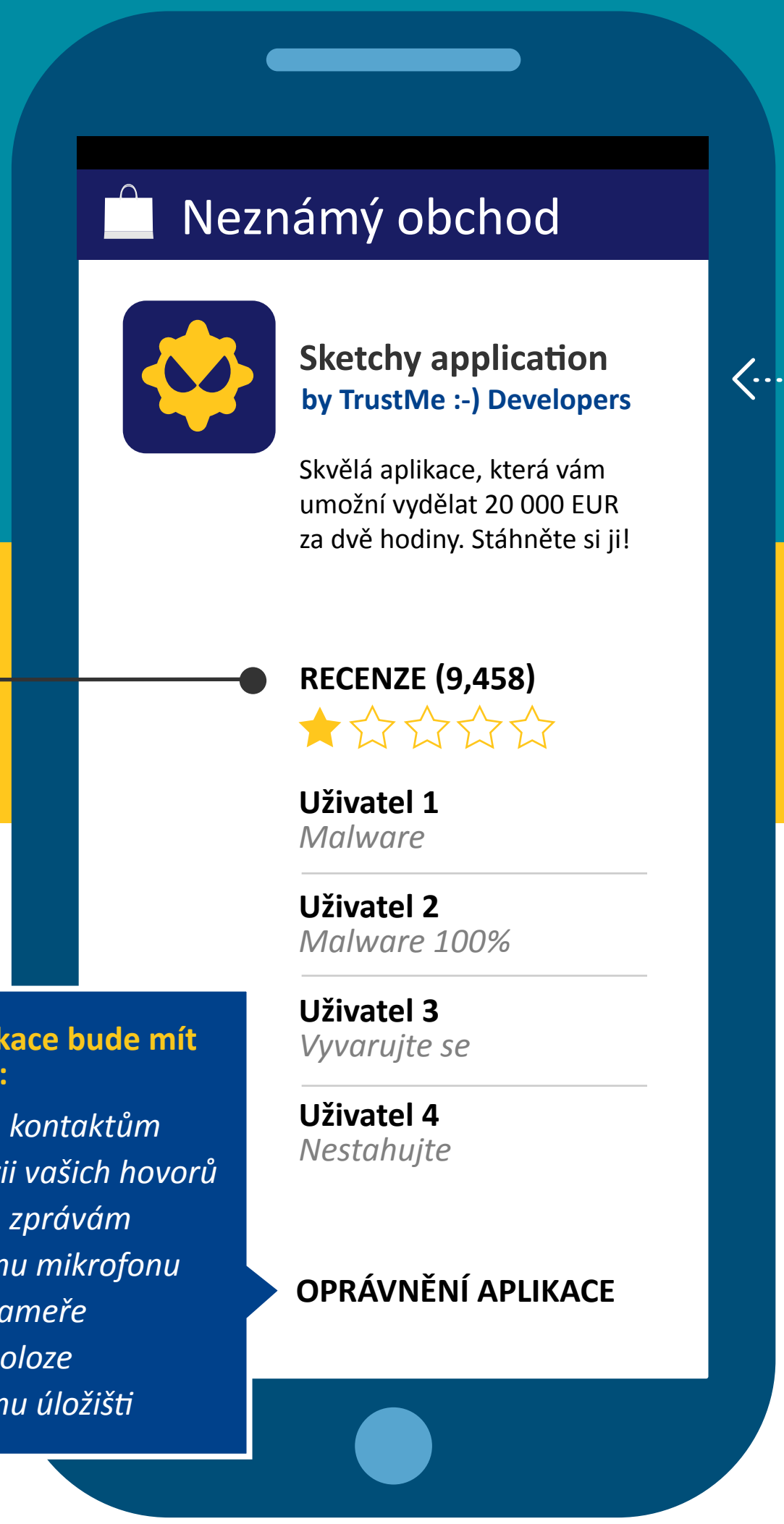
APPS

JENOM HRA?

Instalujte pouze aplikace z oficiálních obchodů s aplikacemi

Před stažením aplikace si zjistěte informace o samotné aplikaci i jejích vydavatelích. Buďte obezřetní v případě, že obdržíte odkaz e-mailem nebo textovou zprávou, kdy můžete být nalákáni k instalaci aplikací třetích stran nebo aplikací z neznámých zdrojů.



PŘEČTĚTE SI RECENZE A HODNOCENÍ JINÝCH UŽIVATELŮ

PŘEČTĚTE SI OPRÁVNĚNÍ APLIKACE

Ověřte si, k jakým informacím má aplikace přístup a zda může tyto informace sdílet s někým dalším. Jsou všechna daná oprávnění potřeba? Pokud ne, aplikaci nestahujte.

NAISNTALUJTE SI APLIKACI PRO ZABEZPEČENÍ MOBILNÍHO ZAŘÍZENÍ

Tato aplikace zkontroluje všechny aplikace ve vašem zařízení a každou novou, kterou později nainstalujete, a upozorní vás, když nalezne škodlivý software.

EUROPOL EC3 European Cybercrime Centre

POLICIE ČESKÉ REPUBLIKY

NCBI #NarodniCentrumBezpecnejsihoInternetu

safer internet.cz

#MobileMalware

MALWARE PRO MOBILNÍ BANKOVNICTVÍ

MALWARE VÁS MŮŽE STÁT PENÍZE

Malware pro mobilní bankovnictví je určený ke krádeži finančních informací uložených ve vašem zařízení.

JAK SE MALWARE ŠÍŘÍ?

- Návštěva škodlivých webových stránek
- Stahování škodlivých aplikací
- Phishing

JAKÁ JSOU RIZIKA?

- Zjištění vašich osobních autorizačních údajů
- Neautorizovaná výběry

CO MŮŽETE DĚLAT?

https://

Stáhněte si oficiální aplikace vaší banky a ujistěte se, že pokaždé navštívíte skutečnou webovou stránku vaší banky.

Nepoužívejte automatické přihlašování v mobilní aplikaci nebo na stránce bankovnictví.

Nesdělujte nikomu číslo své bankovní karty ani heslo.

Pokud je to možné, nainstalujte si aplikaci pro zabezpečení mobilního zařízení, která vás upozorní na jakoukoli podezřelou aktivitu.

Pokud ztratíte svůj mobilní telefon, nebo si změníte telefonní číslo, kontaktujte svou banku, aby si mohli informace aktualizovat.

Neuvádějte informace o svém účtu v textové zprávě nebo e-mailu.

Vždy při používání mobilní bankovní aplikace nebo stránky bankovnictví používejte bezpečnou síť Wi-Fi. Nikdy nepoužívejte nezabezpečenou Wi-Fi síť.

Pravidelně kontrolujte své bankovní výpisy.

EUROPOL EC3 European Cybercrime Centre

POLICIE ČESKÉ REPUBLIKY

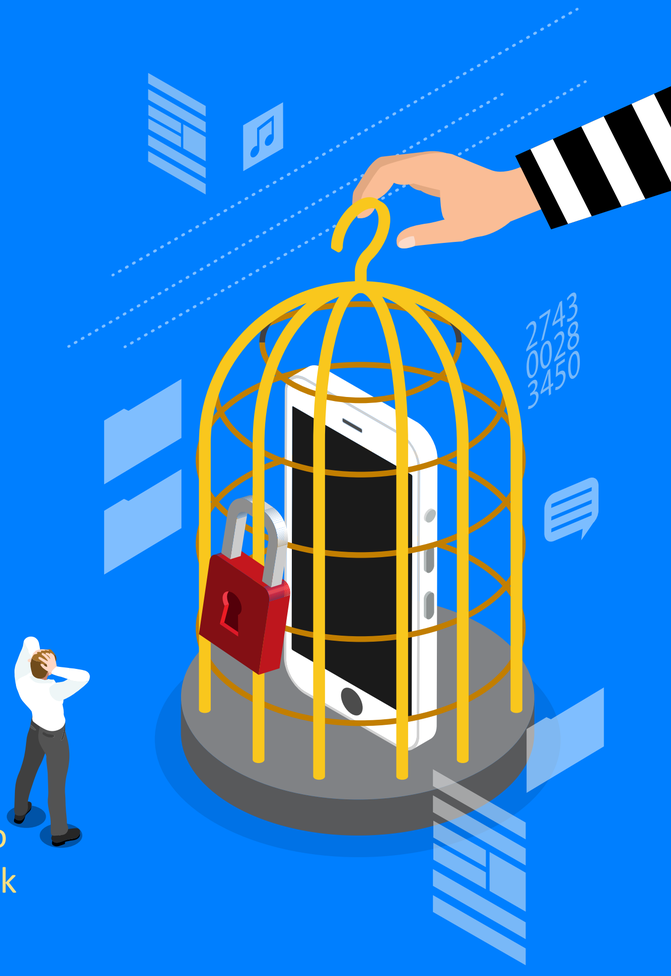
NCBI #NarodniCentrumBezpecnejsihoInternetu

safer internet.cz

#MobileMalware

MOBILNÍ
RANSOMWARE

ROZLUČTE SE SE SVÝMI OSOBNÍMI SOUBORY



Ransomware ovládne váš mobilní telefon a vaše data. Tento typ malwaru uzamkne obrazovku vašeho zařízení nebo znemožní vám přístup k některým souborům nebo funkcím.

JAK SE MALWARE ŠÍŘÍ?

Návštěva napadených stránek.

Stažení falešných verzí legitimních aplikací.

Kliknutí na škodlivé odkazy a přílohy ve phishingových e-mailech.

JAKÁ JSOU RIZIKA?

Může být potřeba obnovit tovární nastavení vašeho zařízení, čímž dojde ke ztrátě všech dat.

Útočník může získat plný přístup k vašemu zařízení a může vaše data sdílet s třetími stranami.

CO MŮŽETE DĚLAT?

Pravidelně zálohujte svá data a aktualizujte své aplikace a operační systém.

Nenakupujte aplikace v obchodech třetích stran.

Pokud je to možné, nainstalujte si aplikaci pro zabezpečení mobilního zařízení, která vás upozorní, když je vaše zařízení napadeno.

Buďte opatrní v případě e-mailů a webových stránek, které vypadají podezřele nebo se zdají být příliš lákavé.

Neposkytujte nikomu jinému administrátorská práva.

Neplaťte výkupné. Budete financovat kriminálníky a podporovat je v další ilegální činnosti.

EUROPOL EC3 European Cybercrime Centre | POLICIE ČESKÉ REPUBLIKY | NCBI #NárodníCentrumBezpečnějšíhoInternetu | saferinternet.cz

#MobileMalware

WEBOVÉ HROZBY

DVAKRÁT SE PODÍVEJTE, NEŽ KLIKNETE

Mohli byste přijít o peníze, své osobní informace nebo dokonce o svá uložená data, když vaše zařízení přestane fungovat. Nenechejte se nachytat!

JAK K TOMU MŮŽE DOJÍT?

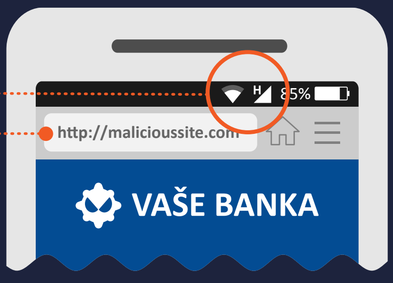
PHISHINGOVÉ ÚTOKY: Nalákají uživatele k poskytnutí osobních informací tím, že se vydávají za důvěryhodnou organizaci. Šíří se e-mailem, textovou zprávou nebo přes sociální média.

PROHLÍŽENÍ WEBOVÝCH STRÁNEK: Vaše mobilní zařízení může být napadeno při pouhé návštěvě nebezpečné stránky.

STAHOVÁNÍ SOUBORŮ: Škodlivé odkazy a přílohy mohou být součástí e-mailu.

PROČ TO FUNGUJE?

Mobilní zařízení jsou cNEUSTÁLE PŘIPOJENÁ k internetu.



Obecným problémem je OMEZENÁ PLOCHA OBRAZOVKY. Uživatelé mobilních zařízení zobrazují adresy URL na malé ploše. To znamená, že je obtížné vidět, zda je doména legitimní.

DŮVĚRA UŽIVATELE v osobní charakter mobilního zařízení.

CO MŮŽETE DĚLAT?

Mějte se na pozoru, pokud obdržíte SMS nebo hovor od společnosti žádající vaše osobní informace. Takovou zprávu nebo hovor můžete ověřit, když zavoláte na oficiální číslo společnosti.

Při prohlížení webu na vašem mobilním zařízení se ujistěte, že je vaše připojení zabezpečené přes HTTPS. Můžete to vždy zkontrolovat na začátku adresy URL.

Nikdy neklikejte na odkaz/přílohu v nevyžádaném e-mailu nebo SMS. Okamžitě takovou zprávu smažte.

Buďte obezřetní, pokud se dostanete na stránku s řadou gramatických chyb překlepů nebo na stránku s nízkým rozlišením.

Pokud je to možné, nainstalujte si aplikaci pro zabezpečení mobilního zařízení, která vás upozorní na jakoukoli podezřelou aktivitu.

EUROPOL EC3 European Cybercrime Centre | POLICIE ČESKÉ REPUBLIKY | NCBI #NárodníCentrumBezpečnějšíhoInternetu | saferinternet.cz

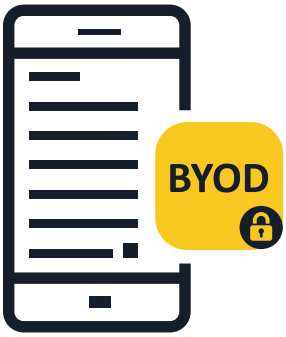
#MobileMalware

MALWARE V MOBILNÍCH ZAŘÍZENÍCH

TIPY A RADY PRO FIRMY

1 Informujte své zaměstnance o rizicích používání mobilních zařízení

- Práce na mobilních zařízeních smazává hranice mezi profesním a soukromým využitím. Firmy mohou být velice vážně poškozené útokem mířeným původně na mobilní zařízení jednotlivce. Mobilní zařízení je počítač, které by mělo být jako počítač chráněné.



2 Implementujte ve firmě zásadu, aby každý používal vlastní mobilní zařízení

- Zaměstnanci by se při přístupu k firemním údajům a systémům z vlastních mobilních zařízení (i pouhý e-mail, kalendář či databáze kontaktů) měli řídit firemními zásadami. Pečlivě vyberte, které technologie budou používány ke správě a zabezpečení mobilních zařízení, a nabádejte své zaměstnance k opatrnosti.

3 Zahrňte zásady používání mobilních zařízení do vašeho celkového bezpečnostního systému

- Pokud zařízení není v souladu s bezpečnostními zásadami, nemělo by být používáno k připojení k firemní síti a k přístupu k firemním údajům. Společnosti by měly zavést vlastní systém správy mobilních zařízení (Mobile Device Management nebo Enterprise Mobility Management).
- Kromě toho je nutné nainstalovat řešení na ochranu před mobilními hrozbami. To zajistí lepší viditelnost a kontextuální povědomí o hrozbách na úrovni aplikací, sítí a operačních systémů.

4 Buďte opatrní při používání veřejných sítí Wi-Fi pro přístup k firemním údajům

- Veřejné Wi-Fi sítě nejsou zpravidla bezpečné. Pokud zaměstnanec přistupuje k firemním údajům prostřednictvím sítě Wi-Fi na letišti nebo v kavárně, údaje mohou být vystavené útočným uživatelům. Je vhodné, aby společnosti v tomto ohledu vytvořily zásady „efektivního používání“.

5 Provádějte průběžné aktualizace operačních systémů a aplikací

- Poraďte svým zaměstnancům, aby si do svých mobilních zařízení stahovali aktualizace softwaru ihned, jakmile jsou k tomu vyzváni.Obzvláště v případě operačního systému Android by poskytovatelé mobilních aplikací a výrobci mobilních zařízení měli znát zásady aktualizací.Nejnovější aktualizace zajistí nejenom bezpečnost mobilního zařízení, ale také lepší výkon.

6 Instalujte pouze aplikace z důvěryhodných zdrojů

- Firmy by měly povolovat instalaci aplikací na mobilních zařízeních, která se připojují k firemní síti, pouze z oficiálních zdrojů. Také můžete zvážit vytvoření firemního obchodu s aplikacemi, ze kterého si koncoví uživatelé mohou stahovat a instalovat firmou schválené aplikace. Poraďte se se svým poskytovatelem zabezpečení nebo vytvořte své vlastní řešení.

7 Vyvarujte se jailbreakingu

- Jailbreak je proces odstranění bezpečnostních omezení nastavených prodejcem operačního systému, což umožňuje získat plný přístup k operačnímu systému a nastavení. Provedením jailbreaku na vašem zařízení můžete podstatně snížit bezpečnost a vytvořit slabiny v zabezpečení, které nemusí být zřejmé. Ve firemním prostředí by neměla být povolena rootovaná zařízení.

8 Zvažte využití cloudových úložišť

- Uživatelé mobilních zařízení často chtějí přistupovat k důležitým dokumentům nejen z pracovních počítačů, ale také ze svých osobních telefonů nebo tabletů mimo kancelář. Firmy by měly vyhodnotit vytvoření cloudového úložiště a využití služeb pro synchronizaci souborů, aby se požadavky tohoto typu vyřešily bezpečným způsobem.

9 Požádejte zaměstnance, aby si nainstalovali software pro zabezpečení mobilních zařízení

- Všechny operační systémy mohou být napadeny. Pokud je to možné, ujistěte se, že používají zabezpečení mobilního zařízení, které slouží k detekci a prevenci malwaru, spywaru a škodlivých aplikací a zároveň má další funkce chránící soukromí a bezpečnost zařízení.

EUROPOL EC3 European Cybercrime Centre

POLICIE ČESKÉ REPUBLIKY

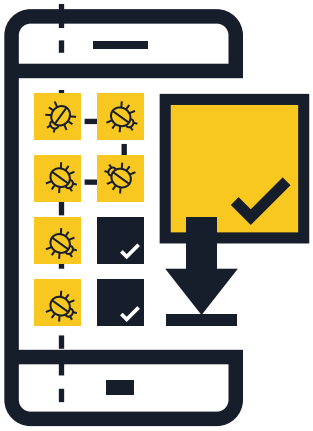
NCBI #NárodníCentrumBezpečnějšíhoInternetu

safer internet.cz

#MobileMalware

MALWARE V MOBILNÍCH ZAŘÍZENÍCH

TIPY A RADY JAK SE CHRÁNIT



1 Instalujte pouze aplikace z důvěryhodných zdrojů

- **Nakupujte ve spolehlivých obchodech s aplikacemi** — Před stažením aplikace si zjistěte informace o samotné aplikaci i jejích vydavatelích. Buďte obezřetní v případě, že obdržíte odkaz e-mailem nebo textovou zprávou, kdy můžete být nalákáni k instalaci aplikací třetích stran nebo aplikací z neznámých zdrojů.
- **Pokud je to možné,** přečtěte si recenze a hodnocení jiných uživatelů.
- **Přečtěte si oprávnění aplikace** — Ověřte si, k jakým informacím má aplikace přístup a zda může tyto informace sdílet s někým dalším. Pokud máte podezření nebo se vám podmínky nelíbí, aplikaci si nestahujte.

2 Neklikejte na odkazy nebo přílohy v nevyžádaných e-mailech nebo textových zprávách

- **Nedůvěřujte odkazům v nevyžádaných e-mailech nebo textových zprávách** (SMS a MMS) — Okamžitě je smažte.
- **Zkontrolujte zkrácené adresy URL a kódy QR** — mohly by vás navést na nebezpečné webové stránky nebo přímo stáhnout malware do vašeho zařízení. Před kliknutím na odkaz zobrazte náhled webu, abyste ověřili, že je webová adresa legitimní. Před naskenováním kódu QR vyberte čtečku kódu, která zobrazí náhled obsažené webové adresy a použije mobilní zabezpečovací software, který vás upozorní na rizikové odkazy.

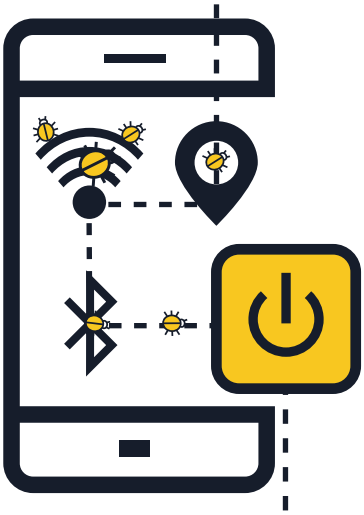
3 Po provedení platby se ze stránky odhlaste

- **Nikdy si do prohlížečů nebo aplikací v mobilním zařízení neukládejte uživatelská jména a hesla** — Pokud je vám váš telefon či tablet odcizen nebo jej ztratíte, kdokoli by se k vašim účtům mohl přihlásit. Po dokončení transakce se namísto pouhého zavření prohlížeče ze stránky odhlaste.
- **Nepoužívejte bankovnictví a nenakupujte online prostřednictvím veřejné sítě Wi-Fi.** — Transakce provádějte pouze prostřednictvím sítí, které znáte a kterým důvěřujete.
- **Zkontrolujte adresu URL** — Před přihlášením nebo odesláním citlivých informací se ujistěte, že je webová adresa správná. Je vhodné stáhnout si oficiální aplikaci vaší banky, abyste si byli jistí, že se vždy připojujete přes správnou stránku.

4 Průběžně aktualizujte svůj operační systém a aplikace

- **Stáhněte si do svého mobilního zařízení aktualizace operačního systému ihned, jakmile jsou vám nabízeny.** — Nejnovější aktualizace zajistí nejen bezpečnost vašeho zařízení, ale také jeho dobrý výkon.

5 Vypněte Wi-Fi, služby zjišťující polohu a Bluetooth, když je zrovna nevyužíváte



- **Vypněte síť Wi-Fi, když ji nepoužíváte.** — Když není připojení bezpečné, kybernetičtí útočníci se mohou dostat k vašim informacím.Pokud je to možné, používejte datové připojení 3G nebo 4G namísto hotspotů. Můžete také využívat virtuální privátní síť, aby byla přenášená data šifrovaná.
- **Nepovolujte aplikacím přístup k vaší poloze, pokud to není nutné.** — Tyto informace mohou být sdílené nebo mohou uniknout a mohou být použity ke zobrazování reklam podle vaší polohy.
- **Vypněte technologii Bluetooth, když ji nepoužíváte.** — Ujistěte se, že je zcela vypnutá, a že není pouze přepnuta do neviditelného režimu. Výchozí nastavení zpravidla umožňuje připojení ostatních zařízení bez vašeho vědomí. Útoční uživatelé by mohli zkopírovat vaše soubory, získat přístup k dalším připojeným zařízením nebo dokonce získat vzdálený přístup k vašemu telefonu a uskutečňovat hovory nebo odesílat textové zprávy, což by mohlo vést k vysokým účtům.

6 Vyhněte se sdílení svých osobních informací

- **Nikdy neuvádějte své osobní informace** do textových zpráv nebo e-mailů, které jsou údajně zaslané vaší bankou nebo jinou legitimní organizací. Kontaktuje přímo danou organizaci a jejich požadavek si ověřte.
- **Pravidelně kontrolujte výpis služeb od operátora, abyste zjistili jakoukoli podezřelou aktivitu.** — Pokud zjistíte, že jsou vám účtovány výdaje za úkony, které jste neprovedli, kontaktujte okamžitě svého operátora.

7 Neprovádějte jailbreak mobilního zařízení

- Jailbreak je proces odstranění bezpečnostních omezení nastavených prodejcem operačního systému, což umožňuje získat plný přístup k operačnímu systému a nastavení **Provedením jailbreaku na vašem zařízení můžete podstatně snížit bezpečnost** a vytvořit slabiny v zabezpečení, které nemusí být zřejmé.

8 Zálohujte svá data

- **Mnoho smartphonů a tabletů umožňuje bezdrátové zálohování dat.** — Zjistěte, jaké možnosti nabízí vaše zařízení v závislosti na operačním systému. Vytvořením zálohy pro váš smartphone nebo tablet můžete snadno obnovit svá osobní data v případě že dojde ke ztrátě, krádeži nebo poškození vašeho zařízení

9 Nainstalujte si aplikaci pro zabezpečení mobilního zařízení

- Všechny operační systémy mohou být napadeny. Pokud je to možné, **využijte zabezpečení mobilního zařízení,** které zajišťuje detekci a prevenci malwaru, spywaru a škodlivých aplikací a zároveň má další funkce chránící soukromí a bezpečnost zařízení.

EUROPOL EC3 European Cybercrime Centre

POLICIE ČESKÉ REPUBLIKY

NCBI #NárodníCentrumBezpečnějšíhoInternetu

safer internet.cz

#MobileMalware