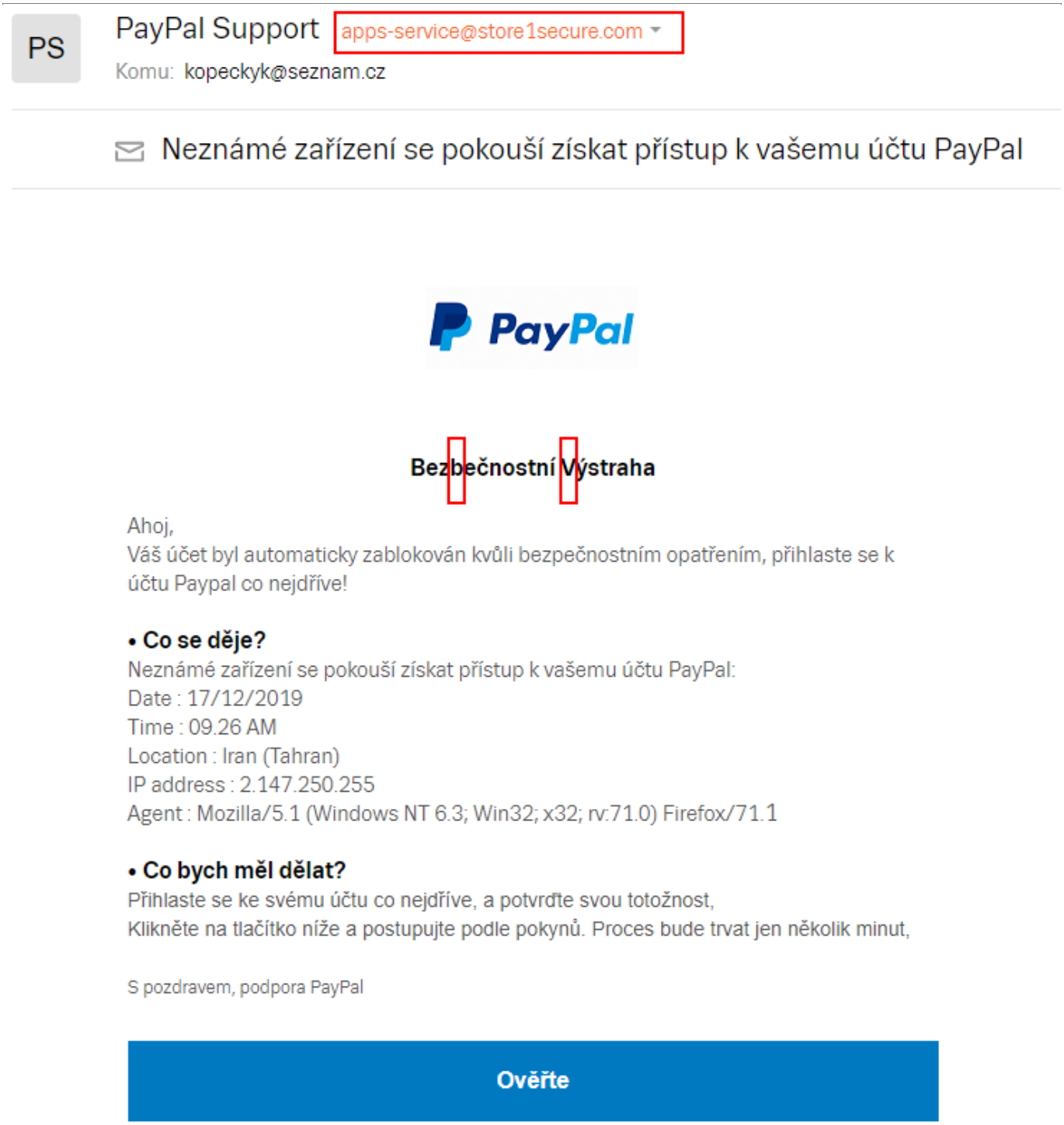
E-Bezpečí 2019, 4(2): Page 109-110. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1719

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.



(Phishingový e-mail)

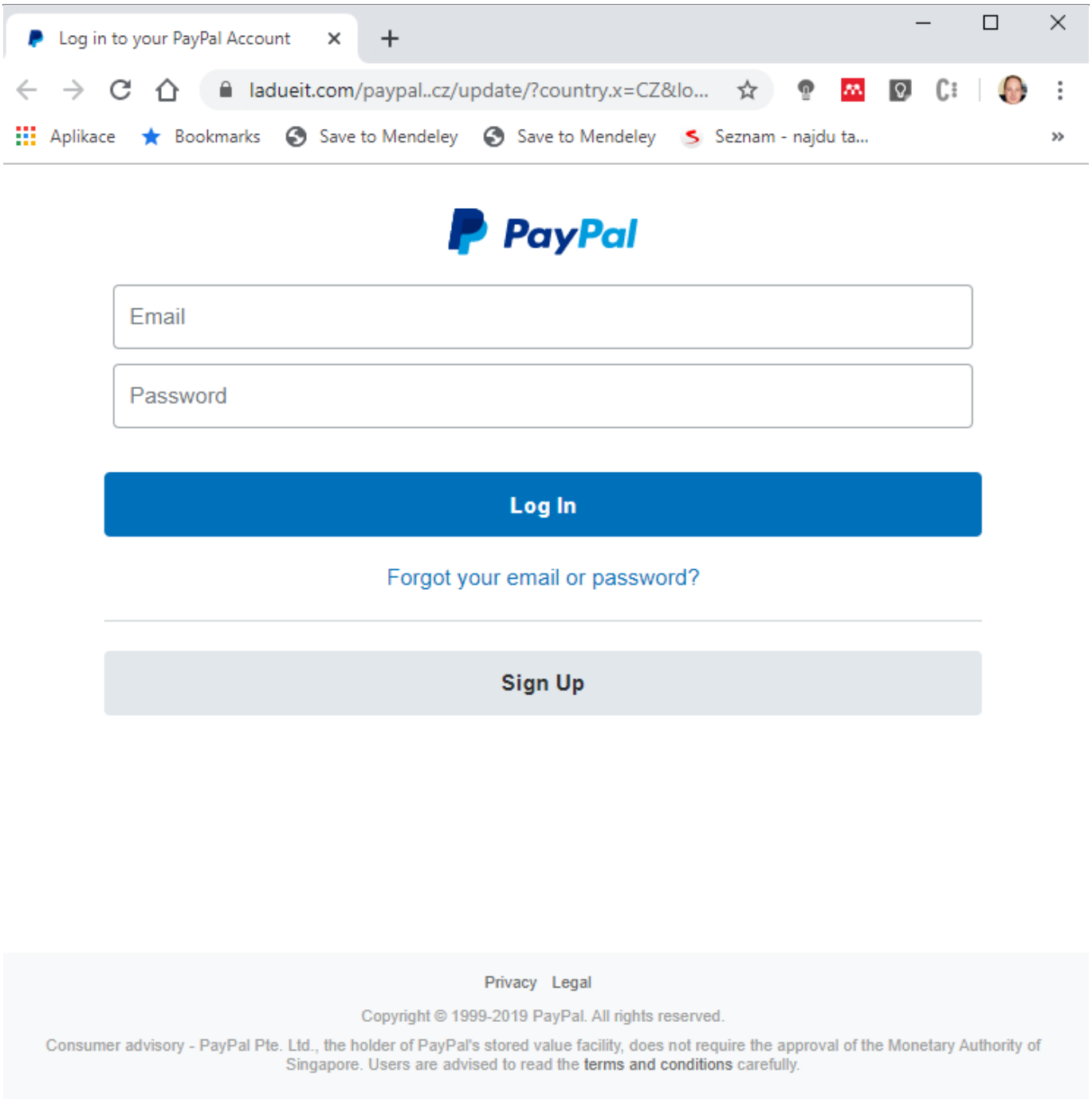
Charakteristické znaky phishingu jsou patrny hned na první pohled:

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

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

3. **Odkaz v e-mailu s názvem Ověřte směřuje na podvodný web**: https://n9.cl/msr7 (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** (Samozřejmě 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