

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **138** ze dne **24.3.2026**

Quishing: Myslete, než skenujete, QR kód může být past

QR kódy se během pandemie staly běžnou součástí každodenního života – platíme s nimi parkovné, objednáváme v restauracích nebo se přes ně přihlašujeme do služeb. Právě jejich samozřejmost ale otevírá prostor pro nový typ podvodu, kterému odborníci říkají "quishing" – phishing přes QR kódy.

V těchto útocích kyberzločinci umísťují falešné QR kódy na veřejná místa, například na parkovací automaty, do restaurací nebo na kiosky, případně je posílají e-mailem. Důsledkem mohou být finanční ztráty, krádež osobních údajů nebo dokonce napadení a ovládnutí zařízení.

Na začátku ledna 2026 vydal americký Federální vyšetřovací úřad (FBI) varování před útoky severokorejských kyberzločinců, kteří používali falešné QR kódy k získávání osobních informací. Podle expertů nejde o problém omezený jen na Spojené státy – podobné podvody se objevují i v dalších zemích, protože útočníci hledají nové cesty, jak na lidech vydělat. Podstata je jednoduchá: uživatel naskenuje QR kód a je přesměrován na podvodnou webovou stránku, která napodobuje legitimní web, například stránky restaurace nebo platby za parkování.

Podvodníci často přelepují nebo překrývají původní, legitimní QR kódy vlastními nálepkami. V minulém roce tak například britské úřady varovaly před falešnými QR nálepkami na parkovacích automatech, které oběti vedly na falešné platební stránky. Podobná varování vydala i americká Federální obchodní komise v souvislosti s nečekanými zásilkami s QR kódy, které směřovaly na phishingové weby.

Falešné QR kódy se přitom nemusí objevit jen fyzicky – FBI popsala i případy, kdy severokorejská skupina Kimsuky rozesílala zaměstnancům organizací e-maily s vloženými škodlivými QR kódy vydávanými například za odkaz na další informace.

Podle expertů z Planet VPN je schéma útoků vždy podobné: po naskenování kódu je uživatel nasměrován na falešný web, kde útočníci zkoušejí vylákat čísla platebních karet, přihlašovací údaje nebo přimět oběť k instalaci škodlivého souboru.

Spoluzakladatel Planet VPN Konstantin Levinzon upozorňuje, že quishing může vést nejen k přímým finančním ztrátám, ale také k ohrožení či ovládnutí samotného zařízení. QR kód podle něj snižuje ostražitost uživatelů – technologie se masově rozšířila teprve nedávno a rizika s ní spojená nejsou tak známá. Namísto "kliknutí na podezřelý odkaz" jde o rychlé skenování, které lidé často nevyhodnocují jako nebezpečné.

Dalším důvodem, proč podvodníci QR kódy tolik využívají, je to, že často obcházejí běžné ochranné mechanismy. Antiphishingové a antispamové filtry v e-mailech se většinou zaměřují na text a odkazy, ale obrázky – včetně QR kódů – analyzují méně podrobně. I tam, kde už systémy rozpoznávají QR kódy zavedly, útočníci hledají cesty, jak je obejít, například použitím nezvyklých barev nebo tvarů.

Odhady kyberbezpečnostních výzkumníků z firmy Proofpoint mluví o 4,2 milionu hrozeb souvisejících s QR kódy jen v první polovině minulého roku. Skutečný počet incidentů však bude podle Levinzona ještě vyšší, protože mnoho útoků není nikdy odhaleno nebo nahlášeno. Proto odborníci doporučují, aby lidé začali přistupovat k QR kódům podobně obezřetně jako k e-mailovým odkazům.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **138** ze dne **24.3.2026**

Základní pravidlo zní: vždy si rozmyslete, kdy a proč QR kód skenujete. Pokud vás po naskenování kód přesměruje na stránku, která po vás chce platbu nebo přihlášení, zbystřete – zvláště pokud jste kód našli na nálepce v ulici nebo v nečekaném e-mailu. U zpráv s QR kódem od neznámých odesílatelů je lepší si jeho pravost ověřit přímo u údajného odesílatele jiným kanálem. Odborníci také radí posílit vlastní digitální hygienu: používat silná hesla, zapnout dvoufázové ověřování a pravidelně aktualizovat software.

AV centrum ČR