Čím dál více využíváme moderních technologií – každý den brouzdáme po internetu, dostáváme a odpovídáme na emaily, pracujeme s internetovým bankovnictvím nebo nakupujeme v e-shopech.

Jsme často vystavováni kybernetickým útokům, které, v případě naší nepozornosti či špatného rozhodnutí, mohou vést ke ztrátě naší identity či peněz z bankovního účtu.

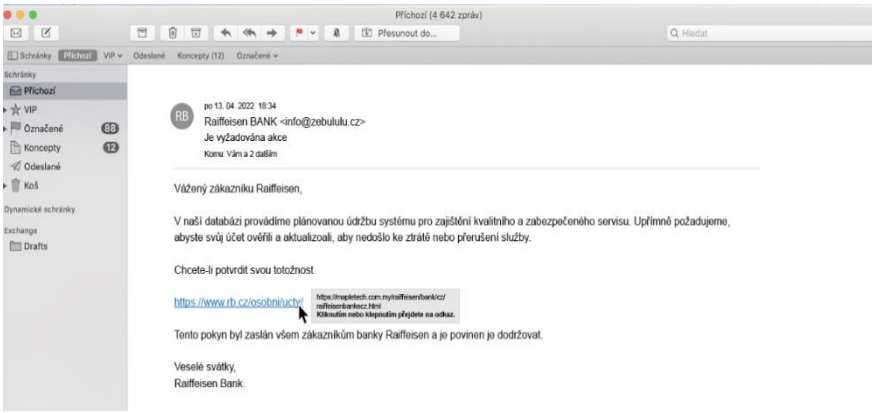
Podvodníci mají stále nové metody, jak nás okrást. Kromě falešných mailů a sms zpráv prudce rostou podvody na sociálních sítích a hlavně podvodné telefonáty. Ty patří k vůbec nejzákeřnějším metodám.

Cílem podvodníků jsou všichni - od teenagerů až po seniory.

Jejich metody jsou dnes daleko sofistikovanější a kombinují nedostatečné zabezpečení vašich chytrých telefonů a PC, znalost vašich osobních dat, umění manipulace a moment překvapení. Mezi nejčastější typy podvodů patří..

Podvodné e-maily — phishing

útoku v podobě podvodného e-mailu nebo zprávy na sociálních sítích. Cílem těchto útoků je buď od vás získat vaše citlivé údaje (např. číslo platební karty a přístup do on-line bankovnictví), nebo vás donutit k nechtěnému stažení škodlivého softwaru



Špálova 3
702 00 Ostrava

Tel.: +420 974 722 233
Email: krpt.prevence@pcr.cz

Podvodné SMS (tzv. smishing)

Velmi často se jedná o zprávy, které vypadají, jako by je zaslala některá z doručovacích společností či vaše banka, nebo vás lákají na vyzvednutí výhry apod. Všechny tyto SMS mají opět jediný cíl: vylákat z vás údaje o vaší platební kartě, internetovém bankovnictví či jiné citlivé informace nebo vás navést na odkaz se škodlivým malwarem.

Podvodné telefonáty údajných bankéřů, policistů či investičních poradců (vishing)

Tento způsob je o to zákeřnější, že se jedná o telefonní hovor s „živým“ člověkem, který chce svou oběť vystrašit a zároveň vzbudit důvěru, že je tím, kdo vám pomůže. Může volat z čísla podobného či stejného, jako má vaše banka, policie nebo příbuzný – podvodníci totiž umějí i napodobit různá telefonní čísla (spoofing). S vámi získanou důvěrou vás pak bude nutit k okamžité reakci. Scénáře se mohou lišit – útočník po vás bude chtít vaše přihlašovací údaje, údaje z vaší platební karty či potvrzovacích SMS, případně umožnit vzdálený přístup k vašemu počítači. Závěr je ale stejný – nakonec vás připraví o vaše peníze, které pravděpodobně již nikdy neuvidíte.

Podvodné m-platby

Mobilní platba (m-platba) funguje podobně jako platba platební kartou, avšak na rozdíl od placení kartou vám nejsou peníze strženy z účtu, ale z vašeho předplaceného kreditu nebo měsíčního tarifu u mobilního operátora. Mobilní platbou je možné hradit různé on-line nákupy. Při využití m-platby nemusíte prodejci poskytovat údaje o své platební kartě, ale nákup potvrdíte jednorázovým kódem, který vám operátor zašle v SMS.

Cílem podvodníka je získat vaše telefonní číslo. Buď se naboural do vašeho profilu na sociální síti, nebo napodobí profil někoho jiného a následně jménem této jiné osoby rozesílá zprávy do profilů v adresáři.

Reverzní inzertní podvody

Pachatel zareaguje na váš inzerát. Podstrčí vám fiktivní platební bránu, kde vyplníte citlivé bankovní údaje a místo peněz za inzerované zboží přicházíte o všechny úspory.

Nabídka výhodných investic

Přesvědčivá lákavá reklama a manipulativní jednání. Cílem pachatele je vylákat z oběti co možná nejvíce finančních prostředků a využívá k tomu přirozenou ziskuchtivost každého z nás.

Podvody typu Nigerijské dopisy:

Princip, který funguje už více jak 100 let. Pachatelé sázejí na kvantitu. Vždy se najde někdo, kdo se nechá nachytat na slibovanou cennou zásilku nebo domnělou pomoc. Často zde hraje velkou roli láska (legenda americký voják)

Podvodné veřejné WiFi sítě

Podvodníci mají stále nové metody, jak nás okrást. Kromě falešných mailů a sms zpráv prudce rostou podvody na sociálních sítích a hlavně podvodné telefonáty.

Naším cílem je upozornit na kybernetické podvody a naučit, jak jim nenaletět, jak se chovat v internetovém prostředí bezpečně. Každoročně v předvánočním období zaznamenáváme zvýšený nárůst kyberpodvodů (e-shopy, reverzní inzertní podvody). V příloze zasíláme přehled nejčastěji páchané trestné činnosti v oblasti virtuálního prostředí, o které na přednáškách hovoříme a na příkladech z praxe

PREVENCE a dostatek informací je v této oblasti nejúčinnější metodou, jak předejít ztrátě financí a Vašich dat. Právě ona DATA si musíme pečlivě chránit a přemýšlet, komu, proč a za jakým účelem je poskytujeme. I v bezbřehém virtuálním prostředí se potřebujeme cítit v bezpečí a chránit sebe i své blízké.

Krajské ředitelství policie Moravskoslezského kraje
Oddělení prevence
nprap. Bc. Vladimíra Faferková