# Kyberbezpečnost

# Metodický list

## Úvodní pokyny

Jedná se o materiály pro podporu výuky na téma kyberbezpečnost. Součástí je úvodní dotazník, prezentace a závěrečný test.

Vše by mělo odpovídat zhruba jedné vyučovací hodině, přičemž závěrečný test je možné studentům zadat až v následující hodině, abyste měli přehled, co ve studentech zůstalo.

## Úvodní test

Nejprve nechte děti vyplnit následující dotazník:

Buď pomocí odkazu **wordwall.net/cs/resource/84327987**

nebo QR kódu (v prezentaci)

* Má šest otázek
* Každá má více správných odpovědí
* Pokud děti vyberou libovolnou správnou odpověď je otázka vyhodnocená jako správná
* Zajímejte se o to, kolik dětí mělo vše správně
* Ještě lepší je, pokud máte svůj účet na Wordwallu, dotazník sdílet a mít tak přesný přehled o odpovědích dětí, kde dělají chybu
* Doba vyplnění včetně spuštění by měla být maximálně pět minut

## Vysvětlení pojmů – typy útoků

Než budete pokračovat k vysvětlení testu a správných pojmů, nadefinujte si některé typy útoků.

### Sociální inženýrství

Jedná se o snahu získat přihlašovací údaje konkrétního uživatele k jeho zdrojům (bankovní účet, heslo k mailu, účty na sociálních sítích, přihlášení k počítači, školní síti atd.). Tyto informace útočník zkouší získat např. podvržením korektních stránek, falešným mailem, falešnou zprávou atd. Vždy je snaha, aby napadený vyplnil někde své přihlašovací údaje.

Takto získané údaje pak použít pro přístup k výše zmíněným zdrojům a získat např. finance z bankovního účtu nebo citlivé zprávy, choulostivé fotografie atd. Také je možné nově vzniklá práva použít k získání dalších zdrojů např. k útoku na jiné uživatele, kdy se útočník vydává, za majitele právě získaného účtu.

### Man-in-the-middle

Jedná se o typ útoku, kdy útočník odposlouchává komunikaci mezi nějakými uživateli např. při neoprávněném průniku do vnitřní sítě (firemní nebo domácí), odposloucháváním komunikace na této síti. Takto útočník buď přímo získá nějaké přihlašovací údaje anebo získá informace pro útok pomocí sociálního inženýrství.

### Ransomware

Jedná se o typ útoku, kdy na napadeném počítači je zašifrován disk a útočník požaduje po uživateli platbu za poskytnutí hesla, k rozšifrování napadeného disku (ransome = výkupné). Rozhodně se nedoporučuje platit, protože se málo kdy stane, že napadený skutečně heslo obdrží.

Obrana proti tomuto typu útoku, kromě zachovávání bezpečnosti spočívá i v pravidelném zálohování svých dat.

## Rozbor testu

Nyní s dětmi proberte test a jednotlivé otázky. Promítněte na tabuli přiloženou prezentaci. Nejprve diskutujte o jednotlivých možnostech, nechte děti přijít na všechna správná řešení a pak je seznamte s odůvodněním.

Pojem důvěryhodný dospělý v následujících znamená například učitele, rodiče, dospělého sourozence apod. někoho, komu můžeme důvěřovat.

1. Na tvé oblíbené sociální síti ti přijde žádost o přátelství od kamaráda, kterého již máš v přátelích s tím, že zapomněl své heslo k původnímu účtu.
   1. Žádost přijmu, je to známý sklerotik
   2. Žádost odmítnu, pokud bude opravdu chtít, abych si ho přidal, řekne mi to ústně.
   3. ﻿Je sice možné mít dva účty na stejné síti, ale určitě by mne kontaktoval jiným způsobem.
   4. Počkám a kontaktuji jej jiným způsobem, například se jej zeptám druhý den ve škole.
   5. Poradím se s důvěryhodným dospělým.
   6. Žádost přijmu, cítím se poctěn, že si mne přidává i do druhého účtu.

Tato otázka má navést děti k tomu, aby bezmyšlenkovitě nepřijímali žádosti o přátelství. Proč má mít kamarád nový účet. Opravdu zapomněl heslo? Nevím to, tak počkám a vše si ověřím.

Děti mohou namítat, že se vlastně nic nestane. Ale je třeba si uvědomit, že útočník získá přístup například i k jejich fotkám, které nejsou veřejně přístupné. A navíc v okamžiku, kdy se stane jejich přítelem snadněji získá i přístup k jejich kamarádům. Zejména k těm, kteří údajného majitele dosud v přátelích nemají. Navíc může nyní snadno komunikovat a může se stát, že se spletou a svěří se mu s něčím co určitě nechtějí zveřejnit.

Je sice možné mít na stejné sociální síti více účtů, ale obvykle je to tak, že jeden máte pro rodinu a druhý pro kamarády a ne dva na stejné úrovni.

1. Od banky, u které máš dětský účet, ti přijde email s tím, že je nějaký problém s tvým účtem a máš kliknout na odkaz a přihlásit se, aby se vše dalo do pořádku.
   1. Rychle to udělám, abych nepřišel o peníze
   2. Ignoruji to
   3. Napíšu dopis do své banky a zeptám se
   4. Poradím se s důvěryhodným dospělým.
   5. Je třeba to udělat, banka si takto ověřuje, zda je účet používaný.

Z této situace se může stát velmi nepříjemná záležitost, někdo vám může vybrat peníze z účtu. Banka by tímto způsobem (mailem nebo zprávou na sociální síti) nekontaktovala, pokud by hrozilo nebezpečí z prodlení. V každém případu, při každém přístupu přes prohlížeč na bankovní server je třeba zkontrolovat certifikát serveru. Tady je třeba dětem ukázat a vysvětlit co to je certifikát a kde jej v prohlížeči najdou (v adresním řádku). Banka si rozhodně takto nebude ani ověřovat, zda je účet používaný.

Dále je třeba říci dětem, jak postupovat, když už něco udělají špatně. Okamžitě kontaktovat dospělého, který má na starost jejich dětský účet a jeho prostřednictvím banku. Rovněž je dětem třeba vysvětlit, že si mají dát pozor na situaci, kdy jim najednou přijde do mobilu nějaký pin a vzápětí jim někdo volá nebo píše, že omylem zadal jejich číslo. Pin nesdělovat naopak kontaktovat dospělého a změnit heslo. Podiskutovat s dětmi o tom co je to tzv. 3D ověření (obvykle pomocí pinu zaslaného na mobil) přístupu.

1. Od kamaráda ti přišel mail, ve kterém ti píše, že máš otevřít soubor v příloze. Otevřel jsi jej, počítač se tě zeptal, zda jej opravdu chceš otevřít a potvrdil jsi to. Počítač dvakrát zablikal, pak se na chvíli otevřelo černé okno, a to je vše. Co uděláš?
   1. Teď můžeš pomlouvat kamaráda, že posílá divné maily.
   2. Mohl to být virus, ale nechává tě to klidným, v tvém počítači není nic, co by ti mohl ukrást
   3. Mohl by to být virus, spustíš antivirový program
   4. Poradíš se s důvěryhodným dospělým
   5. Raději zavoláš kamarádovi, co to mělo znamenat.
   6. Nikomu nic neřekneš, stydíš se, že neumíš správně otevřít přílohu.

Častý případ samostatně se šířícího viru typu červ. Vysvětlit dětem co je to tento typ viru. Virus, který se samostatně replikuje pomocí kontaktů nalezených v napadeném počítači. Kamarád možná vůbec neví, že od něj přišel mail.

Není dobrý nápad, nechat vše až na druhý den, pokud se jedná o vir, hrozí nebezpečí z prodlení. Rozhodně není špatný nápad, udělat následující kroky:

* Spustit antivir
* Kontaktovat kamaráda např. mobilem
* Informovat důvěryhodného dospělého

Často se setkáváme s názorem: „Tak je to virus, no a co, u mne v počítači nic není.“ To ale není pravda. Mohl by to být ransomware – virus, který zašifruje disk. A přijít například o seminárku, na které dělali několik dní ve třech. Dále tento virus například se může replikovat na všechny kontakty, které v počítači nalezne a majitel počítač tak získá pověst šiřitele viru. Stejně tak může odchytávat všechna hesla, které jsou nyní v počítači zadány a získat tak přístup ke všem sociálním sítím, který napadený uživatel používá.

Dále je možné zmínit následující modelové případy, které se skutečně staly:

* Virus použil počítač napadeného počítači k rozesílání ohromného množství mailů, protože získal přístup k školnímu mailovému účtu žáka. Škola přes jejíž mailový server byly maily posílány se dostala na takzvaný black list a několik dnů nemohli ostatní uživatelé včetně učitelů posílat přes tento server maily.
* Virus získal přístup k sociální síti napadeného, předal jej útočníkovi a ten pomocí této sítě začal jménem napadeného rozesílat hanlivé a pomlouvačné zprávy. Napadenému dalo mnoho práce vše vysvětlit a možná se mu to ani úplně nepovedlo.
* Zde útočníkovi nešlo o napadeného žáka, ale věděl, že žák používá bývalý pracovní notebook svého otce, který s i na něm ponechal (pro jistotu) i své pracovní věci (na jiném účtu). Virus díky chybě operačního systému tak ukradl materiály, které v otcově firmě měly charakter tajných materiálů.

1. Od kamaráda ti přišel mail nebo vzkaz na sociální síti, že si máš stáhnout do počítače nebo do mobilu skvělou hru a odkaz na tuto hru. Při prvním spuštění se hra ptá na hodně údajů, včetně tvého rodného čísla a/nebo čísla účtu a hesla k tvému účtu. Co uděláš?
   1. Rychle to vyplním, těším se až zapaříme.
   2. To se mi nelíbí, nic nevyplním, hru smažu a kamarádovi vynadám.
   3. Pátrám na internetu po informacích o této hře
   4. Zeptám se důvěryhodného dospělého.
   5. Protože telefon odmítne hru instalovat s odkazem, že se jedná o nedůvěryhodný zdroj, budu na internetu pátrat, jak to obejít.

Ukázkový příklad toho, jak z dětí vytáhnout citlivé údaje. Útočník může získat přístup k bankovnímu účtu napadeného.

Daleko nebezpečnější je situace, kdy se takto povede získat přístup například k rodnému číslu. Útočník může toto číslo někam uložit. Pak třeba několik let vyčká, než je napadený dospělý a pak s jeho pomocí (a např. zcizeného dokladu) získá půjčku jménem napadeného žáka.

Je třeba si uvědomit, jaké informace po vás mohou žádat při registraci hry. Jméno, příjmení je v pořádku. Věk také – např. kvůli věkovému omezení, ale už ne datum narození a rozhodně ne rodné číslo. V pořádku je i mail – aby mohli zákazníka, kontaktovat dalšími nabídkami. Ale určitě ne přístup k zákazníkovo účtu.

Rozhodně také není dobrý nápad obcházet zabezpečení telefonu a instalovat aplikaci z neznámého zdroje. Nikdy nevíte, co si spolu se hrou nainstalujete navíc.

1. Instaluješ si do mobilu logickou hru, která je zadarmo. Při prvním spuštění chce hra přístup k fotoaparátu na tvém mobilu. Co uděláš?
   1. Povolím to. Nevím sice na co jej potřebuje, ale nevidím v tom problém
   2. Zamítnu přístup a pokud nebude bez něj fungovat, raději jí smažu
   3. Podívám se do diskuse na store nebo na internetu
   4. Zeptám se důvěryhodného dospělého.
   5. To je běžné, že hry chtějí přístup k fotoaparátu, mám již takových několik.

Na co by takováto hra chtěla přístup k fotoaparátu. I kdyby si chtěla pořídit vaší fotografii kvůli výsledkové listině vítězů, nemá na to s ohledem na pravidlo GDPR nárok (vysvětlit dětem co je GDPR). V dnešní době si vůbec nemusíte všimnout, že váš mobil pořizuje fotografie a odesílá je někam bez vašeho vědomí. Ostatně váš mobil to dělá normálně – vaše fotografie ukládá do cloudu. Takže si ani děti nemusí všimnout, že telefon odložený na poličce vedle postele pořizuje jejich fotografie (videa), když se převlíkají a někam je posílá.

Zde je třeba vysvětlit, že tyto fotografie (videa) se mohou objevit kdykoliv někde na internetu. A mohou být třeba použity až za několik let bude žák žádat o pracovní místo nebo třeba výměnný pobyt na škole v zahraničí atd.

Je třeba při instalaci všech aplikací do mobilu nebo tabletu apod. sledovat o jaká práva při instalaci žádají a přemýšlet na co je potřebují. Jsme-li na pochybách, raději aplikaci neinstalujeme i kdyby vypadala sebelákavěji.

1. Existují počítačové viry??
   1. Neexistují, neznám nikoho, kdo by si nakazil PC počítačovým virem.
   2. Ano, existují, proto používám antivir.
   3. Počítačový virus je mýtus, který vymyslely firmy vyrábějící antiviry.
   4. Myslím si, že ano, raději se poradím s důvěryhodným dospělým.
   5. Existují, ale když má uživatel v PC více antivirových programů, nemůže se mu nic stát.
   6. Existují, ale když se chovám zodpovědně, nemohu se nakazit.

Dnes už se asi nenajde žák, který by si myslel, že počítačové viry neexistují. Stále je, ale možné se setkat s názorem, že počítačové viry šíří a vyvíjejí firmy, které vyrábí antivirové programy, aby více vydělaly.

Je třeba dětem vysvětlit, že je třeba používat antivirové programy, ale v žádném případě více najednou. Dva a více antivirových programů na jednom PC se mohou vzájemně blokovat. Rozhodně také není pravda, že kdo se chová zodpovědně nemůže se nakazit. Sice se možnost nákazy minimalizuje, ale není úplně vyloučená. Můžeme to přirovnat k šíření chřipky.

## Závěrečné shrnutí

* Nereagovat unáhleně – při používání PC, mobilu, tabletu se před každým krokem vyplatí přemýšlet. Následky mohou být fatální.
* Zjistit si informace – obvykle po chvíli hledání lze na internetu nalézt nějaké zkušenosti uživatelů. Je třeba, ale vše podrobit kritickému myšlení. Pokud se jedná o falešnou aplikaci, často si její autoři zajistí falešné pozitivní recenze.
* Jsme-li na pochybách kontaktujeme „odesílatele“ – to je vždy dobrý nápad. Často můžeme zjistit, že odesílatel o ničem neví a my mu tím vlastně oznámíme, že má napadený počítač. Jakkoliv se jedná o nepříjemnou skutečnost, tak už kvůli popsaným příběhům je dobré o tom vědět a zareagovat.
* Vždy je dobrý nápad zeptat se důvěryhodného dospělého – děti se často setkávají se situací, že důvěryhodný dospělý na ně nemá čas. V tom případě je třeba, aby si zkusili najít jiného například učitele, vedoucího kroužku atd.

## Závěrečný test

Nyní je čas vyzkoušet, co v dětech naše aktivita zanechala. Doporučuji proto tento test provést např. s týdenním odstupem.

<https://1url.cz/71SPM>

nebo přímo:

[Test ke kyberbezpečnosti - Details - Kahoot!](https://create.kahoot.it/details/c8325a96-ed51-4051-b52e-2fa9d107743a)

## 