

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **94** ze dne **17.12.2024**

Jak dokáží podvodníci získat vaše telefonní číslo?

Vaše soukromé telefonní číslo je cennější, než si možná myslíte. Přečtěte si, jak se může dostat do nepovolaných rukou a jak si telefon uchránit před podvodníky.

Podvody s telefonním číslem patří mezi nejúspěšnější. Pravděpodobně proto, že telefonním číslem a hovorům více důvěřujeme, obzvláště, pokud se na displeji objeví nějaké konkrétní jméno. Jsme tak důvěřivější a snáze naletíme. Jenomže existuje trik, jak volající jméno podvrhnout.

Okolo podvodných hovorů se točí velký byznys. Cílem útočníků jsou nejčastěji vaše bankovní účty. Šikovnou manipulací se vás pokoušejí přimět, abyste jim sami své peníze převedli, nebo jim dali údaje z karet.

Telefonní čísla patří mezi osobní údaje a jsou cenným zdrojem pro identifikaci i reklamu. Toto spojení si vysvětlíme na příkladu, který popsala televize CNBC:

Baseballový fanďa vložil vstupenky do košíku ve speciální aplikaci, ale nákup nedokončil. Přesto mu krátce po zavření aplikace zavolá prodejce a nabídne slevu na vstupenky. Náš fanoušek bude asi trochu zmatený, protože své číslo nikam nezadával. Odkud tedy jeho číslo mají?

Odpověď zní – prostřednictvím sledování. Některé trackery mohou shromažďovat konkrétní informace z webové stránky. Například pokud vyplníte své telefonní číslo do formuláře, tracker jej uloží a vytváří tak to, čemu se často říká personalizovaný obsah. Existuje celý obchodní model známý jako „zprostředkování údajů“ a špatnou zprávou je, že stačí málo, aby se údaje staly veřejnými.

Zprostředkovatelé dat a úniky informací

Zprostředkovatelé dat získávají vaše osobní údaje z veřejně dostupných zdrojů (veřejné rejstříky), komerčních zdrojů (obchodní partneři, jako jsou poskytovatelé kreditních karet nebo obchody) a také sledováním vašich online aktivit (aktivity na sociálních sítích, kliknutí na reklamu atd.) a poté vaše údaje prodávají dalším subjektům. Většinou se tato data využívají k cílení reklamy a prodeji služeb.

Toto není nelegitimní. Určitě si ale říkáte, jak se k takovým datům dostanou podvodníci.

Čím více společností, webů a aplikací své osobní údaje poskytujete, tím podrobnější je váš osobní „marketingový profil“. Tím se také zvyšuje vaše riziko úniku dat, protože u samotných zprostředkovatelů dat může docházet k bezpečnostním incidentům. Zprostředkovatel údajů by také mohl vaše údaje prodat jiným subjektům.

Zprostředkovatelé údajů nebo úniky, které se jich týkají, však nejsou jediným zdrojem telefonních čísel pro podvodníky.

Pět způsobů, jak se zločinci mohou dostat k vašemu telefonnímu číslu

1. **Veřejné zdroje** - Na sociálních sítích nebo na pracovních portálech se může objevit vaše telefonní číslo jako způsob, jak vás kontaktovat. V případě, že nemáte správně nastavenou ochranu osobních údajů nebo jej dokonce sami sdílíte, může být vaše číslo dostupné komukoli, dokonce i AI robotům.
2. **Ukradené účty** - Různé online služby vyžadují vaše telefonní číslo, ať už k potvrzení vaší totožnosti,

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **94** ze dne **17.12.2024**

k zadání objednávky nebo jako ověřovací faktor. Pokud dojde k prolomení vašich účtů kvůli slabým heslům nebo dojde k úniku dat, může snadno uniknout i vaše číslo.

3. **Automatické vytáčení** - Automatické vytáčení volá na náhodná čísla, a jakmile hovor přijmete, můžete se stát terčem podvodu. Někdy tyto automatické vytáčení služby volají jen proto, aby potvrdily, že číslo někdo používá a jde tedy o relevantní cíl potenciálního útoku.
4. **Pošta** - V některých případech může být vaše číslo nebo e-mail vytištěné na balíku.
5. **Phishingové a podvodné účty** - V neposlední řadě svá čísla můžeme odevzdat sami v různých chatovacích aplikacích. A to v účtech, jejich jediným cílem je sběr takovýchto údajů. Pár ukázek najdete níže. V chatovacích aplikacích se útočníci vydávají za firmy nebo se s vámi jinak snaží navázat konverzaci. Kromě čísla se pokusí zjistit pár dalších údajů, které lze použít pro sociální inženýrství.

Jak chránit své telefonní číslo

- Dávejte si pozor na phishing. Nikdy neodpovídejte na nevyžádané zprávy/volání z cizích čísel, neklikejte na náhodné odkazy v e-mailech a nezapomeňte zachovat chladnou hlavu a přemýšlet, než zareagujete na zdánlivě naléhavou situaci.
- Chraňte své účty dvoufaktorovým ověřováním, ideálně pomocí speciálních bezpečnostních klíčů, aplikací nebo biometrických údajů namísto ověřování pomocí SMS. Ty mohou být poměrně snadno zachyceny hackery.
- Dobře zvažte, zda webové stránky poskytnete své telefonní číslo. Je sice užitečné, máť jej vyplněný v e-shopu nebo zadáný pro obnovu účtu, když zapomenete heslo, ale není to nejbezpečnější varianta.
- Při online nákupech na nespolehlivých e-shopech zvažte použití předplacené SIM karty nebo služby VoIP místo svého běžného telefonního čísla.
- Používejte mobilní bezpečnostní řešení s filtrováním hovorů a také se ujistěte, že jsou ve vašem webovém prohlížeči zablokovány soubory cookies třetích stran, a prozkoumejte další nástroje a technologie zvyšující soukromí.

Je důležité dbát na správnou kybernetickou hygienu a být si vědom, jaká data o sobě sdílíme. Ostražitosť je na místě, zejména pokud vezmeme v úvahu důsledky tohoto nového světa poháněného umělou inteligencí.

Zdroj: AVcentrum ČR