Veřejné Wi-Fi? Vstupní brána pro hackery

11.4.2022 - Daniel Prokop | INFOPROFI GROUP s.r.o.

Představte si, že jste navštívili kavárnu s názvem „Mango“ a při pohledu na dostupné možnosti Wi-Fi jste viděli „Mango Free Wi-Fi“. Jak víte, že to není podvodný hotspot, který prostě používá toto jméno? Pro hackery je velmi snadné vytvořit takové nastavení a mohou snadno provést útok typu man-in-the-middle (MitM), pokud se připojíte k podvodné síti. Jde o běžnou taktiku kyberzločinců a i přes svou jednoduchost může být vysoce účinná.

Zatímco mnozí z nás využívají na cestách mobilního internetu prostřednictvím 4G/5G, připojení k bezplatné veřejné Wi-Fi je stále žádoucí, protože šetří spotřebu dat a je rychlejší.

Bezplatné Wi-Fi je nyní všudypřítomné, zejména ve městech. Pokud jste v kavárně, hotelu, baru, nákupním centru nebo na letišti, bylo by překvapivé, kdybyste své zařízení nemohli připojit k veřejné síti Wi-Fi. V dnešní době se můžete připojit k Wi-Fi ve vlacích, letadlech a dokonce i na venkově.

Zatímco přístup k bezplatné Wi-Fi je pro většinu z nás přínosem, je to také běžný vstupní bod pro kyberzločince. Veřejné Wi-Fi je ze své podstaty otevřené a nechráněné, aby k němu mohl kdokoli přistupovat. Díky tomu je síť zranitelná vůči hackerům. Veřejná Wi-Fi není bezpečná, pokud nemáte ochranu Wi-Fi pro svá mobilní zařízení.

Jedno z rizik je v tom, že se hacker umístí mezi vás a bod připojení, což znamená, že cokoli, co hodláte poslat do hotspotu při procházení internetu, jde místo toho k hackerovi. Může se jednat o jakýkoli typ dat, včetně finančních informací (kreditní karty), hesel, citlivých obchodních informací apod. Jak jsou hackeři schopni umístit se uprostřed? Jedním důvodem je použití zastaralých metod

šifrování používaných v hotspotech Wi-Fi. Tyto hotspoty často používají pro šifrování starší standardy, jako je WEP (Wireless Encryption Protocol), které jsou zranitelné. Dokonce i WAP (Wi-Fi Protected Access), který byl navržen jako náhrada WEP, má mnoho nedostatků a lze jej snadno nabourat.

Udržujte svůj mobil v bezpečí při používání veřejné Wi-Fi

Falešné webové stránky se mohou zdát legitimní

Jakmile hackeři otevřou vstupní bod, ať už prostřednictvím zranitelnosti v síti Wi-Fi hotspot nebo vytvořením falešného, mají řadu možností, které mohou ohrozit vaši mobilní bezpečnost. Pro začátek ovládání Wi-Fi mohou hackeři vytvořit falešný DNS (Domain Name System). V podstatě se jedná o druh phishingového útoku, který zajistí, že navštívíte falešný web místo skutečného. Falešným webem může být banka nebo jiná platforma, která vás vybízí k zadávání citlivých finančních údajů. Kromě pokusu o krádež vašich dat prostřednictvím phishingového útoku mohou nepoctiví aktéři také distribuovat malware prostřednictvím sítě. Minulý rok se například objevily zprávy o novém typu malwaru Emotet, který se pomocí botnetů snadno šířil přes nezabezpečené veřejné Wi-Fi sítě. Toto je jen jeden z řady malwarových útoků, které lze rozpoutat. Abychom to znovu zdůraznili, je to vektor útoku (zranitelný vstupní bod veřejné Wi-Fi), který kyberzločincům umožňuje řadu nevyzpytatelných možností, pokud vaše zařízení není plně chráněno.

Jak získat kompletní ochranu mobilní sítě

Jak tedy zajistíte bezpečné prohlížení při používání veřejné Wi-Fi? Z toho, co jsme si dosud řekli, můžete uvažovat o tom, že veřejnou Wi-Fi nebudete používat vůbec. Vaše mobilní internetová síť (4G/5G) totiž nabízí mnohem lepší šifrování (ačkoli není zcela chráněna) než veřejné sítě. Pokud se však rozhodnete pro přístup k veřejné Wi-Fi, existují kroky, které můžete podniknout ke zmírnění rizika. Mezi kroky, které je třeba podniknout k ochraně sebe a dat, patří zdržení se přístupu k osobním, finančním nebo obchodním datům při používání veřejné sítě Wi-Fi a dále změna nastavení tak, aby se vaše zařízení automaticky nepřipojovalo k síti Wi-Fi v okolí.

Můžete dokonce chtít použít VPN, která skryje vaši IP adresu, což je obvykle klíčová informace, kterou hackeři potřebují pro přístup k vašemu zařízení. Samozřejmě, jak stále více lidí pracuje na dálku, výše uvedené metody nemusí být praktické. Nejlepší ochranou pro mobily je však implementace kompletního bezpečnostního řešení.