O2 | Chytrá škola

Základy bezpečnosti, tvorba hesla

Metodické náměty pro výukové aktivity

1. Východiska

Následující aktivity jsou orientovány na základy bezpečného používání počítače a online technologií. Cílem je zopakovat si a prohloubit znalosti z oblasti technologického zabezpečení počítače.

2. Cíle výukových aktivit

Cílem výukových aktivit je připomenout si zásady počítačové bezpečnosti – především pak zásady pro tvorbu bezpečného hesla, rozeznávání a nakládání s viry atd. Aktivity nasazujeme úměrně věku dítěte.

1. **Aktivita** Tvorba hesla
2. **Aktivita** Co je a co není na internetu bezpečné?
3. **Aktivita** Viry a jak na ně!

Spolupráce na projektu:
Univerzita Palackého v Olomouci

Aktivita 1/3

Tvorba hesla

Zadání

Pokuste se vytvořit co nejbezpečnější, ale přitom zapamatovatelné heslo pro přístup do vašeho Minecraft účtu.

Metodika k aktivitě

Při tvorbě hesla je třeba dodržet několik bezpečnostních standardů

1. **Ideální heslo by mělo být dlouhé minimálně 8 znaků.**
2. **Při tvorbě hesla používejte číslice, velká i malá písmena abecedy a speciální znaky.**
3. **Nikdy nepoužívejte heslo, které lze najít ve slovníku! Rovněž nepoužívejte křestní jména ani příjmení.**
4. **Pro přístup k různým online službám (e-mail, sociální sítě) nepoužívejte stejné heslo.**
5. **Po ukončení práce v prostředí internetu se nezapomeňte odhlásit z účtu, který právě používáte. Zavření prohlížeče vás z účtu neodhlásí!**
6. **Heslo uchovejte v tajnosti, nikomu jej neprozrazujte, ani svému nejlepšímu kamarádovi.**
7. **Důležité účty zabezpečte dvojfázovým (dvojúrovňovým) ověřováním, které kombinuje heslo a kód na mobilním telefonu.**

Poznámka

Podle posledních bezpečnostních analýz a matematických výpočtů je bezpečnější dlouhé heslo s méně typy znaků (např. pouze s velkými a malými písmeny abecedy), než heslo krátké s více variantami znaků (písmena, číslice, speciální symboly) – rozdíl je však v zásadě zanedbatelný, oba způsoby tvorby hesla jsou vysoce bezpečné.

Otázky

1. **Jakým způsobem jste vaše heslo vytvořili?**
   Řešení: Např. kombinace jména a číslice apod.

2. **Posuďte, zda vaše heslo vyhovuje bezpečnostním standardům.**
   Řešení: Tj. porovnáme, zda heslo, které žák vymyslel, odpovídá bodům 1–3 výše uvedených standardů.

3. **Odhadněte, jak dlouho by trvalo průměrně výkonnému počítači prolomit heslo dlouhé 6 znaků standardním útokem (tj. kombinace znaků), které:**

   A. Bude složeno pouze z číslic? *Řešení: 3 hodiny*
   B. Bude používat číslice a malá písmena abecedy? *Řešení: 8 měsíců*
   C. Bude používat číslice, malá a velká písmena abecedy? *Řešení: 18 let*
   D. Bude používat číslice, malá a velká písmena abecedy a speciální znaky? *Řešení: 120 let*

   Navíc u drtivé většiny online služeb platí, že při opakovaném zadání hesla nás počítač automaticky odpojí a např. na několik hodin zablokuje přístup. Doba průniku na účet se tak násobí.

4. **Zkuste odhadnout žebříček tří nejčastějších hesel v ČR.**
   Řešení: 12345, 123456, heslo, na dalších příčkách je heslo123, 123heslo321, aaaaa a qwertz

5. **Navrhněte způsob, jak vytvořit zapamatovatelné a přitom bezpečné heslo.**
   Řešení: Např. zvolíme nějakou známou větu a písmena s diakritikou nahradíme číslicemi,
   V Českých Budějovicích by chtěl žít každý = v4esk7chbud2jovic9chbycht2l69tka6d7

Aktivita 2/3

Bezpečnostní zásady

Zadání

Pročtete si následující situace a rozhodněte, co je a co není v online prostředí bezpečné.

1. Jirka se ve školní učebně připojil na svůj účet na Facebooku, chatoval, vkládal posty na svou zeď, lajkoval příspěvky kamarádů. Poté zavřel prohlížeč a šel do další výuky…
2. Hance přišla na Facebooku zpráva od její kamarádky Jany, která ji požádala o pomoc. Jana zapomněla heslo do svého facebookového účtu a potřebuje si ho obnovit pomocí mobilního telefonu, vybil se jí ale zrovna telefon. Prosí proto Hanku, zda by jí neposlala kód, který jí dorazí na její mobilní telefon. Hanka Janě kód poslala.
3. Honzovi přišel tzv. hoax (nepravdivá, často poplašná zpráva) o tom, že se Bill Gates z Microsoftu rozhodl podělit o své bohatství. A pokud Honza e-mail přepošle dalším lidem, tak mu za každého člověka, který e-mail pošle dál, zaplatí Microsoft 243 EUR. Honza e-mail přeposlal všem svým kamarádům.
4. Kláře přišel e-mail: Gratulujeme, vyhrála jsi IPhone X. Každé pondělí vybíráme 10 náhodných výherců. Nyní se štěstí usmálo na tebe. Svou výhru potvrď odesláním SMS ve tvaru GIFT 1133567 na číslo 90399. Klára SMS odeslala.
5. Petr umí skvěle pracovat s počítačem, a proto si vytvořil složité heslo obsahující písmena, číslice i speciální znaky. Aby heslo nezapomněl, napsal si ho na zadní část svého notebooku.

Metodika k aktivitě

V rámci aktivity využíváme několik situací, se kterými se děti v online prostředí mohou setkat. Situace můžeme doplnit o jakékoli další, v kterých figuruje zabezpečení počítače, mobilního telefonu apod.

Vyhodnocení úkolu

1. Jirka se neodhlásil ze svého účtu na Facebooku, pouze zavřel prohlížeč na počítači v počítačové učebně. Kdokoli, kdo si otevře prohlížeč po Jirkovi, bude mít přístup do jeho účtu.
2. Náš příklad je ukázkou podvodu s tzv. m-platbou (mobilní platbou) – pokud Hanka Janě odešle kód, který jí dorazil na mobilní telefon, přijde o část kreditu, kód je potvrzením online platby za zboží či službu. Pachatelé tohoto typu nejdříve zkopírují facebookový profil vašeho přítele či přítelkyně a poté se vás pod falešnou identitou pokusí oslovit a vylákat z vás potvrzující kód.
3. Přeposílání hoaxů podporuje šíření spamu a s každým přeposláním se e-mailová adresa Honzy dostala k dalšími neznámým lidem. Je pak snadné zařadit adresu do reklamní spamové sítě a zaplavit ji nevyžádanou poštou, přeposláním totiž Honza potvrdil, že jeho e-mailová schránka je skutečně aktivní a má smysl ji zaplavit reklamou všeho druhu.
4. Jedná se opět o druh podvodu – odesláním SMS se na telefonním čísle Kláry aktivovalo předplatné, které jí bude každý týden odečítat z účtu 99 Kč (poslední dvě číslice telefonního čísla). V e-mailu, který jí přišel, budou někde ve spodní části definovány drobným téměř neviditelným písmem obchodní podmínky, se kterými odesláním SMS souhlasí. Předplatné je nutné zrušit odesláním jiného kódu. Podrobnosti o tomto typu podvodu najdete například v tomto článku.
5. Heslo nepatří ani na zadní stranu notebooku, ani na spodní stranu klávesnice či na lísteček přilepený na monitor. Heslo si buď pamatujeme, nebo k jeho uložení využijeme specializované aplikace (LastPass, 1Password, KeePass, Sticky Password, Dashlane).

Aktivita 3/3

Viry a jak na ně

Zadání

Kamilovi se najednou na obrazovce počítače objevil následující obrázek. Obrázek nejde odstranit, okno nejde zavřít, nefunguje klávesová zkratka CTRL+F4, po restartu naskočí pouze tento obrázek s aktivním formulářem. Co byste dělali na jeho místě?

Metodika k aktivitě

V rámci aktivity se zaměřujeme na problematiku počítačových virů a způsoby, jak s nimi bojovat.

Odpověď na úvodní otázku

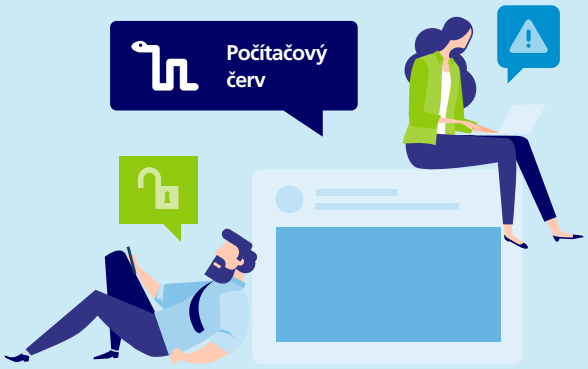
Na obrazovce je napsáno, že jste se dopustili trestného činu, ze kterého se můžete vykoupit zaplacením pokuty. Tu musíte zaplatit pomocí systému Paysafecard či Ukash (anonymní platební systémy). Jde však o VIRUS – tzv. ransomware (někdy se označuje jako **policejní virus**), který je popsán např. zde. Postup pro odstranění viru najdete například na této stránce.

Otázky

1. **Podle čeho se dá poznat, že jde o virus?**
   Chybná čeština, nepovedené koláže, nesmyslná loga, podivná URL adresa…
2. **Co je to vlastně virus?**
   Škodlivý program, který se umí kopírovat a rozšiřovat, ke svému šíření potřebuje hostitele – třeba soubor s počítačovou hrou.
3. **Jakým způsobem se lze před viry chránit?**
   Antivirové programy.
4. **Znáte nějaké antivirové programy či firmy, které je vyrábějí?**
   Avast, Eset, AVG, Kaspersky…
5. **Znáte nějaký antivirový program, který by byl naprosto zdarma?**
   Třeba Avast nebo Defender jako součást Windows.
6. **Jakými způsoby se dostane virus do počítače?**
   Třeba při stahování filmů, her, surfováním po internetu, od kamaráda přes USB apod.
7. **Čím jsou viry nebezpečné? Jak nám mohou ublížit?**
   Např. smažou soubory, zašifrují počítač, ukradnou obsah mailu a pošlou ho vyděrači, aktivují webkameru a natočí nás apod.
8. **Může počítačový virus napadnou člověka?**
   Zatím ne, ale může napadnou třeba čip, který si můžeme nechat implantovat pod kůži třeba kvůli placení, otvírání dveří apod. Případně např. kardiostimulátor a další elektronická zařízení. Podrobnosti si můžete přečíst například na tomto webu.
9. **Může být zavirován i chytrý telefon? Třeba se systémem Android či iOS?**
   Ano, stejně jako běžný počítač.

Zadání

Spojte nebezpečné programy s jejich správným popisem



Zablokuje vám počítač a nutí zaplatit částku za odblokování. Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu.

Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.

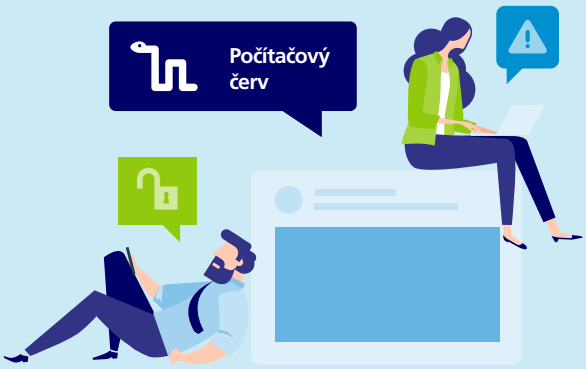
Program, který na počítači bez souhlasu uživatele zobrazuje reklamy (vyskakovací okna v prohlížeči).

Na první pohled vypadá jako užitečný program, nicméně umožňuje svému tvůrci otevřít do počítače „zadní vrátka“ a pronikat do něj.

Program, který z počítače tajně odesílá data – třeba vaše soubory.

Správné řešení úkolu

Druh nebezpečného programu



Nepotřebuje k šíření hostitelský program. Jakmile napadne počítač, začne své kopie bez vědomí uživatele posílat na další počítače a „prolézá“ tak internetem.

Na první pohled vypadá jako užitečný program, nicméně umožňuje svému tvůrci otevřít do počítače „zadní vrátka“ a proniknout do něj.

Zablokuje vám počítač a nutí zaplatit částku za odblokování. Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu.

Program, který na počítači bez souhlasu uživatele zobrazuje reklamy (vyskakovací okna v prohlížeči).

Program, který z počítače tajně odesílá data – třeba vaše soubory.