

# **MEATEST spol. s r.o.** - sdělení pověření pro ochranu osobních údajů číslo **66** ze dne **16.4.2024**

---

## **Kyberpodvodníci se schovávají za hlasový automat a zneužívají jméno virtuální asistentky Kate**

Tento podvod je již poměrně sofistikovaný. Zazvoní vám telefon, po jeho zvednutí se ozve hlasový automat vydávající se za naši virtuální asistentku Kate s upozorněním, že vaše mobilní aplikace ČSOB Smart potřebuje update a pokud ho chcete provést, máte stisknout „jedničku“.

Pokud jedničku skutečně na svém mobilním telefonu stisknete, hlas vydávající se za „Kate“ vám oznámí, že vám do SMS zprávy zasílá odkaz pro stažení nové verze, poděkuje vám za spolupráci a zavěsí.

V tuto chvíli zdánlivě nic nenasvědčuje tomu, že by se mohlo jednat o podvod a možná si ani neuvědomíte, že jste právě naletěli Volačovi, který hlasový automat zneužil pro své podvodné jednání.

Podvod totiž pokračuje dál a přichází na řadu Klikáč. Do mobilu vám přijde SMS zpráva obsahující odkaz na provedení aktualizace mobilního bankovníctví. Odkaz však ve skutečnosti vede na podvodnou stránku, která vás vybízí k instalaci falešné aplikace.

Odborně se tomu říká Smishing. Pokud si takovou aplikaci skutečně nainstalujete může dojít k napadení vašeho telefonu, ztrátě důvěrných informací a dat. Je to jako byste přihlašovací údaje odevzdali přímo útočníkům, kteří se tak mohou zmocnit vašich emailů, vašeho internetového bankovníctví či mohou získat údaje z vaší platební karty.

### **Jak phishing prostřednictvím SMS (tzv. Smishing) funguje:**

Po kliknutí na odkaz se ocitnete na falešné stránce. Ta může mít podobu obchodu s aplikacemi, může se ale také tvářet jako internetové bankovníctví a nabádá vás ke stažení aplikace nebo k přihlášení.

Pokud si aplikaci stáhnete, může dojít k zavirování vašeho chytrého telefonu, pokud zadáte přihlašovací údaje, odešlou se podvodníkům a ti je obratem zadají do opravdového internetového bankovníctví.

Za malou chvíli vám banka pošle ověřovací SMS kód nebo Smart klíč, tak jak jste zvyklí. Protože stále nic netušíte, vložíte kód na falešnou stránku a ten se tak dostane k útočníkům nebo operaci potvrdíte Smart klíčem.

Podvodníci teď mají přihlašovací údaje i SMS klíč případně jste je nechali vstoupit přímo do aplikace. Tedy všechno, co potřebují, aby se přihlásili do internetového bankovníctví místo vás.

Nakonec na vás vyskočí chyba a žádost o nové ověření. Dalším SMS kódem už ale potvrzujete převod vašich peněz nebo aktivaci aplikace Smart klíč.

Podvodníci spoléhají mimo jiné na to, že někteří klienti nedávají pozor a nečtou všechny informace, které banka posílá v ověřovacích SMS nebo notifikacích do aplikací typu ČSOB Smart klíč. Ty jsou přitom pro bezpečnost vašich peněz důležité, proto jim prosím vždy věnujte pozornost.

Vyplatí se také sledovat notifikace prohlížečů a antivirových programů, které vás na nebezpečné webové stránky upozorní notifikacemi.

Zdroj: ČSOB