

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **87** ze dne **22.10.2024**

Proč chtějí kyberútočníci váš telefon?

Vaše telefonní číslo je víc než jen způsob, jak vás kontaktovat – podvodníci ho mohou využít k rozesílání škodlivých zpráv, a dokonce ho zneužít k získání přístupu k vašemu bankovnímu účtu nebo ke krádeži citlivých dat.

Pojďme se podívat na to, proč jsou telefonní čísla vyhledávaným cílem kyberútočníků, a probrat rizika spojená s jejich vyzrazením.

Scam jako předmět podnikání

Nelehko se to říká, ale kyberzločin pořád ohromně vynáší. Tolik, že vznikají celé zločinecké gangy, které vymýšlejí propracované způsoby, jak uživatele okrást. Typickým příkladem může být budování falešného vztahu nebo volání falešného pracovníka technické podpory nebo bankéře.

Jádrem mnoha takových scénářů je phishing a další útoky zneužívající postupy sociálního inženýrství. Útočníci se snaží vyvolat emoce (typicky strach) a pracují s naléhavostí. Zkrátka musíte teď hned něco udělat, abyste zabránili katastrofě.

Navzdory nárůstu digitální komunikace telefonní hovory a zprávy zůstávají pro mnoho lidí důvěryhodnou metodou výměny informací. Často máme dojem, že když slyšíme druhého a vidíme na displeji jeho číslo, je všechno tak, jak má být.

Jak lze zneužít vaše telefonní číslo?

Vishing

Pokud útočník zná vaše telefonní číslo, může zkusit tzv. vishing. Jde o podvodný telefonát, jehož cílem je vylákat z vás osobní, platební nebo přístupové údaje. Patrně vás kontaktuje jménem nějaké autority. Často se zločinci vydávají za pracovníky bank, policisty nebo státní úředníky. Často argumentují tím, že vás zrovna někdo okrádá a abyste své úspory zachránili, musíte okamžitě převést peníze jinam, nebo nahlásit do telefonu své heslo k internetovému bankovníctví.

Smishing

Typickým podvodem je smishing, kdy útočníci rozesílají SMS zprávy s infikovaným nebo škodlivým odkazem, který odkazuje na phishingové stránky. Typicky přijde jménem nějaké renomované společnosti, často takto zneužívají platební službu PayPal nebo přepravní společnosti. Evidujeme třeba také zprávy, které přišly zdánlivě z finančního úřadu.

Cílem je vylákat z vás přihlašovací údaje nebo jiné osobní údaje na phishingových webových stránkách nebo si stáhnout nějaký malware.

Přesměrování hovorů

K podvodům lze využít přesměrování hovorů. Jak to funguje? Ozve se vám podvodník a vydává se za nějakou autoritu, třeba pracovníka technické podpory vašeho operátora. Vyzve vás, abyste vytočili specifické telefonní číslo (většinou začíná *).

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **87** ze dne **22.10.2024**

Jakmile oběť toto číslo vytočí, neúmyslně přesměruje volání na útočníky. Ti teď budou za vás přijímat hovory a v nich mohou odposlouchávat cenné informace.

Výměna SIM karet

Podvodníci se mohou pokusit přimět operátora, aby aktivoval vaši starší SIM nebo vám vydal novou. Nejdříve si sežene potřebné informace a poté kontaktuje mobilního operátora a požádá o přenos telefonního čísla na SIM kartu, kterou vlastní pachatel. Podvodník nejčastěji tvrdí, že je nutné SIM vyměnit kvůli krádeži nebo ztrátě telefonu.

Po provedení tohoto procesu oběť ztratí přístup k mobilní síti a telefonnímu číslu, zatímco útočník bude nyní přijímat hovory a textové zprávy oběti. Tohoto podvodu byste si ale rychle všimli, protože v jeho důsledku ztratíte přístup k telefonní síti.

Spoofing

Podvodníci mohou maskovat svou identitu a vydávat své číslo za jiné, známé. Této metodě se říká spoofing. V praxi se to projeví tak, že vám místo náhodného čísla vyskočí telefonní číslo, které znáte. V takovém případě na straně oběti odpadá prvotní podezřívavost.

Na vašem soukromém telefonu loví útočníci služební data

V dnešní době mnoho zaměstnanců používá ke kontrole služebních e-mailů mobilní telefony. Vzniká tím pro útočníky zcela nový prostor. I oni totiž vědí, že mobilní telefony máme méně zabezpečené než počítače.

Útočník si dá více práce s rešerší a podvod cílí na konkrétní firmu (tomu se říká spearphishing). Takže si spojí telefonní číslo a veřejně dostupné informace (například jména vedoucích pracovníků, interní software nebo výše obrátů). A tyto informace využije, aby se vydával za někoho, s kým pracujete nebo třeba za dodavatele.

Konečným cílem mnoha podvodníků je totiž získat přístup k podnikovým systémům a finančním prostředkům.

CEO fraud

Specifickým typem spear phishingu je takzvaný CEO fraud. V takovém případě se útočník vydává za vysoce postaveného manažera (například výkonného ředitele, anglicky CEO).

Představte si, že jste účetní ve velké společnosti. Právě řešíte mzdy, práce máte nad hlavu a do toho, vám zavolá šéf šéfa a požádá vás o převod peněz. Jde o urgentní záležitost. Je potřeba zaplatit zálohu na akvizici, o které se už dlouho šušká. Musíte ale jednat ihned. Obchodní partner čeká.

Sice víte, jak se vedení firmy jmenuje, ale běžně s ním nejednáte. Nechcete jej ztrapnit na tak důležitém obchodním jednání. Navíc má informace, která dávají smysl: oslovil vás jménem, volal na služební číslo. A šéfům s přece neodmlouvá. Tak transakci provedete.

Bohužel i když se jedná o telefonát, může to být podvod. Existují AI nástroje, které například z veřejných rozhovorů umí napodobit tón hlasu.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **87** ze dne **22.10.2024**

Jak se před telefonními podvody chránit?

Prověřujte, prověřujte, prověřujte. Nikdy nereagujete na nezvyklé požadavky ihned, ani když jsou od vašich blízkých. Nejdříve vždy sami kontaktujte tazatele a ověřte si, že opravdu potřebuje pomoci. V případě, že vám volá kolega, můžete jej kontaktovat prostřednictvím interních komunikačních nástrojů. Blízkým klidně zavolejte na jejich číslo. Naklonovat číslo tak, aby podvodník uměl i přijímat hovor, zatím možné není. Zeptejte se na něco, co nikdo nepovoláný nemůže vědět.

Obracejte se na poskytovatele služby. Pokud vám volá bankéř, policista nebo jiný důvěryhodný pracovník, neplňte požadavek hned. Zavolejte zpět na číslo poskytovatele služby, které běžně používáte. Doptejte se, zda vám skutečně volal někdo s urgentním požadavkem, případně poskytovatele informujte, že někdo zkouší podvést jejich zákazníky.

Nebuďte slušní. Útočníci s vámi po telefonu budou manipulovat, často jsou hrubí a vydírají své oběti argumentem na jako "Jsem policista, nespolupracovat je trestný čin." "To opravdu chcete přijít o všechno, jak vám to mám jako vysvětlit." Klidně telefon uprostřed věty típněte a vraťte se k předchozímu kroku a volejte sami zpět na vám známé číslo.

Dávejte pozor na to, co sdílíte. Abyste zabránili podvodníkům ve shromažďování dalších údajů o vás, dávejte si pozor na to, co o sobě sdílíte online. Impersonizace spočívá v tom, že útočník použije veřejně dohledatelné informace, aby vás přesvědčil že je váš kamarád, šéf nebo kolega.

Používejte vícefaktorovou autentizaci. Povolte ve všech službách vícefaktorové ověřování. Upřednostněte raději aplikace namísto SMS. Je to bezpečnější.

Pro útočníky jsou takové podvody poměrně nízkonákladové, potenciální zisk vysoký. Navíc je velmi složité najít a usvědčit skutečného viníka. Ke všemu může stačit jeden "úspěšný" telefonát, aby se celá operace vyplatila.

Proč jsou všechny tyto podvody takovou hrozbou? V dnešní době se mnoho online služeb spoléhá při ověřování a obnově účtu na mobil. Kompromitace telefonního čísla může vést k obejití bezpečnostních opatření, včetně dvoufaktorového ověřování (2FA). Podvodníci se navíc mohou vydávat za vás a podvést vaše přátele nebo vašeho zaměstnavatele.

Zdroj: AVcentrum ČR