OCHRANA PLATEBNÍCH NÁSTROJŮ PŘED ZNEUŽITÍM

Vážení klienti,

poslední dobou se napříč celým tuzemským bankovním sektorem, setkáváme s řadou více či méně úspěšných pokusů o cílené zneužití různých platebních nástrojů, jako jsou platební karty, internetové bankovnictví a podobně. Chtěli bychom tak touto cestou poukázat na některé bezpečnostní zásady, jejichž dodržování je tou nejlepší prevencí před vznikem případných škod.

Případy, o které se jedná, jsou souhrnně nazývány “phishing” a jejich společným znakem je snaha pachatele získat od klienta banky jeho autorizační údaje k platební kartě, elektronickému bankovnictví či jinému elektronickému platebnímu prostředku. Nekalé praktiky na bázi phishingu se v zásadě dají rozdělit na dvě skupiny:

1. Pokus vylákat autorizační údaje vytvořením dojmu, že klient komunikuje se svojí bankou.
2. Pokus získat autorizační údaje prostřednictvím elektronických nástrojů, např. virů.

Obrana před oběma formami phishingu je velmi prostá, vyžaduje však ze strany klienta, tj. držitele platebního nástroje, důsledné dodržování bezpečnostních zásad, z nichž ty nejdůležitější vám nyní chceme v zájmu ochrany vašich peněžních prostředků připomenout:

- Nikdy nesdělujte jakékoliv autorizační údaje (login a heslo k Internetbankingu, číslo platební karty, datum platnosti karty, CVC/CVV kód z rubu karty, PIN ke kartě apod.) třetím osobám. Pokud se jakákoliv osoba vydává za zástupce banky a požaduje po vás sdělení některého z těchto údajů, jedná se s největší pravděpodobností o pokus o podvod! Fio banka po vás nikdy nebude chtít, abyste jí takovéto údaje sdělili. Nanejvýše může jako součást identifikace na dálku chtít sdělit určitou sekvenci z čísla platební karty, nikdy však celé její číslo.

- V prostředí internetu zadávejte autorizační údaje k platební kartě pouze na důvěryhodných platebních bránách. Nikdy nevyplňujte formuláře vyžadující sdělení autorizačních údajů ke kartě, jež nemají přímou souvislost s prováděním platebních transakcí. Fio banka vám nikdy nebude předkládat k vyplnění formulář sdělující, že údaje potřebuje z důvodu jejich ověření, což je poměrně obvyklá mystifikace ze strany pachatelů elektronického phishingu.

- Důsledně chraňte svoje prostředky elektronické komunikace (PC, notebook, tablet, mobilní telefon atd.) před elektronickými útoky zvenčí. Používejte aktualizovaný operační systém a pravidelně aktualizujte internetový prohlížeč ve vašem zařízení. Využívejte aktualizovaný antivirový program, je-li pro vaše zařízení k dispozici. Z nechráněného zařízení může vzdálený útočník snadno získat jakékoliv vaše autorizační údaje, které na něm zadáváte.

- Neotvírejte přílohy e-mailů, které vykazují podezřelé znaky (např. špatná čeština, nesprávná gramatika, apod.) a neinstalujte aplikace z nedůvěryhodných zdrojů. Zejména pro chytré telefony platí, že každý jejich uživatel by měl instalovat aplikace stažené výhradně z autorizovaných uložišť pro jednotlivé operační systémy (App Store, Google Play, Windows Phone Store).

- Buďte obezřetní na sociálních sítích a nikomu neposílejte své přihlašovací údaje, informace o platební kartě ani informace z autorizační SMS.

- Přistupujte do aplikace Internetbanking a e-Broker prostřednictvím stránek Fio banky.

- Sledujte novinky v oblasti bezpečnosti nejen v bankovnictví.

Závěrem připojujeme odkaz na tiskovou zprávu České bankovní asociace ze dne 20. 11. 2015, která vzrůstající riziko phishingu vnímá rovněž velmi vážně a považuje za nezbytné dát tomuto tématu dostatečnou publicitu.

https://www.czech-ba.cz/sites/default/files/20112015_cba_varuje_pred_kybernetickymi_utoky_final.pdf

Váš tým klientské podpory