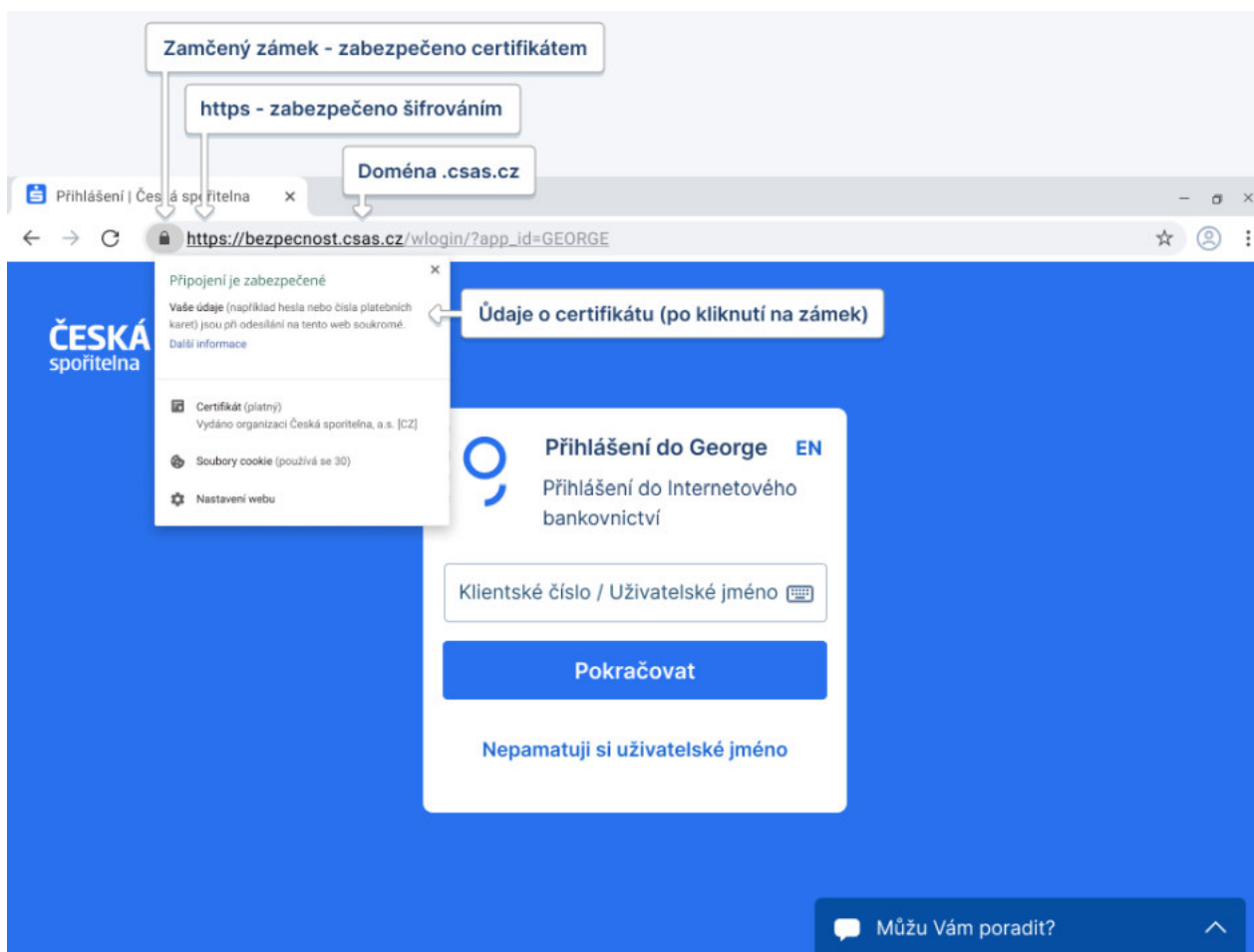


Bezpečnostní desatero

Dodržujte tyto zásady, a minimalizujete tak možnost zneužití svých bezpečnostních údajů

1. Chraňte své bezpečnostní údaje

Nikdy nesdělujte své osobní bezpečnostní prvky jiným osobám a nezasílejte je na jiných doménách než na: https://bezpecnost.csas.cz/wlogin/?app_id=GEORGE. V případě mobilních aplikací zadávejte prvky pouze do mobilních aplikací, které patří České spořitelně.



Vždy si zkontrolujte v adresní řádce svého prohlížeče, že je Vaše připojení zabezpečeno platným certifikátem. Současně také zkontrolujte jméno služby/e-shopu, ke kterému se přihlašujete, na příkladu vidíte George. Pokud se chcete přihlásit do elektronického bankovníctví Business24, použijte vždy doménu <https://www.business24.cz>. Kromě zmíněných domén jsou součástí našeho internetového a elektronického bankovníctví také mobilní aplikace. Jejich seznam naleznete zde: <https://www.csas.cz/cs/mobilni-aplikace>.

2. Přistupujte k službám s využitím Bankovní IDentity výhradně ze svého počítače či mobilního zařízení. Pozor na free Wi-Fi sítě

Nikdy se nepřihlašujte nebo neověřujte svou totožnost s využitím Bankovní IDentity pomocí technického zařízení, které je veřejně přístupné (např. z počítače v internetové kavárně), které vám není známé nebo jeho prostřednictvím může k vašim aplikacím internetového nebo elektronického bankovníctví přistupovat cizí osoba. Vždy využívejte důvěryhodné Wi-Fi sítě nebo mobilní data operátora. Na otevřených Wi-Fi sítích může být vaše komunikace odposlouchávána a vaše osobní bezpečnostní prvky přesměrovány, kam nechcete, nebo zneužity.

3. Zvolte si silné a bezpečné heslo

Vaše heslo k Bankovní IDentity by mělo být **unikátní** a nemělo by se shodovat s vaším heslem do e-mailu nebo k jiné službě. Měli byste jej **pravidelně měnit**.

Aby heslo bylo dostatečně silné, mělo by mít **min. 12 znaků a obsahovat kombinaci čísel, písmen a jiných znaků (např. !, * apod.)**.

Pro větší bezpečí i používejte naši bezpečnostní mobilní aplikaci **George klíč**.

4. Pozor na podvodné e-maily, neotvírejte neznámé odkazy na cizí servery

Ignorujte e-maily a jiné zprávy, které jste obdrželi od neznámých odesílatelů, nebo zprávy s podezřelým názvem či obsahem. Nikdy neotvírejte jejich přílohy a neklikejte na odkazy, které obsahují. Při práci na internetu neotvírejte odkazy na podezřelé neznámé servery (např. s nelegálním software nebo erotickým obsahem) a ty, s kterými se setkáte v podezřelých e-mailech.

Používejte ve své e-mailové schránce ochranu proti spamu. Dále doporučujeme použít další ochranné nástroje – označované jako anti-spyware, anti-adware apod.

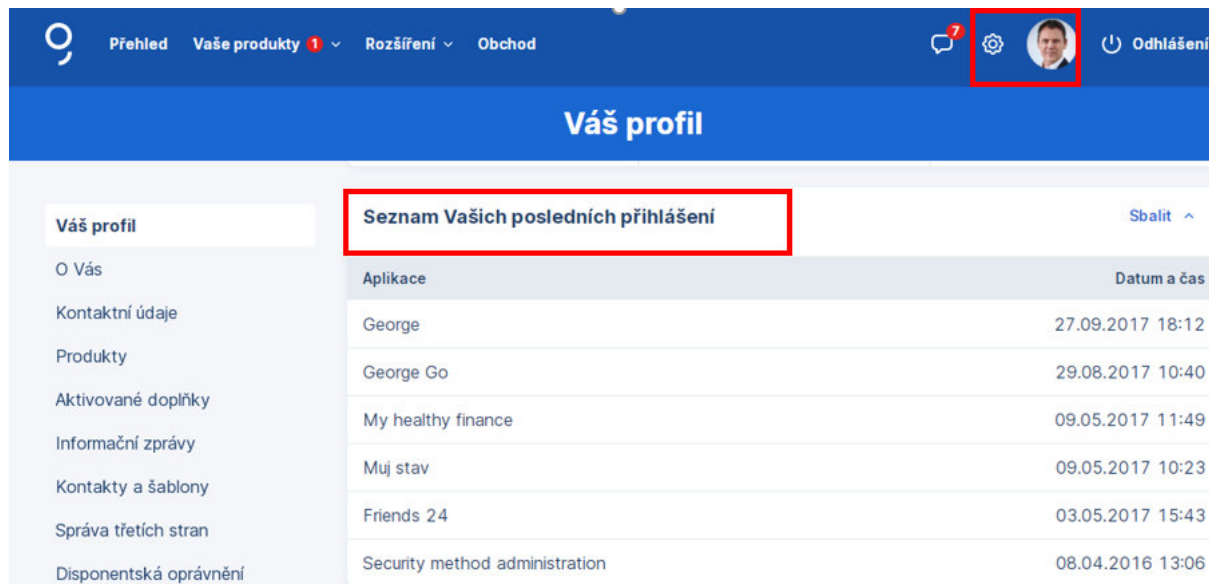
5. Chraňte si svůj počítač a mobilní zařízení a využívejte antivirové programy

Pravidelně aktualizujte svůj operační systém a internetový prohlížeč. Instalujte si aplikace výhradně z oficiálních obchodů – Google play <https://play.google.com/>, App store <https://www.apple.com/app-store/>, Windows Store <https://www.microsoft.com/cs-cz/store/apps/windows>, popř. z oficiálních obchodů výrobce svého zařízení. Nikdy neinstalujte programy z neoficiálních zdrojů.

Používejte jen originální operační systém. Aktualizujte ho a vyhněte se zásahům, které umožňují plný administrativní přístup typu root nebo jailbreak. Takto upravená zařízení nekupujte a nepoužívejte.

Na svůj počítač i mobilní zařízení si nainstalujte antivirový program a pravidelně ho aktualizujte. Nevypínejte „osobní firewall“, který vás chrání při komunikaci na internetu.

6. Kontrolujte poslední úspěšné přihlášení a nezapomeňte se odhlásit



Váš profil

Seznam Vašich posledních přihlášení [Sbalit](#)

Aplikace	Datum a čas
George	27.09.2017 18:12
George Go	29.08.2017 10:40
My healthy finance	09.05.2017 11:49
Můj stav	09.05.2017 10:23
Friends 24	03.05.2017 15:43
Security method administration	08.04.2016 13:06

Pravidelně kontrolujte **poslední přihlášení a ověření s využitím své Bankovní IDentity**.

Po přihlášení přejděte vpravo nahoře do nastavení (ozubené kolečko) a následně vyberte sekci „Váš profil“. Uvidíte seznam svých posledních přihlášení do jednotlivých bankovních aplikací.

Až budete mít hotovo, nezapomeňte se z George odhlásit. Tlačítko „Odhlášení“ najdete vpravo nahoře.

Zvažte aktivaci zasílání informačních SMS zpráv o pohybu na svém účtu. Pozorně čtěte obsah všech SMS zpráv, popř. si zapněte push notifikace na svém mobilním zařízení.

7. Zkontrolujte si, pro co udělujete souhlas a co potvrzujete

Pokud používáte služby třetích stran, jako je nepřímý platební příkaz, informování o platebním účtu, popř. jiné, kontrolujte, či služby využíváte a zda skutečně provádíte zamýšlený úkon. Výčet služeb třetích stran, které využíváte, naleznete ve správě třetích stran, resp. Správě IDentity.

Vždycky také kontrolujte, jestli se kontext a čas úkonů, které právě provádíte, shodují s textem na shrnující obrazovce ve službě, kterou používáte.

Ukázka platby v Georgi a autorizace v aplikaci George klíč

George

https://george.csas.cz/index.html?country=CZ

Jiří Spokojený
48 923,00 Kč

Potvrzení

ZAVŘÍT ×

Jiří Spokojený → Lucie Spokojená
Číslo účtu: 1144111302/0800

-500,00 Kč

Úhrada celkem

-500,00 Kč

Pokračujte v autorizaci za použití aplikace George klíč ve Vašem chytrém telefonu.

Zpět

9:41

Potvrzení platby

Potvrzujte jen to, co sami provádíte.
Bud'te pozorní.

500 Kč

Název aplikace
George

Datum a čas transakce
17.10.2022 9:41:31

Číslo účtu
259459101/0800

Na účet
1144111302/0800

ID transakce
200805783427882

Potvrdit

Zamítnout

Ukázka platby v Georgi a následná autorizace kódem z SMS

George

https://george.csas.cz/index.html?country=CZ

☆ ⓘ ⋮



Jiří Spokojený
48 923,00 Kč

Potvrzení

ZAVŘÍT ×



Lucie Spokojená
000000-1144111302 / 0800 / CZ
CZ
-500,00 Kč

Název odesílatele

Jiří Spokojený

Datum splatnosti

ihned po potvrzení

Úhrada celkem

-500,00 Kč

Zadejte prosím ověřovací kód

Potvrdit kód

Zpět

9:41



5130 >



CS-GEORGE: Potvrzení platby
ve výši 500,00 CZK na účet
0-1144111302/0800.
Autorizační SMS kód: 123456

NIKDY nepotvrzujte něco, co zrovna sami neděláte, a nepředávejte osobní bezpečnostní prvky nebo faktory pro autentizaci třetím osobám.

Stejně obezřetně postupujte také, pokud používáte Bankovní IDentitu jako prostředek pro elektronickou identifikaci. Seznam těchto případů využití Bankovní IDentity naleznete ve Správě IDentity – https://bezpecnost.csas.cz/flfe/?client_id=ssp.

8. Bud'te obezřetní při svých nákupech na internetu

Při nákupech na internetu bud'te opatrní, dávejte si pozor, od koho nakupujete. Čtěte recenze a různá upozornění od ostatních uživatelů.

Ověřte si v obchodních podmínkách, jaká je doba dodání (*někteří obchodníci uvádí dobu dodání až 180 pracovních dní*).

V případě, že platíte kartou, zvažte, zda dovolíte e-shopu, aby si zapamatoval údaje o vaší kartě.

9. Pravidelně sledujte informace o bezpečnosti

Sledujte informace o bezpečnostní situaci na stránkách <https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat>. Zde upozorňujeme na aktuální hrozby a popisujeme různé metody podvodů a útoků.

10. V případě podezření na podvod se s námi spojte

Jakmile budete mít podezření na zneužití svého internetového nebo mobilního bankovníctví, ohlaste nám to na telefonní číslo **800 207 207** (ze zahraničí volejte na číslo +420 956 777 956) nebo na e-mail **csas@csas.cz**.

Pokud jste obdrželi podezřelý e-mail, který má vzbudit dojem, že jej odeslala Česká spořitelna, budeme rádi, když nám jej pošlete na adresu podvody@csas.cz (phishing@csas.cz).