

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **111** ze dne **17.6.2025**

Smishing: Co to je a proč na něj snadno naletíme?

Pokud nakupujete online, zprávy od dopravních společností určitě dostáváte a většinou nemáte důvod nad nimi moc přemýšlet. Často se stává, že lidé ztratí v objednávkách přehled. Takže SMS od DPD nebo pošty nevyvolává žádné zvláštní podezření. A to ani, když je v nich uveden odkaz pro více informací o zásilce. Může se ale jednat o podvod, tzv. smishing.

Termín smishing ale není tak známý jako phishing, byť využívá stejné psychologické principy. SMS zprávy nemají adresu odesílatele, kterou byste si mohli rychle ověřit. Některé se dokonce mohou chytře připojit k předchozím chatovacím vláknům v rámci legitimní korespondence v telefonu, a tak mohou na první pohled vypadat jako pravé i pro bezpečnostní profesionály.

Jak funguje smishing

S podvodnými SMS jako by se roztrhl pytel a ubývat jich nebude. Útočníci dobře vědí, že SMSkám a telefonátům obecně důvěřujeme více. Pokud tedy napodobují nějakou známou značku, je pravděpodobnost, že někdo na podvod naletí, vyšší.

Typické je, že se jedná o urgentní záležitost: Například vás varuje platební aplikace, že dojde ke zrušení účtu, v případě balíků musíte doplatit clo nebo nějaký drobný poplatek, aby vám je doručili, a podobně. V podvodné SMS je vždy odkaz pro více informací, který vede na podvodnou phishingovou stránku. Cílem smishingu je získat od vás osobní údaje, hesla nebo informace z platebních karet. To vše pak útočníci mohou prodat nebo dále zneužít.

Co se stane, když kliknu na podvodnou SMS?

Celý podvod bývá dobře promyšlený a věrně napodobuje legitimní značky. Ty se samozřejmě brání, ale dopadnout podvodníky je bohužel oříšek. Odkaz z SMS vede typicky na falešnou stránku. Z SMS se prokliknete přímo na platební bránu, která vypadá zcela standardně. Podvodníci často napodobují oficiální adresy, ale přidají třeba pár slov navíc nebo změni znak. Ve spěchu takový detail mnoho lidí zkrátka přehlédne. Platební brána je falešná. Vytvořit věrnou vizuální kopii je bohužel snadné.

Naletěl jsem na smishing, co mám dělat?

Pokud na falešné stránce vyplníte údaje a uvědomíte si to pozdě, nepanikařte. Vzpomeňte si, jaké údaje jste vyplnili. Pokud šlo o heslo, okamžitě jej změňte. Pokud to samé heslo používáte i do jiných služeb, změňte jej i tam. Doporučujeme používat vždy unikátní přihlašovací údaje. Ukládat si je bezpečně můžete ve správci hesel.

Pokud jste vyplnili údaje ke kartě nebo zadali platbu, neprodleně kontaktujte svou banku na oficiální infolince. Někdy je možné platbu stornovat. Pravděpodobně vám doporučí danou kartu zablokovat a vystavit novou.

Vyplnili jste osobní údaje jako je e-mail či adresa? To vrátit zpátky nepůjde a budete muset být obezřetní. Pak si dávejte pozor na jakékoliv nevyžádané zprávy.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **111** ze dne **17.6.2025**

Jak se chránit před smishingem?

V dnešní rychlé době je důležité při čtení zpráv zpomalit. Trochu knížecí rada, ale je to tak. Obzvláště, pokud jde o zprávu, která vás děsí nebo z ní naopak máte radost, případně vyžaduje okamžitou reakci. Útočníci se vás snaží dostat pod emoční a časový tlak.

Pokud byste si v klidu přečetli adresu jako ceskaposta-poslatexpres.com, bude vám patrně připadat podezřelá. Je-li zpráva urgentní, ale vy si nevybavujete, že byste si balík či službu vyžádali, navštivte nejprve oficiální stránky firmy nebo zavolejte na oficiální telefon a situaci si ověřte nezávisle na SMS.

Doporučujeme do každého telefonu, ze kterého přistupujete na internet, nainstalovat bezpečnostní aplikaci. Ta totiž podvodné stránky zablokuje dříve, než někde vyplníte svá citlivá data.

O SMS podvodech se stále mluví málo, upozorněte na ně i vaše blízké. Na SMS podvody mohou naletět i dospívající nebo senioři, kteří se s technologiemi třeba ještě učí zacházet.

Shrnutí, podtrženo:

- Smishing jsou podvody prostřednictvím SMS zpráv, které se tváří jako zprávy od známých služeb, například České pošty nebo DHL.
- SMS zprávy obsahují odkaz na phishingovou stránku, cílem je vylákat z obětí osobní údaje, hesla nebo údaje z platebních karet.
- Útočníci využívají psychologické manipulace, například tlačí na urgentní akci nebo vyvolávají emoce.
- Pokud na podvod naletíte, je důležité ihned změnit heslo, zablokovat kartu nebo kontaktovat svou banku, podle typu údajů, které jste zadali.
- Urgentní SMS zprávy si vždy nezávisle ověřte a používejte antivir do mobilu.

Zdroj: AVcentrum ČR