



DOVOLENÁ BEZ STAROSTÍ

Pravidla kybernetické bezpečnosti , která
zajistí **bezpečí**, když jste mimo kancelář



Používání osobního zařízení pro osobní informace

K veřejným počítačům je třeba přistupovat jako k veřejným toaletám: **při jejich používání buďte opatrní**

U veřejných zařízení:

Vyhňte se přístupu k osobním informacím.
Pokud není jiná možnost, otevřete prohlížeč v režimu inkognito či soukromém režimu



Poříd'te si mobilní datový tarif

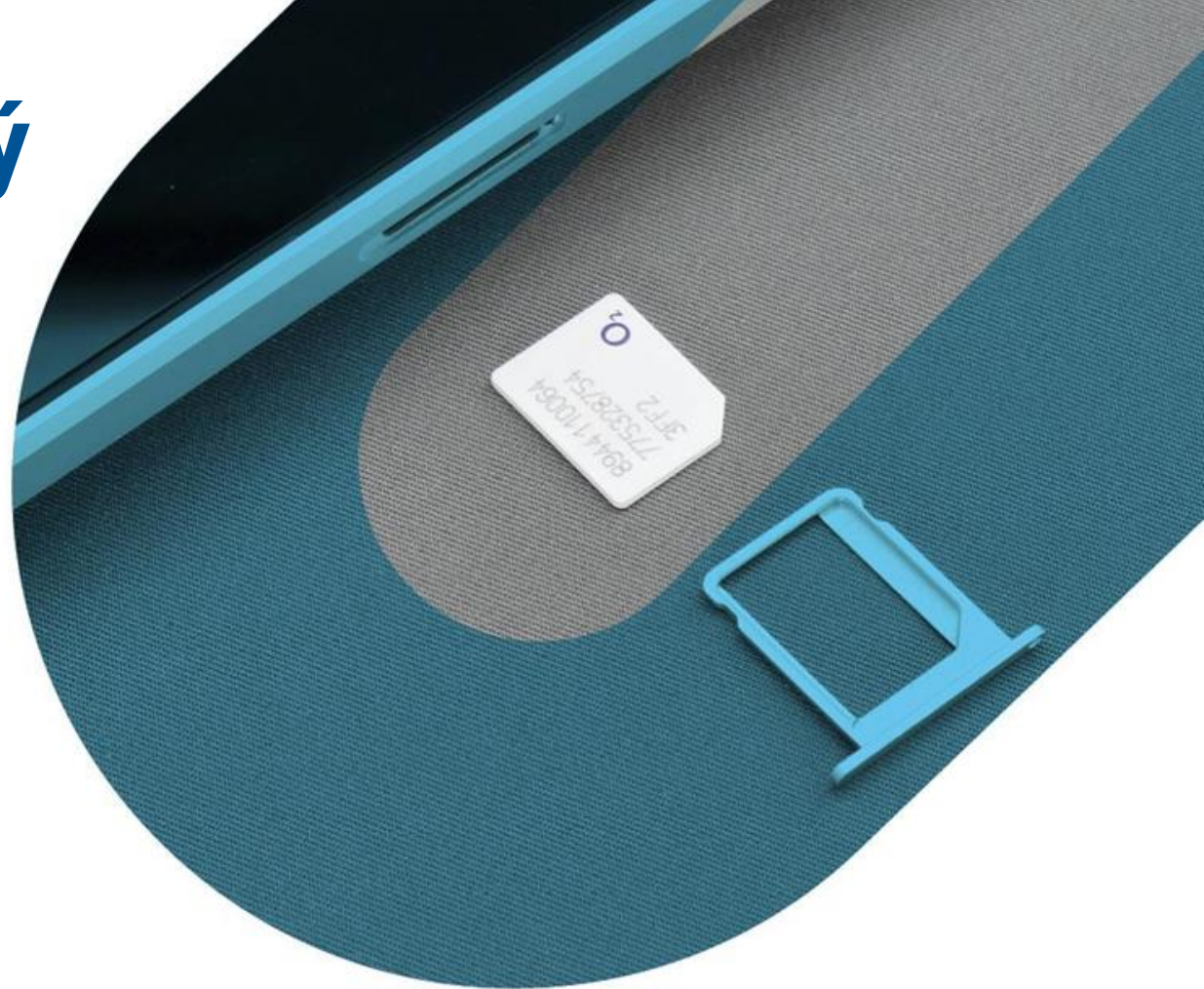
Ačkoliv je její používání pohodlné, veřejná síť Wi-Fi poskytuje hackerům snadnou cestu, jak ukrást hesla a peníze.

Nejbezpečnější možnost: mobilní data vašeho telefonu. Letíte do zahraničí? Zvažte místní SIM kartu, protože datové tarify jsou tak obvykle levnější.

Dobrou možností je také použití VPN. pokud jí dáváte přednost a víte jak ji sami nastavit

Použití veřejné Wi-Fi?

- Přístup k finančním informacím pomocí mobilních aplikací
- K webovým stránkám přistupujte zadáním jejich adresy URL *a neklikejte na žádné odkazy!
- Vidíte nějaké varování v prohlížeči? Hned se zastavte. Vaše síť je pravděpodobně narušena





Připravte se na nejhorší

Telefony se kradou, váš může být další na řadě.



Ověřte si, že máte aktivní zálohování
iCloud pro iPhone, Google Photos pro Android



Aktivujte zámek obrazovky
To brání přístupu k vašim citlivým datům



Aktivujte sledování polohy a vzdálené vymazání

"Find My iPhone" (u telefonů iPhone) nebo "Find My Device"
(u telefonů se systémem Android)

Uložte si papírové podklady

Mějte u sebe tištěnou kopii letenek, pasu, a dalších důležitých dokumentů



Cestujete s dětmi?



Připravte si akční plán: co dělat,
když se někdo ztratí



Aktivujte sledování polohy rodiny na zařízeních iPhone
a Android



Shrnutí

Používejte osobní zařízení pro osobní informace

Poříd'te si mobilní datový tarif

Připravte se na možnou krádež telefonu

Uchovávejte papírovou zálohu důležitých dokumentů

Připravte bezpečnostní plán rodiny (podle potřeby)

