Manažer kybernetické bezpečnosti resortu MV

Č. j. MV- 1877-10/OKB-2020

Praha 16. dubna 2020

Informace Manažera kybernetické bezpečnosti

Varování před podvodnými e-maily

Manažer kybernetické bezpečnosti resortu MV varuje uživatele kybernetického prostoru resortu MV **před trvající kampaní různých podvodných e-mailů**, které jsou doručovány uživatelům resortu MV. Útočníci využívají e-maily s prvky sociálního inženýrství. Úspěšná kompromitace počítače či účtu jednoho uživatele může vést k napadení celé počítačové sítě resortu MV.

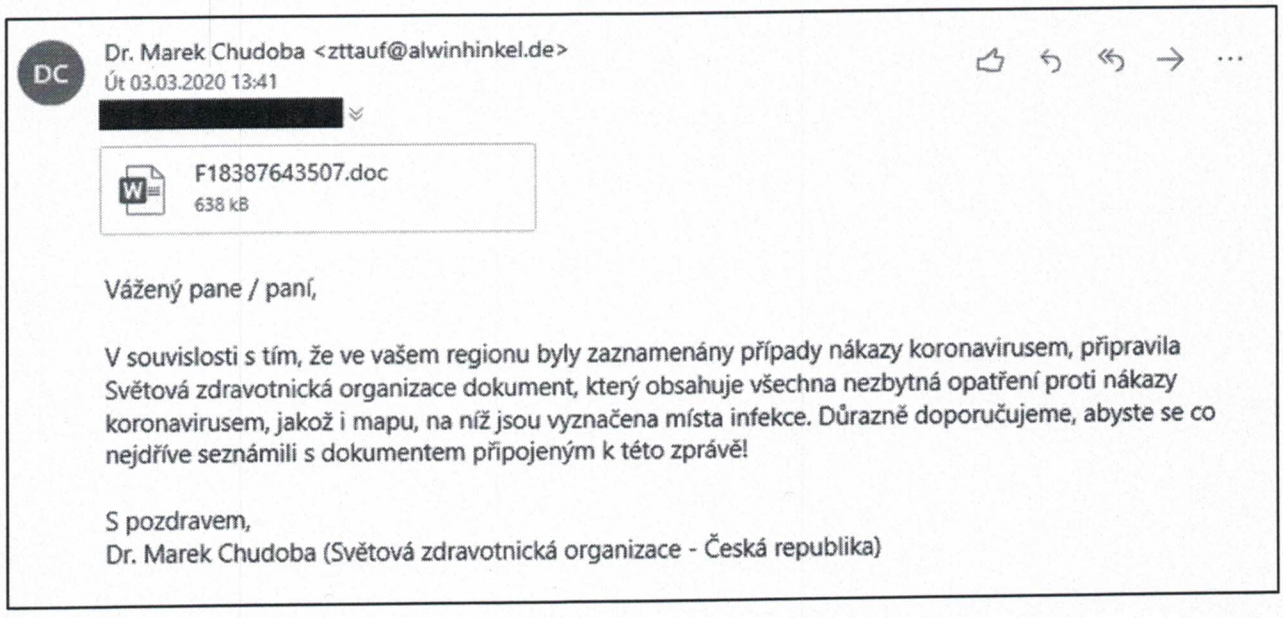
Obsah e-mailu se snaží nejčastěji přimět uživatele k otevření přílohy nebo hypertextového odkazu. V podvodných e-mailech se nejčastěji opakuje následující tématika:

- informace o koronaviru (Covid-19),
- nevyzvednutý balíček u dopravní společnosti,
- nezaplacené faktury nebo daně,
- potřeba ověření účtu z důvodu zaplnění kapacity poštovní schránky.

Otevření souboru v příloze nebo jeho stažení z přiloženého odkazu může vést k infikování pracovní stanice škodlivým kódem. V případě podvodných e-mailů typu phishing může dojít k odcizení přihlašovacích údajů uživatele a k jejich následnému zneužití.

Útočníci posílají e-maily z různých adres a není výjimkou i podvržená adresa odesílatele. Vyskytují se i podvodné e-maily s důvěryhodným zpracováním psané velmi dobrou češtinou.

Náhledy podvodných e-mailových zpráv



DC

Dr. Marek Chudoba <zttauf@alwinhinkel.de>
Út 03.03.2020 13:41
[redacted]

F18387643507.doc
638 kB

Vážený pane / paní,

V souvislosti s tím, že ve vašem regionu byly zaznamenány případy nákazy koronavirusem, připravila Světová zdravotnická organizace dokument, který obsahuje všechna nezbytná opatření proti nákazy koronavirusem, jakož i mapu, na níž jsou vyznačena místa infekce. Důrazně doporučujeme, abyste se co nejdříve seznámili s dokumentem připojeným k této zprávě!

S pozdravem,
Dr. Marek Chudoba (Světová zdravotnická organizace - Česká republika)

TNT Express delivery Consignment Notification

TE TNT EXPRESS CONSIGNMENT <diamond@tnt.com>
Komu

Kliknutím sem stáhnete obrázky. Za účelem ochrany vašeho soukromí zabránila aplikace Outlook stažení některých obrázků v této zprávě.

TNT EXPRESS CONSIGNMENT.ace
410 KB

Dear Customer,

A shipment has been arranged for you via TNT.

The shipment is scheduled for delivery MARCH 31th, 2020 and has **TNT consignment number: 213596003.**

SHIPMENT DETAILS OVERVIEW: (**View Enclosed**)

Pieces : 1
Weight : 0.5 KG
Shipment reference : Invoice # 10623-24
Description : document

Download Attachment for invoice and full shipment details.

faktura_13205461.doc
657 KB

From: Anna Pivonkova <Anneka.Prately83580@gmx.com>
Sent: Friday, January 10, 2020 12:28 PM
To: hr-berlin@parexel.com
Subject: Připomenutí platby daně z příjmu podniku

Dobrý den,
Po prozkoumání vaší zprávy jsme zjistili, že jste za rok 2019 nezaplatili daň z příjmu právnických osob. Číslo vašeho případu je #090/59287. K vyřešení této pohledávky je třeba zaplatit daň + pokutu ve výši 11 780,00 Kč nejpozději do 15/02/2020. Přikládáme dokument s podrobnějšími informacemi o tomto případě pro vaši potřebu. Pokud jste již zaplatili pokutu za tuto pohledávku, okamžitě nám to nahlaste, abychom to mohli potvrdit.

S úctou, Anna Pivoňková

faktura_8603073.doc
654 KB

Od: ortanova@porte.italiaunica.it
Odesláno: 10. ledna 2020 13:26
Komu: bohuslav.zubek@mvcr.cz
Předmět: Nemohli jsme doručit váš balíček.

Dobrý den, Váš balíček dorazil do našeho skladu 9. ledna 2020 roku v 13:10 ráno. Číslo sledování zásilky-CZ7654[redacted] Náš kurýr bohužel nemohl doručit zásilku na vaši adresu kvůli nesprávným nebo neúplným informacím v adrese. Zdá se, že v celním prohlášení došlo k chybě. Informovali jsme odesílatele a on nám předal vaši e-mailovou adresu, abychom mohli tento problém vyřešit co nejdříve. Abychom mohli doručit váš balíček, musíte potvrdit adresu. Za tímto účelem si stáhněte dokument připojený k tomuto dopisu, vyplňte ho a pošlete nám ho. S úctou, Romana Švecová

[CMS2-SUSPECTED SPAM]Váš balíček byl doručen

ČP bol.poner@nc6jan20limer.co za uživatele Česká Pošta <contact@hellonoreply.com>
Komu

Odpovědět | Odpo

Pokud se vyskytly potíže se zobrazením této zprávy, kliknutím sem ji zobrazíte ve webovém prohlížeči.
Kliknutím sem stáhnete obrázky. Za účelem ochrany vašeho soukromí zabránila aplikace Outlook stažení některých obrázků v této zprávě.

Váš balíček byl doručen

Oznámení o doručení

Nyní si svůj balíček můžete vyzvednout na poštovním úřadu

Balíček č.: TX43121XN3122

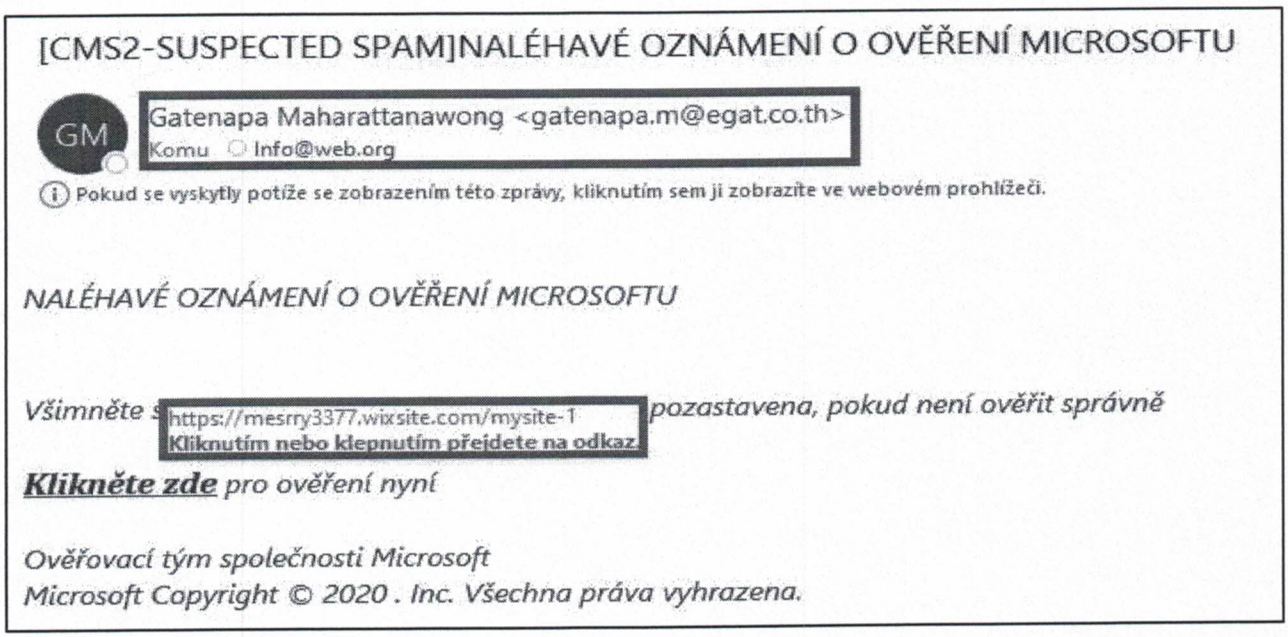
Stav doručování: Doručeno

Při v[redacted]zít svůj občanský průkaz a sledovací číslo Vaší

http://balu.nc6jan20limer.co/mail/countlink.aspx?sid=72670665158&lid=45844089
Kliknutím nebo klepnutím přejdete na odkaz.

Najit poštovní úřad

Toto je automaticky vygenerovaná zpráva týkající se Vaší zásilky **#TX43121XN3122,** neodpovídejte na ni prosím.



[CMS2-SUSPECTED SPAM]NALÉHAVÉ OZNÁMENÍ O OVĚŘENÍ MICROSOFTU

GM Gatenapa Maharattanawong <gatenapa.m@egat.co.th>
Komu Info@web.org

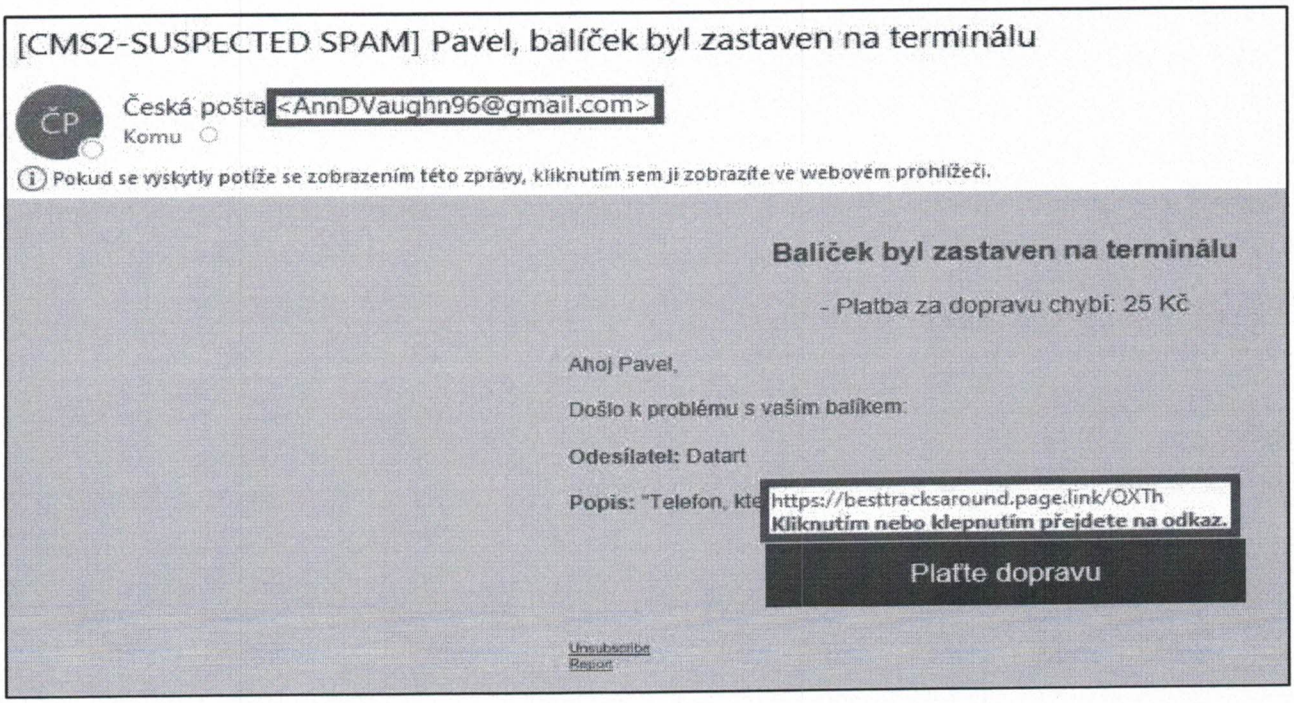
Pokud se vyskytly potíže se zobrazením této zprávy, kliknutím sem ji zobrazíte ve webovém prohlížeči.

NALÉHAVÉ OZNÁMENÍ O OVĚŘENÍ MICROSOFTU

Všimněte s https://mesrry3377.wixsite.com/mysite-1 Kliknutím nebo klepnutím přejdete na odkaz. *pozastavena, pokud není ověřit správně*

Klikněte zde *pro ověření nyní*

Ověřovací tým společnosti Microsoft
Microsoft Copyright © 2020 . Inc. Všechna práva vyhrazena.



[CMS2-SUSPECTED SPAM] Pavel, balíček byl zastaven na terminálu

ČP Česká pošta <AnnDVaughn96@gmail.com>
Komu

Pokud se vyskytly potíže se zobrazením této zprávy, kliknutím sem ji zobrazíte ve webovém prohlížeči.

Balíček byl zastaven na terminálu

- Platba za dopravu chybí: 25 Kč

Ahoj Pavel,

Došlo k problému s vaším balíkem:

Odesílatel: Datart

Popis: "Telefon, kte https://besttracksaround.page.link/QXTh Kliknutím nebo klepnutím přejdete na odkaz.

Plaťte dopravu

Unsubscribe
Report

Obecná doporučení pro všechny uživatele e-mailových služeb

- Věnovat zvýšenou pozornost přijímaným podezřelým e-mailovým zprávám od nedůvěryhodných kontaktů, na podezřelé e-maily nereagovat, neotevírat soubory v příloze a neklikat na odkazy.
- Kontrolovat e-mailovou adresu odesílatele.
- Být na pozoru v případě urgentních nebo neobvyklých požadavků.
- Nebezpečné jsou dokumenty kancelářské sady Office, které vyžadují povolení spuštění maker. Nepovolovat makra u dokumentů z nedůvěryhodného zdroje.
- Obzvláště nebezpečné jsou přílohy typu .exe, .vb, .vbs, .bat, .iso, .dll, .js, .jar apod.
- Omezit sdílení informací o zaměstnání na sociálních sítích.

V případě nejistoty nebo podezření o škodlivosti e-mailu kontaktujte Dohledové centrum eGovernmentu – DCeGOV. Neprodleně kontaktujte pracoviště i v případě, že jste otevřeli přílohu podezřelého e-mailu, anebo Vám mohly být odcizeny přihlašovací údaje.

Kontakty na dohledové centrum:

Telefon: 974 801 131

E-mail: dohled@mvcr.cz

Ing. Bohuslav Zůbek, CMICT
Manažer kybernetické bezpečnosti resortu MV

Ing. Bohuslav Zůbek

Digitally signed by Ing. Bohuslav Zůbek
Date: 2020.04.16 14:38:09 +02'00'