ZÁKLADY BEZPEČNOSTI, TVORBA HESLA

Metodické náměty pro výukové aktivity

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

Aktivita 1/3

Tvorba hesla

Zadání

Pokuste se vytvořit co nejbezpečnější, ale přitom zapamatovatelné heslo pro váš Minecraft účet.

Materiál vznikl ve spolupráci
s projektem E-Bezpečí,
Univerzita Palackého Olomouc

Metodika k aktivitě

Při tvorbě hesla je třeba dodržet několik bezpečnostních standardů

1. Ideální heslo by mělo mít minimálně 15 znaků a obsahovat čísla, velká i malá písmena abecedy a speciální znaky.
2. Nikdy nepoužívejte snadno odhadnutelná hesla, jako jména nebo slova ze slovníku.
3. Pro různé online služby (e-mail, sociální sítě) nepoužívejte stejné heslo.
4. Když chcete z prostředí internetu odejít, nezapomeňte se vždy odhlásit ze svých účtů. Samotné zavření prohlížeče nestačí.
5. Když chcete z prostředí internetu odejít, nezapomeňte se vždy odhlásit ze svých účtů. Samotné zavření prohlížeče vás neodhlásí.
6. Heslo nikomu neprozrazujte, ani svému nejlepšímu kamarádovi.
7. Důležité účty zabezpečte dvoufázovým (dvojúrovňovým) ověřováním, které kombinuje heslo a kód na mobilu.

Poznámka

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

Otázky

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

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

3.) Odhadněte, jak dlouho by trvalo průměrně výkonnému počítači prolomit standardním útokem (tj. zkouší kombinace znaků) heslo o 6 znacích:

- **A.** složené jenom z čísel? Řešení: 3 hodiny
- **B.** kombinující čísla a malá písmena? Řešení: 8 měsíců
- **C.** kombinující čísla a malá i velká písmena? Řešení: 18 let
- **D.** kombinující čísla, malá a velká písmena a speciální znaky? Řešení: 120 let

Poznámka: Pokud by došlo k zneužití AI k odhalování hesel, čas potřebný k jejich prolomení by se výrazně zkrátil. Při použití hesla o 6 znacích by bylo prolomení okamžité. Na druhou stranu většina online služeb po opakovaném zadání špatného hesla automaticky zablokuje přístup na několik hodin, což čas potřebný k prolomení účtu naopak prodlužuje.

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

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 online prostředí bezpečné.

1.) Jirka se na školním počítači přihlásil na Facebook, kde chatoval, lajkoval příspěvky kamarádů a sám je i přidával. Pak zavřel prohlížeč a odešel na hodinu angličtiny.

2.) Hance přišla na Facebook zpráva od její kamarádky Jany, která ji požádala o pomoc. Jana zapomněla heslo do svého facebookového účtu a potřebuje si ho pomocí mobilu obnovit, ten se jí ale zrovna vybil. Prosí proto Hanku, aby jí poslala kód, který jí přijde v SMS. 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, čísla i speciální znaky. Aby heslo nezapomněl, napsal si ho na zadní část svého notebooku.

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

Metodika k aktivitě

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

Vyhodnocení úkolu

1.) Jirka se neodhlásil ze svého účtu na Facebooku, jenom 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 přišel v SMS, přijde o část kreditu, kód je potvrzením online platby za zboží či službu. Pachatelé tohototypu nejdříve zkopírují facebookový profil vašeho kamaráda a poté se vás pod falešnou identitou pokusí oslovit a vylákat z vás potvrzovací 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.

4.) Jedná se zase 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.

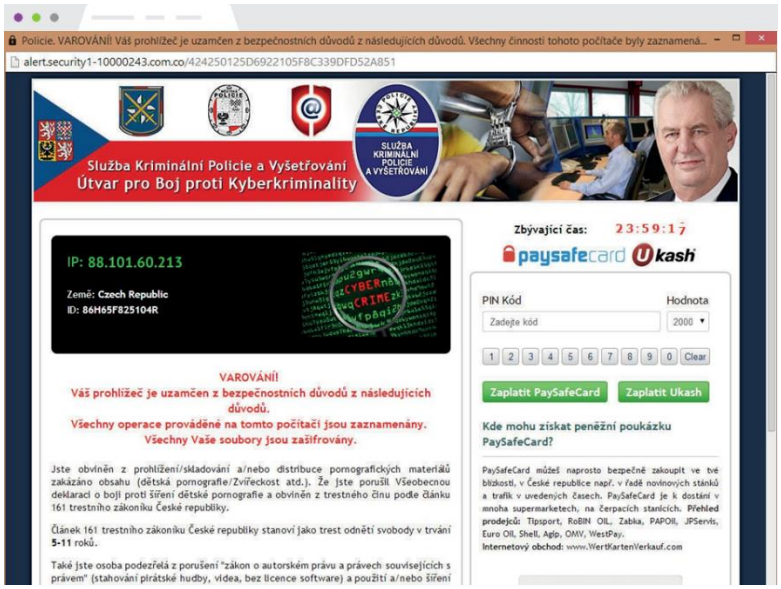
5.) Heslo na zadní stranu notebooku nepatří, ani na spodní stranu klávesnice nebo na lísteček přilepený na monitor. Heslo si musíme pamatovat, případně ho můžeme uložit do specializované aplikace (LastPass, 1Password, KeePass, Sticky Password, Dashlane).

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

Viry a jak na ně

Zadání

Kamilovi se najednou na počítači objevilo následující okno. Nejde zavřít a nefunguje ani klávesová zkratka CTRL+F4. Po restartu se zase objeví tenhle 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. tady.

Otázky

1.) **Podle čeho se dá poznat, že jde o virus?**
Chybná čeština, nepovedené koláže, nesmyslná loga, podivná URL adresa...

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

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 dá před viry chránit?**
Antivirové programy.

4.) **Znáte nějaké antivirové programy nebo firmy, které je vyrábějí?**
Avast, Eset, AVG, Kaspersky...

5.) **Znáte nějaký antivirový program, který je úplně 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 můžou ublížit?**
Např. smažou soubory, zašifrují počítač, ukradnou obsah mailu a pošlou ho vyděrači, aktivují webkameru a natočí nás apod.

8.) **Může počítačový virus napadnout člověka?**
Zatím ne, ale může napadnou třeba čip, který si necháme implantovat pod kůži třeba kvůli placení, otvírání dveří apod. Případně např. kardiostimulátor a další elektronická zařízení.

9.) **Může být zavirován i chytrý telefon? Třeba se systémem Android nebo iOS?**
Ano, stejně jako běžný počítač.

Zadání

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

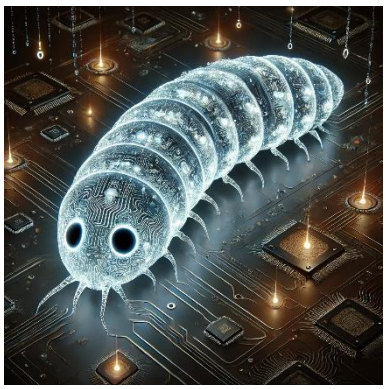
Spojte nebezpečné programy s jejich správným popisem. Obrázky jsou generované AI.

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

Zablokuje počítač a nutí vás zaplatit za odblokování.

Vyhrožuje vám např. tím, že jste spáchali trestný čin a musíte uhradit pokutu.

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



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

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

Správné řešení úkolů

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc

Druh nebezpečného programu.

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

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

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

Zablokuje počítač a nutí vás zaplatit 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).

Aktualizace 23. 1. 2025

Materiál vznikl ve spolupráci s projektem E-Bezpečí, Univerzita Palackého Olomouc