18. 10. 2022

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Jak předcházet zneužití Vaší identity, zvláště při online nákupech

Online prostředí umožňuje pohodlné nakupování, neboť si můžeme skrze pár kliknutí objednat zboží klidně až z druhého konce naší planety. Absence osobního kontaktu však skýtá i svá rizika. Jedním z rizik, před nímž je třeba mít se obzvláště na pozoru, je zneužití Vašich identifikačních údajů, jež Vás může v krajním případě připravit i o značnou část Vašeho majetku. Abyste toto riziko eliminovali a mohli si v klidu vychutnávat taje internetových nákupů, připravil jsem pro Vás tento doporučující článek, který nahlíží na zneužití identity právě především prizmatem nákupů v e-shopech.

Doporučení k obecnému chování ve virtuálním světě

Nejprve shrnu, jak byste se v obecné rovině měli chovat poté, co zapnete počítač, tablet nebo jiné elektronické zařízení.

Stejně jako je třeba chránit své tělo před průnikem nežádoucích bakterií a virů, **je třeba náležitě chránit před viry a podobnými škodlivými elementy i počítače a jiná elektronická zařízení**, využívaná k připojování k internetu a ostatním virtuálním aktivitám.

Podle odborné literatury **lze zneužití virtuálního účtu klást k tíži toho, jehož účet byl zneužit, pokud tato osoba neučiní veškerá rozumně očekávatelná opatření směřující k zabezpečení svých zařízení**.[1] Nemáte tedy povinnost využívat nejmodernějších a placených antivirových programů, postačuje klidně, když **využijete bezplatného antiviru či když učiníte podobná vhodná opatření**.[2] Výslovně lze doporučit, abyste **se zdrželi deaktivace brány firewall**, která je předinstalovaná v operačním systému. Také doporučuji, abyste **neotevírali webové stránky**, které jsou zejména kvůli gramatickým chybám či nedobré grafice **zjevně phishingové**, tj. takové webové stránky, jež se snaží vyvolat dojem oficiálního webu důvěryhodné instituce jako je banka či státní úřad, byť jde o napodobeninu takovéhoto webu vytvořenou podvodníky s cílem získat Vaše citlivé údaje.[3]

Rovněž je třeba, abyste do svých účtů zvolili **dostatečně silná hesla**, jejichž prolomení nebude pro hackera otázkou pár vteřin. Zcela nevhodné je třeba heslo v podobě Vašeho jména nebo po sobě jdoucích znaků (např. 123456).[4]

Doporučení k obecnému chování mimo virtuální svět

I mimo virtuální prostředí je zapotřebí chovat se obezřetně a nezavdat příčinu ke zneužití Vaší identity. Je třeba, abyste **uchovávali v soukromí veškeré listiny, z nichž by bylo možné poznat Vaše přihlašovací údaje do různých aplikací a webových služeb.** Pokud tedy například necháte bankou vydaný dokument obsahující přihlašovací údaje do internetového bankovnictví v místě, kde se k němu bez problému dostanou i nepovolané osoby, nebo pokud si dokonce nalepíte lísteček s heslem k notebooku na jeho víko, pak mohou nastat značně negativní konsekvence.

Celkově vzato je tedy třeba **vyvarovat se veškerých konání nebo opomenutí, kvůli kterým by**

třetí osoby mohly neoprávněně zjistit a následně zneužít Vaše citlivé údaje.

Nad rámec výše uvedeného ještě předestírám, že v současné době využívají podvodníci také metody tzv. **vishingu či spoofingu**. Tyto podvody typicky spočívají v tom, že se Vám ozve osoba vydávající se za zástupce Vaší banky (v některých případech dokonce zneužije skutečné telefonní číslo Vaší banky) a **bude se Vás snažit přesvědčit, že Váš bankovní účet** (nebo jiný produkt) **je v ohrožení a že je třeba převést peníze** jinam (ve skutečnosti na podvodníkův účet).[5] Pokud se na Vás někdo obrátí v takovéto věci (a to i jinak než telefonicky), **zkontaktuje raději samostatně danou banku a ověřte si, zda se vskutku jedná o jejího zástupce.**

Doporučení k chování v e-shopech

Předně je vhodné, abyste vždy ověřovali důvěryhodnost e-shopu, v němž hodláte nakupovat. Výrazně Vám může napovědět již samotná podoba e-shopu. Na pozoru byste se měli mít zvláště tehdy:

- **nemůžete-li z e-shopu zjistit, kdo je jeho provozovatelem**, a na koho se tedy můžete obrátit ve věci reklamace či jiného uplatňování Vašich práv;
- **nabízí-li e-shop v porovnání s konkurencí zboží za mimořádně výhodnou cenu nebo nabízí-li zboží, které je jinak vyprodané;**
- **byl-li daný e-shop Českou obchodní inspekcí shledán jako rizikový**.[6]

Pakliže Vámi zvolený e-shop ani není na „black listu" ČOI, ani na jeho webu nelze nalézt žádné podezřelé elementy, **ověřte si zkušenosti zákazníků daného e-shopu**, jež zpravidla jednoduše naleznete po zadání názvu e-shopu do internetového vyhledavače.

Jestliže ani reference ostatních zákazníků nenasvědčují tomu, že by určitý e-shop byl podezřelý, můžete jej využít k uspokojení svých nákupních tužeb. Pokud byste se přeci jen **rozhodli využít potencionálně problematického e-shopu, zvolte způsob úhrady zboží na dobírku a nezadávejte raději nikam své platební údaje.** Jestliže by e-shop možnost dobírkové platby nenabízel, raději v něm nenakupujte.

V případě důvěryhodného internetového obchodu můžete využít i takový způsob platby, při němž budete při objednávce zadávat údaje o své platební kartě či jiné údaje diskrétního charakteru. Tyto **údaje však nezadávejte, pokud jste zrovna připojeni na veřejnou wifi** – v takovém případě raději posečkejte a vyřešte nákup až z pohodlí domova nebo z jiného místa, kde budete připojeni na lépe zabezpečenou síť.

Možné negativní důsledky zneužití Vaší identity nebo nedostatečné prevence zneužití a závěrečné shrnutí

Nedostatečná obezřetnost, ať již při používání elektronických zařízení a internetu nebo při výběru e-shopu či při realizaci objednávky z něj, **může mít především tyto následky:**

- **neobdržíte objednané zboží či služby;**
- **budete připraveni o** (v krajním případě veškeré) **prostředky ze svého účtu;**
- **svých práv vůči e-shopu** (resp. jeho provozovatelům) **se jen stěží domůžete;**
- **vznikne Vám dluh Vůči bance**, protože pokud se podvodníci dostanou až přímo do Vašeho internetového bankovnictví, mohou si Vaším jménem vzít online úvěr/zápůjčku.[7]

Podvodná jednání e-shopů jistě v mnoha případech **naplňují i znaky skutkové podstaty trestného činu**, a teoreticky by tedy e-shopu (resp. jeho provozovatelům) mohlo hrozit i trestní stíhání. Problémem však je, že dopátrat se provozovatelů podvodných e-shopů **je** v mnoha případech **nemožné**, protože podvodníci logicky o své pravé identitě veřejnost neinformují[8] a zpravidla vytvářejí své e-shopy tak, aby se policie nemohla jednoduše dopátrat původce webu.

Jak jsem již naznačil výše, v souladu se závěry odborné literatury a v souladu s § 444 občanského zákoníku, **pokud byste na zneužití své identity měli podíl viny** (byť v podobě nedbalosti), **pak by šla jednání podvodníka učiněná s využitím Vaší identity k Vaší tíži**.[9] Nemusíte se bát, že kupříkladu každý úvěr, který by si podvodník vzal na Vaše jméno, byste museli do poslední haléře splatit (korektivem příliš tvrdých dopadů by zde totiž mohly být přinejmenším soukromoprávní principy). Toto riziko zde však existuje, **a proto na závěr shrnuji, že nejlepší je dbát na náležité zabezpečení své identity**, ať již se právě nacházíte ve virtuálním či reálném světě.

Kristián Fischer,
student Právnické fakulty Univerzity Karlovy,
pomocná vědecká síla Katedry občanského práva PF UK,
paralegal ve spol. ZVOLSKÝ ADVOKÁTI s.r.o.

ZVOLSKÝ ADVOKÁTI s.r.o.

Pařížská 7
110 00 Praha 1

Tel: +420 222 317 579
e-mail: office@akzvolsky.cz

---

[1] Srov. MÜLLER-BROCKHAUSEN, M. Haftung Für Den Missbrauch von Zugangsdaten Im Internet. 1. vydání. Nomos Verlagsgesellschaft mbH, 2014, s. 335. Počítačové viry apod. přitom představují riziko pro zařízení se všemi operačními systémy, včetně iOS.

[2] Srov. tamtéž.

[3] Srov. tamtéž.

[4] Sílu hesla můžete bezplatně otestovat kupříkladu >>> zde.

[5] K této problematice srov. Vishing a spoofing - Policie České republiky. [online]. [cit. 16.09.2022]. Dostupné >>> zde.

[6] Seznam rizikových e-shopů naleznete >>> zde.

[7] Stranou pozornosti dále nelze ponechat ani mimoprávní důsledky, například negativní vliv zneužití identity na Vaši psychiku.

[8] Neuvedení identity a kontaktních údajů provozovatele e-shopu není přitom pouze porušením právních norem, nýbrž i varovným signálem pro Vás jako návštěvníky e-shopu, jak jsem blíže vysvětlil v kapitole 3 tohoto článku.

[9] Pokud by totiž aktivita z určitého uživatelského účtu vyvolala v druhé straně legitimní očekávání, že původcem dané aktivity je oprávněný uživatel účtu, a současně by daný uživatel přispěl k vyvolání tohoto legitimního očekávání svým zaviněním, pak by se postupovalo podle § 444 občanského zákoníku. – srov. DOBROVOLNÁ, Eva. [§ 444]. In: LAVICKÝ, P. a kol. Občanský zákoník I. Obecná část (§ 1−654). 2. vydání. Praha: C. H. Beck, 2022, s. 1393, marg. č. 8.

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory