



# BEZPEČNÝ MOBIL

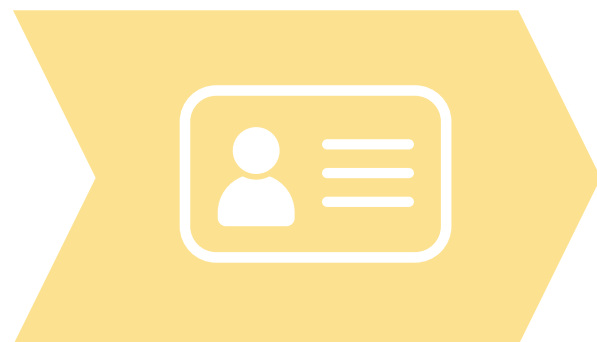
Jak chránit telefon, aplikace a on-line služby.



# OSNOVA

## Bezpečný mobil

**1 - Silné heslo a  
dvoufázové  
ověření**



**2 - Ochrana mobilu  
a aplikací**



**3 - Bezpečné  
připojení a veřejné  
Wi-Fi**



**4 - Nainstalujte si  
antivirus**



**5 - Zabezpečení  
digitálních služeb  
státu**



# Pár slov úvodem



Proč je důležité chránit mobil a aplikace?



Nejčastější hrozby:  
krádež dat - phishing - malware - neoprávněný přístup



Stejná hesla pro více služeb?

...a mnohem víc!



# Jak vypadá podvodná zpráva?

Příklad podvodného e-mailu (phishing) – falešná zpráva od „banky“



**Důležité: Váš účet bude zablokován!**



Doručená pošta x





komu: mně ▼

10:38 (před 0 minutami) ☆ ↶ ⋮



Vážený zákazníku,

Zaznamenali jsme neobvyklou aktivitu na vašem bankovním účtu. Abychom zabránili jeho zablokování, prosím ověřte svou identitu kliknutím na následující odkaz:



[www.moje-banka-verifikace.com](http://www.moje-banka-verifikace.com)

Pokud neprovedete ověření do 24 hodin, váš účet bude trvale omezen.

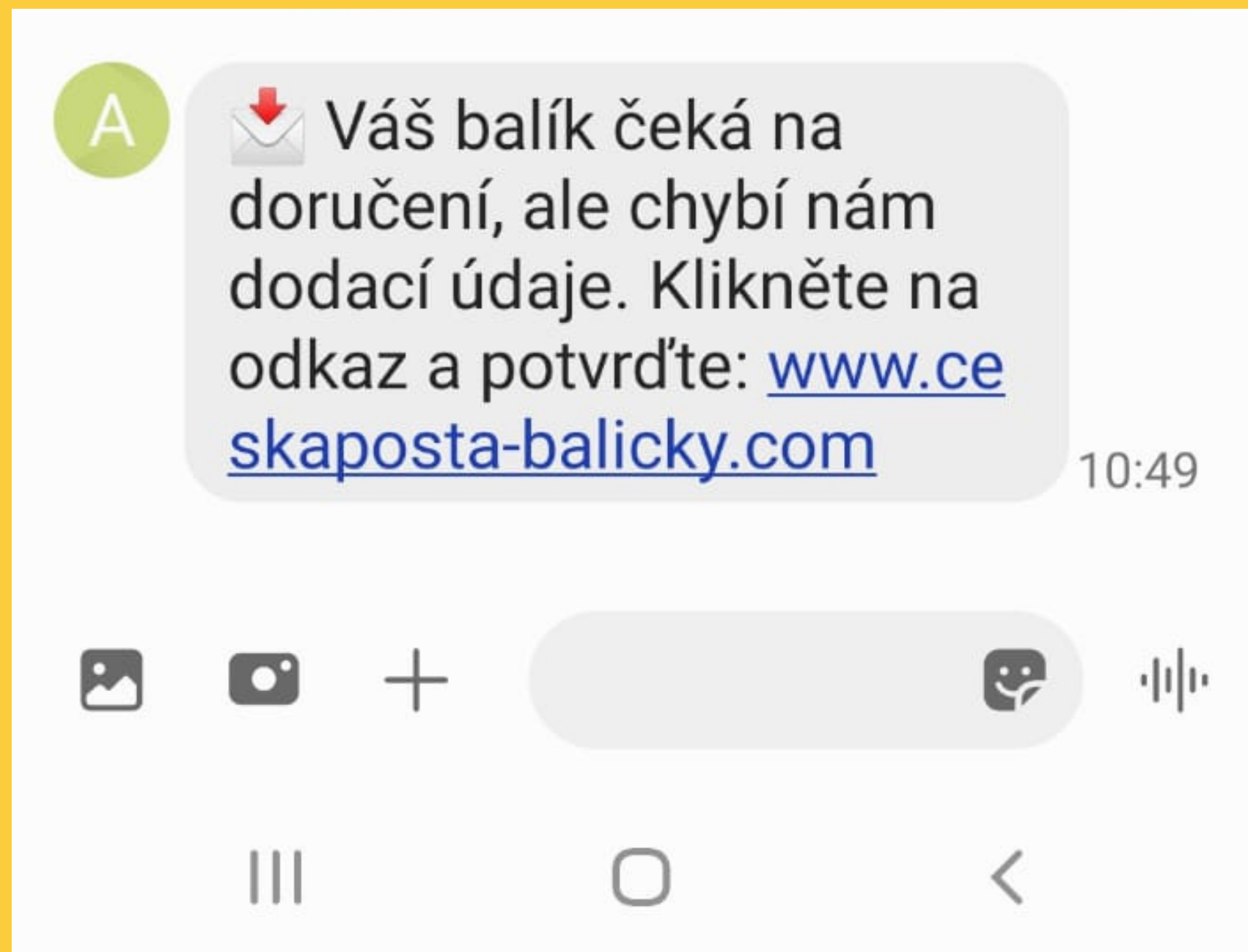
Děkujeme za spolupráci.

**Vaše banka**



# Jak vypadá podvodná zpráva?

Příklad podvodné SMS – falešný balík od „České pošty“





# Na co si dát pozor?

- ✗ Gramatické chyby
- ✗ naléhavost
- ✗ podezřelé odkazy

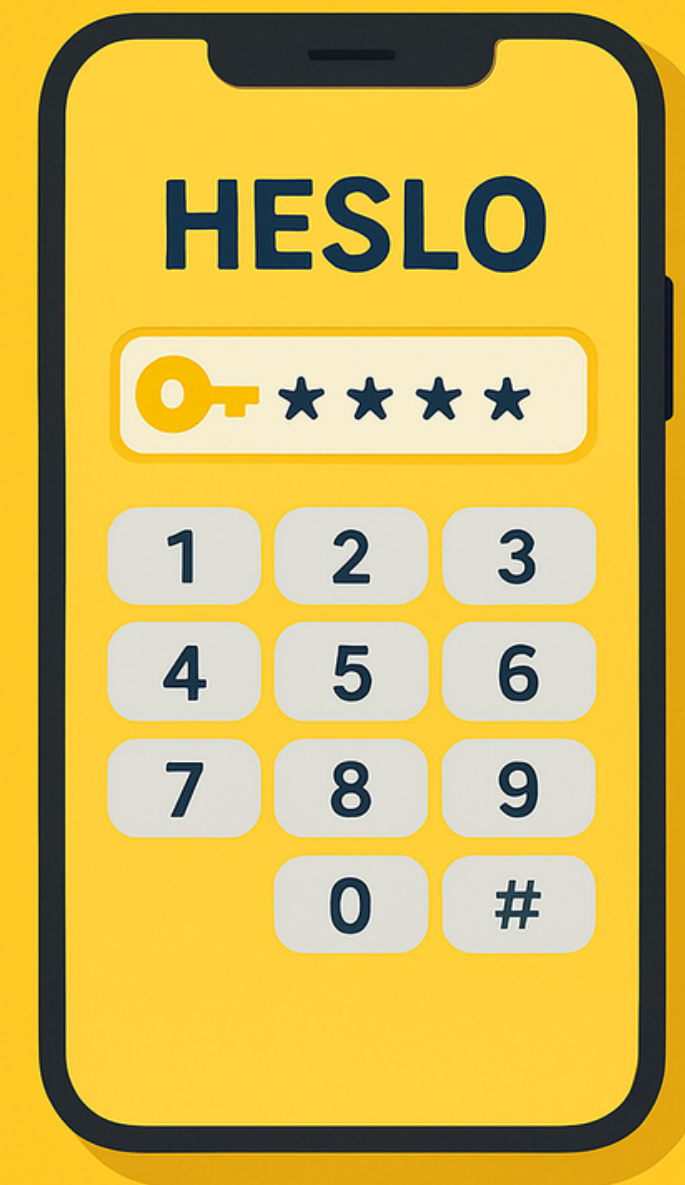


# Jak se chránit?

- ✓ Neklikat na podezřelé odkazy, raději si otevřít oficiální stránku služby.
- ✓ Neposkytovat citlivé údaje přes e-mail nebo SMS.
- ✓ Ověřit si informace přímo u banky nebo kurýrní služby.
- ✓ Používat dvoufázové ověření pro přihlášení ke službám.

# Jak vytvořit silné heslo?

- dlouhé (alespoň 12 znaků)
- unikátní pro každou službu
- správce hesel:
  - Bitwarden (zdarma)
  - StickyPassword (zdarma)
  - LastPass (zdarma pro jednoho uživatele)
  - 1Password (placený)
  - prohlížečové správci hesel (Google Chrome, Firefox, Edge)
- použít větu (např. MojeKniha2024JeSkvělá!)
- dvoufázové ověření (2FA)



# **Stránky, na kterých se můžete při vytváření hesla inspirovat**

<https://www.avast.com/cs-cz/random-password-generator>

<https://www.eset.com/cz/generator-hesel/>

<https://www.nove-heslo.cz>



---

**Byl váš účet nebo vaše heslo zneužito?**

<https://haveibeenpwned.com>





# Ochrana telefonu a aplikací



Zamykání obrazovky

- PIN
- gesta (symbol na obrazovce)
- biometrické údaje (otisk prstu, sken obličeje)



Aktualizace aplikací a systému



Opatrnost u oprávnění aplikací



Instalace pouze z oficiálních obchodů (Google Play, App Store)



# Co je IMEI a k čemu je potřeba?

 IMEI = unikátní patnáctimístné číslo mobilního telefonu, které mu přiděluje jeho výrobce. Mobilní operátor ho ukládá do speciálního registru. Po nahlášení krádeže telefonu pak přístroj na základě tohoto čísla může operátor zablokovat.

Kde najdu IMEI?

- na zadní straně telefonu nebo pod jeho baterií
- na dokladu o zakoupení telefonu
- většina telefonů ho dokáže zobrazit na dispeji po zadání

**\*#06#**

# Veřejná Wi-Fi: skryté nebezpečí



Rizika:



Odposlech dat, falešné Wi-Fi sítě

Jak se ochránit:



Používat mobilní data pro citlivé služby



Vypnout automatické připojování k Wi-Fi,  
pozor na sítě, které se tváří jako “free” nebo  
“public



používat zašifrované stranky HTTPS



# Paní Jana na cestách



Paní Jana si ráno v kavárně na nádraží otevře notebook a připojí se na bezplatnou Wi-Fi "FREE-Coffee-WiFi". Během čekání na vlak se rozhodne zkontrolovat, zda jí přišla výplata, a přihlásí se do internetového bankovníctví.

Neví ale, že Wi-Fi síť není chráněná heslem a ve skutečnosti ji založil podvodník sedící o pár stolů dál.

Ten díky tzv. „man-in-the-middle“ útoku odchytní přihlašovací údaje a během pár minut se pokusí její účet vybrat.

Naštěstí má paní Jana zapnuté dvoufázové ověření (2FA), takže útočník nezíská přístup bez kódu z SMS. Ale kdyby 2FA neměla? Útočník by se dostal do banky snadno.

# Je potřeba mít antivir v telefonu?

Tipy na dobré antivirové aplikace:

- Norton Mobile Security
- ESET Mobile Security
- Avast Mobile Security
- Total AV
- Bitdefender Antivirus
- Panda
- Avira

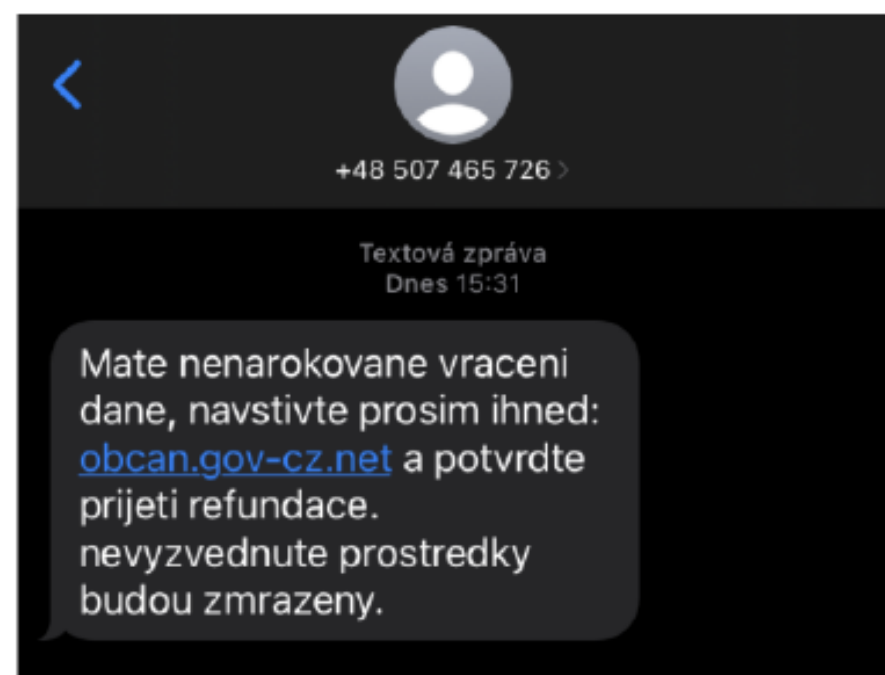
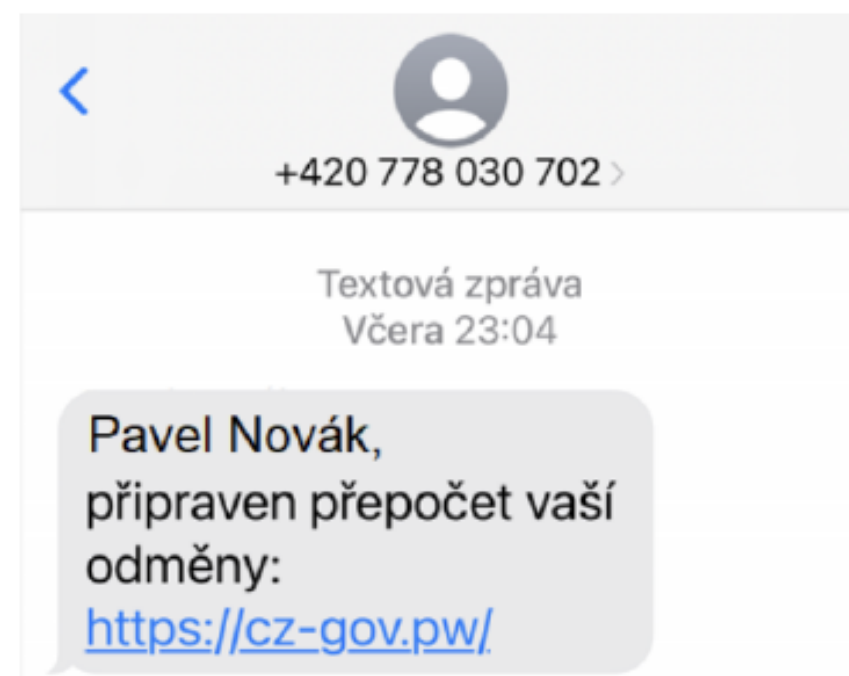
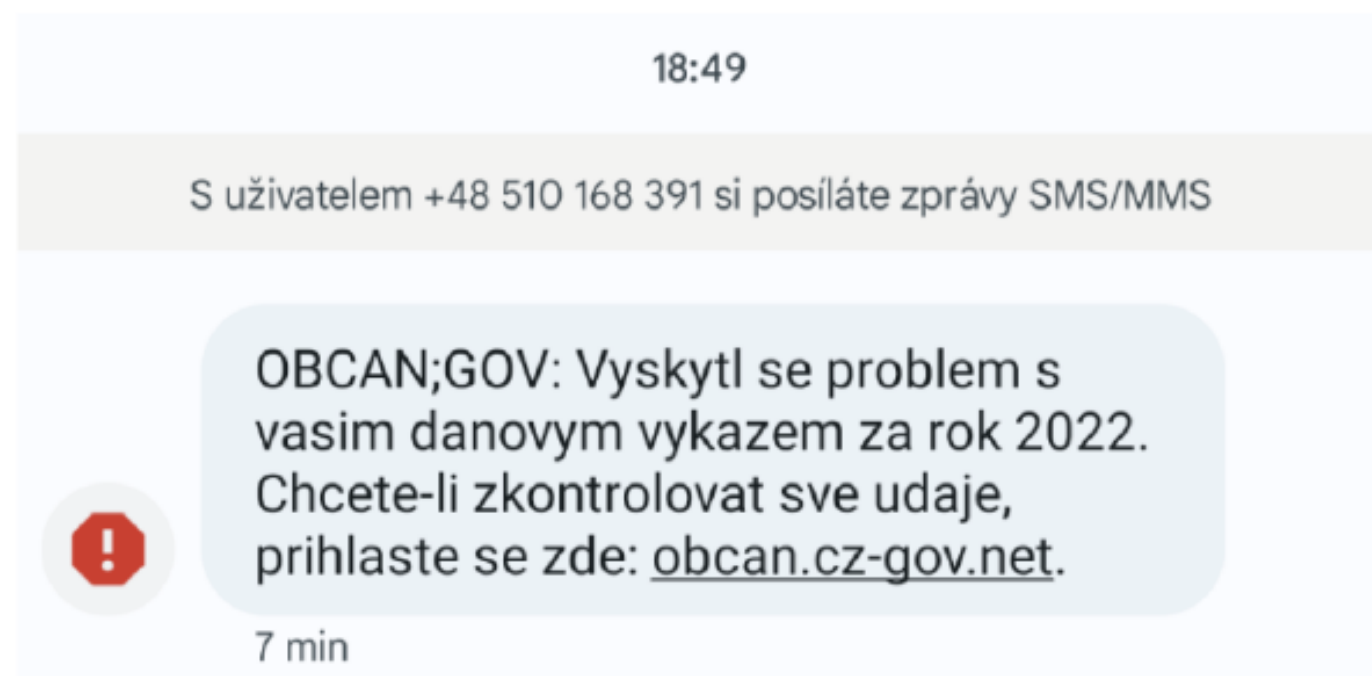


# Jak se chránit při využívání digitálních služeb státu?

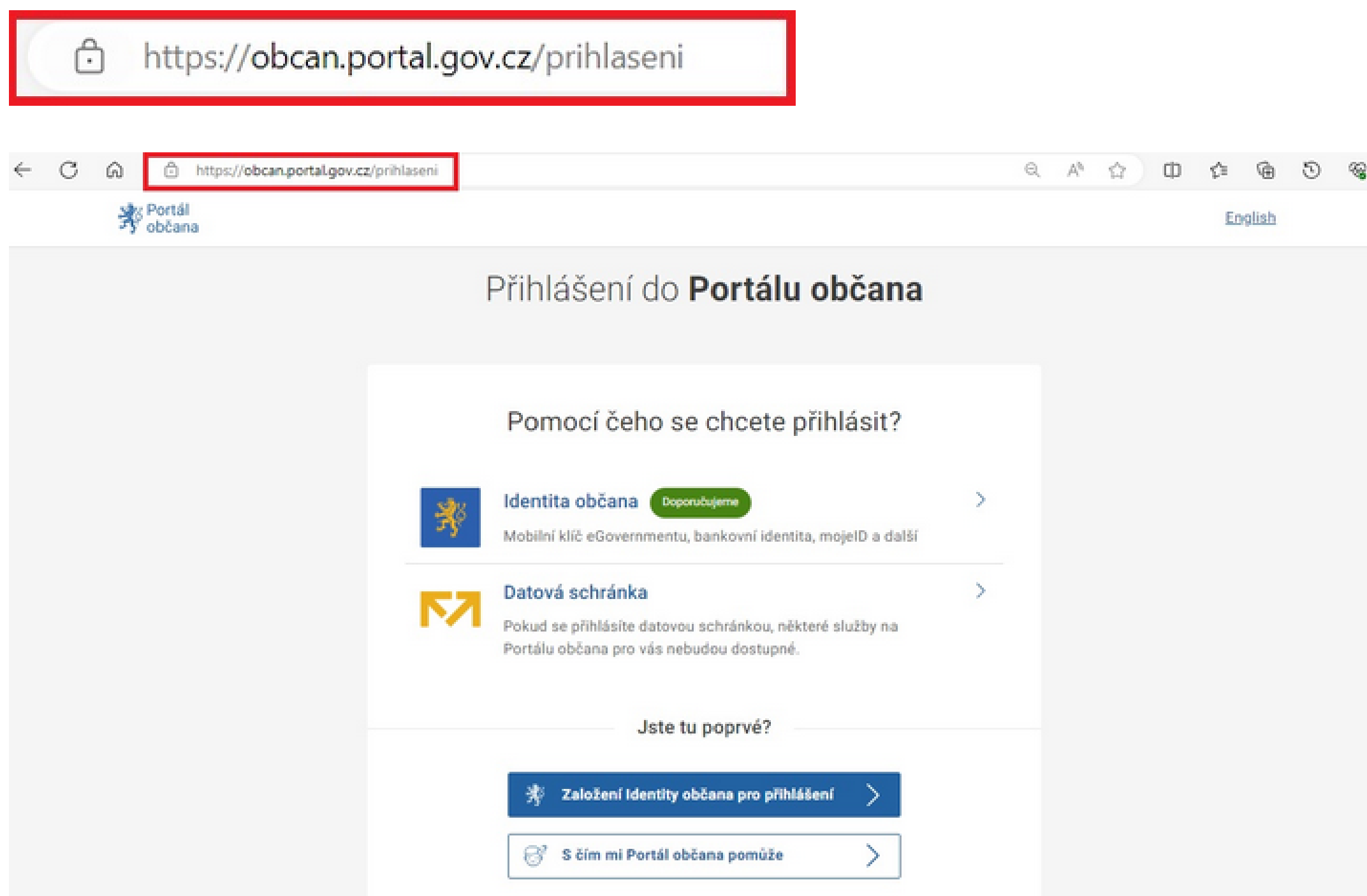
## PORTÁL OBČANA – BEZPEČNÉ PŘIHLÁŠENÍ

- Bankovní identita vs. Mobilní klíč eGovernmentu
- Opatrnost při zadávání osobních údajů





# Jak rozpoznat bezpečnou stránku Portálu občana?





# KLÍČOVÉ RADY

Používejte silná hesla a 2FA

Chraňte svůj mobil – zamykání, aktualizace

Buďte opatrní na podvodné zprávy a Wi-Fi

Používejte bezpečné přihlášení k digitálním službám státu



Prostor pro dotazy



# BEZPEČNÝ MOBIL

Děkuji za pozornost!

