Nový podvod, který nachytává stále více lidí. Tváří se jako pomoc od státu

SZ | seznamzpravy.cz/clanek/ekonomika-finance-osobni-novy-podvod-ktery-nachytava-stale-vice-lidi-tvari-se-jako-pomoc-od-statu-223169

Elektroničtí zločinci přišli s novou doménou, která se snaží lidi přesvědčit o tom, že jim stát aktivně nabízí pomoc v podobě finančního příspěvku. Stát takovou pomoc v rámci standardních příspěvků Ministerstva práce a sociálních věcí nebo speciálních v programu Deštník proti drahotě skutečně nabízí, ale jeho stránky vypadají jinak a jinou adresu má i doména.

Zatímco státní stránky mají doménu mpsv.cz nebo destnikprotidrahote.cz, podvodné, na které přijde upozornění v podobě SMS zprávy, znějí aktuálně npsv.online (první s podobnou tematikou se objevily v loni v srpnu a zněly například mpsv-prihlaseni.cz, mpcv.cz, mpvs-bydleni.cz). Po kliknutí na ně se otevře stránka vypadající na první pohled seriózně.

Foto: Iva Špačková, Seznam Zprávy
SMS lákající na státní pomoc.

Obsahuje logo Ministerstva práce a sociálních věcí (MPSV) i logo vládního programu s piktogramem deštníku, obrázek lva spojený s elektronickou občankou (Identitou občana) a také upozornění na to, že pokud jste se na stránky dostali pomocí linku v esemesce nebo z e-mailu, „je vše v pořádku, protože stát má povinnost taková hlášení rozesílat v rámci zákona o ochraně osobních údajů podle paragrafu 88“.

I pravý web MPSV upozorňuje na odkazy šířené SMS zprávami a e-maily, takže vše vypadá povědomě a v pořádku. Krátkým pátráním lze zjistit, že zákon o ochraně osobních údajů obsahuje jen 51 paragrafů a podobná norma, zákon o zpracování osobních údajů, jich obsahuje 68. Citovaný paragraf tedy neexistuje a je to jedna z jasných známek podvodu.

Foto: MPSV
Takto vypadají skutečné stránky Ministerstva práce a sociálních věcí.

Kdo je v nouzi a ve stresu, hasí oheň a nemá většinou čas zkoumat, zda jsou tyto informace pravdivé. Stačí, že na první pohled vypadají důvěryhodně, a klikne dál. V dalším okně mu podvodník nabídne několik bank, na které stačí kliknout a zobrazí se stránky vypadající stejně jako opravdová stránka banky, přes níž se klienti hlásí do internetového bankovnictví.

Adresa obsahuje dokonce znak uzamčeného zámku, což má nabudit dojem chráněného portálu, avšak doména zní jinak, než když se člověk hlásí přes oficiální stránky institucí.

Foto: MPSV
Takto vypadají opravdové stránky programu Deštník proti drahotě.

Počet tzv. phishingových útoků podle bank i Policie ČR významně roste a roste také počet lidí, kteří se přes různá upozorňování na elektronické zločiny nechají nachytat.

„Rok 2022 byl ve znamení více než dvojnásobného nárůstu phishingových útoků. Přímo úměrně jejich nárůstu vzrostl i počet klientů, kteří phishingovým podvodníkům podlehnou," říká Filip Hrubý, mluvčí České spořitelny.

Banka podle něj měsíčně identifikujeme stovky klientů, kteří se stanou obětí phishingových útoků, přičemž výše odcizených finančních prostředků se pohybuje měsíčně v řádu vyšších jednotek milionů korun.

Foto: Iva Špačková, Seznam Zprávy
Takto vypadá jedna z verzí podvodných stránek státní pomoci. Pomocí obrázků připomínajících loga MPSV, Identity občana a programu vládní pomoci se snaží navodit dojem serióznosti.

Výrazný nárůst případů eviduje i banka ČSOB. Od loňského srpna, kdy se objevil první útok snažící se lidem podsunout podvodný link v podobě příspěvku na bydlení, zaznamenala podobných domén na dvě desítky. „Počet útoků i napadených klientů prostřednictvím odkazů zasílaných v SMS a ve WhatsApp zprávách ve srovnání s minulostí prudce roste," říká mluvčí ČSOB Patrik Madle.

Více falešných webů zaměřených na státní instituce zaznamenala v minulém roce i Raiffeisenbank. Podíl lidí, kteří se napálí, však podle ní není tak velký.

„Nemáme přesný odhad, kolik klientů na takové zprávy zareaguje. Hodně z nich včas pochopí, že jde o podezřelé stránky, takže je opustí a bance to nehlásí. Dle nám dostupných informací jde o nižší desítky případů měsíčně, kde ke ztrátě dojde u jednotek případů," říká mluvčí banky Tereza Kaiserštotová.

Foto: Iva Špačková, Seznam Zprávy
Kdo má počítač chráněný, bude se ho před dalším chybným kliknutím snažit odradit varovná hláška. Je dobré její varování vyslyšet.

Že však dochází ke skutečnému nárůstu úspěšně provedených útoků, potvrzuje Policie ČR, která vede statistiky trestné činnosti v online prostředí, tedy skutečně nahlášených a vyšetřovaných případů. Do kyberzločinců se počítají všechny trestné činy vzniklé v elektronickém prostředí, tedy například nenávistné projevy, mravnostní delikty i podvodná jednání. Právě ta podle Vinčálka zaujímají největší část všech zločinů.

„Statistiky sledujeme od roku 2011. Počet případů každým rokem od té doby narůstá v řádu procent. Loni to však byl prudký nárůst v řádu několika desítek procent," říká kapitán Vinčálek. Přesné statistiky zveřejní Policejní prezidium ČR dnes.

Kromě krádeže peněz z účtu mohou být podle něj citlivá data klientů využita k praní špinavých peněz nebo k vyjednání půjčky.

Foto: Iva Špačková, Seznam Zprávy
Banky se snaží své klienty varovat před útočníky různými způsoby. Obrazovkou na přepážce, zprávou v internetovém bankovnictví nebo v aplikaci, na svých stránkách nebo mailem.

Banky se snaží své klienty upozorňovat na nové útoky, ať už na svých stránkách, nebo pomocí zpráv v internetovém bankovnictví či v mobilní aplikaci, nebo i prostřednictvím obrazovek na přepážkách.

Hlavní však podle nich je, aby lidé byli obezřetní a dodržovali základní zásady bezpečného používání internetového a mobilního bankovnictví. Mezi ně patří to, že lidé nemají reagovat na odkazy ve zprávách, obzvlášť když jsou zaslány z neznámých telefonních čísel nebo e-mailových adres.

Nikomu nemají sdělovat své přihlašovací údaje k internetbankingu, protože žádná banka ani bankéř po nich tyto údaje nikdy nebude chtít znát, a vždy se mají přihlašovat přes oficiální stránky institucí, a to jak bankovních, tak státních. Nemají však vypisovat do vyhledávače název banky nebo státní instituce, ale rovnou mají do adresního řádku napsat oficiální webovou adresu dané instituce.

Foto: Česká spořitelna

Při přihlašování se na stránkách institucí a firem je dobré si ověřit, zda mají certifikát vystavený právě pro jejich organizaci. Ověření se ukáže po kliknutí na symbol zavřeného zámečku v adresním řádku.

Ten, kdo využívá Bankovní identitu, by se měl podle Filipa Hrubého z České spořitelny ujistit, že daná internetová stránka má v adrese symbol zámečku a po jeho rozkliknutí se ujistit, že je bezpečnostní certifikát vystaven na instituci, která po vás přihlášení přes Bankovní identitu požaduje.

Kdo by se chtěl otestovat, jak dobře dokáže odolat phishingovým výpadům, může si spustit kybertest na stránkách České bankovní asociace, která ho zhotovila proto, aby klienti bank dokázali ochránit své peníze před útoky hackerů a podvodníků.

Ministerstvo práce a sociálních věcí uvedlo, že od léta spolupracuje se sdružením CZ.nic, které blokuje falešné weby napodobující komunikaci ministerstva s občany. „Takových falešných webů už vzniklo od léta více než sto. Vždy okamžitě zareagujeme a stejně tak se stalo i v tomto případě, kdy do několika hodin od spuštění nebyl již zmíněný web funkční," uvedl Jan Mikulecký, ředitel odboru kybernetické bezpečnosti MPSV.