

Pozor na sociální sítě

30.3.2023 - Lucie Korbeliusová | DTest

Nakupování přes sociální sítě Samotné nákupy nemusí být vůbec ničím rizikovým. Máte doma přebytečné oblečení, kterého se chcete zbavit a ideálně si pár korun přivydělat? Prodej je skvělou možností, přičemž spousta sociálních sítí nabízí možnost prodeje přes pár kliků. Pokud jste na opačné straně a zboží nakupujete, může se stát, že zboží nedorazí v pořádku, případně vůbec. Výjimkou bohužel nejsou ani případy, kdy spotřebitelé (ať na straně kupujícího, tak na straně prodávajícího) přijdou o mnohem větší množství peněz pomocí promyšlených podvodů. O této problematice jsme psali více [zde](#).

Podezřelé odkazy

Dalším velkým rizikem jsou podezřelé odkazy. Na ty spotřebitelé mohou narazit jak při nákupech či prodejkách, tak i při běžné komunikaci. Většina uživatelů sociálních sítí se setkala se situací, kdy jim přišel odkaz od kamaráda, příbuzného nebo kolegy z práce, u kterého byl například text „Jsi to ty?“, přičemž uživatelé na odkazy často klikají. Bohužel odkaz často nepříjde od kamaráda, ale pouze z účtu, který kamaráda připomíná nebo z jeho napadeného účtu.

Obrana před těmito praktikami není snadná. Samozřejmě je ideální žádné odkazy nerozklikávat, avšak v běžné komunikaci jsou odkazy často užitečnými pomocníky. Doporučujeme však kamaráda kontaktovat nazpět s bližším popisem odkazu, neboť napadené účty zpravidla pošlou jen tuto zprávu s odkazem a následně již nereagují. Pokud poté odesílatel zprávy nebude vědět, že odkaz poslal, pravděpodobně se jedná o napadený účet.

Jestliže byl odkaz odeslán z vašeho účtu, doporučujeme neprodleně odhlásit se ze všech zařízení (většina sociálních sítí nabízí tuto možnost na jedno kliknutí) a změnit heslo na bezpečnější variantu. Stejně tak doporučujeme změnit hesla i na přidružených účtech, tedy například na přihlašovacím e-mailu.

V případě, že máte problém si zapamatovat různá hesla, můžete využít služeb manažera hesel. Několik rad lze nalézt i v našem článku.

Soutěže

Časté problémy nabízejí i různé soutěže na sociálních sítích. Největším problémem je zde to, že mnoho soutěží je skutečných, a ne vždy tak je snadné rozpoznat, zda se nejedná o podvod. Důležitým bodem je kontrola profilu, který soutěž sdílí. Jestliže se jedná o celosvětovou společnost a na těchto stránkách je pouze pár stovek sledujících, je pravděpodobné, že jde jen o napodobeninu těchto stránek. Je také dobré sledovat URL adresu, s jejíž pomocí lze podvod v některých případech také odhalit. Časté jsou také „překlepy“ v názvech stránek, případně nahrazení písmen jinými znaky (například znak | místo písmene I nebo číslo 0 místo písmene O).

Zároveň je dobré se nad soutěží zamyslet i kriticky. Vyplatí se společnosti všem soutěžícím rozdat vouchery v hodnotě 5 000 Kč? Přestože soutěže často vyvolávají dojem, že společnost „utrácí“ pro spotřebitele, mnohem častěji se jedná o promyšlené marketingové akce, které společností ve výsledku vydělají mnohem více.

V neposlední řadě spotřebitelům doporučujeme, aby si soutěže ověřili přímo na stránkách dané

společnosti. Ve většině případů bude tato stížnost propagována i mimo sociální síť, aby ji našel co nejvyšší počet potenciálních soutěžících. „Jestliže je akce propagována pouze na jedné sociální síti, doporučujeme zvýšit obezřetnost a pečlivě zvážit, zda se do ní zapojit,“ upozorňuje Eduarda Hekšová, ředitelka spotřebitelské organizace dTest.

Výsledkem těchto podvodných soutěží je často zpráva, případně odpověď na komentář, který obsahuje odkaz. Ten může být škodlivý již sám o sobě a napadnout účet, v jiných případech si na něm podvodník vyžádá údaje, které poté může zneužít. „Může se jednat například o číslo platební karty,“ upřesňuje Hekšová.

Slibovaný dar

Čas od času se stane, že se na sociálních sítích objeví zcela cizí osoba, která tvrdí, že má přístup k vyššímu obnosu (např. dědictví), nicméně potřebuje zaplatit poplatek, aby s penězi mohla nakládat. „Může se jednat o osoby, které se vydávají za zahraniční vojáky, případně doktory na misích,“ doplňuje Hekšová. Zpravidla však tyto osoby po zaslání částky zcela zmizí a nejsou dohledatelné, v jiných případech však požadují ještě další doplatek. Spotřebitelé by si však měli uvědomit, že zcela cizí osoba nebude mít zájem dělit se o peníze s náhodným člověkem, na kterého narazila na sociálních sítích.

V podobném duchu se nesou i podvody, při kterých se dotýčný „zamiluje“ a potřebuje půjčit peníze na cestu do České republiky. Spotřebitelé by proto měli být velmi obezřetní a na podobné zprávy ideálně vůbec nereagovat.

Problematikou podvodných schémat na internetu jsme se v minulosti zabývali i v našem článku.

Výhodné investice

Méně časté, ale rozhodně ne výjimečné jsou nabídky výhodných investic. Může se jednat o investice do kryptoměn, kdy společnost zaručuje jistý výnos. Mezi sportovními nadšenci se však můžeme setkat i s tipy na sázky, které „zaručeně znásobí vklad“. Je důležité upozornit, že žádná investice není jistotou výdělkem a peníze spotřebitelů jsou tak v nebezpečí. Investice samotné samozřejmě špatné nejsou, ale měly by probíhat u ověřených společností a s penězi, o které si spotřebitelé mohou dovolit přijít.

Zneužití údajů ze sociálních sítí

Závěrem je vhodné spotřebitele upozornit, že údaje na sociálních sítích mohou být využívány i jinde. V poslední době jsme se setkali s několika případy, kdy podvodníci využili údaje (jméno, příjmení a datum narození), které poté zaslali spotřebitelům k ověření formou SMS, přičemž se vydávali za státní instituce. „V jedné SMS podvodníci žádali potvrzení osobních údajů kliknutím na odkaz. Údajným odesílatelem bylo Ministerstvo práce a sociálních věcí a účelem mělo být potvrzení příspěvků na bydlení,“ uvádí Hekšová konkrétní případ. Lidé by však i zde měli zpozornět a zkontrolovat si přímo na stránkách dané instituce, zda žádosti o takový příspěvek vůbec probíhají. Zároveň je silně nepravděpodobné, že by podobné příspěvky probíhaly formou SMS.

Předejit těmto problémům lze i pomocí omezení viditelnosti těchto údajů. Většina sociálních sítí požaduje zveřejnění pouze jména – datum narození a další údaje lze poté omezit tak, aby je neviděl nikdo nepovolaný.

Jak se vyvarovat problémům

Obecnou radou pro tyto případy je nerozklikávat odkazy, u kterých si spotřebitel není zcela jistý, kam vedou. Ani odkaz, který přijde z profilu známého není bezpečný a je dobré si ověřit, zda jej skutečně odeslala právě tato osoba.

U ostatních případů je důležité dobře promyslet, zda je reálné, aby byla určitá akce (či jistý přivýdělek) skutečná. Od věci není probrat situaci s blízkou osobou, která může situaci zhodnotit s určitým odstupem a pomoci tak předejít ztrátě financí či osobních údajů. Jakmile spotřebitel peníze zašle, je poté velmi těžké získat je zpět. Při vyplnění osobních údajů zároveň prakticky nelze zamezit jejich dalšímu šíření.

Pomoci ke zlepšení bezpečnosti na internetu Vám může i naše brožura Bezpečně na internetu.

dTest, o.p.s. je největší českou spotřebitelskou organizací, která v ČR působí již od roku 1992. Je vydavatelem spotřebitelského časopisu dTest, na jehož stránkách jsou publikovány výsledky nezávislých a objektivních testů produktů, varování před nebezpečnými a zdravotně závadnými výrobky, informace o spotřebitelských právech a rady, jak tato práva účinně uplatňovat. dTest je součástí mezinárodní organizace International Consumer Research and Testing (ICRT) a evropské spotřebitelské organizace BEUC.

Poradenská linka časopisu dTest - 299 149 009 - je v provozu každý pracovní den od 9 do 17 hodin a spotřebitelé na ní mohou konzultovat s právními poradci časopisu dTest nejrůznější spotřebitelské problémy, a to za cenu běžného tarifu volání. Od spuštění v roce 2010 této možnosti využily již statisíce spotřebitelů a poradenská linka časopisu dTest se tak stala první a nejvyhledávanější cestou k řešení potíží, se kterými se zákazníci na trhu setkávají.

<https://www.dtest.cz/clanek-10106/dtest-pozor-na-socialni-site>