



Kapitola [Bezpečnost používání mobilních telefonů]

Projekt: B-SAFE

Číslo: 2018-1CZ01-KA204-048148

Jméno autora: bit schulungscenter

Poslední úprava: 14.08.2020

Jméno autora: bit cz training

Poslední úprava: 24.6.2020

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."



Téma Bezpečnost používání chytrých telefonů

Úvod

Sociální média, ~~instant messenger~~ instant messaging, nakupování, hry, aplikace, rychlé pořizování rychlé fotografie nebo nějaké ~~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 ted' psaní namísto telefonování. To ukazuje i ~~pohled na~~ počet uživatelů služeb rychlých zpráv 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 ~~dětská hra~~ opravdu hračka. Jaká nebezpečí jsou však ěňhají spojená při s používáním služeb „instant messenger“ (okamžité zasílání zpráv) nebo jiných aplikací chytrých telefonů s ohledem na soukromí dat? ~~Není~~ bez důvodně, že Facebook nebo jiní poskytovatelé bezplatných aplikací pro chytré telefony jsou opakovaně kritizováni ochránci dat a ne bez důvodně. 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 ~~náplně~~ výuky kapitoly budete moci dokázete 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 jak nejen váš mobilní telefon, tak ale také vaše soukromí před nežádoucími riziky.



Přehled výukových cílů a získaných kompetencí

V LOHVC – Bezpečnost používání mobilních telefonů_01 obdržíte informace o některých základních bezpečnostních opatřeních v případě ztráty nebo odcizení vašeho smartphonu. V LOHVC – 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 LOHVC – Bezpečnost používání mobilních telefonů_03 se dozvíte o slabinách v zabezpečení rychlého zasílání zpráv a dalších aplikací. V LOHVC – 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
LOHVC – Bezpečnost používání mobilních telefonů_01 Znáte některá základní ochranná opatření pro vaše chytré telefony.	FODVC – Bezpečnost používání mobilních telefonů_01_01: Umíte přijmout opatření na ochranu svého mobilního telefonu před neoprávněným přístupem. FODVC – Bezpečnost používání mobilních telefonů_01_02: Umíte jmenovat některá užitečná opatření v případě ztráty nebo krádeže vašeho smartphonu.
LOHVC – 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.	FODVC – Bezpečnost používání mobilních telefonů_02_01: Umíte vysvětlit, co znamená rychlé zasílání zpráv instant messaging (IM), a dokážete uvést příklady oblíbených služeb rychlého okamžitého zasílání zpráv. FODVC – Bezpečnost používání mobilních telefonů_02_02: Umíte vysvětlit pomocí <u>na příkladu</u> aplikace WhatsApp jako příklad, které předpoklady musí být obvykle splněny pro použití aplikace. FODVC – Bezpečnost používání mobilních telefonů_02_03: Umíte uvést příklady, kdy <u>a jak</u> má smysl přizpůsobit <u>upravit</u> oprávnění aplikace a pochopit, jak je to v zásadě možné.
LOHVC – Bezpečnost používání mobilních telefonů_03 Znáte bezpečnostní problémy a nežádoucí důsledky používání služeb rychlého zasílání zpráv nebo jiných aplikací pro chytré telefony.	FODVC – Bezpečnost používání mobilních telefonů_03_01: Umíte uvést důvody, proč se uživatelé aplikací stále více obávají o ochranu <u>bezpečnost svých dat</u> . FODVC – 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.
LOHVC – Bezpečnost používání mobilních telefonů_04 Znáte opatření a tipy pro bezpečné používání aplikací chytrých telefonů.	FODVC – Bezpečnost používání mobilních telefonů_04_01: Umíte <u>Dokážete</u> vysvětlit, co je třeba vzít v úvahu <u>potaz</u> při používání aplikací <u>v mobilních telefonech pro to</u> , abyste ochránili



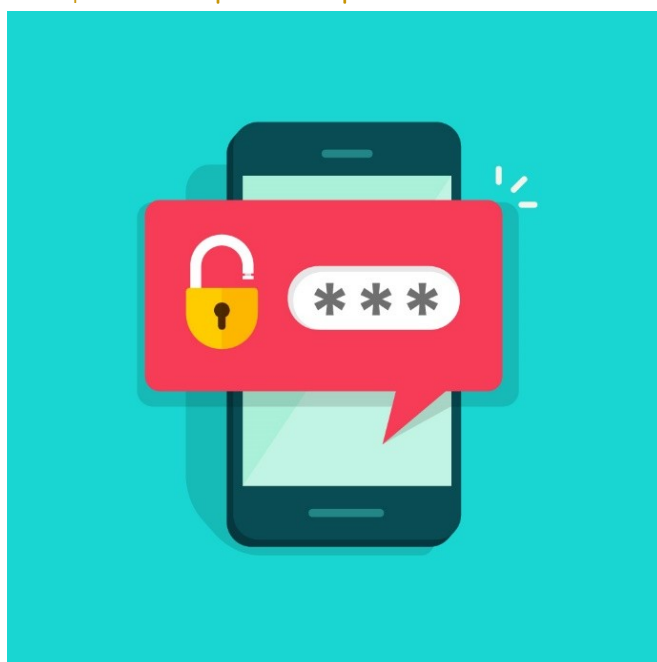
Co-funded by the
Erasmus+ Programme
of the European Union

	sebe a své soukromí. FODVC_Bezpečnost používání mobilních telefonů_04_02: U oblíbených aplikací, jako je WhatsApp nebo Facebook Messenger, umíte dokážete upravit nastavení ochrany osobních údajů.
--	---



1. Budujte znalosti — 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 bez něj se na jeden den 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 potenciálně velmi Vaše -soukromá data, která ukládá, měli byste být schopni podniknout v případě ztráty nebo krádeže podniknout příslušná opatření.



To zahrnuje například ochranu mobilního telefonu proti neoprávněnému přístupu prostřednictvím 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 je váš mobilní telefon odcizen nebo ztracen dojde ke ztrátě nebo odcizení Vašeho mobilního telefonu, měli byste mít SIM kartu (modul identity předplatitele 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 nevznikly 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 náleze.

Pokud se váš iPhone ztratil nebo byl ukraden, můžete ho obvykle vyhledat přes iCloud, pod podmínkou, že je zařízení zapnuté a má ~~přijem dat~~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. ~~Příkazy k tomu potřebné~~, 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 nainstalovanu aplikaci proti krádeži. Pokud je však aplikace nainstalována, SIM karta by neměla být blokována, dokud nejsou data lokalizována a vzdáleně odstraněna. ~~Jinak~~ 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 ~~na~~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 zabránil ~~někomu v používání mého telefonu a vyhnul se tak vysokým nákladům, které by tak mohly vzniknout. ,aby mi nezpůsobil vysoké náklady používáním mého telefonu.~~
-

2. ~~Budujte znalosti~~ Okamžité zprávy 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 ~~rychlého zasílání zpráv~~ tzv. instant messaging, zkráceně (IM (česky "služba pro okamžité zasílání zpráv"))).

Definice

Na rozdíl od SMS služeb, IM je ~~internetová 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 ~~rychlé zasílání zpráv~~ 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.

K ~~naplnění~~ splnění požadovaného účelu však aplikace obvykle vyžaduje různé autorizace. Proto ~~chce~~ aplikace ~~přistupovat~~ aplikace vyžaduje přístup -k určitým funkcím zařízení vašeho smartphonu; jako je



kalendář, kamera, kontakty, mikrofon, SMS, paměť, poloha nebo k jiným ~~telefonním funkcím~~ funkcím telefonu.

Důležité

Jste jedním z 1,6 miliardy uživatelů WhatsApp na celém světě? Pak byste si měli být vědomi toho, že aplikace WhatsApp ~~přistupuje~~ má přístup alespoň minimálně ke všem ~~kontaktním adresám~~ 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

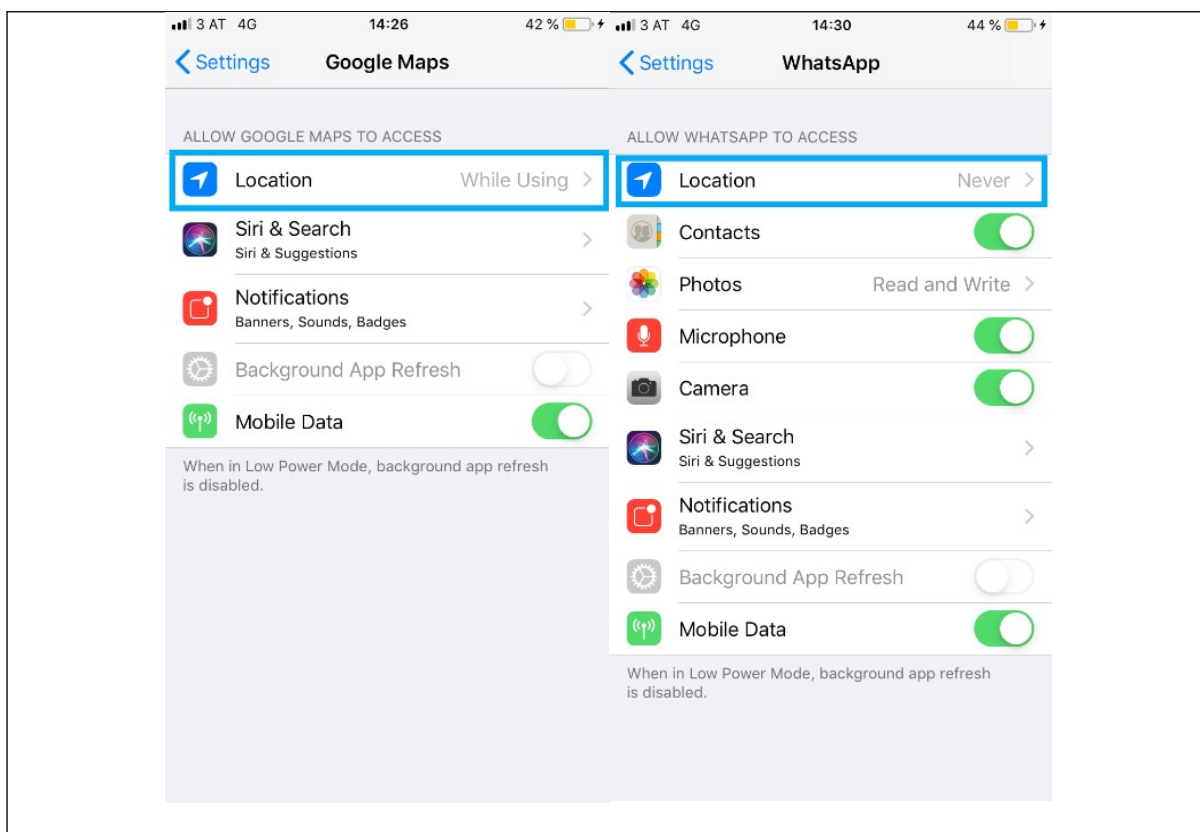
Z důvodů ochrany údajů se vyplatí být opatrný při přidělování autorizací aplikacím a také se vyplatí snížit autorizace na nezbytnou úroveň.

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



Příklad

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



2. Procvičte si znalosti

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 přijme-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 ~~jako-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 ~~být vyžadováno povolit aplikaci~~ aplikace ~~požadovat~~ přístup k vašim obrázkům, kameře, mikrofonu nebo ~~místům~~ údajům o Vaší poloze.
- WhatsApp automaticky přistupuje ke všem kontaktům uloženým ve Vašem mobilním telefonu, k Vaším 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 ~~má aplikace~~ 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. Budujte znalosti – 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 rychlého okamžitého zasílání zpráv a dalších aplikací? Zde je několik příkladů:

- Stejně jako u jiných online komunikačních médií, i v případě odesílatelů 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, ~~mobilitní surfovací~~ návky; návyky v surfování na internetu, uložené kontaktní údaje nebo hesla. Kromě ztráty soukromí může být nepříjemným důsledkem také zneužití v 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 to bude fungovat, bude vysvětleno na příštím sezení.~~ 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. Znáмым příkladem je Facebook nebo WhatsApp.
- Protože aplikace jsou stále dražší.
- Protože v posledních letech vyšlo 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 více 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 rychlého zasílání zpráv 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 riskují 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 aplikací.
- Velkým problémem jsou spíše vysoké-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. Budujte znalosti – Opatření a tipy pro bezpečné používání mobilních aplikací chytrých telefonů

Vzhledem k možným bezpečnostním rizikům používání aplikací ve vašem mobilním telefonu váš 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 vhodnými úpravami provedením vhodných úprav. Z tohoto důvodu je například vhodné vždy používat nejnovější verzi aplikace WhatsApp Messenger.

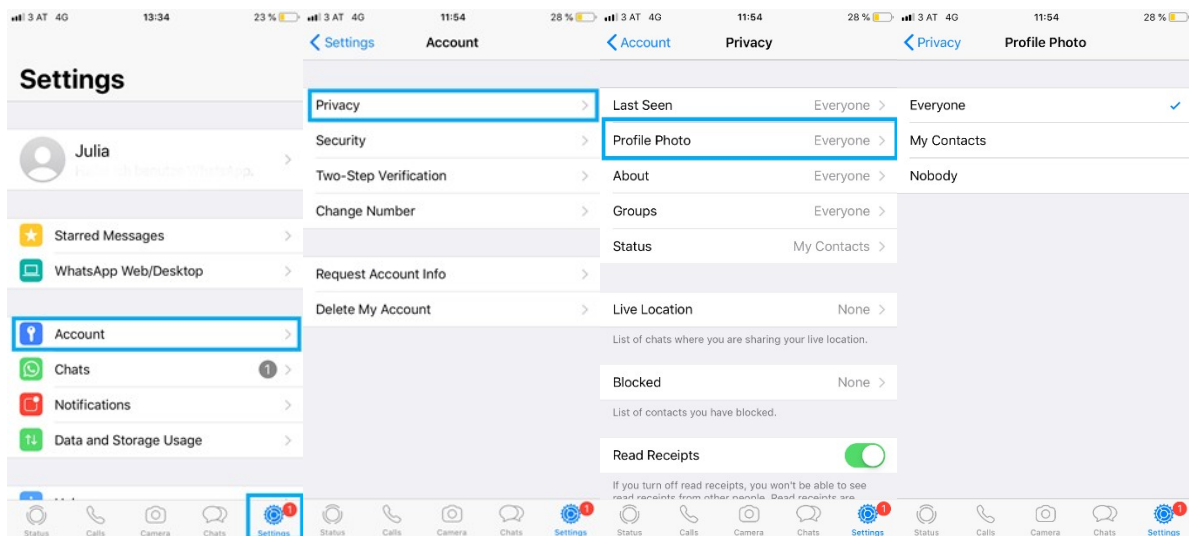
Chcete-li předejít problémům s autorskými právy, měli byste se na svém profilu zdržet používání obrázků, které nevlastníte, jako profilové obrázky.

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 při jejich instalaci. 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 snadné pochopit, že například aplikace počasí, která zobrazuje předpověď počasí, musí být schopna zjistit vaši polohu a poskytnout přesnější informace o předpovědi. Je například samozřejmé, že aplikace pro předpověď počasí musí být schopna zjistit Vaši polohu, aby dokázala poskytnout přesnější informace o předpovědi. Proč by tato aplikace může potřebovat přístup k fotoaparátu vašeho mobilního telefonu, však již není tak zřejmé. 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 nabízí možnost umožňují zabránit ostatním, aby věděli, že jste online, kdy jste byli naposledy online, nebo

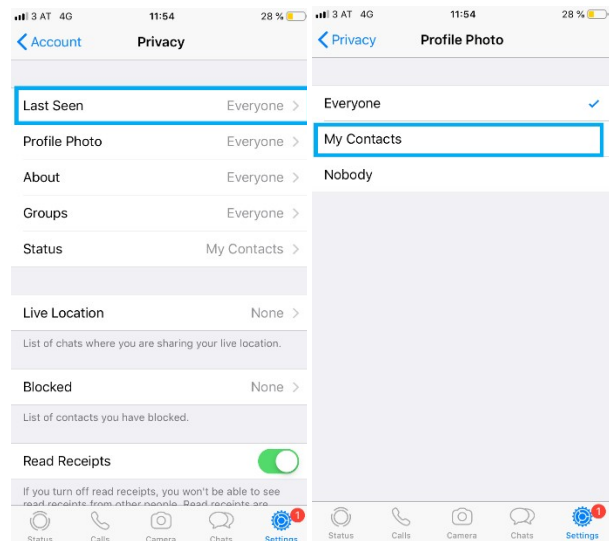
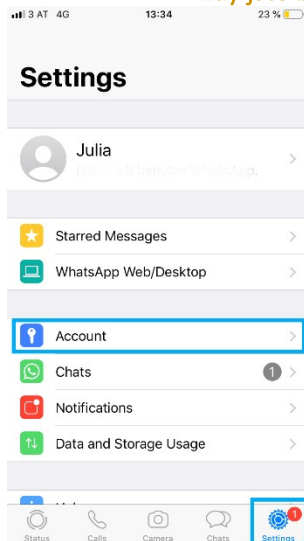


vypnout automatická potvrzení čtení. Jak to funguje, dokládá následující příklad aplikace WhatsApp:

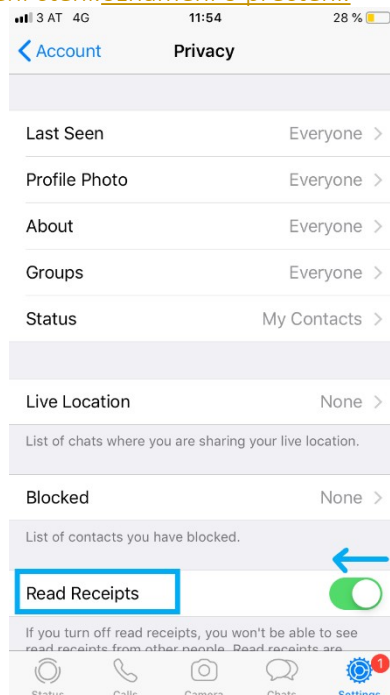
- Jak skrýt „Naposledy viděno“: Otevřete aplikaci WhatsApp a klepněte na tlačítko „Účet“. Pak klepněte na tlačítko



„Soukromí“, vyberte „Naposledy viděno“ a vyberte, kdo nebo jestli někdo může vidět, kdy jste byli naposledy online.



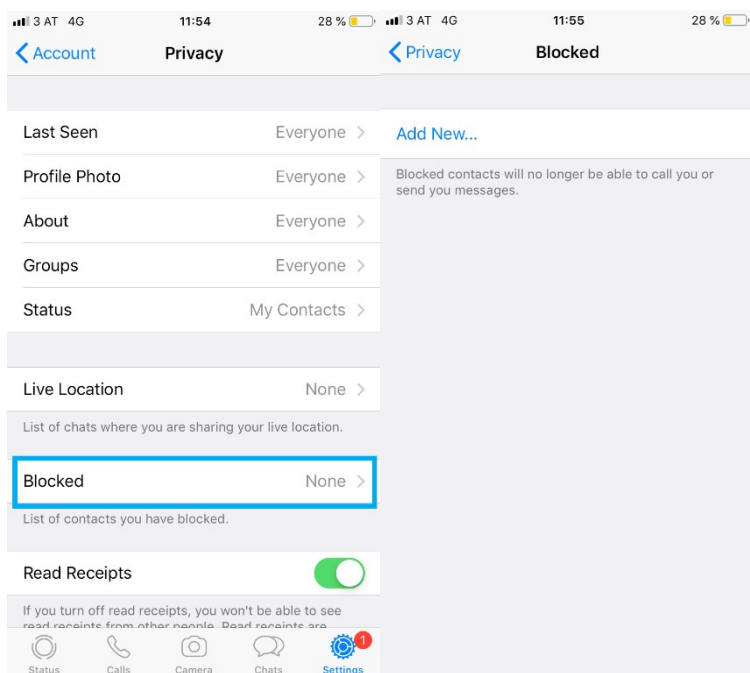
- Jak vypnout potvrzení o přečtení: Klepněte znovu na „Nastavení“, „Účet“ a „Soukromí“. Pak jednoduše deaktivujte potvrzení o přečtení.



Abychom se předešlo kontaktu předešli nevyžádanému kontaktu s cizími lidmi, je třeba v první řadě vždy pečlivě zvážit, v jakých případech by mělo být číslo mobilního telefonu uvedeno bychom měli své telefonní číslo uvést, a především komu by mělo být sděleno 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 blokové kontakty.



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



Důležité

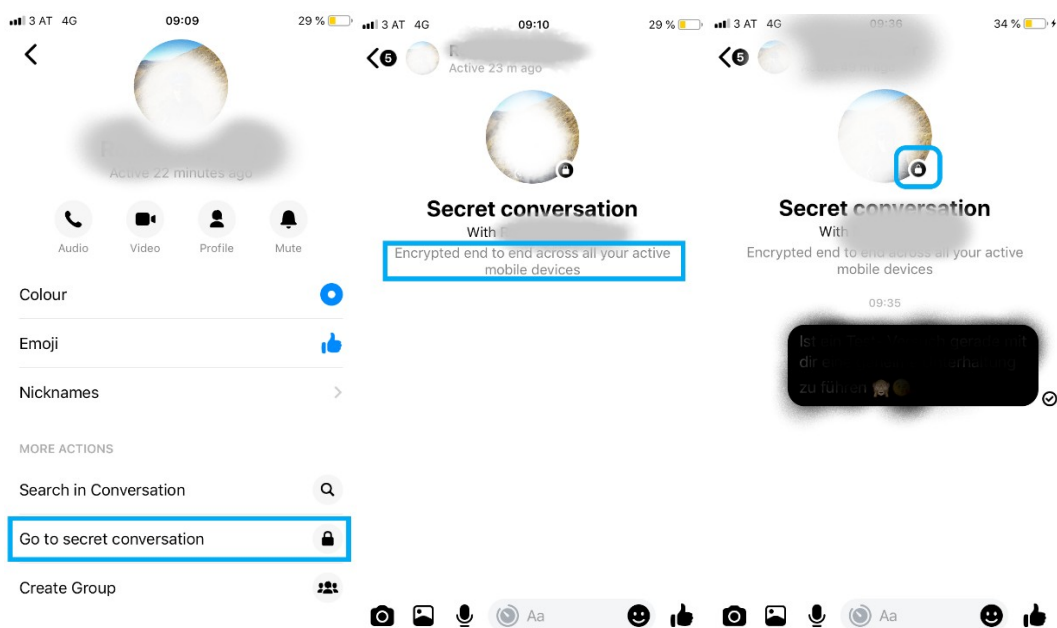
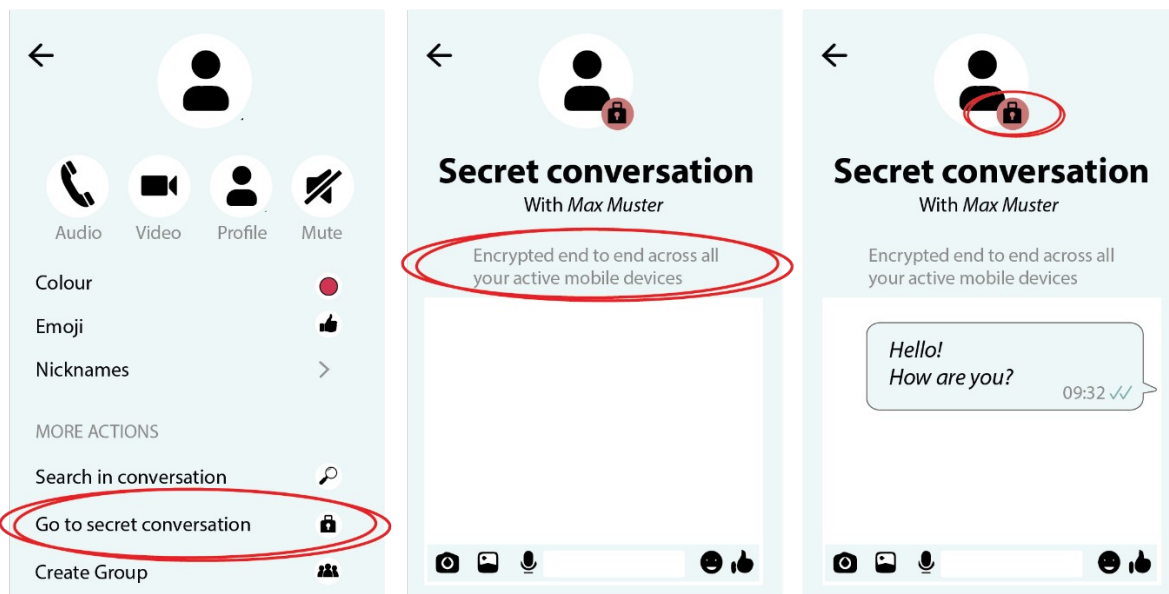
Blokujte ty kontakty, pokud u kterých si nejste jisti, kdo jsou a koho se jedná nebo pokud vás někdo obtěžuje obtěžují. Veškeré urážky, sexuální obtěžování, vydírání nebo hrůzby vyhrůžky nahlasejte policii.

Některé aplikace, jako je Facebook Messenger, Vaše zprávy automaticky nešifrují. Pokud je to možné, měli byste nastavení změnit 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 neuvídí nikdo jiný neuvídí - kromě Vás a partnera na chatu vašeho chatového partnera, dokonce ani Facebook.



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



Tip

Šifrovaný chat poznáte podle toho, že uživatelské rozhraní je šedočerné. Také na profilu partnera chatu uvidíte také 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.

Cvičení VÍCE MOŽNOSTÍ

Související dílčí výukový cíl: FO_04_02

Zadání: Co můžete udělat s nastavením? Jak můžete upravit nastavení ochrany soukromí v populárních aplikacích jako je WhatsApp nebo Facebook Messenger pro zlepšení vašeho soukromí/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 mohou v části Nastavení a Soukromí zakázat, aby ostatní uživatelé viděli, kdy jsem byl naposledy online.
- Mohu například ~~zakázat~~ zamezit WhatsApp aplikaci v přístupu ke svým kontaktům v části Nastavení a Soukromí.
- Při používání aplikace WhatsApp také mohou 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/verschluesst 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>

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

Co byste měli znát Zapamatujte si

Shrnutí

Pro většinu z nás je jejich mobilní telefon nedílnou součástí každodenního života. Proto bychom neměli zapomenout odpovídajícím způsobem chránit soukromé informace a data na nich uložená. Například ~~v případě~~ 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 ~~okamžitých zpráv~~ 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 ~~aplikaci~~, a ~~udržovat~~ 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).

~~Převzetím~~ Po převzetí WhatsApp aplikace společností Facebook ~~učinilo~~ zaujalo mnoho uživatelů ~~kritičtějších~~ kritičtější ~~postoj k~~ ohledně zásadám ochrany osobních údajů ~~v těchto službách~~. Aplikace jsou proto neustále optimalizovány s ohledem na jejich ~~ustanovení~~ 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 ~~aplikace, kterou používáte~~, 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.



Správné odpovědi

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.

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 zabránil používání mého telefonu a vyhnul se tak vysokým nákladům, které by tak mohly vzniknout.

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.



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 Vaším obrázkům a údajům o Vaší poloze. To je jediný způsob, jak aplikace může fungovat.

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.

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 fotografiích a dalších souborů do svých smartphonů, a proto je kapacita úložiště jejich telefonu brzy vyčerpána.



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.

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.

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 mohou 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 mohou 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“.