DALÅ Ã• METODY PODVODNÃ•KÅ®

StÅ™eda, 05 kvÄ›ten 2021

KriminalistÃ© Å™eÅ¡Ã- desÃ-tky pÅ™Ã-padÅ¯ se Å¡kodami v Å™Ã¡du milionÅ¯ korun. Policie ÄŒeskÃ© republiky v posledn
zaznamenala vzrÅ¯stajÃ-cÃ- aktivitu skupiny osob, kterÃ© vyuÅ¾Ã-vajÃ- jednu z metod sociÃ¡lnÃ-ho inÅ¾enÃ½rstvÃ- a to
takzvanÃ½ vishing. JednÃ¡ se o princip, kterÃ½ je zaloÅ¾enÃ½ na telefonnÃ-ch hovorech, kdy se volajÃ-cÃ- (podvodnÃ-ci)
zpravidla pÅ™edstavujÃ- jako pracovnÃ-ci banky, kteÅ™Ã- zjistili napadenÃ- vaÅ¡eho bankovnÃ-ho ÃºÄ•tu.

Tito domnÄ›lÃ- pracovnÃ-ci banky svÃ½mi tvrzenÃ-mi vystraÅ¡Ã-
osobu, kterÃ© volajÃ-, pÅ™iÄ•emÅ¾ jejich hlavnÃ-m cÃ-lem je zÃ-skat jejÃ- penÃ-ze. SdÄ›lÃ-,
Å¾e je nutnÃ©, aby finanÄ•nÃ- prostÅ™edky byly z vlastnÃ-ho ÃºÄ•tu okamÅ¾itÄ›
pÅ™evedeny na jinÃ½ ÃºÄ•et s tÃ-m, Å¾e budou po vyÅ™eÅ¡enÃ- celÃ© vÄ›ci nÃ¡slednÄ›
vrÃ¡ceny, coÅ¾ se samozÅ™ejmÄ› nestane. PodvodnÃ-ci tÃ-mto zpÅ¯sobem mohou vylÃ¡kat
i dalÅ¡Ã- citlivÃ© Ãºdaje, kterÃ© nÃ¡slednÄ› zneuÅ¾ijÃ-.

Tento typ podvodnÃ©ho jednÃ¡nÃ- je nebezpeÄ•nÃ½ zejmÃ©na v
tom, Å¾e faleÅ¡nÃ- pracovnÃ-ci bank mohou jiÅ¾ pÅ™ed hovorem nejenom znÃ¡t rÅ¯znÃ©
informace o osobÃ¡ch, kterÃ© kontaktujÃ-, ale hlavnÄ› pÅ™i hovorech uÅ¾Ã-vajÃ- tak
zvanÃ½ spoofing telefonnÃ-ho Ä•Ã-sla,
pÅ™i kterÃ©m dokÃ¡Å¾ou napodobit jakÃ©koliv telefonnÃ- Ä•Ã-slo, vÄ•etnÄ› infolinek bank.
RovnÄ›Å¾ bylo zaznamenÃ¡no nÄ›kolik pÅ™Ã-padÅ¯, pÅ™i kterÃ½ch telefonicky kontaktujÃ-
dalÅ¡Ã- osoby, kterÃ© vystupujÃ- jako policistÃ©, s cÃ-lem ujistit o pravdivosti
tvrzenÃ- ohlednÄ› napadenÃ- bankovnÃ-ho ÃºÄ•tu a nutnosti pÅ™evodu penÄ›z na â€žbezpeÄ•nÃ½â€œ
bankovnÃ- ÃºÄ•et dle pÅ™edchozÃ-ch instrukcÃ- domnÄ›lÃ½ch pracovnÃ-kÅ¯ bank.

ObecnÃ© zÃ¡sady

Nereagujte na podobnÃ© hovory a v Å¾Ã¡dnÃ©m pÅ™Ã-padÄ› nesdÄ›lujte
k VaÅ¡Ã- osobÄ› Å¾Ã¡dnÃ© citlivÃ© Ãºdaje ani bezpeÄ•nostÃ- Ãºdaje z vaÅ¡Ã-
platebnÃ- karty, nebo pÅ™Ã-stupovÃ© Ãºdaje k online bankovnictvÃ-.Nikdy nikomu nesdÄ›lujte a ani nepÅ™eposÃ-lejte
bezpeÄ•nostnÃ- /
autorizaÄ•nÃ- kÃ³d, kterÃ½ VÃ¡m pÅ™iÅ¡el formou SMS zprÃ¡vy.Myslete na to, Å¾e ÃºtoÄ•nÃ-k dokÃ¡Å¾e napodobit jakÃ©
telefonnÃ- Ä•Ã-slo,
odesÃ-latele SMS zprÃ¡vy, ale tÅ™eba i e-mailovou adresu.Nikdy nikomu podezÅ™elÃ©mu neumoÅ¾Åˆujte vzdÃ¡lenÃ½ pÅ
do VaÅ¡eho
poÄ•Ã-taÄ•e.Sledujte a peÄ•livÄ› Ä•tÄ›te informace od VaÅ¡Ã- banky v internetovÃ©m
bankovnictvÃ-.PÅ™i kaÅ¾dÃ©m vstupu do internetovÃ©ho bankovnictvÃ- kontrolujte, zda
odpovÃ-dÃ¡ domÃ©na pÅ™ihlaÅ¡ovacÃ- strÃ¡nky. Toto platÃ- vÅ¾dy, kdyÅ¾ nÄ›kam zadÃ¡vÃ¡te
svÃ© osobnÃ- nebo pÅ™ihlaÅ¡ovacÃ- Ãºdaje.Aktualizovat software, antivirovÃ½ program, firewall.BuÄ•te neustÃ¡le ostraÅ¾
protoÅ¾e i vy se mÅ¯Å¾ete stÃ¡t cÃ-lem podobnÃ©ho
podvodnÃ©ho jednÃ¡nÃ-.BÄ›hem, nebo po takovÃ©mto podezÅ™elÃ©m hovoru, si zaznamenejte Ãºdaje,
kterÃ© VÃ¡m ÃºtoÄ•nÃ-k sdÄ›lil (jmÃ©na, e-mailovÃ© adresy, Ä•Ã-sla ÃºÄ•tÅ¯, odkazy na
webovÃ© strÃ¡nky, apod.)

Nereagujte

na telefonnÃ- hovory, SMS zprÃ¡vy,
e-maily, kde se vÃ¡s nÄ›kdo pokouÅ¡Ã- vmanipulovat do situace, Å¾e jsou vaÅ¡e finanÄ•nÃ- prostÅ™edky v ohroÅ¾enÃ- a vy musÃ-te udÄ›lat dalÅ¡Ã- kroky pro jejich zÃ¡chranu. Kdyby byly vaÅ¡e penÃ-ze v ohroÅ¾enÃ-, tak banka sama zareaguje a uÄ•inÃ- dalÅ¡Ã- opatÅ™enÃ-. V pÅ™Ã-padÄ› pochybnostÃ- vÅ¾dy kontaktujte svou banku. Pokud vÃ¡s shora naznaÄ•enÃ½m zpÅ¯sobem jiÅ¾ nÄ›kdo kontaktoval, nevÃ¡hejte se rovnÄ›Å¾ obrÃ¡tit na tÃ-sÅˆovou linku Policie ÄŒeskÃ© republiky na Ä•Ã-sle 158 a celou zÃ¡leÅ¾itost oznamte.

Zdroj: plk. OndÅ™ej MoravÄ•Ã-k

tiskovÃ½ mluvÄ•Ã-, PolicejnÃ- prezidium ÄŒR