UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Interaktivní mobilní aplikace pro výuku bezpečnosti na internetu

BAKALÁŘSKÁ PRÁCE

2023 Jiří Píše

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jiří Píše**
Osobní číslo:	**I20144**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Interaktivní mobilní aplikace pro výuku bezpečnosti na internetu**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem bakalářské práce je vytvoření mobilní aplikace pro systém Android, která bude sloužit k výuce bezpečného chování na internetu.

Aplikace uživatele seznámí s nejčastějšími bezpečnostními hrozbami. Interaktivní formou uživatele naučí hrozby rozpoznat a předcházet jim.

Dále nabídne rady, jak se zachovat, pokud byl již uživatel napaden. Aplikace bude napsána tak, aby dokázala reagovat na výskyt nových bezpečnostních hrozeb.

Rozsah pracovní zprávy: **min. 30 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

- HANÁČEK, P; STAUDEK, J. Bezpečnost informačních systémů. Praha: Úřad pro státní informační systém, 2000. ISBN: 80-23854-00-3
- ŠEBESTA, V; ŠTVERKA V; STEINER F; ŠEBESTOVÁ M. Praktické zkušenosti z implementace systému managementu bezpečnosti informací podle ČSN BS 7799-2:2004 a kompletované vydání ISO/IEC 27001:2005. Praha: Český normalizační institut, 2006, ISBN:, ISBN:80-7283-204-2.
- Jan Kolouch, Pavel Bašta a kol. CyberSecurity, CZ.NIC, z. s. p. o., Praha, ISBN 978-80-88168-34-8
- Karel Burda, Kryptografie okolo nás, CZ.NIC, z. s. p. o., Praha, ISBN 978-80-88168-52-2

Vedoucí bakalářské práce: **Ing. Martin Pozdílek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **12. května 2023**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

Ing. Jan Panuš, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 28. února 2023

Prohlašuji:
Práci s názvem Interaktivní mobilní aplikace pro výuku bezpečnosti na internetu
jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.
Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 9. 5. 2023

Jiří Píše

PODĚKOVÁNÍ

Poděkování patří vedoucímu práce Ing. Martinu Pozdílkovi, Ph.D. za cenné rady a odborné konzultace. Také bych chtěl poděkovat rodině a přátelům, kteří mě při tvorbě bakalářské práce podporovali.

ANOTACE

Tato práce se zabývá tvorbou mobilní aplikace, která slouží k vzdělávání uživatelů o bezpečném chování na internetu. Aplikace je vytvořena pro systém Android v jazyce Kotlin. V teoretické části jsou popsány nejčastější bezpečnostní hrozby. V praktické části je vytvořena aplikace, která o těchto hrozbách uživatele informuje a učí je jim předcházet.

KLÍČOVÁ SLOVA

Internet, mobilní aplikace, Android, Kotlin, bezpečnostní hrozby

TITLE

Interactive mobile application for teaching security on the Internet

ANNOTATION

This work deals with the creation of a mobile application that serves to educate users about safe behavior on the internet. The application is created for the Android system in the Kotlin language. In the theoretical part, the most common security threats are described. In the practical part, an application is created that informs users about these threats and teaches them how to prevent them.

KEYWORDS

Internet, mobile application, Android, Kotlin, security threat

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK A ZNAČEK

Antivirus	Antivirový software
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet protokol
JSON	JavaScript Object Notation
JVM	Java virtual machine
MITM	Man in the middle
P2P	Peer to peer
VPN	Virtual private network
Wi-fi	Wireless Fidelity
XML	Extensible markup language

ÚVOD

V dnešní době internet používá téměř každý. Internet přináší nejen mnoho výhod, ale také mnoho bezpečnostních rizik a hrozeb. Nebezpečné chování na internetu může ohrozit soukromí, finance a osobní život uživatelů. Je potřeba uživatele informovat o bezpečnostních hrozbách, aby se jim byli schopni vyvarovat.

Každý se na internetu chováme jinak. Navštěvujeme jiné stránky a používáme jiné služby. Pro každého z nás jsou relevantní jiné hrozby. Tato práce je zaměřena na mladé lidi se znalostmi moderní techniky. Tomu je přizpůsoben způsob prezentace, styl vysvětlování a seznam hrozeb.

Cílem této bakalářské práce je vytvoření mobilní aplikace pro systém android, která bude sloužit k výuce bezpečného chování na internetu. Aplikace uživatele seznámí s nejčastějšími bezpečnostními hrozbami a interaktivní formou je naučí, jak se hrozbám vyvarovat. V teoretické části práce budou hrozby popsány podrobněji. V aplikaci budou informace ve stručnější formě, aby byly zábavné a vstřebatelné pro mladé lidi. Aplikace bude uživatelům umožňovat procházet informace o jednotlivých hrozbách. Následně jim umožní vyzkoušet své nově získané znalosti. Protože nové hrozby mohou vznikat velice rychle, aplikace bude navržena tak, aby byla lehce rozšiřitelná o nová témata. Součástí bakalářské práce bude popsáno rozložení aplikace, způsob vkládání dat a další informace o vývoji aplikace.

1 Nejčastější hrozby

Počet hrozeb na internetu neustále roste. Objevují se hrozby nové nebo aktualizované tak, aby je nebylo snadné najít. V této kapitole budou popsány nejčastější hrozby, které uživatel na internetu může potkat.

1.1 Škodlivý software

Jednou z nejčastějších hrozeb na internetu je stažení takzvaného malwaru (česky škodlivý software). Jedná se o software, který vykonává nevyžádané akce v počítači uživatele. **[1]** Tento software může například poškodit počítač uživatele, může odesílat soukromá data, aniž by o tom uživatel věděl, nebo může sloužit k převzetí úplné kontroly nad systémem. Tento software může být ve formě samostatného spustitelného souboru, ale také může být součástí normálně funkčního programu, který se navenek tváří jako správně fungující program. Na pozadí vykonává činnosti, které by normálně tato aplikace nedělala. Ve druhém zmíněném případě může být velice obtížné škodlivý soubor odhalit.

Existuje mnoho druhů malwaru. Jednotlivé druhy budou podrobněji popsány v této kapitole.

1.1.1 Viry

Počítačový virus je software, který je schopen infikovat další programy v počítači. Virus může programy infikovat pomocí různých strategií. Například přidáním kódu před původní program. Tento kód se vykoná před spuštěním programu a slouží k dalšímu infikování a poškození počítače, případně k ukradení dat uživatele. **[2]** Škody, které počítačový virus napáchá, mohou být od zpomalení počítače, až po úplné poškození systému, které už se nedá zpětně opravit. Je tedy vhodné snažit se vyvarovat infikování počítače virem.

1.1.2 Trojské koně

Trojský kůň je typ viru, který se tváří jako legitimní. Tento software obsahuje přidaný kód. Tento kód slouží útočníkovi jako vstupní brána do počítače uživatele. Útočník tak může sledovat co uživatel na počítači dělá, může krást jeho data, případně může sám převzít plnou kontrolu nad počítačem. Trojské koně mají často schopnost sledovat jakou klávesu uživatel zmáčkl. **[3]** Pro útočníka je tedy velice jednoduché získat přihlašovací údaje a jiné soukromé informace uživatele.

Nejčastější cesta nakažení trojským koněm je stahování neznámých souborů z internetu nebo otevíráním pošty s přílohou od neznámých uživatelů.

1.1.3 Červi

Na rozdíl od trojského koně, kterého musí uživatel sám nainstalovat do počítače, červ se šíří samostatně. Červ se šíří po síti například tak, že hledá zranitelný počítač, na který by se mohl nakopírovat. Pokud takový počítač najde, nakopíruje se na něj. Oba infikované počítače se snaží hledat dál. Této metodě se říká skenování. **[4]**

Další metoda, jak se červ může šířit, je pasivní metoda. Spočívá v tom, že červ pasivně čeká na zranitelný počítač, až se připojí k infikovanému počítači (například pomocí P2P sítě). Po připojení se červ zkopíruje do druhého počítače. Tato metoda je velice těžká na odhalení, jelikož červ během čekání nevykonává žádné akce. **[4]**

Třetí metodou je potom metoda Generovaného seznamu obětí. Útočník při vytváření červa vytváří také seznam potenciálních obětí, které se následně červ snaží infikovat. **[4]**

1.1.4 Spyware

Dalším druhem softwaru, který škodí uživateli, je takzvaný spyware. Cílem tohoto softwaru není poškodit počítač, jako tomu bylo u předchozích druhů škodlivého softwaru. Spyware slouží ke sledování aktivit uživatele. Může sledovat jaké věci uživatel hledá na internetu, jak se na internetu chová a jaké stránky nejčastěji navštěvuje. Může také ukrást uživatelova hesla. **[5]**

Data získaná tímto softwarem se následně odesílají tvůrci spywaru, aniž by o tom uživatel věděl. Tato data se často používají pro cílenou reklamu. Cílená reklama slouží k doporučování produktů podle toho, co uživatel často vyhledává. Data může také útočník prodávat společnostem pro provádění průzkumů.

1.1.5 Adware

Adware je druh malwaru, který v zařízení uživatele zobrazuje reklamy. Tyto reklamy jsou nejčastěji formou vyskakovacích oken zobrazovány na místech, kde by reklama normálně nebyla. Adware může sbírat data o uživateli (podobně jako spyware) a následně uživateli cíleně zobrazovat reklamy. Uživatel tedy uvidí reklamy především na produkty, o které by mohl mít zájem. Reklamy také mohou obsahovat odkazy na falešné stránky, které vypadají jako oficiální stránky produktů z reklamy. Tyto podvodné stránky mohou uživateli odcizit peníze či jinak uživateli ublížit, viz kapitola Phishing.

1.1.6 Ransomware

Ransomware je druh škodlivého softwaru, který po nakažení počítače uživateli zašifruje nebo jinak omezí přístup k datům. **[6]** Následně je po uživateli vyžadováno výkupné za obnovení přístupu k těmto datům. Uživatel běžně dostane varovné upozornění, že pokud výkupné nezaplatí, tak už se ke svým datům nedostane nebo že budou jeho data zveřejněna. Ransomware se do počítačů uživatele dostává nejčastěji přílohou v phishingových e-mailech. **[6]** Proto by uživatel neměl otevírat žádné přílohy e-mailů od neznámých uživatelů. Ransomware je normální druh malwaru, proto by se uživatel měl řídit všemi poučkami, jak se škodlivému softwaru vyvarovat.

Pokud je počítač nakažený ransomwarem, je velice těžké se ho zbavit. Jako u jiného malwaru je užitečné vyzkoušet analyzovat systém antivirovým softwarem, který by tento software mohl najít a odebrat. Důležité je si uvědomit, že i když antivirový software odebere ransomware z počítače uživatele, data jsou již zašifrována a dešifrovat je bez klíče, který vlastní útočník je matematicky téměř nemožné. **[6]**

1.1.7 Ochrana před škodlivým softwarem

Nejjednodušší ochranou před nakažením škodlivým softwarem je aktualizace operačního systému na nejnovější verzi. Nejnovější verze vždy obsahuje záplaty na ty nejnověji objevená bezpečnostní rizika systému.

Další možností, jak se vyvarovat nakažení počítače, je stahování souborů a aplikací pouze z autorizovaných stránek nebo z ověřených obchodů jako je Google Play, Apple Store, Microsoft Store a podobně. Případně na operačním systému Linux využívat ověřené repository. Pokud uživatel stahuje soubory, měl by je stahovat pouze z oficiálních stránek tvůrců případně distributorů souboru. Uživatel by neměl stahovat ani žádné e-mailové přílohy, které přišli od neznámých e-mailových adres. Pokud je uživatel z nějakého důvodu donucen stáhnout nějaký neznámý soubor, existují programy, které se snaží chránit uživatelův počítač před nakažením.

Jako ochrana před škodlivým softwarem byly vytvořeny nástroje, které automaticky analyzují kód stažených programů. Tyto nástroje analyzují kód staticky a dynamicky. Statická analýza zkoumá samotný kód a hledá části, které by mohly počítač poškodit, nebo jinak uživateli ublížit. Dynamická analýza pracuje na principu spuštění analyzovaného kódu a sledování, jak kód ovlivňuje systém, na kterém běží. **[1]** Programům, které provádějí tyto analýzy, se říká antiviry. Antivirus po objevení malwaru zastaví běh nebezpečné aktivity, kterou tento malware

vykonává a varuje uživatele o nebezpečnosti tohoto souboru. Antivirus může tento soubor hned odstranit případně zabránit jeho další činnosti.

Uživatel by však neměl spoléhat pouze na antivirus. Nové hrozby vznikají velice rychle a vývojářům antivirových softwarů trvá, než antivirový software přizpůsobí novým hrozbám. Nové hrozby mohou být vytvořeny tak, že se antivirovým kontrolám snaží vyhnout. Ne proti všem hrozbám může být momentální verze antivirového softwaru schopna reagovat. Uživatel by měl svůj antivirový software pravidelně aktualizovat, protože nové verze obsahují ochranu proti nově objeveným hrozbám. Nikdy si však nemůže být jistý, že tato ochrana platí proti všem. Dalším důvodem, proč se uživatel nemůže spoléhat na naprostou ochranu, je možnost chyb v antivirovém softwaru. Antivirus je software jako každý jiný a může obsahovat nedokonalosti, které mohou způsobit problémy v ochraně počítače uživatele.

1.1.8 Rozpoznání nakažení škodlivým softwarem

Rozpoznat, zda počítač uživatele byl nakažen malwarem může být obtížné. Mnoho škodlivých softwarů je navrženo tak, aby nebylo jednoduché rozpoznat, že se jedná o malware ani po jeho spuštění. Například spyware běžně nedělá žádné škody počítači. Pouze sbírá a odesílá uživatelova data. Nakažení malwarem, který škodí počítači (či uživateli) se dá rozeznat například podle následujících příkladů: **[7]**

- Počítač je výrazně pomalejší než dříve
- Počítač se sám vypíná, nebo opakovaně zobrazuje chybové hlášky
- Systém zobrazuje vyskakovací okna s nevyžádaným obsahem
- Uživateli se samovolně mění nastavení používaných aplikací (například domovské stránky prohlížeče)
- Jsou odesílány e-maily z uživatelova účtu, které uživatel nenapsal
- V počítači je nainstalován software, který uživatel nenainstaloval

Toto je pouze pár příkladů. Může se vyskytnout i mnoho dalších problémů. Jaké problémy se v počítači uživatele vyskytnou, závisí na typu malwaru v počítači.

1.1.9 Řešení po napadení škodlivým softwarem

Prvním krokem řešení napadení škodlivým softwarem by mělo být okamžité omezení jakýchkoliv aktivit, při kterých jsou používány nebo zobrazovány jakékoliv soukromé informace. Uživatel by se také neměl přihlašovat do žádné služby, aby mu nebyla odcizena hesla.

Dalším krokem je použít antivirový software, který analyzuje soubory a programy v počítači a pokusí se najít veškerý výskyt škodlivého kódu. Po analýze odstraní všechny soubory obsahující tento kód. Po tomto kroku může veškerý problém zmizet. Uživatel by si ale stále měl dávat pozor. Antivirovému programu se nemuselo podařit odebrat veškeré nakažené soubory. Je tedy potřeba obezřetnost. Je důležité zmínit, že antivirový software by měl být aktualizován na nejnovější verzi. Nejnovější verze by měla obsahovat nejnovější metody pro nalezení výskytu škodlivého softwaru.

Pokud předchozí krok nedokázal vyřešit malware v uživatelově počítači, může uživatel použít nejefektivnější metodu zbavení se malwaru. Přeinstalováním systému se uživatel zbaví veškerého malwaru, který se v počítači nachází. Je důležité upozornit, že uživatel přijde i o veškerá svá data uložená v tomto počítači. Pokud by uživatel chtěl tato data uložit před přeinstalováním, riskoval by, že některá tato data budou obsahovat škodlivý kód, který by si tím přenesl do nového systému. Uživatel by si tedy měl svoje data pravidelně zálohovat, aby v případě problému o svá data nepřišel úplně. **[7]**

1.2 Phishing

Phishing je druh útoku, jehož cílem je získat například uživatelova hesla, přihlašovací jména, kreditní kartu a podobné citlivé informace. Phishing spočívá v tom, že útočník podvrhne uživateli falešnou stránku, která se tváří jako ta oficiální. Tyto stránky bývají vytvářeny jako přesné kopie originálních a většinou jsou od nich nerozeznatelné. Uživatel vyplní své soukromé údaje do této stránky, aniž by věděl, že jeho údaje právě získal útočník. Útočník data může následně využít například k ukradení účtů, odcizení peněz či jinému poškození nic netušícího uživatele. **[8]**

1.2.1 Šíření falešných stránek

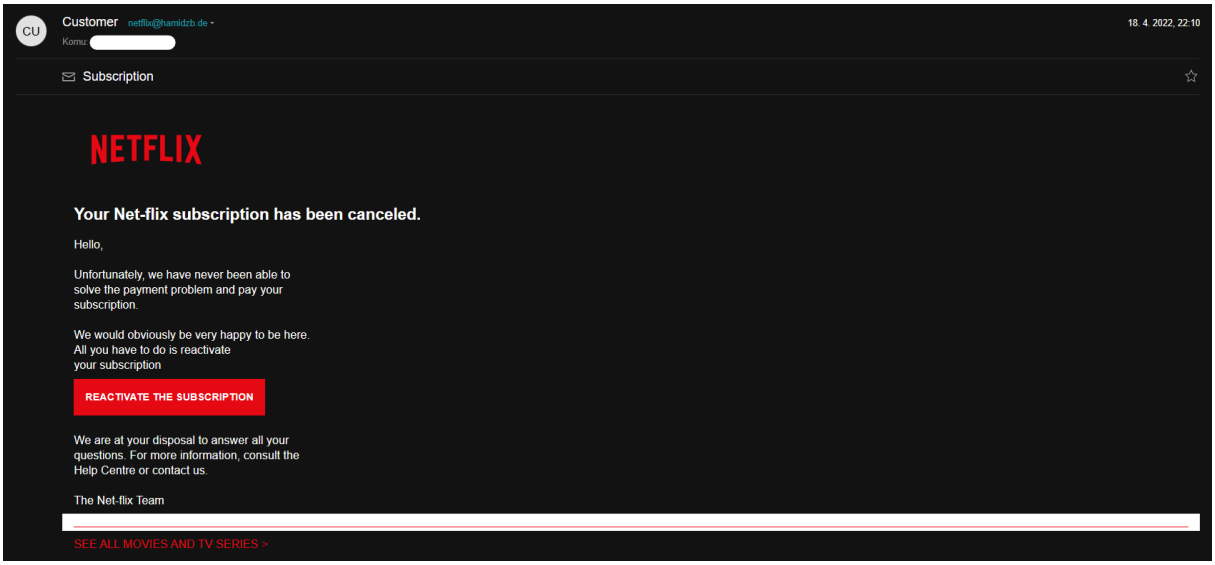
Útočník většinou rozesílá e-maily, které obsahují odkaz na tyto falešné stránky. Podvod začíná už u těchto stránek. Útočníci se často vydávají za legitimní internetové bankovnictví, aby mohli uživatelům vykrást bankovní účty. Častým phishingovým e-mailem je například e-mail, který vypadá, že uživateli přišel od jeho banky. E-mail oznamuje uživateli, důležitou informaci o jeho účtu, či změně pravidel v bankovnictví. Následně vyzývá uživatele, aby se přihlásil a provedl nějakou akci. K tomu je přiložen odkaz na internetové bankovnictví. Tento odkaz nevede na oficiální stránku, ale na falešnou stránku, která následně uživateli odcizí přihlašovací údaje, které do ní uživatel zadá. Toto byl pouze příklad. Útočník se může vydávat za jakoukoliv organizaci.

1.2.2 Jak rozeznat pokus o phishing

Pokus o phishingové útoky se dá běžně rozeznat podle základních pouček:

- phishingové e-maily běžně chodí z neznámých e-mailových adres
- tyto e-maily běžně obsahují neúplné či nesprávné informace
- urgentní žádost o provedení akce (například „Váš účet byl napaden, urychleně pošlete vaše heslo na tento e-mail pro restartování hesla.")
- e-maily obsahují odkazy na neznámé stránky (je třeba kontrolovat adresu stránky, protože stránka může vypadat jako známá, ale ve skutečnosti tak pouze vypadá)
- podvodné stránky často nejsou zabezpečené viz 2.1.2 Zabezpečené připojení, to ale neznamená, že stránka s označením zabezpečeno není podvodná
- phishingové e-maily i podvodné stránky běžně obsahují pravopisné chyby

1.2.3 Příklad phishingového e-mailu



Obrázek 1: Příklad phishingového e-mailu

Na obrázku č. 1 je příklad phishingového e-mailu. Tento e-mail vypadá jako oficiální e-mail od společnosti Netflix. E-mail poukazuje na problém se zaplacením předplatného pro službu Netflix. Vyzývá uživatele k další aktivaci předplatného a poskytuje odkaz pro aktivaci. E-mail však přišel na e-mailovou schránku, na které není vázaný žádný Netflix účet. E-mail také přišel z neznámé e-mailové schránky. E-maily, které uživateli zašle Netflix jsou vždy odesílány z adresy info@mailer.netflix.com. **[9]**

1.3 Prolomení hesla

Volba silného hesla je velice důležitá. Silné heslo je vytvořené tak, že nebude jednoduché pro útočníka toto heslo prolomit. V dnešní době většina přihlašovacích formulářů obsahuje určitou ochranu před volbou příliš slabého hesla. Tato ochrana většinou uživateli nedovoluje zvolit příliš krátké heslo nebo heslo které neobsahuje číslici či velké písmeno. Tato ochrana je však velice základní a není dostatečná.

1.3.1 Poučky pro tvorbu hesel

Uživatel by měl volit co nejsilnější hesla. Pro tvorbu hesel existuje několik pouček: **[10]**

Heslo by mělo být co nejdelší. Čím delší uživatelovo heslo je, tím delší dobu trvá toto heslo prolomit. Délka hesla je obzvláště důležitá proti takzvaným útokům hrubou silou, při kterých útočník zkouší všechna možná hesla, dokud jedna z těchto možností není ta, co uživatel zvolil. Těmto útokům je často zabráněno už webovou službou, například pomocí zablokování přihlášení po opakovaném neúspěšném přihlášení. **[11]**

Síla hesla se dá kontrolovat podle počtu možných kombinací znaků. Počet kombinací lze kromě délky hesla zvýšit také použitím kombinace malých i velkých písmen, číslic a nejlépe i speciálních znaků (!, $, ?, @, #, & a další). Těchto znaků je mnoho a jejich použitím se zvyšuje počet možných hesel, tudíž i bezpečnost hesla. Je důležité upozornit, že speciální znaky by se neměly používat jako náhrada za konkrétní znak. Například nahrazení znaku „a“ znakem „@“ nebo znak „e“ znakem „3“ a další podobné znaky. Tyto náhrady jsou lehce odhadnutelné a na složitosti hesla tolik nepřidávají.

Heslo by nemělo být tvořeno osobními údaji uživatele. Nemělo by obsahovat například datum narození, jména dětí, jména partnera ani podobné informace.

Pokud bude uživatel používat všechny tyto poučky, může pro něho být náročné tato hesla si pamatovat. Pro vyřešení tohoto problému může uživatel použít hesla tvořená ze slov, které se upraví tak aby se nedala lehce odhalit útočníkem. Možnosti, jak tvořit taková hesla: **[10]**

- napsání slova (nebo části slova) pozpátku
- spojení více slov dohromady
- používání velkých písmen uprostřed slov (na náhodných místech)

Existují služby, které vygenerují náhodné heslo, které bude bezpečné. Tyto aplikace běžně generují pseudonáhodnou posloupnost znaků pro vytvoření bezpečného hesla. Tato vygenerovaná hesla jsou většinou tak složitá, že uživatel má velký problém si tato hesla zapamatovat. Proto tyto služby většinou obsahují také možnost ukládání hesel. Uživatel si nemusí tato hesla pamatovat, ale má je uložena v této službě, ze které si svá hesla získává. Více o tomto tématu v kapitole 1.3.3 Uchovávání hesel.

1.3.2 Volba hesel

Uživatel by neměl volit často opakovaná hesla jako například: **[10]**

- „123456789“
- „qwertz“
- „Heslo“
- „Admin“
- „Heslo1“
- A podobně

Tato hesla jsou často opakována a pro útočníka je velice jednoduché takové heslo odhadnout. Útočník může zkoušet tato hesla pro více uživatelských jmen. **[10]** Pokud narazí na uživatelské jméno, které má přidělené takové heslo, útočník získá kontrolu nad tímto účtem.

Pří volbě hesla je také důležité nepoužívat stále stejné heslo. Pokud by uživateli nějakým způsobem bylo odcizeno heslo na jednom účtu, mohl by útočník použít toto heslo pro odcizení dalších účtů tohoto uživatele. Hesla by měla být rozdílná pro každý uživatelský přístup. Útočník by mohl použít heslo i na jiných službách, než na které toto heslo odcizil.

1.3.3 Uchovávání hesel

Nejlepším způsobem, jak uchovávat hesla, je hesla si pamatovat. Pokud se však uživatel řídí všemi poučkami, bude mít mnoho různých hesel, která budou velice složitá. Uživatel pak může mít velký problém, udržet všechna tato hesla ve své paměti a pamatovat si, jaké heslo patří k jakému účtu a na jaké službě.

Jednou z možností, jak tomuto problému předejít, je si svá hesla někam poznamenat. Uživatel může mít doma sešit určený na zapisování přihlašovacích údajů. Tento způsob je bezpečný proti útokům po síti. Uživatel by si však měl dát pozor, aby se poznámky s přihlašovacími údaji nedali nijak získat někým, kdo by k nim neměl mít přístup.

Další možností je uživatelova hesla napsat například do poznámkového bloku, či jiného programu, který neslouží primárně k ukládání hesel, uloženého v jeho počítači. Tato metoda je však nebezpečná z důvodu absence ochrany hesel. Pokud útočník, jakkoliv získá přístup k tomuto souboru, může nezabezpečená hesla ze souboru získat a následně zneužít.

Pro předcházení těchto problémů byly vytvořeny aplikace, které ukládají uživatelova hesla. Takzvaní správci hesel obsahují několik funkcí. Hlavní z nich je ukládání hesel uživatele. Dále také poskytují možnost generovat hesla, která jsou dostatečně bezpečná. Správce hesel často dokáže za uživatele vyplnit přihlašovací formulář. Uživatel tedy nemusí heslo přepisovat, ani znát, pokud bylo heslo správcem vygenerováno. Správce obsahuje ještě další funkce jako sdílení hesel, jednorázová hesla a další funkcionality, které slouží k usnadnění bezpečné správy hesel. **[12]** Správce hesel může být online či offline. Online správce hesel uchovává hesla na serveru mimo počítač uživatele. Offline správce ukládá hesla v počítači uživatele. Správce hesel je bezpečnější než psaní hesel do obyčejného textového souboru díky tomu, že uložená hesla jsou šifrována. Nedají se tedy útočníkem jednoduše přečíst. Správce hesel může být součástí prohlížeče nebo jako samostatná aplikace.

1.3.4 Dvoufázová autentizace

Pokud chce uživatel zvýšit bezpečnost svých účtů, tak se vyplatí kromě silného hesla, použít dvoufázovou autentizaci. Dvoufázová autentizace je proces ověření totožnosti dvěma různými způsoby. Tento proces přidá k základnímu ověření totožnosti další nezávislou metodu. **[13]** Pro přihlášení je nejdříve použité heslo a následně je třeba ještě přihlášení potvrdit. Potvrzení přihlášení může být například zasláním kontrolního e-mailu s odkazem pro potvrzení. Toto řešení je však pomalé, protože se musíte přihlásit do e-mailu. Častěji se tedy volí řešení zaslání kódu v SMS zprávě. Tento krátký číselný kód následně uživatel zadá do aplikace a až následně je uživatel přihlášen. Místo zpráv SMS se dají také použít speciální aplikace, které slouží přímo k této autentizaci. Fungují na stejném principu, pouze kód zobrazují v aplikaci telefonu, a ne v SMS zprávě.

Dvoufázová autentizace rapidně zvyšuje zabezpečení, protože útočník musí získat uživatelovo heslo a zároveň přístup ke kódu pro ověření. Proto je dvoufázovou autentizaci doporučováno používat. A to především u účtů obsahující citlivá data, jako bankovní účty a podobně.

1.4 Nevyžádané zprávy

Do e-mailových schránek uživatelů často chodí nevyžádané zprávy. Tyto zprávy se masově šíří po internetu. Většinou se jedná o phishingové e-maily, které se snaží uživatele dostat na podvodné stránky, nebo e-maily, které šíří poplašné zprávy či hoax. Nevyžádané zprávy také často obsahují reklamy na produkty, o které uživatel nežádal. Těmto reklamním sdělením se říká spam. **[14]**

1.4.1 Ochrana před nevyžádanou poštou

E-mailové služby dnes poskytují základní ochranu proti nevyžádané poště. Filtrují příchozí e-maily a pokud vyhodnotí e-mail jako nevyžádaný, přesunou tento e-mail do kategorie spam. Uživatel pak nevidí tento e-mail mezi ostatními a musí otevřít kategorii spam pro přečtení tohoto e-mailu. E-mailové služby používají mnoho metod pro detekci spamu. Mezi nejznámější metody patří například analýza obsahu pomocí klíčových slov. Podle klíčových slov e-mailový klient vyhodnocuje, zda je tento e-mail spam. Zároveň se vytváří takzvaný whitelist, což je seznam známých odesílatelů, od kterých nechodí nevyžádané zprávy. Dále také blacklist, což je seznam odesílatelů, kteří naopak nevyžádanou poštu odesílají. **[14]**

1.5 Hoax

Hoax je záměrně vytvořená falešná, poplašná a podvodná zpráva. **[15]** Hoax může sloužit k cílenému poškození osoby, organizace apod. Dále může sloužit k šíření chaosu, strachu a jiné podobné manipulaci. To může mít vážné následky pro oběti, či celou společnost.

1.5.1 Šíření hoaxu

Hoax se běžně šíří přes nevyžádané e-mailové zprávy. Často je ale také šířen pomocí článků, příspěvků na sociálních sítích a podobných službách. Hoax běžně není snadné rozeznat od pravdivé informace. Je tvořen velice precizně a je snadno uvěřitelný. Hoax se může šířit také nevědomě. Hoax se totiž běžně šíří řetězově. Uživatel sdělí informaci získanou z tohoto falešného článku jiným uživatelům. Ti této informaci uvěří a mohou ji sdělovat dále. Je tedy velice důležité si ověřovat pravdivost informací, hledat původní zdroje těchto informací a ověřovat věrohodnost těchto zdrojů.

1.6 Zveřejňování osobních informací na internetu

Internet je veřejné místo, na které má volný přístup skoro každý. V době sociálních sítí má uživatel mnoho možností, jak sdílet události ze svého života se svými přáteli. Uživatel si však musí být vědom toho, že informace, které sdílí na internetu, se mohou snadno dostat na

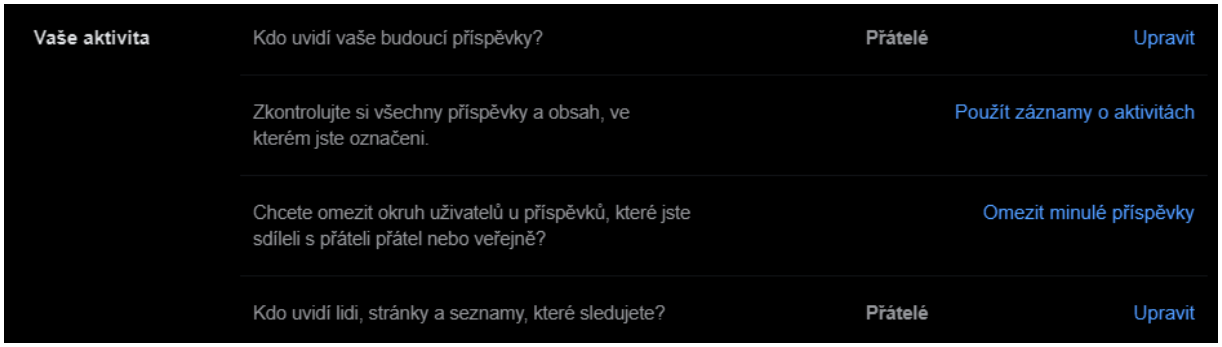
veřejnost. Tyto informace mohou být zneužity nebo mohou poškodit pověst osoby, která je sdílela. Mezi tyto osobní informace patří kromě informací o osobě a blízkých také osobní fotografie, videa, myšlenky v podobě textových příspěvků a další. Příkladem zneužití informací sdílených na internetu může být například vloupání se do bytu uživatele, po tom, co zloděj viděl na sociálních sítích, že uživatel je na dovolené v exotické zemi. Zloděj tedy věděl, že nebude nikdo doma a vloupání pro něho bylo jednodušší.

1.6.1 Krádež identity

Sdílení osobních informací na internetu také může vést ke krádeži identity. Útočník odcizí citlivá data, která uživatel sdílel na internetu. Například číslo občanského průkazu, podrobnosti o platební kartě a podobná citlivá data. Útočník data může využít ke krádeži peněz z platební karty, nákupům na internetu, žádostem o půjčku a jiným podobným nezákonným činnostem. **[16]** Uživatel často nezjistí, že tato citlivá data byla odcizena, až do okamžiku jejich zneužití. Proto pokud něco přidá na sociální síť a následně to vzápětí smaže, nemůže si být jistý, že soukromé informace nemá nějaký útočník již uložená ve svém zařízení.

1.6.2 Možnosti ochrany sdílených informací

Většina moderních sociálních sítí umožňuje nastavit, kdo bude mít k informacím přístup.



Obrázek 2: Možnosti nastavení pro ochranu soukromí na sociální síti Facebook ***[17]***

Na obrázku č. 2 je vidět možnost nastavení pro ochranu soukromí na sociální síti Facebook. Je umožněno uživateli nastavit, kdo uvidí jeho budoucí příspěvky. Umožňuje příspěvky sdílet s veřejností, přáteli či pouze s vybranými osobami. Tato nastavení lze také následně měnit u jednotlivých příspěvků. Dále Facebook umožňuje mnoho dalších nastavení, které mohou skrýt aktivitu uživatele. Tato nastavení jsou specifická pro vybranou sociální síť. Každá sociální síť dává uživateli možnosti, jak své osobní informace chránit.

2 Připojení k internetu

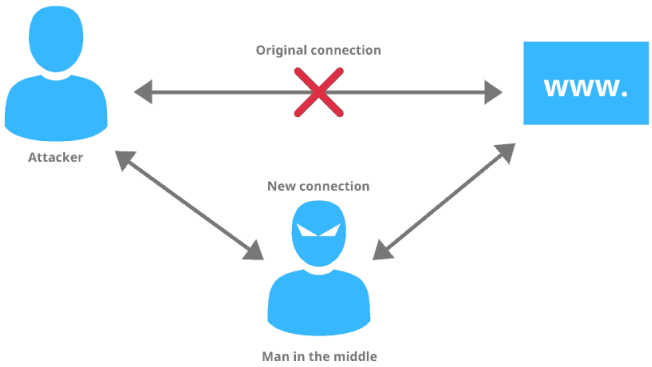
Tato kapitola není tolik o chování na internetu, jako spíš o samotném bezpečném připojení k internetu. Internet je celosvětová síť počítačových sítí. Pokud chce uživatel využívat internetové služby jako komunikaci, či přístup k informacím, musí se do této sítě připojit zařízením, které toto připojení umožňuje. Takové zařízení může být osobní počítač, chytrý telefon, chytré hodinky, televize a mnoho dalších zařízení. K internetu se dá připojit mnoha způsoby. Například pomocí domácí sítě, která poskytuje připojení k internetu, připojení pomocí mobilního internetu, či připojení pomocí veřejné wi-fi sítě. Právě na té uživatelům může hrozit největší nebezpečí.

2.1 Připojení pomocí veřejné wi-fi

Wi-fi je síť určená pro bezdrátový přenos dat. **[18]** Sítě wi-fi mohou být veřejné nebo soukromé. Soukromá wi-fi síť pro připojení vyžaduje heslo a je určena pouze pro určité skupiny lidí. Do veřejné wi-fi sítě se může připojit kdokoliv, protože není zaheslovaná anebo je heslo veřejně dostupné. Připojení k veřejné wi-fi s sebou nese mnoho rizik. Veřejná wi-fi nemusí mít nastavena veškerá bezpečnostní opatření. Data uživatele tedy mohou být ohrožena. Veřejnou wi-fi si může vytvořit téměř kdokoliv. V dnešní době pro vytvoření wi-fi stačí samotný chytrý telefon. Útočník může vytvořit „falešné" veřejné wi-fi sítě. Tato síť může odposlouchávat uživatelovu komunikaci, včetně hesel a podobných soukromých informací. Tato síť uživateli slouží k přístupu k internetu, ale veškerá komunikace je zachycena záškodníkem, který tuto síť vytvořil. Dalším rizikem, kterou připojení veřejné wi-fi síti nese, je napadení malwarem. Veřejná wi-fi může být infikována škodlivým softwarem, kterým se po připojení může infikovat zařízení uživatele. **[19]**

2.1.1 Man-in-the-middle

Jedním z častých útoků pomocí veřejné wi-fi je takzvaný útok man-in-the-middle (zkráceně MITM). Man-in-the-middle je útok, kde útočník naruší komunikaci mezi dvěma stranami. **[20]** Útočník následně komunikuje s oběma stranami tak, aby to vypadalo, že komunikace je v pořádku. Útočník může takto komunikaci odposlouchávat, nebo do komunikace zasahovat a ovlivňovat ji. Ani jedna strana komunikace však nemusí tušit, že nekomunikují s tím, s kým chtějí, ale s útočníkem, který komunikaci narušil. Následující obrázek č. 3 ukazuje schéma útoku man-in-the-middle.



Obrázek 3: Man in the middle – schéma útoku ***[20]***

Narušení komunikace pomocí man-in-the-middle lze předejít například šifrováním komunikace. Útočník pak nebude komunikaci rozumět a nebude ji tedy moci sledovat, ani měnit. Šifrovat komunikaci se dá například pomocí použití virtuální privátní sítě, viz kapitola Virtuální privátní síť.

2.1.2 Zabezpečené připojení

Když uživatel zapne jakoukoliv webovou stránku, uvidí ve svém prohlížeči vedle adresy stránky také ikonku zámku či nějaké výstrahy. Pokud si uživatel ikonu rozklikne, uvidí zde, že je připojení zabezpečené či nezabezpečené. Pokud je zabezpečené, neznamená to, že webová stránka, na které se uživatel právě nachází, je bezpečná. Značí to pouze, že komunikace mezi webem a uživatelem probíhá pomocí protokolu HTTPS a pro útočníka je obtížnější tuto komunikaci odposlouchávat, než kdyby probíhala pomocí HTTP. HTTP a HTTPS jsou protokoly, které slouží ke komunikaci mezi webovým prohlížečem a webovým serverem. **[21]** Protokol HTTP posílá nešifrované informace v čitelné formě. Kdokoliv, kdo komunikaci zachytí, může si ji přečíst a získat z ní citlivá data, jako jsou přihlašovací údaje, a následně je zneužít. **[21]** Protokol HTTPS komunikaci šifruje pomocí šifrovacího protokolu. Pokud je komunikace šifrovaná, útočník nebude schopný si data přečíst, nezná-li klíč k dešifrování.

Protokol HTTPS využívá pro ověření, že se uživatel připojuje ke správné webové stránce a že je komunikace šifrována, takzvané certifikáty. Certifikát je elektronický dokument, který obsahuje informace o doméně, informace o vydavateli certifikátu, dobu platnosti certifikátu a další informace. **[21]** Informace o vydavateli certifikátu je třeba uchovávat, pro ověření důvěryhodnosti certifikátu. Pokud bude certifikát neplatný, nebo informace o vydavateli nebudou souhlasit, prohlížeč bude uživatele informovat, že připojení je nezabezpečené. **[21]**

Uživatel si může certifikát zobrazit v prohlížeči. Každý prohlížeč zobrazení certifikátu umožňuje někde jinde. Například po kliknutí na ikonku zámku vedle adresy.

2.1.3 Minimalizace rizik spojených s připojením k veřejné wi-fi

Nejlepším způsobem, jak se vyvarovat rizikům spojeným s připojením k veřejné síti wi-fi, je k veřejné wi-fi se nepřipojovat a používat jiné připojení, jako například mobilní internet. Pokud uživatel potřebuje připojit počítač nebo jiné zařízení, které se nemůže samo připojit k mobilnímu internetu, může použít svůj chytrý telefon, který se připojí do internetové sítě a pomocí funkce hotspot může k internetu připojit také svůj počítač.

Pokud je uživatel připojen k veřejné wi-fi, měl by používat šifrované připojení například pomocí protokolu HTTPS, který ochrání uživatelova data pomocí šifrování. Další možností je použití virtuální sítě, která chrání uživatelova data a pomáhá s dalšími riziky. Virtuální privátní sítě jsou rozebrány podrobněji v následující kapitole.

Uživatel by se měl vyvarovat používání stránek, jako je internetové bankovnictví a podobné citlivé stránky, je-li připojen na veřejné wi-fi síti. Tím předejte odcizení přihlašovacích údajů či odcizení peněz z účtu. Také by se měl vyvarovat zadávání přihlašovacích údajů a osobních informací typu číslo občanského průkazu nebo platební karty. Tím uživatel předejde odcizení těchto údajů pomocí odposlechu.

Uživatel by měl také dodržovat všechna ostatní doporučení k ochraně svých dat a svého zařízení.

2.1.4 Virtuální privátní síť

Jedním ze způsobů, jak zabezpečit svoje fungování na internetu, je použít službu VPN. Virtuální privátní síť totiž umožňuje šifrovat datové přenosy mezi zařízeními. Pro útočníka je tedy obtížnější tuto komunikaci odposlouchávat. Další výhodou VPN je schopnost schovat vaši identitu na internetu. VPN funguje na principu připojení šifrovaným spojením k takzvanému VPN serveru. S internetem potom nekomunikuje přímo počítač uživatele, ale samotný VPN server. Uživatel následně vystupuje na internetu pod IP adresou VPN serveru. To, že komunikace přes internet probíhá přes VPN server, může vést ke zvýšení latence kvůli přenosu dat přes větší počet komunikačních bodů. **[22]**

VPN má další uživatelské výhody. Jednou z nich je možnost využít služby, které nejsou povolené v lokaci, ve které se uživatel zrovna nachází. Pokud je uživatel například na dovolené

v zemi, kde není dostupná jeho oblíbená internetová služba, může se uživatel připojit přes VPN na český server. Získá tedy českou IP adresu a služba, která je v česku povolená, se mu stane dostupnou. VPN také může umožnit práci na dálku. Uživatel se pomocí VPN připojí do firemní sítě zaměstnavatele a může práci vykonávat téměř odkudkoli, aniž by společnost musela zveřejňovat své služby veřejně na internetu. **[23]**

3 Tvorba aplikace

3.1 Existující aplikace

Existující aplikace na systému Android téměř nejsou. Konkurenční aplikace se nacházejí především na webu. V následujících kapitolách jsou rozebrány 3 webové stránky pro výuku bezpečnosti na internetu. **[24]**

3.1.1 Google Interland

Interland je interaktivní webová hra určená pro výuku bezpečnosti na internetu. **[25]** Hra je určena především pro děti, což ukazuje její grafické zpracování plné barev a jednoduchých tvarů. Hra je tvořena ze čtyř miniher, které se zaměřují na jiná konkrétní témata nejen bezpečnosti na internetu, ale také správného chování na internetu. Mezi témata patří volba hesla, phishing, motivace ke korektnímu chování na internetu a podobně. Hra je přizpůsobena také pro hraní v prohlížeči mobilního telefonu.

Hra motivuje uživatele, aby se stal internetovým úžasňákem. Vzdělávání hráčů neprobíhá násilnou formou. Hra je velice zábavná a uživatel si často ani neuvědomí, že se zároveň také vzdělává.

3.1.2 Avast Buď safe online

Avast buď safe online je online kurz od společnosti Avast, ve spolupráci s influencerem Jirkou Králem. Tento kurz probíhá pod záštitou Ministerstva školství, mládeže a tělovýchovy České republiky a mohou ho využívat učitelé k výuce ve školách. **[26]** Kurz je dostupný zdarma na https://www.avast.com/cz/besafeonline/ a může si ho tedy vyzkoušet každý.

Uživatel má na výběr z několika témat, o kterých se chce dozvědět informace. Kurz je zaměřen především pro mladou generaci, což je vidět především ve stylu předávání informací. Informace o dané problematice nejsou předávány běžným způsobem, nezahrnují velké množství textu a informací, naopak jsou předávány velmi stručně, za pomocí online konverzace. Uživatel přihlíží konverzaci dvou jiných uživatelů. Jeden uživatel má nějaký problém ohledně internetu a druhý je zkušenější. Prvního uživatele varuje před možným nebezpečím. Tento styl informování je velice efektivní a zábavný, což je jedním z důvodů proč tento program získal již mnoho ocenění, například ceny SDGs 2019, Effie Awards 2019, Effie Awards 2020 a WebTop100. **[26]**

Kurz také vede statistiky o tom, jak se uživateli daří. Pokud uživatel dokončí téma, je mu položena otázka, za kterou uživatel může získat 0–3 hvězdičky, které značí, jestli uživatel odpověděl správně. Kurz uživateli ukazuje, kolik témat už dokončil a kolik získal hvězd. Tím ho motivuje pro dokončení dalších témat a k odpovídání na otázky správně.

Na stránce se vedle kurzu také nachází spousta tipů, jak se na internetu chovat. Tipy jsou zaměřené na konkrétní témata jako například: „Jak zrušit účet na snapchatu", „Ukradený Minecraft účet – co dělat" a podobně. **[26]** Tipy jsou většinou ve formě stručných návodů, jak se k dané problematice stavět. Dále se na stránce nachází informace pro uživatele, jak kurz využít pro výuku. Stránka také obsahuje záložku pro rodiče, kde si rodiče mohou přečíst obsáhlejší články či zhlédnout videa, která jim mohou pomoci s výchovou dětí v dnešní internetové době.

3.1.3 Internet Highway

Internet Highway je vzdělávací hra, která se snaží hráče interaktivní formou informovat o nebezpečí, které na ně může na internetu čekat. Hra je určena pro žáky základních škol. Také volba témat je tím ovlivněna. Mezi témata patří kyberšikana, autorská práva, internetoví predátoři a další. Tato hra vznikla na Pedagogické fakultě Univerzity Palackého v Olomouci. **[27]**

Hra je čistě ve webovém prohlížeči a nemusí se tedy nikam stahovat. Uživateli stačí otevřít jejich webovou stránku a může začít hrát. Ve hře se nachází hlavolamy, různé překážky a úkoly, které musí uživatel projít, aby se posunul dál a dozvěděl se další informace. Hra je rozdělena do více úrovní a po každé úrovni má k dispozici takzvanou paměťovou kartu, která shrne nejpodstatnější informace z každé úrovně. **[24]**

3.2 Technologie

V této kapitole budou popsány použité technologie, přístupy a další věci související s vyvíjenou aplikací.

Zásadní činností pro tvorbu mobilních aplikací je volba platformy, pro kterou bude aplikace vyvinuta. V dnešní době jsou dva nejpopulárnější operační systémy pro mobilní telefony. Android, který je nainstalován přibližně na 72 % mobilních zařízení a iOS, který je na 27 % zařízení. Zbývající procento je rozděleno mezi méně známé systémy. **[28]** Cílem této aplikace je vzdělávat co nejvíce uživatelů. Proto volba bude vyplývat z počtu uživatelů na platformě a aplikace bude vyvinuta pro systém Android.

3.2.1 Android

Android je nejpopulárnější operační systém pro mobilní telefony. Tento open-source operační systém založený na Linuxu je vyvíjen společností Google. Může být nainstalován nejen na mobilní telefony, ale také na tablety, chytré hodinky a další zařízení (většinou s dotykovou obrazovkou). Android je otevřený systém a vývojáři si ho tedy mohou libovolně upravovat a vyvíjet aplikace. Tyto aplikace se následně nahrávají na služby, jako je Google Play a podobně, odkud si je mohou uživatelé stáhnout a nainstalovat do svých zařízení. Android narozdíl od konkurenčního iOS může být nainstalován na zařízeních jiné značky než Google. Tato skutečnost umožňuje uživatelům větší výběr hardwaru, ale vývojářům může přidělat starosti, protože nevědí dopředu, na jaké zařízení se aplikace vyvíjí. Android je sice otevřený systém, ale přesto běžně obsahuje povinný software, který je přidaný výrobci zařízení. **[29]**

3.2.2 Programovací jazyk

Aplikace pro systém Android se dají vyvíjet v mnoha programovacích jazycích. Mezi nejčastější patří Java, Kotlin a C++. **[30]** Tyto a další jazyky nabízí programátorům řadu možností, jak vytvářet aplikace. Každý jazyk má své výhody i nevýhody. Jazyk je potřeba zvolit především podle typu aplikace. Pro vývoj aplikace pro výuku bezpečnosti na internetu není třeba zvýšení výkonu, které by poskytl jazyk C++. Google v roce 2017 ohlásil Kotlin jako preferovaný jazyk pro vývoj Android aplikací. **[30]** Z těchto důvodů je pro tvorbu této aplikace jazyk Kotlin optimální volbou.

3.2.3 Kotlin

Kotlin je staticky typovaný open-source programovací jazyk vyvinutý společností JetBrains. Aplikace napsané v jazyce Kotlin je možné spouštět na všech platformách. Pro běh Kotlin aplikací se používá Java Virtual Machine (JVM). Díky tomu je jazyk Kotlin kompatibilní s jazykem Java. Kotlin může využívat veškeré existující knihovny jazyka Java a je velice snadné do existujících Java projektů integrovat kód v jazyce Kotlin. **[31]**

Kotlin je poměrně jednoduchý jazyk. Pro vytvoření proměnné není třeba určit její datový typ. Datový typ se proměnné přidělí při její inicializaci. Kotlin je silně typovaný jazyk, což znamená, že do proměnné lze uložit pouze hodnotu stejného typu, jako byl zvolený při deklaraci či inicializaci této proměnné. Kotlin nevyžaduje středníky na konci řádku a snaží se udělat kód stručnější než Java. Také pomáhá programátorům předejít výjimkám null-pointer tím, že rozlišuje datové typy podle toho, zda umožňují obsahovat hodnotu null. Aby například proměnná mohla obsahovat hodnotu null, musí být za jejím datovým typem otazník. **[31]**

3.2.4 Android studio

Android studio je vývojové prostředí určené pro tvorbu mobilních aplikací na systém Android. Je vyvíjeno společností JetBrains a je schváleno jako oficiální vývojové prostředí pro tvorbu Android aplikací, společností Google. Android studio je postaveno nad IntelliJ IDEA a je zcela zdarma. **[32]**

Android studio umožňuje vývojářům vyvíjet aplikace pro systém Android a poskytuje jim mnoho funkcí, které jim usnadňují práci. Mezi funkce patří například designer aktivit, díky kterému vývojář může přidávat prvky do aktivit velice jednoduše, a to způsobem drag and drop. Jednoduše přetahuje předpřipravené prvky na obrazovku a tím vytváří vzhled aplikace. Následně může upravovat parametry daných prvků hned v designéru. Nemusí tedy prvky přidávat pomocí psaní XML. Další užitečnou funkcí je možnost přidání emulátoru. Emulátor umožňuje vývojáři testovat aplikace ve virtuálním telefonu v počítači, ve kterém aplikaci vytváří. Existuje ale také alternativa připojení mobilního telefonu pomocí kabelu do počítače a spuštění aplikace v telefonu. Místo kabelu se dá také použít připojení přes wi-fi. Podmínkou je, že telefon má nainstalovaný systém Android 11 a vyšší.

3.2.5 Soubory JSON

JSON je zkratka pro JavaScript Object Notation. Vychází ze zápisu objektů v jazyce JavaScript, ale funguje zcela nezávisle na této platformě. Jedná se o formát souborů, který slouží k výměně dat a během posledních let se stal jedním z nejdůležitějších formátů na webu. **[33]** Formát JSON je tvořen datovými typy: **[33]**

- JSONString – textový řetězec
- JSONNumber – číslo
- JSONBoolean – logická hodnota
- JSONNull – hodnota null
- JSONArray – pole
- JSONObject – objekt

Ve většině moderních programovacích jazyků existuje způsob, jak jednoduše z tohoto formátu data vyčíst a rovnou převádět do datových typů jazyka. Nejjednodušší je to samozřejmě v jazyce Javascript, ze kterého notace JSON souboru vychází. Následující obrázek ukazuje příklad, jak se dá z JSON formátu načítat.

```
val jsonString = readJsonToString(context, fileName: "learnitemsmetadata.json")
val jsonArray = JSONArray(jsonString)

for (i in 0 ≤ until < jsonArray.length()) {
    val learnItemJsonObject = jsonArray.getJSONObject(i)
    val label = learnItemJsonObject.getString( name: "label")
    val percentage = learnItemJsonObject.getDouble( name: "percentage")
    val currIndex = learnItemJsonObject.getInt( name: "currIndex")
```

Obrázek 4: Práce s formátem JSON v jazyce Kotlin

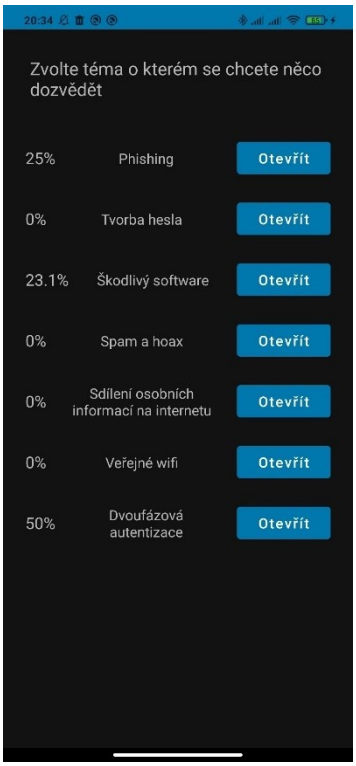
Na obrázku je vidět neúplná metoda updateLearnItemsWithMetaData ze samotné aplikace. Tato metoda má za úkol přečíst soubor obsahující metadata a uložit je do objektů learnItem, která obsahují data pro vzdělávání uživatele aplikace. Na obrázku je dále vidět, jakým způsobem se pracuje s JSON soubory v jazyce Kotlin. Nejdříve se do proměnné načte obsah JSON souboru a následně se vytvoří objekt JSONArray, který obsahuje text z přečteného souboru. V cyklu se následně prochází jednotlivé JSON objekty z pole objektů. Z jednotlivých objektů se následně čtou jednotlivé hodnoty. Například pro čtení řetězcové hodnoty existuje metoda getString(), která přečte a vrátí tento string. Ten je v ukázce uložen do proměnné label a níže v metodě se s touto proměnnou pracuje. Podobně je to i pro jiné datové typy, které JSON umožňuje používat.

3.3 O aplikaci

Aplikace je rozdělena do dvou částí. Obě části budou popsány v následujících kapitolách. Tyto části má uživatel přístupné z hlavní obrazovky aplikace.

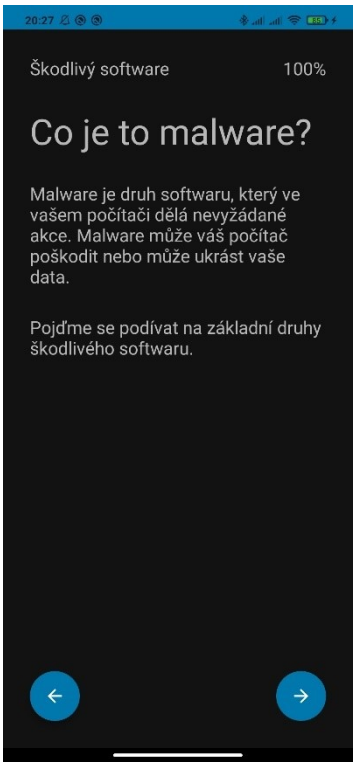
3.3.1 Vzdělávat se

První částí aplikace je takzvaná část „Vzdělávat se“. Tato část, jak název napovídá, slouží k vzdělávání uživatelů aplikace. Když uživatel otevře tuto část, dostane na výběr z možných témat, o kterých se může dozvědět užitečné informace. Témata jsou načítána ze souboru learnitems.json do třídy LearnItem. Více o načítání dat v kapitole 3.3.3 Načítání dat. Tato témata jsou vypsána pod sebou v komponentě recyclerView. Pro zobrazování těchto learnItemů v recyclerView je vytvořen adaptér LearnItemAdapter. Adaptér vždy obsahuje název tématu, tlačítko pro otevření tématu a ukazatel procent do dokončení tohoto tématu.



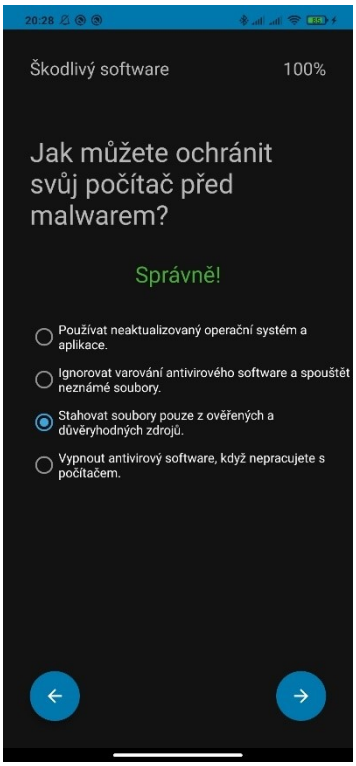
Obrázek 5: Ukázka LearnMenuActivity

Po zvolení tématu a kliknutí na tlačítko otevřít je uživatel přesměrován na aktivitu LearnActivity, která slouží k samotnému vzdělávání. Tato aktivita slouží podobně jako snímek prezentace. Ze třídy LearnItem si načte stránku (třída Page) podle aktuálního indexu v objektu learnItem. Data z této stránky se zobrazí uživateli. Na stránce je zobrazen nadpis stránky a následně dva texty a jeden obrázek. Stránka nemusí obsahovat ani text, ani obrázek. Záleží tedy na obsahu aktuálního objektu Page, co uživatel uvidí. Na této aktivitě vždy může uživatel vidět název tématu, které prochází a také procento dokončení tématu. Ukázku aktivity LearnActivity je možné vidět na následujícím obrázku.



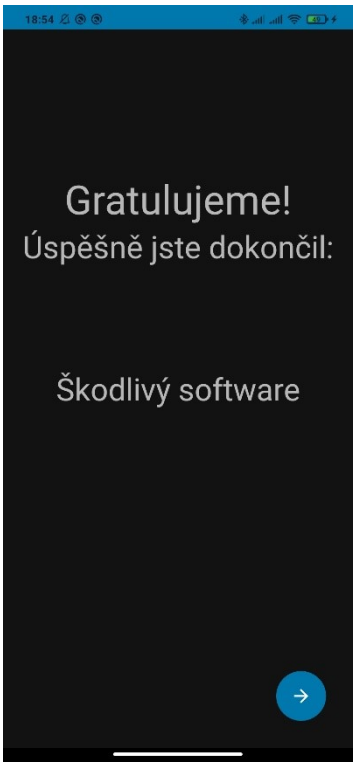
Obrázek 6: Ukázka LearnActivity

Pokud uživatel projde všechny stránky zvoleného tématu, následuje sekce otázek. Uživatel je přesměrován na další aktivitu, kde dostane závěrečné otázky, které musí projít, aby dokončil zvolené téma. Počet otázek se může lišit téma od tématu, ale běžně jsou to otázky dvě. Aktivita, na které uživatel vidí otázky, se nazývá LearnQuestionActivity. Tato aktivita obsahuje samotnou otázku a následně čtyři možné odpovědi.



Obrázek 7: Ukázka LearnQuestionActivity

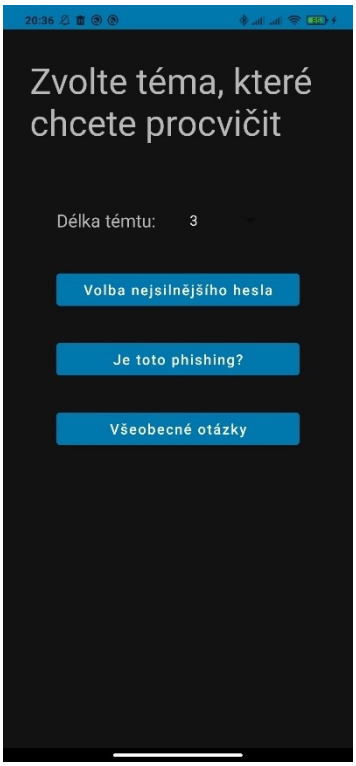
Uživatel zvolí jednu z odpovědí a může pokračovat na další stránku. Pokud je odpověď špatně, je na to upozorněn a musí zvolit jinou odpověď. Pokud je odpověď správná, je přesměrován na závěrečnou aktivitu. A to aktivitu LearnCongratulationActivity, kde je mu poblahopřáno k úspěšnému dokončení tohoto tématu. Následně je přesměrován zpět k volbě témat. Témata může uživatel otevírat i opakovaně. Závěrečné otázky jsou vždy stejné.



Obrázek 8: Ukázka LearnCongratulationActivity

3.3.2 Prověřit znalosti

V druhé části, která se nazývá „Prověřit znalosti" si uživatel může vyzkoušet své nově získané znalosti ohledně bezpečnosti na internetu. Zkoušení znalostí neprobíhá obyčejným testováním uživatele, ale snaží se to dělat zábavnější formou. První aktivita této stránky se nazývá TestMenuActivity. V této aktivitě si uživatel může vybrat, které z témat chce procvičit. Nad tlačítky, které slouží k otevření aktivit k samotnému procvičení, se nachází komponenta spinner, která slouží k volbě délky tématu k procvičení. Tuto délku lze zvolit od 3 do 10. Určuje počet stránek (úkolů), které uživatel bude muset vyřešit.

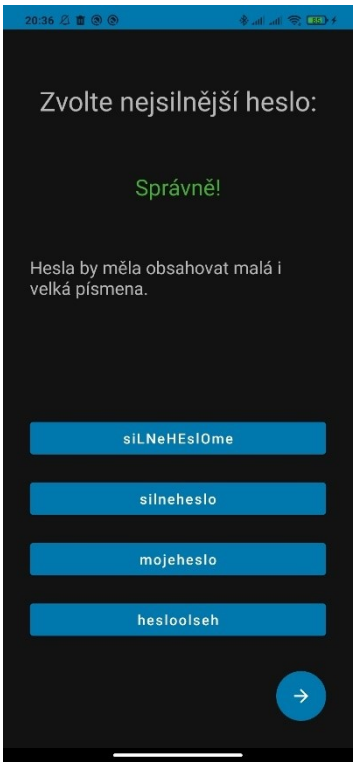


Obrázek 9: Ukázka TestMenuActivity

Následující kapitoly popisují jednotlivá témata části „Prověřit znalosti“.

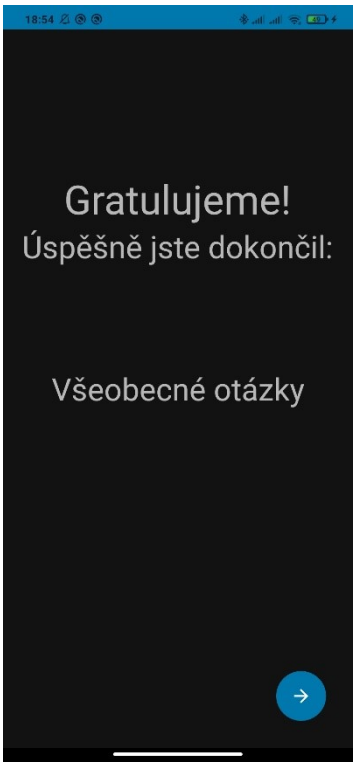
3.3.2.1 Volba nejsilnějšího hesla

Volba nejsilnějšího hesla je prvním tématem v části „Prověřit znalosti”, které může uživatel zvolit. Po otevření tohoto tématu je uživatel přesměrován na aktivitu TestPasswordActivity, na které se nachází nadpis „Zvolte nejsilnější heslo:” a následně čtyři tlačítka, které uživatel může zvolit. Tlačítka reprezentují jednotlivá možná hesla, ze kterých má uživatel za úkol vybrat to nejsilnější. Po zmáčknutí zvoleného tlačítka se uživateli zobrazí, zda je zvolená možnost nejsilnější nebo ne. Pokud ano, je vypsáno zdůvodnění a je zpřístupněno tlačítko pro zobrazení nového setu hesel. Ukázka této aktivity je na následujícím obrázku.



Obrázek 10: Ukázka TestPasswordActivity

Po dokončení uživatelem zvoleném počtu setů hesel je uživatel přesměrován na aktivitu TestCongratulationActivity, která mu poblahopřeje k dokončení tohoto tématu. Tato aktivita je společná pro všechny témata v části „Prověřit znalosti". Mění se pouze nadpis dokončeného tématu.

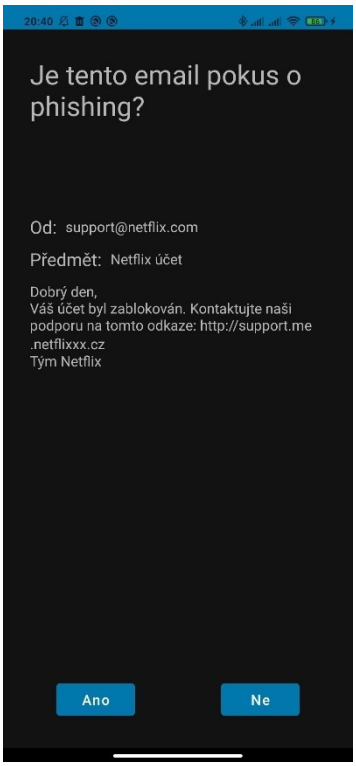


Obrázek 11: Ukázka TestCongratulationActivity

Následně je uživatel přesměrován zpět k výběru témat této části a může si toto téma zopakovat, nebo vybrat jiné. Pokud bude opakovat toto téma, budou mu zvoleny jiné sety hesel. Sety hesel jsou voleny náhodně z přibližně třiceti možných setů, které jsou uloženy v souboru testpassword.json. Každý set je vždy na určité téma. Jedno z hesel například obsahuje speciální znaky a ostatní ne. Je tedy nejsilnější a uživatel po jeho zvolení uvidí hlášku „Hesla by měla obsahovat i speciální znaky. Například: *, /, +, !, @, # a další". Mezi další témata patří například kombinace malých a velkých písmen, číslice, délka hesla a další.

3.3.2.2 Je toto phishing?

Druhé téma části „Prověřit znalosti" je téma je toto phishing? Po otevření tohoto tématu je uživatel přesměrován na aktivitu TestPhishingActivity. Na této aktivitě je uživateli zobrazen příklad e-mailové zprávy. Uživatel má rozhodnout, zda je tento e-mail pokusem o phishing nebo ne. Po rozhodnutí je uživatel informován, zda měl pravdu nebo ne a je informován proč to tak je. Následně po zmáčknutí nově zpřístupněného tlačítka je aktivita aktualizována na nový e-mail a uživatel znovu rozhoduje, zda se jedná o phishing nebo ne.

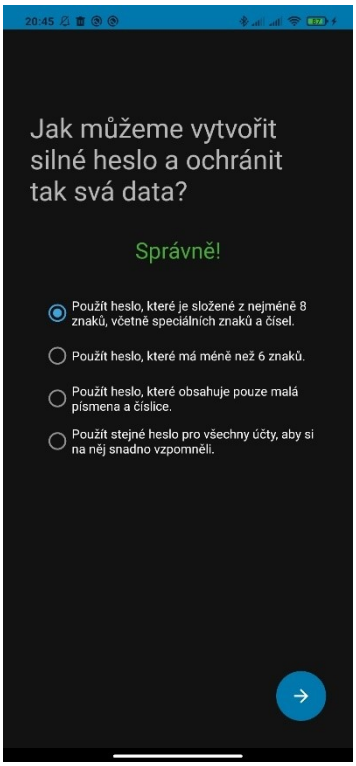


Obrázek 12: Ukázka TestPhishingActivity

Po dokončení uživatelem zvoleném počtu ukázek e-mailů je uživatel přesměrován na aktivitu TestCongratulationActivity, kde je informován o dokončení tématu, stejně jako v tématu Volba nejsilnějšího hesla. Podobně jako v předchozím tématu jsou phishingové e-maily zvoleny náhodně z více než dvaceti možností. Tyto možnosti jsou uchovávány v souboru testphishing.json a podobně jako sety hesel jsou zaměřeny na témata. Mezi témata patří neznámé adresy, pravopisné chyby, žádost o okamžitou akci, falešné odkazy a další ukazatele phishingových útoků. Tento soubor také obsahuje e-maily, které žádné příznaky phishingu neobsahují.

3.3.2.3 Všeobecné otázky

Třetím tématem této části jsou všeobecné otázky. Otázky jsou ve stejné formě, jako na konci tématu v části „Vzdělávat se“. Mají vytvořenou vlastní aktivitu TestQuestionActivity, protože se nepracuje s objekty learnItem, ale se samostatnými objekty třídy questionObject. Uživatel dostane otázku a čtyři možné odpovědi. Po zvolené odpovědi je informován, zda je odpověď správná nebo ne. Po zvolení správné odpovědi je uživateli umožněno jít na následující otázku.



Obrázek 13: Ukázka TestQuestionActivity

Pokud uživatel odpověděl na jím zvolený počet otázek, je přesměrován na aktivitu TestCongratulationActivity, kde je informován o dokončení všeobecných otázek. Objekty jsou načítány ze souboru testquestions.json. Tento soubor obsahuje stejné otázky, které se nacházejí v části „Vzdělávat se“, ale má i vlastní sadu otázek na různá témata bezpečnosti na internetu.

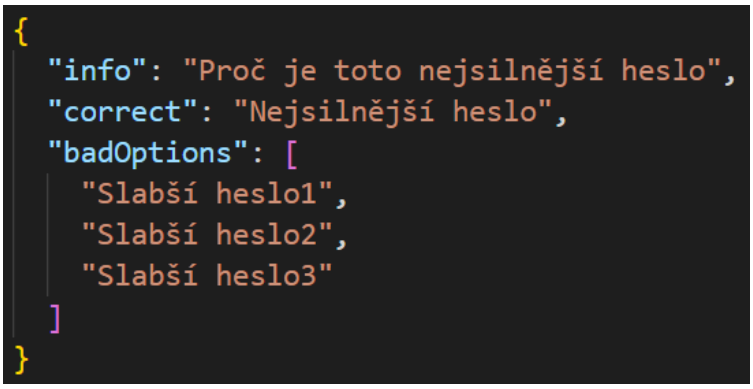
3.3.3 Načítání dat

Aby aplikace byla jednoduše rozšiřitelná po výskytu nových bezpečnostních hrozeb, je aplikace navržena tak, že data zobrazovaná v jednotlivých aktivitách jsou načítána ze souborů JSON. Například pro přidání nového tématu v části „Vzdělávat se” stačí přidat do souboru learnitems.json nový learnItem objekt. Formát uchovávání learnItemů je demonstrován na následujícím obrázku.

Obrázek 14: LearnItem JSON formát

Tyto objekty (a všechny ostatní JSON objekty) jsou čteny pomocí třídy HandlerJSON, která obsahuje statické metody, které slouží k práci s JSON soubory. Soubory obsahující data, jsou uložena v adresáři res/raw. Tento adresář slouží pouze ke čtení. Pro ukládání procenta dokončení tématu je třeba ukládat někam tuto hodnotu. Dále také ukládat index poslední otevřené stránky uživatelem, aby po opětovném otevření tématu mohl uživatel pokračovat tam, kde skončil. Pro ukládání těchto hodnot je vytvořen soubor, který se uloží v uložišti zařízení uživatele. Tento soubor obsahuje label, který je stejný jako label learnItemu. Místo dat ale obsahuje procento dokončení a index. Po načtení dat do třídy learn item jsou načtena tato data z uložiště uživatele, aby uživatel viděl, jak má rozpracovaná témata.

Data z části „Prověřit znalosti" jsou také ukládána v JSON souborech v adresáři raw/res. Data jsou ukládána v následujících formátech.



Obrázek 15: PasswordObject JSON formát

Obrázek 16: PhishingObject JSON formát

3.4 Další možný rozvoj aplikace

Do budoucna by se aplikace mohla rozšířit o nová témata o bezpečnosti v obou částech aplikace. Mohla by se také rozšířit o další nové funkcionality, které by mohly udělat aplikaci poučnější, zábavnější a lehčeji rozšiřitelnou pro vývojáře nebo samotné uživatele. Následuje pár možných rozšíření.

3.4.1 Aktualizace obsahu stahováním ze serveru

V momentální verzi aplikace je obsah načítán ze souborů, které jsou uložené v aplikaci. Pro přidání nového obsahu je třeba udělat aktualizaci aplikace. Tomu by se dalo předejít tím, že by se obsah, který uživatel vidí uložil na server, ze kterého by aplikace obsah stahovala. Obsah aplikace by se tak mohl přidávat a měnit rychleji a nezávisle na vývoji aplikace.

Uživatel má ve svém uložišti uložena procenta dokončení jednotlivých témat. Tato data by se také dala ukládat na server. Aby to bylo možné, muselo by se zavést přihlašování uživatelů do aplikace.

3.4.2 Vytváření individuálních testů

Obsah do aplikace mohou přidávat pouze vývojáři aplikace. Aplikace by se dala rozšířit o přidávání individuálních testů, které si navrhne uživatel. Tyto individuální testy by se daly využít například společnostmi, které by mohly vytvářet vlastní témata a testy pro své zaměstnance. Tím by je mohly vzdělávat o bezpečnostních nařízeních v jejich systémech a předejít tak bezpečnostním problémům.

Pro tuto funkcionalitu by bylo třeba rozšířit aplikaci o přihlašování uživatelů a zavést systém, který by evidoval, do jaké společnosti uživatel patří a jaké individuální testy se mu mají zobrazit. Aplikace by také byla rozšířena o možnost sledování, který z uživatelů již individuální test dokončil. Tato funkce by samozřejmě byla přístupná pouze správci individuálního testu. Správce testu by mohl informovat ostatní uživatele o nutnosti dokončení testu například pomocí notifikací.

3.4.3 Ukládání a sdílení výsledků

Momentálně jsou výsledky uživatelů ukládány pouze v části „Vzdělávat se“ a to ve formě procent dokončení jednotlivých témat. Aplikace by mohla ukládat také výsledky z části „Prověřit znalosti“ a všechny výsledky ukládat na server. A dále umožňovat sdílení svých výsledků s jinými uživateli a porovnávat je. Tím by se uživatelé navzájem motivovali k dokončování dalších témat a testů.

Aplikace by se dala rozšířit o aktivitu, která by sloužila k zobrazování výsledků v přehledné formě. Na této aktivitě by mohl uživatel vidět i výsledky jiných uživatelů, od kterých by měl povolení.

ZÁVĚR

Cílem této bakalářské práce bylo vytvoření mobilní aplikace pro výuku bezpečnosti na internetu. Aplikace uživatele v části „Vzdělávat se“ informuje o jednotlivých hrozbách, na které mohou na internetu narazit. Následně se jich ptá na otázky, kterými si uživatel své nově získané informace utvrdí.

Pokud si chce uživatel více vyzkoušet své znalosti, provede to v části aplikace „Prověřit znalosti“. V této části uživatele čekají tři úkoly. Prvním z nich je „Volba nejsilnějšího hesla“, ve kterém má uživatel na výběr ze čtyř možností a jeho úkolem je zvolit nejsilnější heslo. Dalším úkolem je „Je toto phishing?“, ve kterém se uživateli zobrazí ukázkový e-mail. Jeho úkolem je rozhodnout, zda se jedná o pokus o phishing nebo ne. Posledním úkolem je „Všeobecné otázky“. V tomto úkolu uživatel dostává otázky a ze čtyř možných odpovědí musí zvolit správnou. Aplikace je přizpůsobena na rozšíření po výskytu nových bezpečnostních hrozeb.

POUŽITÁ LITERATURA

[1] OR-MEIR, Ori, Nir NISSIM, Yuval ELOVICI a Lior ROKACH. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Computing Surveys* [online]. 2019, **52**(5), 1 - 48 [cit. 2023-04-16]. Dostupné z: https://dl.acm.org/doi/abs/10.1145/3329786

[2] DAOUD, Essam Al, Iqbal H. JEBRIL a Belal ZAQAIBEH. Computer Virus Strategies and Detection Methods. *Int. J. Open Problems Compt. Math* [online]. 2008, **1**(2), 122 - 129 [cit. 2023-04-16]. Dostupné z: http://emis.math.tifr.res.in/journals/IJOPCM/files/IJOPCM(vol.1.2.3.S.8).pdf

[3] ZHU, Zhenfang. Study on Computer Trojan Horse Virus and Its Prevention. *International Journal of Engineering and Applied Sciences (IJEAS)* [online]. 2015, **2**(8), 95 - 56 [cit. 2023-04-16]. ISSN 2394-3661. Dostupné z: https://www.neliti.com/publications/257840/study-on-computer-trojan-horse-virus-and-its-prevention

[4] PRATAMA, Andhika a Fauzi Adi RAFRASTARA. Computer Worm Classification. *International Journal of Computer Science and Information Security* [online]. 2012, **10**(4) [cit. 2023-04-16]. Dostupné z: https://www.researchgate.net/profile/Fauzi-Adi-Rafrastara/publication/299580232_Computer_Worm_Classification/links/5787544f08aeac8561ddf9fc/Computer-Worm-Classification.pdf

[5] EGELE, Manuel, Christopher KRUEGEL, Engin KIRDA, Heng YIN a Dawn SONG. Dynamic Spyware Analysis. *USENIX Annual Technical Conference* [online]. 2007, 233 - 246 [cit. 2023-04-16]. Dostupné z: https://www.usenix.org/legacy/events/usenix07/tech/full_papers/egele/egele.pdf

[6] FRUHLINGER, Josh. Ransomware explained: How it works and how to remove it. *CSO* [online]. 2020 [cit. 2023-04-15]. Dostupné z: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[7] How To Recognize, Remove, and Avoid Malware. *Federal Trade Commission* [online]. 2021 [cit. 2023-04-15]. Dostupné z: https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware

[8] ALEROUD, Ahmed a Lina ZHOU. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security* [online]. 2017, (68), 160-196 [cit. 2023-04-15]. ISSN 0167-4048. Dostupné z: https://doi.org/10.1016/j.cose.2017.04.006

[9] DEBCZAK, Michele. Warning: Don't Fall for the New Netflix Phishing Scam Going Around. *Mental Floss* [online]. 2018 [cit. 2023-04-15]. Dostupné z: https://www.mentalfloss.com/article/567886/new-netflix-phishing-scam-going-around

[10] Password Selection Tips. *CEFCU* [online]. [cit. 2023-04-15]. Dostupné z: https://www.cefcu.com/post/password_selection_tips.html

[11] FLORENCIO, Dinei, Cormac HERLEY a Baris COSKUN. *Do Strong Web Passwords Accomplish Anything?* [online]. In: . [cit. 2023-04-15]. Dostupné z: https://www.usenix.org/legacy/event/hotsec07/tech/full_papers/florencio/florencio.pdf

[12] KOMÁREK, David. *Služby pro online správu hesel*. Brno, 2014. Bakalářská práce. Masarykova Univerzita, Fakulta Informatiky. Vedoucí práce RNDr. Marek Kumpošt, Ph.D.

[13] SELTENREICH, Marián. Dvoufázová autentizace aneb vyšší bezpečnost! Proč to lidé podceňují?. *eABM* [online]. [cit. 2023-04-28]. Dostupné z: https://eabm.cz/1853-dvoufazova-autentizace-aneb-vyssi-bezpecnost

[14] NEPOŽITEK, Jan. *Antispamming na principu výběru vyžádaných zpráv*. Praha, 2007. Diplomová práce. Univerzita Karlova v Praze, Matematicko-fyzikální fakulta. Vedoucí práce RNDr. Ing. Jiří Peterka.

[15] SEKAL, Monika. Co je to hoax? A proč se posílá?. *Avast* [online]. 2020 [cit. 2023-04-28]. Dostupné z: https://www.avast.com/cz/besafeonline/blog/co-je-to-hoax-a-proc-se-posila

[16] Krádež identity. *ESET* [online]. [cit. 2023-04-15]. Dostupné z: https://www.eset.com/cz/kradez-identity/

[17] Nastavení a nástroje pro ochranu soukromí. *Facebook* [online]. [cit. 2023-04-29]. Dostupné z: https://www.facebook.com/settings?tab=privacy

[18] ZÁKLADNÍ PŘEHLED O TECHNOLOGII WIFI. *FCCPS* [online]. [cit. 2023-04-28]. Dostupné z: https://www.fccps.cz/zakladni-prehled-o-technologii-wifi

[19] DOMINIK, Tomáš. *Poskytování veřejného WiFi připojení*. Brno, 2018. Bakalářská práce. Masarykova Univerzita, Fakulta Informatiky. Vedoucí práce Mgr. Karol Kubanda.

[20] What is a man-in-the-middle attack?. *Mlytics* [online]. [cit. 2023-04-28]. Dostupné z: https://learning.mlytics.com/cyber-attacks/what-is-a-man-in-the-middle-attack/

[21] KOĎOUSKOVÁ, Barbora. HTTPS v kostce: co to je, jak funguje a jak na něj přejít. *Rascasone* [online]. 2021 [cit. 2023-04-29]. Dostupné z: https://www.rascasone.com/cs/blog/co-je-https-http-ssl-tls

[22] ŠPULÁK, Ondřej. Co je VPN a jak funguje?. *PCWorld* [online]. [cit. 2023-04-15]. Dostupné z: https://www.pcworld.cz/clanky/co-je-vpn-a-jak-funguje/

[23] KOLOUCH, Jan, Pavel BAŠTA a kol. *CyberSecurity*. Praha: CZ.NIC, z. s. p. o, 2019. ISBN 978-80-88168-34-8.

[24] Vzdělávací aplikace zaměřené na internetovou bezpečnost. *Šance Dětem* [online]. 2021 [cit. 2023-04-15]. Dostupné z: https://sancedetem.cz/vzdelavaci-aplikace-zamerene-na-internetovou-bezpecnost

[25] Digital Safety Resources. *Be Internet Awesome* [online]. [cit. 2023-04-15]. Dostupné z: https://beinternetawesome.withgoogle.com/en_us/educators

[26] Be Safe Online - Pro média. *Avast* [online]. [cit. 2023-04-15]. Dostupné z: https://www.avast.com/cz/besafeonline/pro-media

[27] Online bezpečnost pro kluky a holky. *Internet Highway* [online]. [cit. 2023-04-15]. Dostupné z: https://www.internethighway.cz/about.html

[28] Mobile Operating System Market Share Worldwide. *GlobalStats statcounter* [online]. [cit. 2023-04-15]. Dostupné z: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201402-202302

[29] CHEN, James. Android Operating System (OS): Definition and How It Works. *Investopedia* [online]. 2022 [cit. 2023-04-15]. Dostupné z: https://www.investopedia.com/terms/a/android-operating-system.asp

[30] Top Programming Languages for Android App Development. *GeeksforGeeks* [online]. 2022 [cit. 2023-04-15]. Dostupné z: https://www.geeksforgeeks.org/top-programming-languages-for-android-app-development/

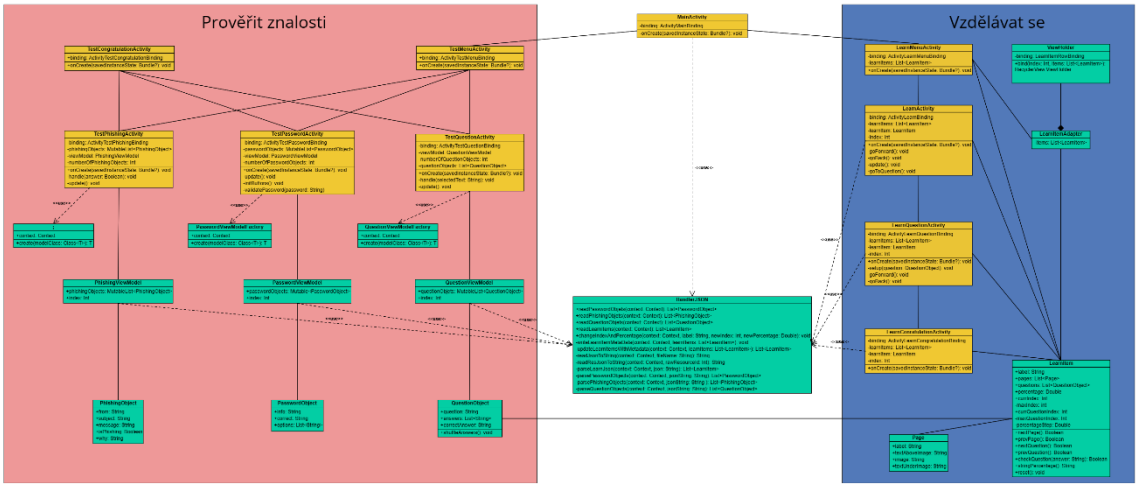
[31] Kotlin | Language for Android, now Official by Google. *GeeksforGeeks* [online]. 2022 [cit. 2023-04-15]. Dostupné z: https://www.geeksforgeeks.org/kotlin-language-android-now-official-google/

[32] SEMECKÝ, Vojtěch. Android Studio – nové vývojové prostředí. *Zdroják* [online]. 2013 [cit. 2023-04-15]. Dostupné z: https://zdrojak.cz/clanky/android-studio-nove-vyvojove-prostredi/

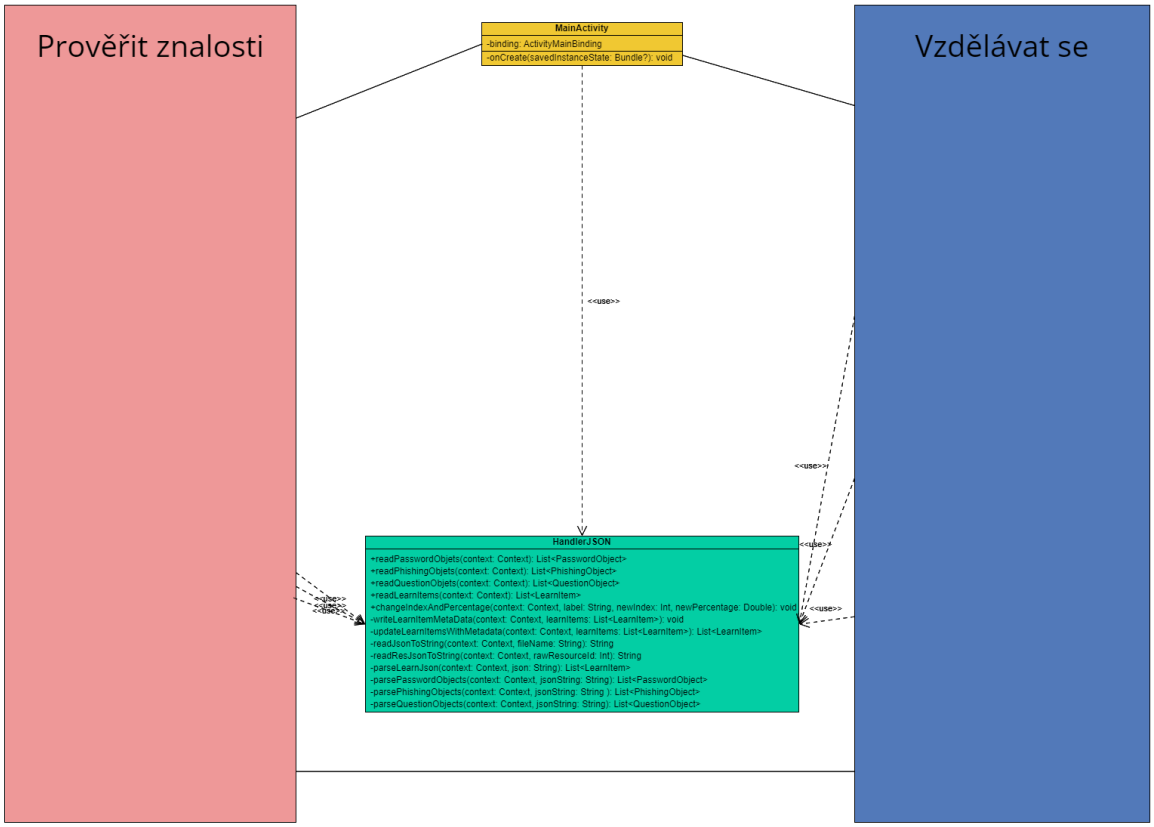
[33] HASSMAN, Martin. JSON : jednotný formát pro výměnu dat. *Zdroják* [online]. 2008 [cit. 2023-04-15]. Dostupné z: https://zdrojak.cz/clanky/json-jednotny-format-pro-vymenu-dat/

SEZNAM PŘÍLOH

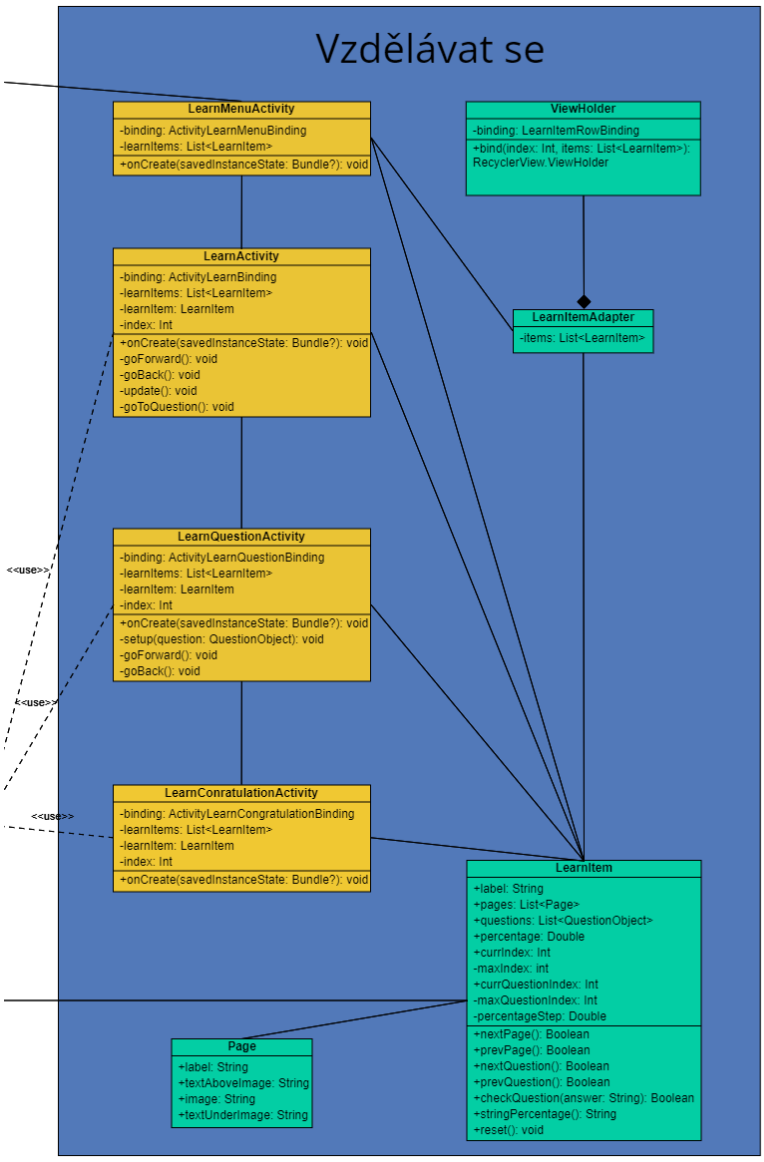
PŘÍLOHA A – kompletní UML diagram tříd



PŘÍLOHA B – zjednodušený UML diagram tříd



PŘÍLOHA C – UML diagram tříd části „Vzdělávat se“



PŘÍLOHA D – UML diagram tříd části „Prověřit znalosti“