Kapitola

[Bezpečnost používání mobilních telefonů]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: bit schulungscenter
Poslední úprava: 14.08.2020

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Co-funded by the
Erasmus+ Programme
of the European Union

Bezpečnost používání chytrých telefonů

Úvod

Sociální média, instant messaging, nakupování, hry, aplikace, rychlé pořizování fotografií nebo obyčejné „googlování“ - mnoho lidí si jen těžko dokáže představit každodenní život bez svého mobilního telefonu. Pro samotné telefonování se však smartphone používá stále méně. Jasným trendem je teď psaní namísto telefonování. To ukazuje i počet uživatelů služeb instant messaging: Asi 1,6 miliardy lidí na celém světě používá WhatsApp a asi 1,3 miliardy komunikuje se svými přáteli prostřednictvím služby Facebook Messenger. Používání těchto služeb je opravdu hračka. Jaká nebezpečí jsou však spojená s používáním služeb „instant messenger“ (okamžité zasílání zpráv) nebo jiných aplikací chytrých telefonů s ohledem na soukromí dat? Facebook nebo jiní poskytovatelé bezplatných aplikací pro chytré telefony jsou opakovaně kritizováni ochránci dat a ne bezdůvodně. Zjistěte, jak můžete lépe chránit svůj mobilní telefon, svá data a své soukromí!

Praktický význam – K čemu získané znalosti a dovednosti využijete

Po dokončení této kapitoly dokážete lépe posoudit rizika spojená s používáním služeb rychlého zasílání zpráv nebo jiných aplikací chytrých telefonů a budete znát některé užitečné kroky, které ochrání před nežádoucími riziky nejen váš mobilní telefon, ale také vaše soukromí.

Přehled výukových cílů a získaných kompetencí

V HVC_ Bezpečnost používání mobilních telefonů_01 obdržíte informace o některých základních bezpečnostních opatřeních v případě ztráty nebo odcizení vašeho smartphonu. V HVC_ Bezpečnost používání mobilních telefonů _02 se z příkladu aplikace WhatsApp dozvíte, proč aplikace vyžadují přístupová práva a proč byste je měli omezit na minimum. V HVC_ Bezpečnost používání mobilních telefonů_03 se dozvíte o slabinách v zabezpečení rychlého zasílání zpráv a dalších aplikací. V HVC_ Bezpečnost používání mobilních telefonů_04 se dozvíte o některých opatřeních a tipech pro bezpečné používání aplikací chytrých telefonů a také jak provést nastavení ochrany soukromí pro často používané aplikace.

Hlavní výukové cíle	Dílčí výukové cíle

HVC_ Bezpečnost používání mobilních telefonů_01 Znáte některá základní ochranná opatření pro vaše chytré telefony.	DVC_Bezpečnost používání mobilních telefonů_01_01: Umíte přijmout opatření na ochranu svého mobilního telefonu před neoprávněným přístupem. DVC_Bezpečnost používání mobilních telefonů_01_02: Umíte jmenovat některá užitečná opatření v případě ztráty nebo krádeže vašeho smartphonu.
HVC_ Bezpečnost používání mobilních telefonů _02 Víte, že používání aplikací jako WhatsApp vyžaduje udělení určitých přístupových oprávnění k aplikaci a víte, že byste je měli omezit na minimum.	DVC_Bezpečnost používání mobilních telefonů_02_01: Umíte vysvětlit, co znamená instant messaging (IM) a dokážete uvést příklady oblíbených služeb okamžitého zasílání zpráv. DVC_Bezpečnost používání mobilních telefonů_02_02: Umíte vysvětlit na příkladu aplikace WhatsApp, které předpoklady musí být obvykle splněny pro použití aplikace. DVC_Bezpečnost používání mobilních telefonů_02_03: Umíte uvést příklady, kdy a jak má smysl upravit oprávnění aplikace.
HVC_ Bezpečnost používání mobilních telefonů_03 Znáte bezpečnostní problémy a nežádoucí důsledky používání služeb rychlého zasílání zpráv nebo jiných aplikací pro chytré telefony.	DVC_Bezpečnost používání mobilních telefonů_03_01: Umíte uvést důvody, proč se uživatelé aplikací stále více obávají o bezpečnost svých dat. DVC_Bezpečnost používání mobilních telefonů_03_02: Umíte uvést příklady toho, jaká bezpečnostní rizika a nežádoucí důsledky mohou služby rychlého zasílání zpráv a další aplikace způsobit.
HVC_ Bezpečnost používání mobilních telefonů_04 Znáte opatření a tipy pro bezpečné používání aplikací chytrých telefonů.	DVC_Bezpečnost používání mobilních telefonů_04_01: Dokážete vysvětlit, co je třeba vzít v potaz při používání aplikací v mobilních telefonech pro to, abyste ochránili sebe a své soukromí. DVC_Bezpečnost používání mobilních telefonů_04_02: U oblíbených aplikací, jako je WhatsApp nebo Facebook Messenger, dokážete upravit nastavení ochrany osobních údajů.

1. Základní ochranná opatření chytrých mobilních telefonů

Pro mnoho lidí je jejich mobilní telefon stálým společníkem v každodenním životě. Patříte také k těm, kteří berou svůj chytrý telefon všude a neobejdou se bez něj ani minutu? Pokud ano, pravděpodobně máte také ve svém telefonu uložena **velmi soukromá nebo citlivá data**, jako jsou fotografie, důvěrné textové zprávy nebo obchodní informace. Chcete-li chránit svůj mobilní telefon a Vaše soukromá data, která ukládá, měli byste být schopni podniknout v případě ztráty nebo krádeže příslušná opatření.

Co-funded by the
Erasmus+ Programme
of the European Union

To zahrnuje například ochranu mobilního telefonu proti neoprávněnému přístupu pomocí **PIN kódu** (Osobní identifikační číslo) a **zámku obrazovky.**

Důležité
Ujistěte se, že **nepoužíváte běžné číselné kombinace**, jako je „1234“, „1111“ nebo podobně. Tyto kombinace jsou velmi snadno hacknutelné neoprávněnými osobami.

Pokud dojde ke ztrátě nebo odcizení Vašeho mobilního telefonu, měli byste mít **SIM kartu** (z angl.”subscriber identity module”, česky „účastnická identifikační karta“) zařízení **zablokovanou** vaším síťovým poskytovatelem tak, aby ji nikdo nemohl používat k telefonování nebo aby vám nemohly vzniknout vysoké náklady spojené s neoprávněným užíváním Vašeho telefonu.

Znáte **sériové číslo vašeho smartphonu**? Nachází se pod baterií, na originálním balení nebo na faktuře za nákup mobilního telefonu. **Toto číslo byste si měli poznamenat**, abyste jej mohli v případě krádeže nahlásit policii.

Všechny běžné operační systémy také nabízejí **různé služby**, které mohou být velmi užitečné v případě krádeže nebo ztráty.

Příklady
Nemůžete najít svůj mobilní telefon? Pomocí **správce zařízení Android** můžete nechat svůj telefon vyzvánět při maximální hlasitosti, i když byl ztlumený. Tímto způsobem můžete rychle najít doma ztracený telefon. Pokud se ztracený telefon nachází na jiném místě, můžete ho najít v reálném čase a nechat zprávu pro nálezce. Pokud se váš iPhone ztratil nebo byl ukraden, můžete ho obvykle vyhledat přes **iCloud**, pod podmínkou, že je zařízení zapnuté a má přístup k mobilním datům.

Pravděpodobně jste již slyšeli o možnosti instalace jakési **aplikace proti krádeži** do vašeho mobilního telefonu. Umožňuje například lokalizovat a zamknout ztracený nebo ukradený smartphone a smazat na něm uložená data. Požadované příkazy mohou být vydány jiným smartphonem, jehož číslo bylo uloženo nebo odesláno na zařízení prostřednictvím online portálu.

Tip
V případě krádeže nebo ztráty byste měli SIM kartu okamžitě zablokovat, pokud **nemáte v telefonu nainstalovánu aplikaci proti krádeži.** Pokud je však aplikace nainstalována, SIM karta by neměla být blokována, dokud nejsou data lokalizována a vzdáleně odstraněna. Po zablokování SIM karty to již není možné.

1. Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_01_01

Zadání: Jaká opatření můžete podniknout k ochraně svého mobilního telefonu před neoprávněným přístupem?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Mohu použít PIN. Tento PIN by měl být co nejsnadněji zapamatovatelný.
- **Měl bych zamknout svůj smartphone pomocí PIN kódu a ujistit se, že se nejedná o kombinaci čísel, jako je 1234 nebo 1111.**
- **Mohu nastavit zámek obrazovky.**
- Mohu nainstalovat placenou aplikaci pro nastavení osobního identifikačního čísla.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_01_02

Zadání: Po odpoledním nakupování ve městě si najednou doma uvědomíte, že jste ztratili svůj mobilní telefon. Jaká opatření mohou být v takové situaci užitečná?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **K vyhledání mobilního telefonu mohu použít správce zařízení Android nebo iCloud.**
- **V takových případech mohu nainstalovat nějaký druh aplikace proti krádeži. To mi umožní vyhledat můj telefon, zamknout jej nebo smazat uložená data v telefonu.**
- Mohu mít zablokovanou SIM kartu, abych mohl lokalizovat svůj telefon.
- **Mohu zablokovat SIM kartu, abych tak někomu zabránilv používání mého telefonu a vyhnul se tak vysokým nákladům, které by tak mohly vzniknout.**

2. Instant Messaging (IM) a aplikace

Možnost výměny textových zpráv prostřednictvím mobilního telefonu není nic nového. V posledních letech však v důsledku rozšířeného používání chytrých telefonů byla komunikace prostřednictvím SMS stále více nahrazována používáním služeb **tzv. instant messaging, zkráceněIM (česky "služba pro okamžité zasílání zpráv").**

Definice
Na rozdíl od SMS služeb, **IM** je **rychlá komunikace** přes internet prostřednictvím **mobilních aplikací**. Jedná se o typ online chatu, který umožňuje výměnu zpráv s ostatními uživateli v téměř reálném čase. K tomu je nutné stáhnout a nainstalovat aplikace pro instant messaging.

Kromě přenosu textů je obvykle možný i přenos souborů jak zvukových, tak i video sekvencí (a tedy i videochatu). Přenos zprávy probíhá v rámci tzv. **push procedury**, která umožňuje, aby texty dorazily k příjemci ihned po odeslání. Na rozdíl například od e-mailů nemusí být zprávy nejprve načteny, ale zobrazí se okamžitě na obrazovce komunikačního partnera.

Příklad:
Příklady populárních služeb rychlého zasílání zpráv: • Windows life messenger • Skype • Facebook Messenger • WhatsApp • WeChat • Telegram

Například přibližně 1,3 miliardy uživatelů po celém světě již ke komunikaci používá službu Facebook Messenger.

Nejčastější využití programů rychlého zasílání zpráv je na mobilních zařízeních jako jsou **smartphony** prostřednictvím **messengerových aplikací**. Aplikace Messenger jsou obvykle zdarma, praktické, snadno použitelné, a proto se těší rostoucí popularitě. Chcete-li například používat aplikaci WhatsApp, stačí si stáhnout bezplatnou aplikaci a zaregistrovat se přes vlastní číslo mobilního telefonu.

Ke splnění požadovaného účelu však aplikace obvykle vyžaduje různé **autorizace**. Proto aplikace vyžaduje přístup k určitým funkcím zařízení vašeho smartphonu jako je kalendář, kamera, kontakty, mikrofon, SMS, paměť, poloha nebo k jiným funkcím telefonu.

Důležité
Jste jedním z 1,6 miliardy uživatelů WhatsApp na celém světě? Pak byste si měli být vědomi toho, že aplikace WhatsApp má přístup minimálně **ke všem kontaktům uloženým ve Vašem mobilním telefonu.**

To je jediný způsob, jak může aplikace určit, který z vašich kontaktů také používá WhatsApp a automaticky je v aplikaci zobrazit. Chcete odeslat obrázky nebo vlastní polohu přes WhatsApp aplikaci nebo ji použít pro videohovor? Pokud ano, měli byste si být vědomi toho, že WhatsApp také potřebuje přístup k vašim snímkům, fotoaparátu, mikrofonu a lokalizačním údajům!

Tip
Z důvodu ochrany údajů se vyplatí být opatrný při přidělování **autorizací aplikacím** a také se vyplatí snížit autorizace na nezbytnou úroveň.

Pokud si nejste jisti, jaká oprávnění má každá aplikace ve vašem smartphonu nastavena, měli byste tato oprávnění z bezpečnostních důvodů zkontrolovat. Nevíte, jak to udělat? Jednoduše vyberte příslušnou aplikaci a v „nastavení“ se podívejte, které přístupy aplikaci povolujete, a v případě potřeby je upravte.

Co-funded by the
Erasmus+ Programme
of the European Union

Příklad

Předpokládejme, že byste chtěli pomocí Google Maps najít konkrétní adresu. V tomto případě má smysl během používání aplikace povolit **přístup k vaší poloze** Pokud však nechcete sdílet svou polohu se svými kontakty prostřednictvím aplikace WhatsApp, nemusí aplikace nutně vědět, kde se nacházíte.

2. Procvičte si znalosti

Co-funded by the
Erasmus+ Programme
of the European Union

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_01

Zadání: Které z následujících výroků o službách rychlého zasílání zpráv (IM) jsou správné?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Stále více lidí používá služby IM k výměně textových zpráv, zatímco komunikace prostřednictvím SMS ztratila na popularitě.**
- **IM je internetová komunikace.**
- **IM umožňuje nejen výměnu textových zpráv, ale také výměnu souborů, audia nebo komunikaci prostřednictvím videochatu.**
- Pokud mnoho lidí používá populární IM služby současně, obvykle trvá několik minut, než příjemce obdrží zprávy.
- **Mezi oblíbené IM služby patří Facebook Messenger, WhatsApp nebo Windows messenger.**
- Populární IM služby jsou Youtube, Twitter, WhatsApp a Google.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_02

Zadání: Chcete pomocí aplikace WhatsApp komunikovat se svými přáteli. Čeho byste si měli být vědomi při instalaci aplikace?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Aplikace Messenger nebo WhatsApp obvykle vyžadují jednorázovou platbu uživatelského poplatku předem.
- Chcete-li používat WhatsApp, musíte si stáhnout aplikaci a zaregistrovat se svým skutečným jménem.
- **WhatsApp přistupuje ke všem kontaktům uloženým ve vašem mobilním telefonu.**
- **Chcete-li používat určité služby WhatsApp, může aplikace požadovat přístup k vašim obrázkům, kameře, mikrofonu nebo údajům o Vaší poloze.**
- WhatsApp automaticky přistupuje ke všem kontaktům uloženým ve Vašem mobilním telefonu, k Vašim obrázkům a údajům o Vaší poloze. To je jediný způsob, jak aplikace může fungovat.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_02_03

Zadání: Kdy má smysl upravovat autorizace aplikací a jak je to v zásadě možné?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **V zásadě si můžete v sekci „Nastavení“ snadno zkontrolovat, které z nainstalovaných aplikací vlastní přístupová práva a v případě potřeby je omezit na skutečně nezbytný rozsah.**
- Chcete-li zjistit, která přístupová práva konkrétní aplikace má, je vhodné zavolat poskytovateli mobilních telefonů.
- **Chcete-li například používat Mapy Google, je dobré povolit aplikaci přístup k vašim údajům o poloze, když ji používáte.**
- Je také dobré povolit aplikaci WhatsApp přístup k vašim údajům o poloze, protože to pomůže rychleji přenášet vaše zprávy.

- Protože většina aplikací je bezplatná, obvykle není možné omezit přístupová práva k aplikacím jednotlivě.

3. Bezpečnostní rizika při používání mobilní aplikace

Pokud také v mobilním telefonu ukládáte a zpracováváte velké množství dat, částečně velmi soukromého charakteru a od třetích stran (např. fotografie), měli byste zvážit, do jaké míry mohou být **neomezená povolení aplikace** problematická.

Není žádným tajemstvím, že mnoho výrobců aplikací má zájem o vaše osobní údaje. Koneckonců potřebují generovat určitou formu příjmů z aplikací, které jsou uživatelům často poskytovány zdarma. **Pokud za produkt neplatíte, pak jste obvykle produktem.** Ale to ještě není důvod k obavám. Ve většině případů je používání našich osobních údajů anonymizováno v rámci právních předpisů na ochranu osobních údajů.

Například převzetí **aplikace WhatsApp společností Facebook** však znamená, že telefonní čísla z adresáře kontaktů jsou předána také společnosti Facebook. Kromě toho, odhalení různých incidentů v oblasti ochrany soukromí v minulosti vedlo také k uvědomění si nebezpečí neoprávněného sledování. Uživatelé se tak stále více zajímají o ochranu údajů.

Zajímá Vás, jaké bezpečnostní problémy a nežádoucí důsledky pro vás může mít používání služeb okamžitého zasílání zpráv a dalších aplikací? Zde je několik příkladů:

- Stejně jako u jiných online komunikačních médií, i v případě messenger aplikací hrozí riziko zasílání **phishingových odkazů nebo přenosu malwaru** prostřednictvím hypertextových odkazů, na které lze kliknout, nebo jiných přenesených souborů.
- Existuje nebezpečí, že se v **aplikacích skrývá malware všeho druhu**, zejména pokud byly aplikace zakoupeny zdarma na internetu od méně známých poskytovatelů aplikací.

- Jak již víte, aplikace získávají oprávnění k provádění funkcí. Tato oprávnění umožňují aplikacím číst data. Existuje tedy **riziko skrytého přístupu k osobním údajům**, jako jsou lokalizační údaje, návyky v surfování na internetu, uložené kontaktní údaje nebo hesla. Kromě ztráty soukromí může být nepříjemným důsledkem také **zneužití Vašich kontaktních údajů**.
- **Problémy s autorským právem** mohou nastat například v případě, že se jako profilové fotografie použijí obrázky, které jste nevytvořili sami a pro které nevlastníte autorská práva.
- **Nešifrovaná komunikace** představuje vysoké bezpečnostní riziko. Od dubna 2016 je tedy například obsah odeslaný prostřednictvím WhatsApp přenášen se zabezpečeným šifrováním typu end-to-end. To se týká textů, obrázků, videí a dalších souborů. End-to-end šifrování znamená, že pouze příslušní komunikační partneři mohou přijímat a číst obsah.

Důležité
Pokud používáte **aplikaci Facebook Message**, měli byste si být vědomi, že vaše komunikace (na rozdíl od WhatsApp) není v zásadě šifrována! Chcete-li chatovat pomocí šifrování typu end-to-end, musíte zahájit „tajnou konverzaci“. Jak taková konverzace funguje, bude vysvětleno v následující kapitole.

3. Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_01

Zadání: Proč se uživatelé aplikací stále více zajímají o ochranu osobních údajů?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- Protože aplikace používá stále víc a víc lidí.
- Protože aplikace jsou primárně vyvíjeny společnostmi se sídlem v zemích, které se nestarají o ochranu dat, a proto neexistují žádná závazná pravidla o ochraně dat pro nakládání s uživatelskými daty. Známým příkladem je Facebook nebo WhatsApp.
- Protože aplikace jsou stále dražší.
- **Protože v posledních letech vyšly najevo některé případy porušení ochrany osobních údajů.**
- Protože uživatelé nemohou pochopit, jaká přístupová práva jsou udělena různým poskytovatelům aplikací.
- Protože uživatelé ukládají stále více a v fotografií a dalších souborů do svých smartphonů, a proto je kapacita úložiště jejich telefonu brzy vyčerpána.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_03_02

Zadání: Jaká bezpečnostní rizika a nežádoucí důsledky mohou služby instant messaging a jiné aplikace způsobit?
Úkol: Vyberte správné možnosti podle principu více možností: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Messengerové aplikace s sebou nesou riziko odesílání phishingových odkazů nebo přenos škodlivého softwaru prostřednictvím klikatelných hypertextových odkazů nebo jiných přenesených souborů.**
- **Malware může být přítomen zejména v bezplatných aplikacích od méně známých poskytovatelů.**
- Velkým problémem jsou spíše skryté vysoké náklady než tajný přístup k osobním údajům.
- Nešifrovaná komunikace, jako je tomu obvykle například přes WhatsApp, je hlavním bezpečnostním problémem.
- Osobní data mohou být ztracena šifrovanou komunikací.

4. Opatření a tipy pro bezpečné používání mobilních aplikací chytrých telefonů

Vzhledem k možným bezpečnostním rizikům používání aplikací ve vašem mobilním telefonu Vás pravděpodobně zajímá, jak můžete lépe chránit sebe a své soukromí. Následuje několik tipů**, co zvážit při používání aplikací ve vašem mobilním telefonu:**

V minulosti byly v různých aplikacích zjištěny závažné bezpečnostní nedostatky. Následně byl učiněn pokus tyto nedostatky napravit provedením vhodných úprav. Z tohoto důvodu je například vhodné vždy používat **nejnovější verzi aplikace WhatsApp Messenger.**

Chcete-li předejít problémům s autorskými právy, měli byste se na svém profilu **zdržet používání obrázků, které nevlastníte.**

Tip
Můžete také použít nastavení ochrany osobních údajů aplikace WhatsApp k **omezení viditelnosti vašeho profilu**: Stačí otevřít aplikaci WhatsApp a klepnout na tlačítko „Nastavení". Potom klepněte na tlačítko „Účet", zvolte možnost „Soukromí" a změňte nastavení profilové fotografie „Všichni" na „Moje kontakty" nebo „Nikdo".

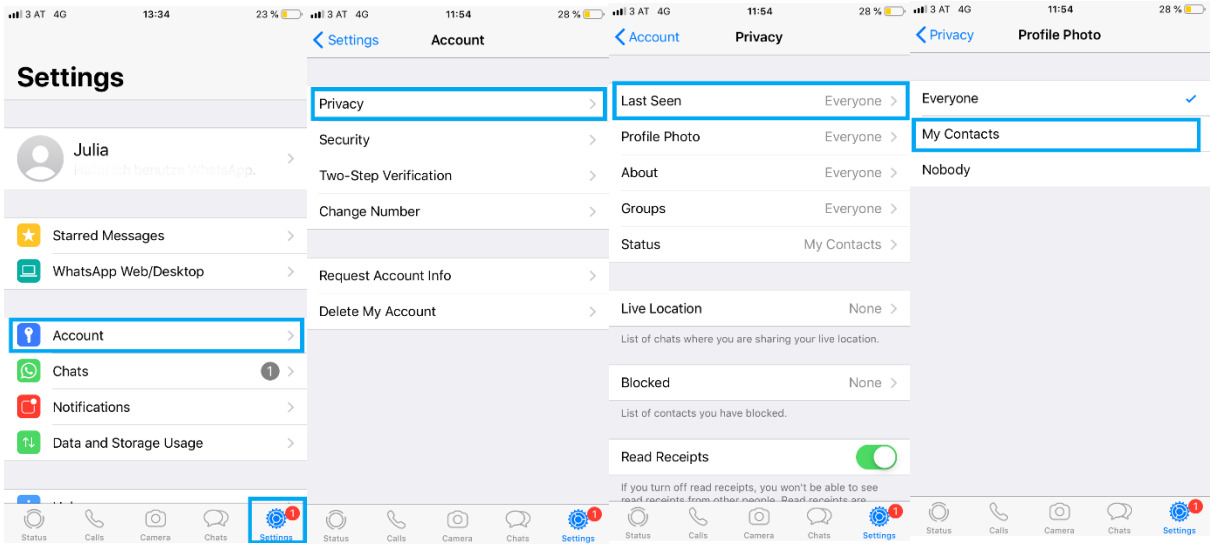
Poskytovatelé aplikací jsou povinni poskytnout uživateli **prohlášení o ochraně údajů**, které obsahuje informace o oprávněních požadovaných aplikací. Většina aplikací dnes navíc vyžaduje, abyste při jejich instalaci s těmito **oprávněními souhlasili**. Před instalací byste si měli důkladně **přečíst zásady ochrany osobních údajů** a podmínky každé aplikace. Měli byste také **kontrolovat přístupová práva aplikací!** Udělená oprávnění lze kdykoli v nastavení pro každou aplikaci zobrazit a zrušit.

Příklad
Je například samozřejmé, že aplikace pro předpověď počasí musí být schopna zjistit Vaši polohu, aby dokázala poskytnout přesnější informace o předpovědi. Není však už tolik zřejmé, proč by tato aplikace měla vyžadovat přístup k Vašemu fotoaparátu.

Měli byste v aplikaci zadat pouze ty nejnutnější údaje. Použijte **zvláštní e-mailovou adresu**, která toho o vás moc neprozradí a nebude vás obtěžovat, pokud jde o spam.

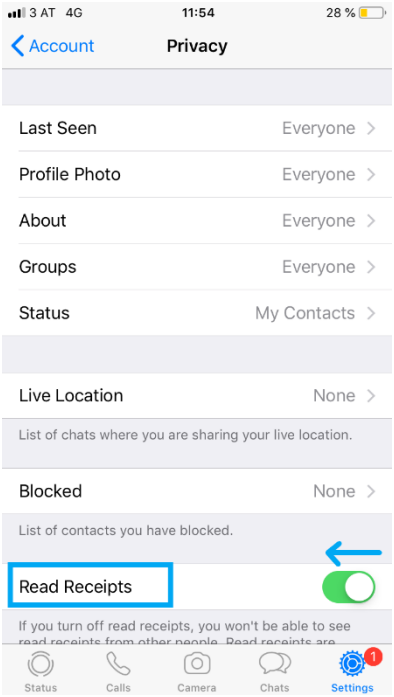
Údajně velkou výhodou IM je to, že je vždy okamžitě zřejmé, kdy je kontakt online nebo kdy byl naposledy online. Nové nastavení ochrany osobních údajů některých messengerů Vám však umožňuje **zabránit ostatním, aby věděli, že jste online, kdy jste byli naposledy online, nebo vypnout automatická potvrzení čtení.** Jak to funguje, dokládá následující příklad aplikace WhatsApp:

- **Jak skrýt „Naposledy“:** Otevřete aplikaci WhatsApp a klepněte na tlačítko „Účet”. Pak klepněte na tlačítko „Soukromí”, vyberte „Naposledy“ a vyberte, kdo nebo jestli někdo může vidět, kdy jste byli naposledy online.

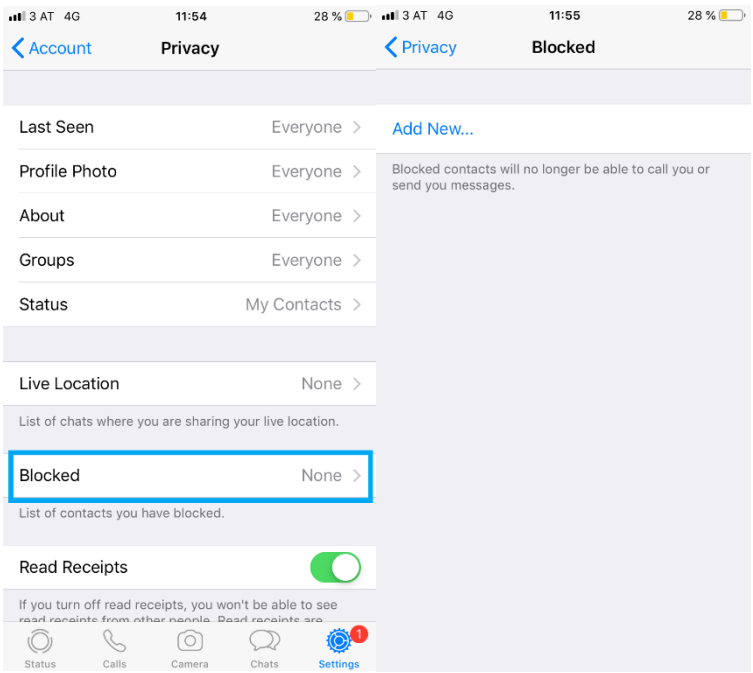


- **Jak vypnout potvrzení o přečtení**: Klepněte znovu na „Nastavení“, „Účet“ a „Soukromí“. Pak jednoduše deaktivujte oznámení o přečtení.

Co-funded by the
Erasmus+ Programme
of the European Union



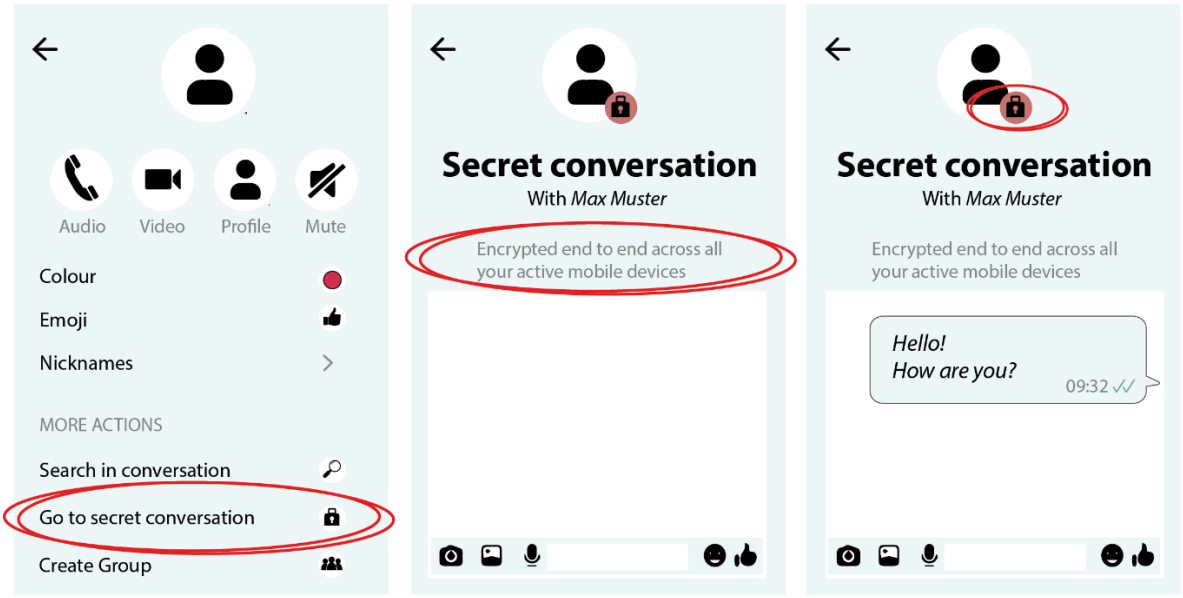
Abychom předešli nevyžádanému kontaktu s cizími lidmi, je třeba v první řadě vždy **pečlivě zvážit, v jakých případech bychom měli své telefonní číslo uvést,** a především komu bychom jej měli sdělit! Pokud se vás nežádoucí osoby pokusí kontaktovat prostřednictvím aplikace WhatsApp, můžete je jednoduše zablokovat. Chcete-li tak učinit, posuňte se dolů v položce „Soukromí“ a klepněte na blokované kontakty.



Důležité
Blokujte ty kontakty, u kterých si nejste jisti, o koho se jedná nebo pokud vás obtěžují. Veškeré urážky, sexuální obtěžování, vydírání nebo vyhrůžky nahlaste policii.

Některé aplikace, jako je Facebook Messenger, **Vaše zprávy automaticky nešifrují**. Pokud je to možné, měli byste šifrování nastavit ručně.

Jak komunikovat šifrovaně pomocí Facebook Messenger: Přejděte na chat, klepněte na jméno osoby a vyberte „Tajná konverzace“. Nyní je výměna zpráv s touto osobou šifrována způsobem end-to-end. Vaše zprávy neuvidí nikdo jiný kromě Vás a partnera na chatu, dokonce ani Facebook.



Tip
Šifrovaný chat poznáte podle toho, že uživatelské rozhraní je **šedočerné**. Také na profilu partnera chatu uvidíte **malý černý zámek**.

4. Procvičte si znalosti

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_04_01

Zadání: Co je třeba vzít v úvahu při používání mobilních aplikací, abyste ochránili sebe a své soukromí?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Před instalací byste si měli důkladně přečíst zásady ochrany osobních údajů a podmínky každé aplikace.**
- Pokud je to možné, neměli byste souhlasit s žádnou aktualizací aplikací.
- Není bezpečné používat profilové fotografie sebe sama. Je lepší používat obrázky, které jste si sami nepořizovali, ale které jste našli někde na internetu.
- **Měli byste kontrolovat přístupová práva aplikací a vhodně je upravovat**.
- K registraci byste měli použít seriózní e-mailovou adresu (např. sestávající z vašeho skutečného jména a příjmení).
- **Měli byste o sobě poskytovat jen tolik informací, kolik je nezbytně nutné.**

Co-funded by the
Erasmus+ Programme
of the European Union

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_04_02

Zadání: Jak můžete upravit nastavení ochrany soukromí v populárních aplikacích jako je WhatsApp nebo Facebook Messenger pro zvýšení ochrany Vašich osobních údajů?
Úkol: Vyberte správné možnosti podle principu více správných odpovědí: Žádná, jedna, více než jedna nebo všechny možnosti mohou být pravdivé.

- **Například při používání WhatsApp aplikace mohu v části Nastavení a Soukromí zakázat, aby ostatní uživatelé viděli, kdy jsem byl naposledy online.**
- Mohu například zamezit WhatsApp aplikaci v přístupu ke svým kontaktům v části Nastavení a Soukromí.
- **Při používání aplikace WhatsApp také mohu deaktivovat potvrzení čtení nebo blokovat nežádoucí kontakty kliknutím na Nastavení, Účet a Soukromí.**
- **Mohu také používat Facebook Messenger pro šifrovanou komunikaci se svými přáteli: Za tímto účelem jdu na příslušný chat, vyberu jméno osoby a jednoduše zahájím tajnou konverzaci.**
- Pro komunikaci s kontakty, které jsou blokovány na aplikaci WhatsApp, vyberu jméno osoby a zahájím „tajnou konverzaci“.

Zdroje

klicksafe.de: https://www.klicksafe.de/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/was-ist-der-whatsapp-messenger/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/probleme-mit-dem-whatsapp-messenger/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/whatsapp/schritt-fuer-schritt/kontakte-blockieren/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/faq/was-ist-eine-geheime-unterhaltung-im-messenger/

saferinternet.at:https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/schritt-fuer-schritt/verschluesselt-chatten/

digitaltrends.com: https://www.digitaltrends.com/mobile/how-to-protect-your-smartphone-from-hackers-and-intruders/

techsafe.org: https://www.techsafety.org/12tipscellphones

avast.com: https://blog.avast.com/9-smartphone-tips-privacy-security

Co-funded by the
Erasmus+ Programme
of the European Union

fraud-magazine.com: https://www.fraud-magazine.com/article.aspx?id=4294992799

Zapamatujte si

Shrnutí

Pro většinu z nás je **mobilní telefon** nedílnou součástí každodenního života. Proto bychom neměli zapomenout odpovídajícím způsobem chránit soukromé informace a data na nich uložená. Například pro případy ztráty nebo odcizení vašeho mobilního telefonu má smysl **používat zabezpečený PIN kód** (nikoli kombinaci čísel jako je 1234) a **zámek obrazovky**. Měli byste také zvážit instalaci nějaké **aplikace proti krádeži**.

Poskytovatelé aplikací instant messagingu, jako je WhatsApp, jsou stále populárnější. Při používání těchto nebo jiných aplikací byste však měli vždy zvážit, jaká **přístupová práva aplikaci udělujete**, a omezit je na minimum.
Už jste někdy přemýšleli, proč je používání WhatsApp aplikace zdarma? Při používání bezplatných aplikací byste si měli být vždy vědomi skutečnosti, že: Pokud za produkt nemusíte platit, **obvykle jste produktem vy nebo vaše data.** Kromě toho existuje nebezpečí, že v aplikacích bude skrytý **různý malware**, zejména pokud jsou tyto aplikace distribuovány na internetu zdarma a málo známými poskytovateli aplikací. Dalším bezpečnostním rizikem je skutečnost, že někteří poskytovatelé online komunikace **nešifrují komunikaci** (např. Facebook Messenger).

Po převzetí WhatsApp aplikace společností Facebook zaujalo mnoho uživatelů kritičtější postoj k zásadám ochrany osobních údajů v těchto službách. Aplikace jsou proto neustále optimalizovány s ohledem na předpisy o ochraně údajů. Z tohoto důvodu například dává smysl vždy používat **nejnovější verzi WhatsApp Messenger**. Před použitím aplikace byste si také měli přečíst **zásady ochrany osobních údajů**, zkontrolovat přístupová práva aplikace a v případě potřeby je upravit. Můžete také snadno **upravit nastavení soukromí aplikací**, například viditelnost profilového obrázku na WhatsApp aplikaci nebo blokování nechtěných kontaktů.