Heslo k wi-fi na jídelníčku znamená malér

K veřejné síti wi-fi se v České republice obvykle přihlásíte bez vlastní identifikace. „Anonymní prostředí je ale rejdištěm hackerů, kteří umějí proniknout do vašich mobilů," varuje MARTIN MEDVĚD, ředitel společnosti MIIA a internetový expert.

Platí, že veřejná wi-fi znamená nebezpečnou wi-fi? Je velký risk používat v jejím rámci třeba e-bankovnictví?
Měl byste si minimálně zjistit, kdo síť provozuje, což najdete ve všeobecných obchodních podmínkách. Díky tomu máte jasno, kam se v případě hackerského útoku obrátit. Pokud na internetových stránkách provozovatele tyto podmínky nejsou nebo vás wi-fi připojí „jen tak", pak do citlivých komunikací s bankou nebo do firemní pošty rozhodně nechoďte. Doporučuji produkty Virtuální privátní sítě VPN, nabízí je mnoho společností. VPN přístup obvykle vyžaduje heslo k ověření uživatele, které jste dostal od správce sítě. Ideální by samozřejmě byla povinnost každého uživatele veřejné wi-fi odhalit svou identitu. To by spoustu hackerů odradilo.

Připojím-li se z chytrého mobilu na veřejnou síť a někdo se mi do něj „naboural", koho mám hnát k odpovědnosti?
Nabízí se říci, že toho, koho chytnou. Ale věc je daleko složitější, což hned pochopíte: ubytujete se dejme tomu v hotelu s pitnou vodou na pokoji. Bude ale závadná, takže vás dostihnou zažívací problémy. Kdo je odpovědný? Výrobce vody, nebo hotel? Po kom budete žádat náhradu škody? Asi po hotelu, protože výrobce vody vůbec neznáte. Majitel tedy musí prokázat, že voda mu byla dodána již závadná. A stejné je to i s internetem. Pokud se ubytujete v hotelu a přes jeho wi-fi vám někdo odcizí peníze z účtu nebo osobní fotky, nebudete žalovat dodavatele internetu, ale hoteliéra. Ten pak bude prokazovat, jak měl svou wi-fi zabezpečenou a že pachatelem nemohli být jeho zaměstnanci nebo správce sítě.

K takovým sporům dochází?
Máme příklad z praxe, kdy provozovatel veřejné wi-fi v jednom tuzemském zábavním centru musel na policii mnohokrát vysvětlovat, že za stalkingem, kterého se někdo z jeho provozovny dopouštěl, nebyl jeho zaměstnanec a už vůbec ne on sám.

Jít na bankovní účet z veřejného internetu je hazard.

Jak ale zkontroluji, že onen hotel síť opravdu chrání?
Je to jednoduché, jeho provozovatel vyžaduje autorizaci uživatelů, ať již pomocí telefonního čísla, nebo přes Facebook, Google a podobně. Pokud je wi-fi přístupná bez hesla nebo se heslo skví napsané na jídelním lístku, máte jasno, že majitel pro vás jako uživatele nedělá nic. A navíc ohrožuje i sám sebe.

Ověření přes Facebook? Takže provozovatel wi-fi se dostane k mým osobním informacím?
Ověření přes Facebook je běžná praxe, i když tuto variantu uživatelům nedoporučujeme, jelikož o svá osobní data opravdu přijdou. Majitel či provozovatel sítě tím však svůj problém vyřešil. Ví, kdo jste, takže pokud byste páchal nějakou nepravost, to znamená, že byste z jeho připojení šířil třeba spam, vyhrožoval, prováděl stalking nebo nabízel drogy, může vaše údaje z Facebooku předat policii.

A co se tím vyřeší? Vždyť i účet na Facebooku přece může být falešný...
To už ale není problém provozovatele wi-fi, nýbrž policie. Předloží-li někdo v hotelu padělaný pas, provozovatel hotelu přece také nemá odpovědnost za to, že je falešný. Stejně jako když jde o předplacenou SIM kartu v mobilu nebo váš Facebook.

Ještě k té odpovědnosti: po kom mám tedy vymáhat škodu, jestliže se připojím k veřejné síti, někdo mi mobil „hackne" a dostane se k mým penězům?
Zde se nejčastěji chybuje. Mnoho lidí zná pouze nadpis z rozsudku Evropského soudu: „Provozovatel veřejné wi-fi neodpovídá za uživatele své wi-fi." Jenže málokdo četl tento dokument či rozsudek celý a pak se mnoho lidí diví, když se po nich někdo domáhá náhrady škody za provoz bezdrátové sítě. Druhá část věty totiž zní: „A to za splnění tří kumulativních podmínek: sám nebyl autorem přenosu, do přenosu nezasahoval a neměnil obsah přenášené informace."

Co z toho vyplývá?
Jinými slovy: provozovatel wi-fi nesmí být sám tím, kdo vás o vaše věci připravil. Jenže jak to prokázat, když heslo k mé síti mají úplně všichni a ve stejný okamžik? Zde je nutné připomenout, že to není žádný převratný fakt. U nás na to pamatuje například zákon o některých službách informační společnosti číslo 480/2004 Sbírky, paragraf 3. Pokud provozovatel nezajistil ochranu wi-fi, není automaticky vinen, ale není také automaticky mimo hledáček policie nebo soudu. I proto je dobré síť zabezpečit. Pro uživatele i provozovatele.

Co mám dělat, když zjistím útok hackera? Obrátit se na policii, která určí viníka?
Určitě ano, je to nejsnazší cesta. Policie rozhodne, zda jde o věc, kterou se bude zabývat ona, nebo vám doporučí řešit celou záležitost přes civilní soud. Jsou to ošidné věci. I proto už dnes v moderních

Foto: **Jakub Stadler**

▲ **POUŽÍVÁNÍ** veřejné wi-fi je pohodlné, ale riskantní. „Jde o ideální prostor pro kybezločince," varuje internetový expert Martin Medvěd.

televizích nebo noteboocích nenajdete kamery. Výrobci nechtějí nést odpovědnost za to, co před ní děláme nebo který hacker vše natáčí.

Při pohledu na spousty lidí surfujících zdarma v obchodních centrech se zdá, že na internetovou bezpečnost příliš nedbáme. Je to tak?

Skutečně to není žádná sláva. Ono ale úplně stačí, když si třeba konkrétně vy odpovíte na otázku, kdo všechno zná heslo do vaší wi-fi. Pokud nikdo, jste v relativním bezpečí. Máte-li heslo napsáno na stole nebo na zdi, jste v relativním nebezpečí. Dal jste někomu přihlašovací údaje ke svému e-mailu? V případě, že ano, může z něj psát. Dal jste někomu PIN ke své kreditní kartě? Pak s ní může platit. Jak jste dopadl?

Na sto procent si jist nejsem. PIN jsem sice nikomu nedal, ale hesla neměním…

Heslo k wi-fi je jako každé jiné. Pokud ho někdo zná, dáváte mu svá práva a může se za vás vydávat. Ale provede-li něco, jak prokážete, že jste to nebyl vy, kdo platil, psal e-mail, objednával zboží? Z obchodů, kaváren, náměstí a sportovišť jsme

Martin Medvěd (46)

Více než dvacet let pracuje v oboru telekomunikací, především výstavby přístupových sítí a obchodní činnosti. Poslední roky se věnuje projektu Czech Wi-Fi Pass, který má za úkol výrazně snížit náklady na mobilní datové připojení pomocí dostupných wi-fi sítí. Rád cestuje a hraje beach volejbal a golf. Má tři děti.

se přesunuli do kyberprostoru, kam pochopitelně zamířil i zločin. Nač odcizit kreditní kartu v obchodě, když ji mohu ukrást na internetu? Proč vyloupit obchod, když se dá vykrást e-shop? Z jakého důvodu někomu vyhrožovat v hospodě, když to mohu udělat na sociálních sítích? Kyberútoků zkrátka bude přibývat a na nás leží úkol naučit se v kyberprostoru žít. Zde je nutná především osvěta, která v Česku hodně chybí. I podle mezinárodních studií patří naše republika mezi nejhůře zabezpečené státy, co se kyberochrany týče.

Ještě k veřejným sítím. Naši fotbaloví fanoušci se na šampionátu v Rusku divili, že i tam je už běžné veřejné připojení k wi-fi v městské dopravě. Nejsme v tomto směru „sto let za opicemi"?

Na uvedeném příkladu je krásně vidět, co zažíváme na dovolených: všichni hledáme levné připojení k internetu. A pokud nemáme unijní roaming nebo je náš tablet bez SIM karty, jsme v pasti. Těžko soudit, zda byla wi-fi v MHD v Moskvě už dva roky, nebo naopak až dva týdny před šampionátem. V každém případě věřím, že to ocenili všichni fanoušci z Evropské unie, protože s Ruskem žádný datový roaming nemáme.

Kdy budeme i my zdarma surfovat na všech linkách MHD?

Wi-fi v MHD či taxíku je u nás skutečně v plenkách. U tramvají a vlaků bývají překážkou přísné normy, které mnoho výrobců hardwaru nesplňuje. Rozšíření veřejných sítí by ale měly rozhýbat dotace na instalaci připojení k wi-fi zdarma, o něž mohou obce a města žádat od tohoto října. Přimlouvám se za jednotnou autorizaci uživatelů, aby se třeba Brňák nemusel podruhé registrovat v Praze a naopak. Provozovatelé by zároveň měli data na jednom místě. My dodáváme na trh Czech Wi-Fi Pass, který jednotné přihlašování využívá. Uživatel se autorizuje a pak se může automaticky připojovat v celé zemi.

Tomáš Loskot ■