



Krajské ředitelství policie
Jihomoravského kraje

PHISHING

Typ kybernetického útoku, kdy se útočník snaží získat důvěrná data zejména k platební kartě nebo přihlašovací údaje k online bankovníctví. Často se k tomuto útoku používá e-mail. Útočník se vydává za důvěryhodnou autoritu.

Jak poznat phishing:

- Neočekávaný e-mail – nevyžádané e-maily od neznámých osob není nutné otvírat, a když už, pak se zvýšenou pozorností.
- Požadavek na osobní údaje – žádná seriózní instituce po vás nebude chtít zadání osobních údajů, popř. hesla k online bankovníctví v e-mailu.
- Špatná gramatika.
- Přílišná naléhavost – pokud na vás e-mail příliš tlačí a nutí kliknout na tlačítko či odkaz a provést zadání vašich citlivých údajů, buďte ve střehu.
- Velmi výhodná nabídka – zboží zadarmo, výhodná služba, nalezený příbuzný v zahraničí, dědictví, to vše je typické pro phishing.
- Podezřelá URL adresa – adresa odkazu, na který máte kliknout, neodpovídá odeslateli. Při přejetí odkazu myší neodpovídá náhled URL adresy názvu odkazu ve zprávě.



Krajské ředitelství policie
Jihomoravského kraje

QUISHING

Forma phishingu, která zneužívá QR kódy, které odkazují na podvodné webové stránky.

Na co si dát pozor:

- Zkontrolujte, zda není původní QR kód překrytý jiným.

Jak se bránit:

- Používat pro skenování QR kódů aplikaci, která nabízí předchozí zobrazení URL adresy před přesměrováním na webovou stránku.

VISHING

Oklamání oběti pomocí telefonního hovoru. Cílem útočníka je vylákání různých informací, které bývají následně zneužity (citlivé informace k osobní identitě, k platební kartě, k platebnímu účtu...).

Podvody jsou založeny na principu telefonního hovoru, kdy se volající představí jako pracovník banky, který zjistil napadení vašeho účtu. Fiktivní bankovník volaného vystraší a přiměje ho převést finance na „bezpečný účet“ s informací, že se jedná o dočasné bezpečnostní opatření. Věrohodnost často umocňuje další telefonát, tentokrát od údajného policisty, který nadiktuje konkrétní kroky k převodu peněz –



Krajské ředitelství policie
Jihomoravského kraje

zaslání odkazu, přihlášení do internetového bankovníctví a převod peněz. POZOR – podvodníci umí napodobit jakékoli telefonní číslo.

Jak se bránit:

- Nikdy nikomu nesdělujte žádné citlivé údaje, údaje k platební kartě ani přístupové údaje k online bankovníctví.
- Nikdy nikomu nesdělujte ani nepřeposílejte bezpečnostní/autorizační kód, který vám přišel formou sms zprávy.
- Nikdy nikomu neumožňujte vzdálený přístup do vašeho počítače.
- Informace ověřujte přímo u vaší banky.
- Nepoužívejte vyhledavače pro přístup do internetového bankovníctví, používejte oficiální adresy.

SMISHING

Forma phishingového útoku prováděná prostřednictvím SMS. Cílem útočníků je vylákání citlivých údajů k účtům popř. platebním prostředkům. SMS zprávy reagují na aktuální dění, např. přeplatek na daních a obsahují odkaz, na který má příjemce kliknout. Tento odkaz důvěřivce přesměruje na webový portál (např. Moje daně) s možností přihlášení pomocí bankovní identity. Pokud člověk falešný přihlašovací formulář vyplní, poskytne



Krajské ředitelství policie
Jihomoravského kraje

podvodníkovi přihlašovací údaje a údaje k dvoufaktorovému ověření.

Jak se bránit:

- Nikdy na základě výzev v SMS zprávách neklikejte na odkazy a nesdělujte své přihlašovací údaje do online bankovníctví ani citlivé údaje o platební kartě.
- Vždy si ověřujte odesílatele a pravost zprávy u instituce, na kterou se zpráva odkazuje (přepravce, pošta, banka, finanční úřad a další instituce).



Krajské ředitelství policie
Jihomoravského kraje

Důležité odkazy:

- www.kybertest.cz
- www.policie.cz
- www.saferinternet.cz
- www.nukib.cz
- www.hoax.cz
- www.csob.cz/BranteSeRozumem

Důležitá telefonní čísla:

Policie ČR ... 158

V dnešním digitálním světě se obětí kyberpodvodů může stát kdokoli.

Internetoví podvodníci se snaží ukrást vaše citlivé údaje, peníze i identitu. Je nezbytné si rizika uvědomovat a chránit se před nimi.



Krajské ředitelství policie
Jihomoravského kraje

KYBERNETICKÉ PODVODY

Buďte obezřetní i v online prostředí.



B | R | N | O