

# **ONLINE PODVODNÍCI BĚŽNĚ ZNEUŽÍVAJÍ FOTOGRAFIÍ ZNÁMÝCH OSOBNOSTÍ, TŘEBA VÝZNAMNÝCH POLITIKŮ, HERCŮ, MODERÁTORŮ ČI SPORTOVců. SLIBUJÍ ZÁZRAČNÉ ZBOHATNUTÍ, VÝSLEDKEM JE VŠAK NAPADENÍ BANKOVNÍHO ÚČTU**

**Kamil KOPECKÝ**

Velká část online podvodníků využívá potenciál online reklamy šířené prostřednictvím sociálních sítí ale i běžných webových stránek. Pro upoutání pozornosti pak často využívají fotografií různých celebrit, které “prozrazují recept na zázračné zbohatnutí”. Ve skutečnosti však mají tyto fotografie pouze upoutat pozornost a vzbudit důvěru uživatelů a přimět je ke kliknutí na odkaz, který vede na podvodné stránky.



Známa osobnost, která je se “zaručenou investicí” vizuálně spojena, samozřejmě o zneužití své identity netuší - vzbuzuje však důvěru a ovlivňuje cílové uživatele ochotné “vydělávat”. Terčem tohoto podvodu se v posledních měsících stal např. [prezident Petr Pavel](#), který měl prostřednictvím podvodné reklamy slibovat zaručený pasivní příjem díky investicím do kryptoměn. Ve skutečnosti však jde o klasickou ukázkou podvodu.

Před podvody s kryptoměnami dlouhodobě varuje Evropská bankovní federace ve spolupráci s Europolem a Kanadským

---

centrem pro boj proti podvodům (CANADIAN Anti-Fraud Centre, CAFC), která připravila osvětovou kampaň upozorňující na podvody s krypto-investicemi, v České republice tuto kampaň zastřešuje [Česká bankovní asociace ve spolupráci s Policií ČR](#).

Na problematiku online podvodů, které jsou součástí běžných reklamních sítí, upozorňuje také tým E-Bezpečí Univerzity Palackého v Olomouci prostřednictvím vzdělávacího cyklu Prevíti na síti například v osvětové videopřednášce věnované podvodné reklamě.

Jakmile tedy v online prostředí narazíte na “inzerát” slibující zázračné zbohatnutí pomocí investic do kryptoměn - zpozorněte! Statisticky policie odhalují, že uživatelů, kteří se nechali na tento podvod nachytat, je skutečně velké množství, stejně tak částky, o které přišly, dosahují v celkovém objemu stovek milionů korun. Příkladů podvedených najdeme mnoho, např. [zde](#), [zde](#) či [zde](#). A pokud jste se již nechali nachytat a pochopili svou chybu, okamžitě kontaktujte Policii ČR a svou banku, aby bylo možné zabezpečit váš účet a zastavit zadané finanční transakce.

Pro E-Bezpečí  
Kamil Kopecký  
Univerzita Palackého v Olomouci