Bezpečák

ÚKOL:

Zná a dodržuje základy bezpečného chování na internetu (V)

POPIS ÚKOLU:

Na internetu číhá spousta různých hrozeb a tvým úkolem bude naučit se je rozeznávat a umět jim předcházet. Seznam se s pravidly zabezpečení počítače, bezpečného chování na internetu, problematikou nevyžádaných e-mailů (SPAMů), počítačových virů, pravidly tvorby a používání hesel a bezpečným chováním na sociálních sítích. Své znalosti si pak ověříš pomocí testu, který ti zadá vedoucí.

Tip: Nezapomeň, že i na tvém mobilním telefonu se musíš chovat obezřetně, pravidelně jej aktualizovat, instalovat do něj pouze prověřené aplikace a mít v něm antivirový program.

POSTUP:

Bezpečnost na internetu

Pouze počítač či telefon, který není vůbec připojen k internetu, je v relativním bezpečí. Při pohybu na internetu se chovej opatrně, na každém kroku tam na tebe totiž mohou číhat různá nebezpečí (počítačové viry; Phishing – podvodné e-maily; Spam – nevyžádaná pošta; podvodníci, kteří se budou vydávat za někoho jiného a budou ti nabízet přátelství na sociálních sítích; programy, které budou sledovat tvůj pohyb apod.) Důvod, proč jsou na světě miliony počítačových virů je prostý, jejich autoři se snaží dostat k tvým osobním či bankovním údajům a ty pak předprodávají, zneužívají, vydávají se se za tebe a snaží se dostat k tvým penězům. Mnozí to však dělají jen pro radost a své potěšení někomu škodit. Počítač či telefon by pro přístup k internetu měl být pravidelně aktualizován a měl by na něm být nainstalován aktualizovaný antivirový program. Ve Windows 10 je základní antivirový program Windows Defender přímo součástí systému. Mezi další bezplatné antiviry se řadí český Avast Free, který našim potřebám určitě vyhovuje. Existují i placené antivirové programy, které poskytují komplexnější úroveň zabezpečení např. slovenský program ESET Smart Security, český Avast Internet Security či ruský Kaspersky Internet Security.

Bezpečné chování v e-mailu

Pokud mi je doručen e-mail od neznámé „podezřelé“ osoby, neočekávaný e-mail či e-mail v cizím jazyce či napsán lámanou češtinou, tak bych měl zpozornět. Platí pravidlo, že pokud si nejsem jistý o co se jedná, tak bych e-mail neměl vůbec otevírat a raději jej smazat. V dnešní době není pro útočníka problém dokonce podvrhnout e-mailovou adresu a vydávat se za kohokoliv. Buď ve střehu, za e-mailem od tvého kamaráda se může skrývat klidně nějaký útočník či virus, který se snaží šířit internetem. Velmi nebezpečné bývají v takovýchto virech přílohy (často se jedná o Word či PDf dokument, který se tváří jako faktura/dokument z banky/informace doručovací služby apod.), které mohou obsahovat škodlivý kód, který může znepřístupnit obsah celého tvého počítače. Velmi často se také vyskytují e-maily, které se tváří jako zpráva z banky, facebooku či jiné internetové služby, které tě žádají o zadání přihlašovacích údajů či změnu hesla. Tyto e-maily často vypadají velmi věrohodně (obsahují stejnou grafiku, kterou používá ona banka či facebook a také obsahují odkaz na věrně vypadající stránku, na které bychom změnu hesla měli provést).

Takovýmto e-mailům se říká Phishing (česky něco jako „rhybaření“) a jsou to jedny z nejzákeřnějších a současně z pohledu útočníka neúspěšnějších bezpečnostních rizik.

Abychom předešli problémům s doručováním nevyžádané pošty, tak je dobré neříkat svou e-mailovou adresu nikomu, koho neznáme a nechceme od něj dostávat poštu. Totéž platí pro uvádění naší e-mailové adresy na internetu (např. na facebooku či instagramu, při registraci do různých internetových služeb, při nákupu na e-shopech apod.). Je doporučeno nepřihlašovat se ke svému e-mailu na cizích počítačích či telefonech. Takové zařízení může obsahovat „vir“, který získá tvé přístupové údaje a pak je může zneužít např. pro rozesílání Spamu. Pokud se přihlašuješ do e-mailu, tak tě počítač či telefon vyzve k tomu, zda si má zapamatovat přístupové údaje. Svému počítači to dovolit můžeš, ale na počítači ve škole či na kamarádově telefonu vždy pamatování hesla zakazuj, jinak se k tvému e-mailu bude moci přihlásit někdo cizí. Nezapomeň používat bezpečné heslo a pravidelně si jej měnit.

Bezpečnost hesel:

Bezpečné heslo by mělo být alespoň 12 znaků dlouhé, mělo by obsahovat malá i velká písmena, čísla a speciální znaky, heslo bychom neměli používat na více místech a ani jej někomu sdělovat. Heslo bychom si měli pamatovat (neměli bychom si jej nikam zapisovat) a pravidelně jej měnit. Nejlepší hesla jsou taková, která „nejsou existující slova“ (na tyto cílí automatické slovníkové útoky), ani nejsou pro tvé okolí lehce uhodnutelná (např. jméno pejska, adresa bydliště či něco jiného, co s tebou souvisí a hrozí, že by to někdo, kdo tě zná, mohl jednoduše uhádnout) a současně jsou pro tebe snadno zapamatovatelná. Občas se stává, že některé internetové službě dokonce uniknou hesla jejích uživatelů a pokud si heslo pravidelně neměníš, tak se může tvého účtu někdo zmocnit („pravidelně“ se to stává např. Facebooku). Z tohoto důvodu je také dobré, aby se hesla pro přístupy do různých služeb neopakovala. Délka hesla souvisí se schopnostmi útočníků a výpočetní silou počítačů např. heslo, které obsahuje 8 znaků (malá a velká písmena, čísla a speciální znaky) a ještě nedávno bylo považováno za bezpečné, se s využitím velmi výkonné skupiny počítačů podařilo uhádnout pomocí útoku „hrubou silou“ za méně než 6 hodin.

Moderní služby jsou si všech těchto rizik vědomy a proto dnes již zabezpečení pouhým heslem mnohdy nestačí. Některé služby to dělají tak, že po uživateli vyžadují kromě hesla také další ověření (např. speciální aplikací či otiskem prstu na mobilní telefonu), jinde má uživatel možnost zadat heslo pouze několikrát (např. 10x) a pokud neuspěje, tak dojde k trvalému zablokování služby. Tyto metody jsou často velmi účinné, podobně je například chráněna i platební karta (obsahuje velmi jednoduchý PIN, který má často pouze 4 číslice, ale pokud jej uživatel zadá 5x chybně, tak dojde k jejímu zablokování).

Způsobů, jak vytvořit bezpečné heslo je více, můžeme si nechat heslo vygenerovat aplikací, ale taková hesla jsou často velmi špatně zapamatovatelná, lepší je použít např. jednu z následujících technik:

- Metoda zvláštní fráze
  Výsledné heslo je dostatečně dlouhé zapamatovatelné a vznikne skládáním několika slov a písmen
  Příklad hesla: KadaoZukalova18-Streda16:00

- Metoda známé věty
  Výsledné heslo je opět dostatečně dlouhé zapamatovatelné a vznikne skládáním několika písmen z každého slova určité věty.
  Příklad hesla: MaRaKa,ByNaZuk18.
  (Heslo vzniklo z věty: Mám rád kafe, bydlím na Zukalově 18.)

Při tvorbě hesla není bezpečné používat ani shluky písmen, které sousedí na klávesnici. Bezpečné heslo nevznikne ani složením jména, příjmení data narození či rodného čísla (všechny tyto údaje jdou „nějak“ dohledat a útočníci se při pokusu o uhádnutí hesla zaměřují na jejich kombinace).

PRAVIDLA PRO DĚTI K BEZPEČNĚJŠÍMU UŽÍVÁNÍ INTERNETU:

1. Nikdy nesděluj adresu svého bydliště, telefonní číslo domů nebo adresu školy, kam chodíš, jména a adresy rodičů a rodinných příslušníků i jejich telefonní čísla do práce, někomu, s kým jsi se seznámil/a prostřednictvím internetu, jestliže Ti to rodiče (nebo lidé, kteří se o Tebe starají) přímo nedovolí.

2. Pokud se neporadíš s rodiči, neposílej nikomu po internetu fotografii, číslo kreditní karty nebo podrobnosti o bankovním účtu a vůbec žádné osobní údaje.

3. Nikdy nikomu, ani nejlepšímu příteli, neprozraď heslo nebo přihlašovací jméno své internetové stránky nebo počítače.

4. Nikdy si bez svolení rodičů nedomlouvej osobní schůzku s někým, s kým jsi se seznámil/a prostřednictvím internetu. Doma musí bezpodmínečně vědět, kam jdeš a proč. I když Ti rodiče (nebo lidé, kteří se o Tebe starají) dovolí se s takovým člověkem sejít, nechoď na schůzku sám/sama a sejděte se na bezpečném veřejném místě.

5. Nikdy nepokračuj v chatování, když se Ti bude zdát, že se tam probírají věci, které Tě budou přivádět do rozpaků nebo Tě vyděsí. Vždy o takovém zážitku řekni rodičům (nebo lidem, kteří se o Tebe starají).

6. Nikdy neodpovídej na zlé, urážlivé, nevkusné nebo hrubé e-maily. Není Tvoje vina, že jsi tyto zprávy dostal/a. Když se Ti to stane, oznam to rodičům.

7. Nikdy neotvírej soubory přiložené k elektronickým zprávám (e-mailům), pokud přijdou od lidí nebo z míst, které neznáš. Mohou obsahovat viry nebo jiné programy, které by mohly zničit důležité informace a významně poškodit software počítače.

8. Vždy řekni rodičům (nebo lidem, kteří se o Tebe starají) o všech případech nepříjemných, vulgárních výrazů na internetu, totéž platí pro obrázky s vulgární tematikou.

9. Vždy buď sám/sama sebou a nezkoušej si hrát na někoho, kým nejsi (na staršího, na osobu jiného pohlaví apod.).

10. Vždy pamatuj na následující pravidlo a chovej se podle něho: jestliže některá webová stránka bude obsahovat upozornění, že je určena jen pro dospělé nebo jen pro lidi od určitého věku, musí se to respektovat a ti, kteří nevyhovují kritériím, nemají takovou stránku otevírat.

11. Domluv se s rodiči na pravidlech používání internetu a poctivě je dodržuj. Především se domluv, kdy můžeš internet používat a jak dlouho.

12. Provždy si zapamatuj další pravidlo: když Ti někdo na internetu bude nabízet něco, co zní tak lákavě, že se to nepodobá pravdě, nevěř mu – není to pravda.

13. Jestliže na internetu najdeš něco, o čem jsi přesvědčen, že je to nelegální, oznam to rodičům.

Zdroj: MŠMT