

PHISHING ZAMĚŘENÝ NA UŽIVATELE PAYPAL OPĚT PROCHÁZÍ ČESKÝMI INTERNETOVÝMI SLUŽBAMI. NENECHTE SE NACHYTAT!

Kamil KOPECKÝ

Možná i vám přišel v těchto dnech e-mail odeslaný z “PayPal Support” s předmětem “Neznámé zařízení se pokouší získat přístup k vašemu účtu PayPal”. Zpráva, která se zdá být velmi důležitá, vás informuje o tom, že se na váš účet pokouší získat přístup neznámé zařízení z Iránu, váš účet byl proto automaticky zablokován a vy se na něj musíte co nejdříve přihlásit a potvrdit svou identitu. Nenechte se však nachytat, jde o klasický phishingový podvod.

PS

PayPal Support apps-service@store1secure.com

Komu: kopecky@seznam.cz

✉ Neznámé zařízení se pokouší získat přístup k vašemu účtu PayPal



Bezpečnostní Výstraha

Ahoj,

Váš účet byl automaticky zablokován kvůli bezpečnostním opatřením, přihlaste se k účtu Paypal co nejdříve!

• Co se děje?

Neznámé zařízení se pokouší získat přístup k vašemu účtu PayPal:

Date : 17/12/2019

Time : 09.26 AM

Location : Iran (Tahran)

IP address : 2.147.250.255

Agent : Mozilla/5.1 (Windows NT 6.3; Win32; x32; rv:71.0) Firefox/71.1

• Co bych měl dělat?

Přihlaste se ke svému účtu co nejdříve, a potvrďte svou totožnost,

Klikněte na tlačítko níže a postupujte podle pokynů. Proces bude trvat jen několik minut,

S pozdravem, podpora PayPal

Ověřte

(Phishingový e-mail)

Charakteristické znaky phishingu jsou patrný hned na první pohled:

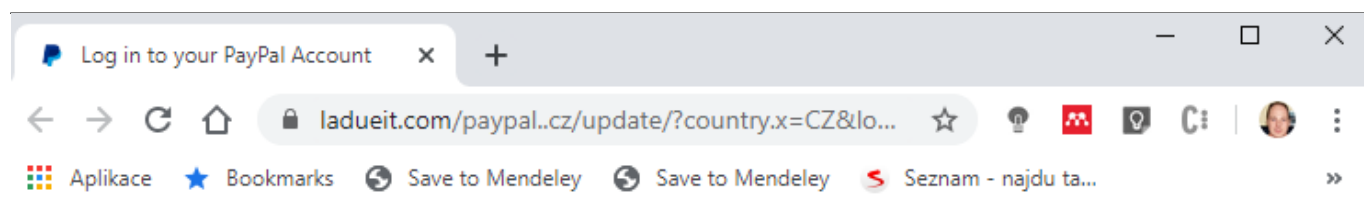
1. **E-mail není odeslán z domény paypal.com**, ale z apps-service@store1secure.com.

2. **Přestože je e-mail psán obстоjnou češtinou, obsahuje četné pravopisné chyby**, např. Bezpečnostní Výstraha (chybné B a velké V).

3. Odkaz v e-mailu s názvem Ověřte směřuje na podvodný web:

(<https://www.ladueit.com/paypal..cz/update/>), který dosud obsahuje napodobeninu přihlašovacího formuláře PayPalu. Spojení s webem je sice zabezpečeno (SSH, symbol zámečku), to však neznamená, že samotný web není podvodný!

3. Pokud byste se pokusili vyplnit přihlašovací údaje a přihlásit se (Samozeřejmě to nedělejte s použitím skutečných údajů, pro účely testování využijte údaje fiktivní! Podvodný web netestuje ani minimální standardy třeba pro e-mailovou adresu apod.), **dostanete se do “[fiktivního prostředí zablokovaného účtu](#)”**, které vás nutí poskytnout velké množství osobních a citlivých údajů. Pokud byste se pak snažili prostředí opustit pomocí běžného odhlášení, stránka vám bude tvrdit, že pokud se odhlásíte, bude váš účet trvale uzamčen.



(Napodobenina přihlašovacího formuláře)

Cílem phishingu je vylákat vaše osobní a citlivé údaje (např. přihlašovací údaje, informace o kreditních a debetních kartách, vaše hesla apod.) a zneužít je. Nejjednodušší obranou je takové e-maily zařadit do spamu.

Pro E-Bezpečí
Kamil Kopecký