

## Phishing Mojebanka.cz – KB – 2. 2. 2015

Dnes se objevily nové podvodné emaily cílené na internetové bankovníctví komerční banky ted aplikaci MojeBanka. Uvedený email vypadá následovně:

Od: MojeBanka <cert@wizardmojebanka.cz>

Komu: ██████████

Datum: 1. 2. 2015 15:17:09

Předmět: Certifikat: error #910



Vážení zákazníci.

Z bezpečnostních důvodů je nutné znovu potvrdit platnost certifikátu.

[Ověřit nyní](#)

Popř. ve variantě vyzývající aktualizaci certifikátu

Po kliknutí na uvedené odkaz **COŽ DŮRAZNĚ NEDOPORUČUJEME!!!** Je oběť přesměrována na phishingové stránky útočnicka, které mají obdobný grafický design jako originální webová aplikace MojeBanka. Na této stránce je zobrazena výzva ke vložení certifikátu

NA PARTNERSTVÍ ZÁLEŽI ENGLISH

Certifikační průvodce

Nový **Nastavení** Partneři Nápověda

**Ověření platnosti certifikátu**

Certifikát v souboru / prohlížeči

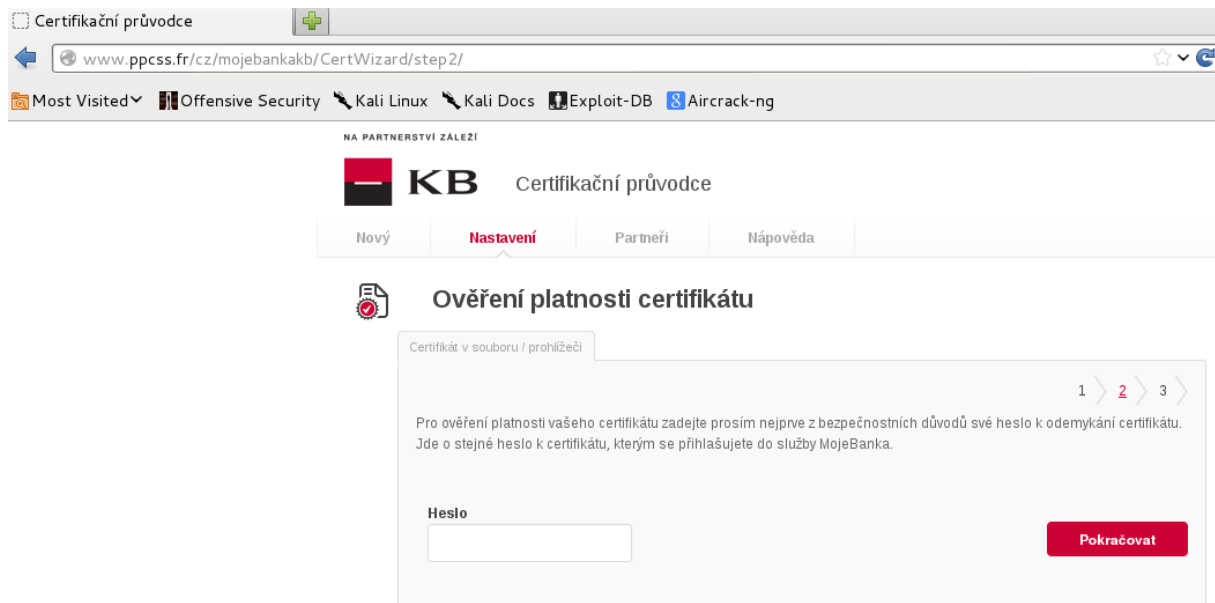
1 > 2 > 3 >

Výběr certifikátu

No file selected.

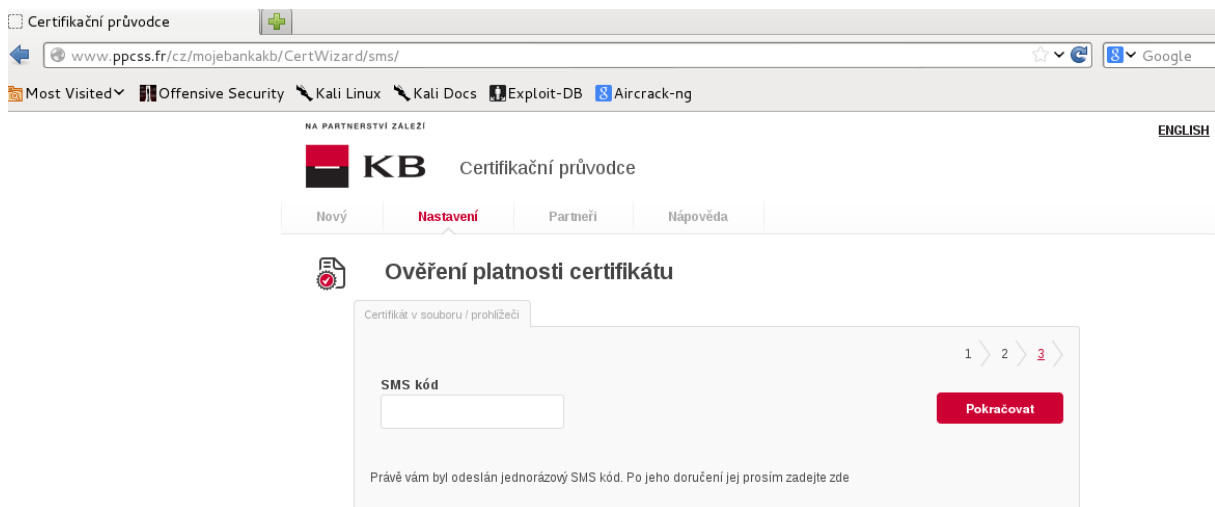
• Nahrajte certifikát pro ověření platnosti.

Po jeho vložení se zobrazí výzva k zadání hesla k certifikátu



The screenshot shows a web browser window with the address bar containing `www.ppcss.fr/cz/mojebankkb/CertWizard/step2/`. The page header includes the KB logo and the text "Certifikační průvodce". A navigation menu contains "Nový", "Nastavení", "Partneři", and "Nápověda". The main heading is "Ověření platnosti certifikátu". Below it, a sub-heading reads "Certifikát v souboru / prohlížeči". A progress indicator shows steps 1, 2, and 3, with step 2 being the active one. The main text states: "Pro ověření platnosti vašeho certifikátu zadejte prosím nejprve z bezpečnostních důvodů své heslo k odemykání certifikátu. Jde o stejné heslo k certifikátu, kterým se přihlašujete do služby MojeBanka." There is a text input field labeled "Heslo" and a red "Pokračovat" button.

A vzhledem k pravděpodobnosti, že banka identifikuje přihlášení jako rizikové a zašle kontrolní SMS kód, je oběť vyzvána k jeho zadání.



The screenshot shows a web browser window with the address bar containing `www.ppcss.fr/cz/mojebankkb/CertWizard/sms/`. The page header includes the KB logo and the text "Certifikační průvodce". A navigation menu contains "Nový", "Nastavení", "Partneři", and "Nápověda". The main heading is "Ověření platnosti certifikátu". Below it, a sub-heading reads "Certifikát v souboru / prohlížeči". A progress indicator shows steps 1, 2, and 3, with step 3 being the active one. The main text states: "Právě vám byl odeslán jednorázový SMS kód. Po jeho doručení jej prosím zadejte zde". There is a text input field labeled "SMS kód" and a red "Pokračovat" button.

Teoreticky tak útočník získal veškeré údaje potřebné k přístupu do elektronického bankovníctví.

Další informace na stránkách internetového bankovníctví

<https://www.mojebanka.cz/InternetBanking/?L=CS>

Kamil Talavašek

Analytik bezpečnosti ICT Kraje Vysočina

talavasek.k@kr-vysocina.cz