

Zavolají, neodpovídají a zavěsí: Robocalling je nový způsob, jak se zloději snaží dostat k vašim účtům

PS poznatsvet.cz/veda-a-technika/robocalling-podvod

Alena Novotná

info

Alena Novotná

1. 10. 2024

clock 5 minut

video

Kybernetická kriminalita neustále roste a s ní i kreativita podvodníků. Jednou z nejnovějších a nejnebezpečnějších metod, jak se zločinci snaží získat osobní údaje nebo dokonce vyprázdnit váš bankovní účet, je tzv. „robocalling“.

Podvodný způsob funguje na principu automatizovaných hovorů, které vás mohou uvést do situace, kdy nevědomky předáte své cenné informace.

Jak robocalling funguje?



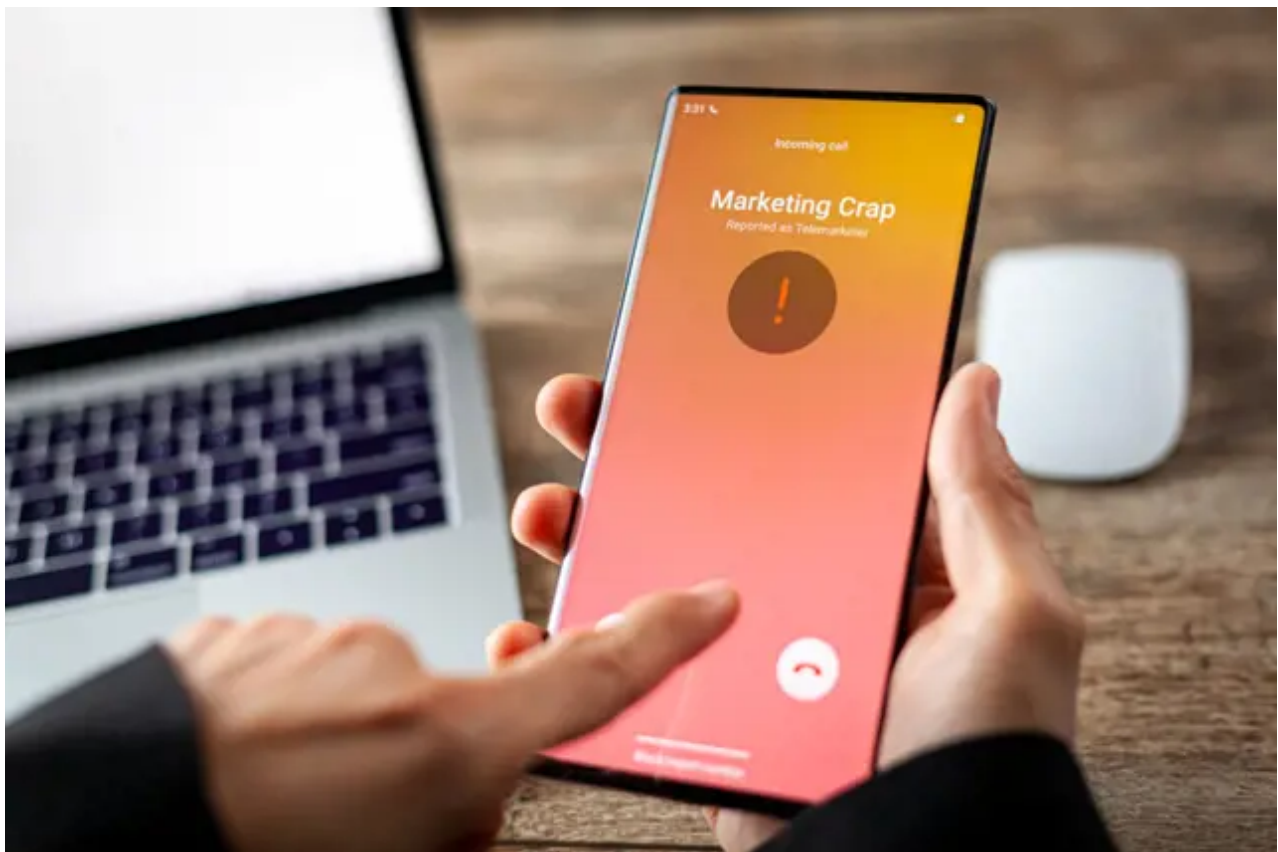
Watch Video At: <https://youtu.be/zBtkdcmUUSE>

Zdroj: Youtube

Podvodný robocalling je technika, při níž automatizovaný systém volá na vaše telefonní číslo. Pokud zvednete telefon, systém zaznamená, že vaše číslo je aktivní, a bez odpovědi zavěsí. To dává podvodníkům signál, že jste ochotni přijímat hovory, a mohou vám začít volat častěji. Cílem je buď přímo získat od vás osobní údaje, nebo vás psychologicky zmanipulovat k tomu, abyste reagovali na jejich další pokusy.

Podvodníci se často vydávají za legitimní organizace, například banky, pojišťovny nebo vládní agentury, aby zvýšili šanci, že jim uvěříte. Jejich taktika je rafinovaná a někdy i velmi přesvědčivá.

Typy robocallů a jaký mají cíl



info

zoom_in

Každý robocall má jiné cíle

Existuje mnoho forem robocallů, přičemž každá z nich má specifický cíl a metody, jak podvodníci dosáhnou svého:

Vymáhání dluhů

Robocall s cílem vymoci dluhy je běžným scénářem. Některé hovory mohou být legitimní, pocházející od agentur, které opravdu spravují pohledávky. Ale existují i podvodné verze, při nichž se falešní vymahači snaží získat platby za neexistující dluhy.

Phishingové podvody

Nejčastěji se phishingové robocally snaží získat vaše osobní a finanční údaje. Podvodníci se mohou vydávat za zástupce bank, poskytovatele kreditních karet nebo dokonce vládních institucí, aby vás přesvědčili, že je třeba okamžitě jednat a sdělit jim své citlivé informace.

Charitativní robocally

I charitativní robocally mohou být jak legitimní, tak i podvodné. Podvodníci se často vydávají za renomované organizace, aby vás přiměli poslat peníze na falešné charitativní účely.

Podvody s půjčkami

V těchto hovorech se vám nabízejí výhodné půjčky s atraktivními podmínkami, které mají jediný cíl – získat vaše peníze nebo osobní údaje. Po zaplacení poplatků často žádné půjčky neexistují.

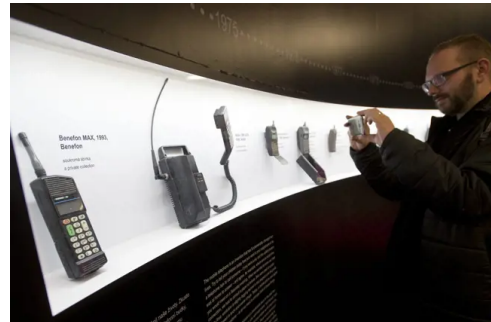
Zahraniční robocally

Mezinárodní hovory, často z neznámých čísel, mohou slibovat falešné výhry nebo výhružky zahraničních vlád. Podvodníci se snaží získat buď vaše peníze, nebo osobní údaje pod falešnými záminkami.

Podvody s technickou podporou

Tyto hovory se snaží přesvědčit oběti, že jejich počítač je napaden nebo má technické problémy, a nabízejí pomoc výměnou za poplatek. Skutečným cílem však je získat vzdálený přístup k vašemu zařízení nebo vás přimět zaplatit za falešné služby.

Věda a technika



Leží vám doma starý telefon? Toto je seznam modelů, za které jsou sběratelé ochotni zaplatit statisíce

video

Jak se vyhnout robocallingovým podvodům?

Prevence je vždy lepší než řešení následků, proto je důležité znát několik základních zásad, jak se podobným podvodům vyhnout:

Neodpovídejte na neznámá čísla: Pokud volající číslo neznáte, neodpovídejte. Zločinci spoléhají na to, že zvednete telefon a potvrdíte aktivitu svého čísla.

Nikdy nesdělujte osobní údaje po telefonu: Legitimizované společnosti vás nebudou žádat o citlivé informace, jako jsou čísla kreditních karet nebo sociálního pojištění, prostřednictvím telefonu.

Blokujte podezřelá čísla: Většina moderních chytrých telefonů nabízí možnost blokování hovorů z určitých čísel, což může snížit počet nežádoucích hovorů.

Nainstalujte si aplikaci na blokování robocallů: Existuje řada aplikací, které dokážou identifikovat a blokovat podezřelé hovory dříve, než vás vůbec obtěžují.

Nepodléhejte panice: Podvodníci často používají taktiku zastrašování nebo vytváření naléhavé situace, aby vás donutili jednat. Nejdříve si ověřte, zda se jedná o skutečnou hrozbu, než začnete jednat.

Cestování



Největší podvodník všech dob: Vymyslel úrodnou zemi zlata a vydělal miliony.

Desatero ochrany před podvody

Kromě základní ochrany před robocallingem je důležité se chránit i před širšími kybernetickými hrozbami. Zde je několik zásad, které byste měli dodržovat:

1. Používejte pro každou aplikaci a službu jiné heslo.
2. Vytvářejte silná a často měněná hesla.
3. Neukládejte hesla do internetových prohlížečů.
4. Vyhýbejte se přihlašování do citlivých aplikací přes veřejné Wi-Fi sítě.
5. Ověřujte e-mailové adresy a domény, než kliknete na odkazy.
6. Nikdy neotevírejte podezřelé odkazy zaslané přes aplikace jako WhatsApp.
7. Nesdílejte ověřovací kódy s nikým, ani když přichází z důvěryhodného zdroje.
8. Pravidelně aktualizujte software, prohlížeče a aplikace.
9. Používejte antivirový a antimalwarový software.
10. Vypínejte polohové služby, kameru a mikrofon, pokud je aktivně nevyužíváte.

Robocalling je stále rostoucí problém, který si vyžaduje opatrnost a informovanost. Podvodníci jsou stále vynalézavější, a proto je důležité být vždy na pozoru a chránit své osobní a finanční údaje.

Zdroje: eldoce.tv, pindrop.com, techzpravy.cz



Alena Novotná

Redaktorka

2144 článků

Newsletter

Odesláním souhlasím se Všeobecnými smluvními podmínkami a beru na vědomí Zásady zpracování osobních údajů spol. VLTAVA LABE MEDIA a.s.