V Praze, dne 8. června 2017

# TISKOVÁ ZPRÁVA

***Falešný web ČSOB ukázal, že třetina lidí se svým účtem stále riskuje***

**Kdyby guerillová kampaň ČSOB za bezpečnější internet byla skutečným hackerským útokem, přišli by důvěřiví klienti až o 20 milionů korun. Banka prostřednictvím falešných webových stránek internetového bankovnictví netradičně testovala obezřetnost klientů. Téměř třetina lidí i přes probíhající edukaci chybu několikrát zopakovala a na falešné stránky se neustále vracela.**

*„Odkaz na falešný internetbanking jsme na měsíc vystavili na Seznam a Google. Častou chybou klientů totiž je, že na stránky banky vstupují přes vyhledávače. Jenže i tady hrozí, že padnou do pasti hackerů,“* říká Jan Vimr, výkonný manažer útvaru Řízení digitálních kanálů ČSOB.

Odvážnou guerillovou akci zvolila ČSOB pro start dlouhodobé kampaně ke zvyšování digitální gramotnosti. Vzdělávání v oblasti digitální bezpečnosti považuje Marek Ditz, člen představenstva ČSOB za velmi důležité. *„Deset procent lidí například netuší, jak se bezpečně dostat na stránky svého internetového bankovnictví. A to je problém. Naším cílem je, aby peníze všech klientů byly v bezpečí, proto posilujeme bezpečnostní opatření nejen na naší straně, ale investujeme i do edukace veřejnosti,“* konstatuje Marek Ditz.

Netradiční kampaň, která měla klienty varovat před útoky hackerů a nasměrovat je k bezpečnému přístupu k internetovému bankovnictví, trvala přesně měsíc. Během té doby "falešnou" stránku banky navštívilo celkem 61 434 lidí. „*Nedopadli špatně, je vidět, že osvěta pomáhá. Zjistili jsme, že 67,5 % uživatelů nereaguje na reklamy a kliká na správné odkazy. Během kampaně se také snížil počet lidí, kteří přes vyhledávače na internetové bankovnictví vstupovali. Alarmující ovšem je, že téměř třetina klientů je nepoučitelná a navzdory edukaci vstupuje na falešný internetbanking opakovaně,“* doplňuje Jan Vimr.

Výsledek kampaně hodnotí banka přesto pozitivně. „*Lidé navíc strávili na speciálně vytvořené stránce průměrně jednu minutu, což znamená, že si zobrazované doporučení přečetli,“* říká manažer bezpečnosti elektronických kanálů ČSOB Petr Vosála.

**Hesla neměníme a nejsou dostatečně silná**

To, že lidé bezpečnost svých dat na sítích stále podceňují, potvrdil ČSOB i nedávno realizovaný průzkum. Lidé v něm mimo jiné odpovídali na dotaz, jak často si mění hesla internetového bankovnictví, zda si hesla či PIN poznamenávají na papírky, které nosí v peněženkách nebo zda poznají zabezpečené webové stránky.

„*Tři čtvrtiny lidí považují pravidelnou změnu hesla do internetového bankovnictví za důležitou. S dodržováním této pravidelnosti jsou už ale na štíru. Jednou měsíčně by měnila heslo jen pětina lidí, jako optimální se dotazovaným zdá, že by měli heslo měnit jednou za půl roku (35,6 %), nebo dokonce jen jednou ročně (34,5 %),“* říká Petr Vosála. Nedostatečná obměna, ale i nedostatečná síla hesla je podle něj poměrně velkým rizikem na internetu, které však uživatelé nevnímají. ČSOB chce na tato nebezpečí upozornit, stejně jako na podvodné e-maily či falešné e-shopy.

ČSOB bude v kampani zaměřené na digitální gramotnost i nadále pokračovat. V oblasti cyber security bude například spolupracovat i s youtubery. „*Chceme ukázat, že i takto vážné téma internetové bezpečnosti lze podat interaktivní a zábavnou formou,“* uzavírá Marek Ditz.

***Online bezpečnost a ČSOB***

Banka zahájila první vlnu dlouhodobé kampaně za kybernetickou bezpečnost loni v dubnu. S ní také spustila webový portál [www.csob.cz/bezpecnost](https://www.csob.cz/portal/bezpecnost/zasady-bezpecneho-chovani).

Úspěšné bylo také "hororové video" nazvané Mrknětenanašenovévideo.cz umístěné na Youtube.

Na stránkách ***www.csob.cz/bezpecnost*** se každý může dovědět, nejen jak bezpečně používat internetové bankovnictví, ale také jak zacházet s platební kartou nebo jak se vyhnout nejběžnějším karetním podvodům. Pokud má klient banky obavy, že došlo ke zneužití citlivých dat, má zde možnost kontaktovat specializovaného operátora.

**Kontakt pro média:**

**Lenka Vosátková**

levosatkova@csob.cz

tel.: 736 165 166