se vztahuje bezpečnost v síti

Předcházení úniku dat

Firmy a asociace musí dbát na bezpečnost citlivých informací a nesmí dovolit, aby byly zveřejněny zaměstnanci.

Technologie jako je Data Loss prevention (DLP) zamezují posílání, přeposílání a dokonce i tisk citlivých informací.

2. K jakým tématům se vztahuje bezpečnost v síti

Bezpečnost e-mailů

Brány elektronické pošty jsou místem, kde dochází k největšímu počtu narušení bezpečnosti.

Útočníci využívají osobní informace a vytříbené taktiky, aby oklamali a infikovali adresáta. Aplikace, které zajišťují bezpečnost e-mailů, blokují příchozí útoky a také kontrolují odeslané maily.

2. K jakým tématům se vztahuje bezpečnost v síti

Bezpečnostní brány

Bezpečnostní brány jsou bariéry situované mezi naší důvěryhodnou sítí a externí sítí, jako je Internet.

Určují pravidla, podle kterých filtrují pakety. Brány se můžou opírat o software, hardware nebo být hybridním řešením.

3. Nebezpečí na internetu

- Kybernásilí
- Závislost
- Nebezpečný obsah (násilí)
- Porušování zákona
- Krádež osobních údajů
- Počítačové loupeže
- Technická rizika (viry)
- Vyloudění důvěrných informací

3. Nebezpečí na internetu

Kybernásilí

Je to nebezpečí založené na ubližování na internetu.

K takovému jednání se řadí mj. nadávání, zastrašování nebo ponižování někoho na internetu. Může to být například focení někoho bez jeho souhlasu a následné zveřejňování a rozesílání fotek po internetu

3. Nebezpečí na internetu

Závislost

Při používání internetu si musíš uvědomovat nebezpečí, jaká se můžou objevit během jeho používání.

Jedním z nich je závislost na internetu, která se může týkat i tebe.

3. Nebezpečí na internetu

Nebezpečný obsah

Mnohý obsah dostupný na internetu má známky násilí a má negativní vliv na psychiku, zvláště u mladých uživatelů.

Porušování zákona

Dávej si pozor na stránky, které ti nabízejí výhru při minimálním úsilí nebo ti sdělují, že jsi byl vylosován a právě jsi vyhrál milión dolarů!

Je to podvod!

3. Nebezpečí na internetu

Krádež osobních údajů

Stránky, které jsou obzvlášť podezřelé, jsou ty, které se snaží vyloudit tvé údaje. Například žádají tvoje heslo pro internetové bankovnictví

Počítačové loupeže

Je to jedno z nejčastějších nebezpečí.

Zdá se ti, že když máš počítač doma a dům má dobré dveře a spolehlivý zámek, tak se ti nikdo nemůže vloupat do počítače?

Nemůžeš se víc mýlit!

Všechno probíhá dálkově!

3. Nebezpečí na internetu

Technická rizika (viry)

Během používání počítače s přístupem k internetu existuje nebezpečí stáhnutí virů, čili programů, které byly vytvořeny, aby poškodily tvůj počítač.

Můžou vymazat data, vypnout počítač, přehrávat nežádoucí zvuky, způsobit pomalejší fungování počítače, krást informace z disku.

3. Nebezpečí na internetu

Technická rizika (viry)

Jedním z nejhorších virů je virus zvaný trojským koněm. Je to program, který špehuje, co děláš, a umožňuje jiným lidem kontrolovat tvůj počítač.

Druhým, stejně populárním virem, je tzv. červ, čili program vytvářející svoje kopie. Jeho aktivita způsobuje především ubývání místa na disku, které bys mohl využít pro své účely.

Vyloudění důvěrných informací

Internet o tobě ví víc, než si myslíš, stačí, že sleduje, jaké stránky navstěvuješ, stačí, že přestaneš dávat pozor!

3. Nebezpečí na internetu

Pamatuj:

- Příliš časté používání internetu může vést k závislosti.
- Nainstaluj si na počítač antivirový program.
- Používej hesla, která se dají těžko uhádnout.
- Kvůli nebezpečí v síti buď opatrný a neuváděj všechny informace o sobě a neposílej svoje fotky.
- Během prohlížení internetových stránek můžeš potkat osobu, která se s tebou bude snažit navázat kontakt a bude předstírat, že je někdo jiný.

4. Co je to antivirus

Antivirový program přefiltruje většinu virů, malwerů, trojských koní a jiných nebezpečí, která číhají na internetu na každého uživatele.

Dobrý antivirový program funguje jako jakýsi pufr mezi nebezpečími a každodenní prací.

4. Co je to antivirus

Nejen viry představují stálé nebezpečí, velké škody můžou napáchat také precizně mířené hackerské útoky.

Bohužel ne všechny antivirové programy disponují takovým modulem a tuto část ochrany přenechávají systémovým nástrojům Windows.

4. Co je to antivirus

Největším zdrojem útoků jsou sociální sítě, z nichž Facebook je superrizikový.

Nejbolestivějším nebezpečím jsou pro uživatele stránky vydávající se za banky, které dokážou zachytávat čísla bankovních účtů, kreditních karet nebo PINy.

Bezplatné programy tě vůbec neochrání! Nevěř tomu, že si stačí stáhnout bezplatný program, který ti doporučil soused, a všechno je vyřešené.

5. Způsoby, jak se chovat na internetu bezpečně

- **Hesla, hesla, hesla!** – je to twoje základní a v podstatě nejdůležitější zabezpečení. Nejdi nejjednodušší cestou a nedávej si všude stejné heslo, třeba jméno svého mazlíčka. Silné heslo je rozhodně lepším zabezpečením.
- **Dávej si obzvlášť pozor při otevírání odkazů** – častým způsobem útoku na soukromí a krádeže dat jsou e-maily obsahující divné přílohy nebo nabádající ke kliknutí na nějaký odkaz. Je to tzv. phishing. Neexistuje jeden a navíc stoprocentně účinný způsob obrany. Nejlepší je prostě dávat pozor a nikdy je neotevírat.

5. Způsoby, jak se chovat na internetu bezpečně

- **Šifrování souborů na disku -** tvůj počítačový disk to je spousta cenných údajů a informací o tobě. Abys ho měl dobře zabezpečený, je nezbytné ho šifrovat.
- **Dvouetapová verifikace -** tam, kde je vyžadována verifikace, například při internetových platbách, je nezbytné, aby měla dvě etapy. Takže kromě přihlášení na dané stránce si navíc nastav třeba kód posílaný přes sms.
- **Virtual Privat Network –** VPN je bezpečným řešením, jak posílat údaje bez zveřejňování lokalizace.

5. Způsoby, jak se chovat na internetu bezpečně

- **Anonymní režim** – pokud zvolíš tento režim, tvůj prohlížeč nebude zapisovat historii a ukazovat polohu.
- **DuckDuckGo –** název internetového prohlížeče, který mnohem lépe než Google chrání uživatelské údaje. Má ale jeden mínus, výsledky vyhledávání nejsou tak přesné.
- **Šifrující komunikátory -** rád hodně píšeš a právě přes internet se nejčastěji spojuješ se svými známými? V tom případě používej komunikátor, který šifruje posílaný text.
- **Odhlašování a používání přezdívek -** vždy, když dokončíš práci, by ses měl odhlásit z dané stránky a z počítače. Týká se to také používání přezdívek, které ztěžují identifikaci tvé osoby, a úvádění na internetu co nejméně informací o sobě.

6. Praktická cvičení

Děkuji za pozornost