FILL:
PICTURE
FROM FILE

Program de conștientizare al utilizatorilor cu privire la atacurile cibernetice

confident
decisions

mercuryresearch

Definiții

Ce este un program malware?

„Malware” se referă la orice tip de software conceput special pentru a afecta un computer. Programele malware pot sustrage informații delicate de pe computer (**phishing**), pot încetini treptat funcționarea acestuia și pot chiar să trimită e-mailuri false din contul dvs., fără să aveți cunoștință de acest lucru. Iată câteva tipuri de malware frecvent întâlnite despre care probabil ați auzit:

- virus: un program de computer care se poate copia singur și poate infecta un computer;
- vierme informatic: un program de computer rău intenționat care trimite copii ale sale pe alte computere prin intermediul unei rețele;
- spyware: programe malware care culeg informații de la utilizatori fără ca aceștia să știe;
- adware: program software care redă, afișează sau descarcă automat reclame pe un computer;
- cal troian: un program distructiv care pretinde a fi o aplicație utilă, dar, după ce este instalat, afectează computerul sau fură informații;
- ransomware: software care, după ce se instalează pe dispozitivul victimei (calculator, smartphone), criptează datele victimei ținându-le „ostatice” sau șantajează victima, pe care o amenință că îi va publica datele dacă aceasta nu plătește o „răscumpărare” ransom.

Definiții

Ce este phishing-ul?

Atacurile de tip phishing reprezintă o crimă cibernetică, în care utilizatoriilor le sunt sustrase datele personale, cum ar fi detaliile cardurilor bancare și datele de logare în general prin diverse metode.

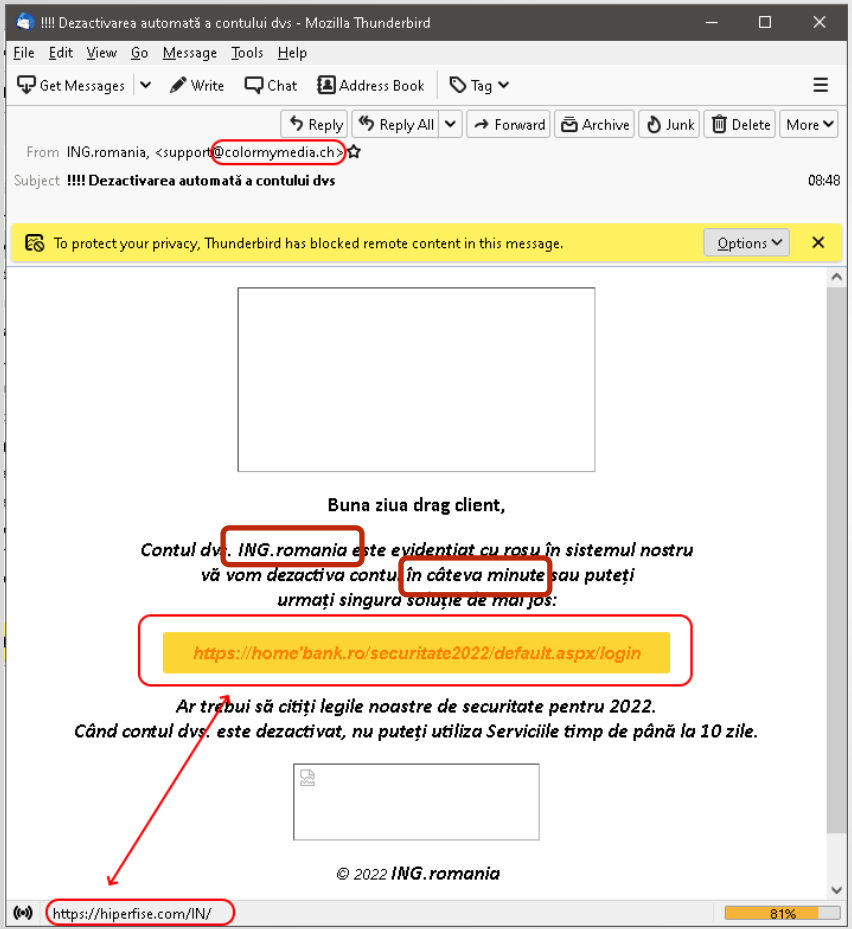
Uneori, phishingul se întâmplă prin descărcarea unui fișier infectat cu malware, primit ori pe e-mail, ori descărcat de pe un site sau alte metode de transfer de fișiere.

Alteori, phishingul se întâmplă prin primirea unui link care imită pagină web a unei entități reale, și care, invocând o anumită urgență, cere introducerea datelor de logare, a datelor bancare, etc.

Linkurile care facilitează phishingul sunt de obicei transmise prin:

- SMS
- E-Mail
- Ferestre pop-up
- Aplicații de mesagerie (FB Messenger, Whatsapp, Telegram, Signal, Viber etc)

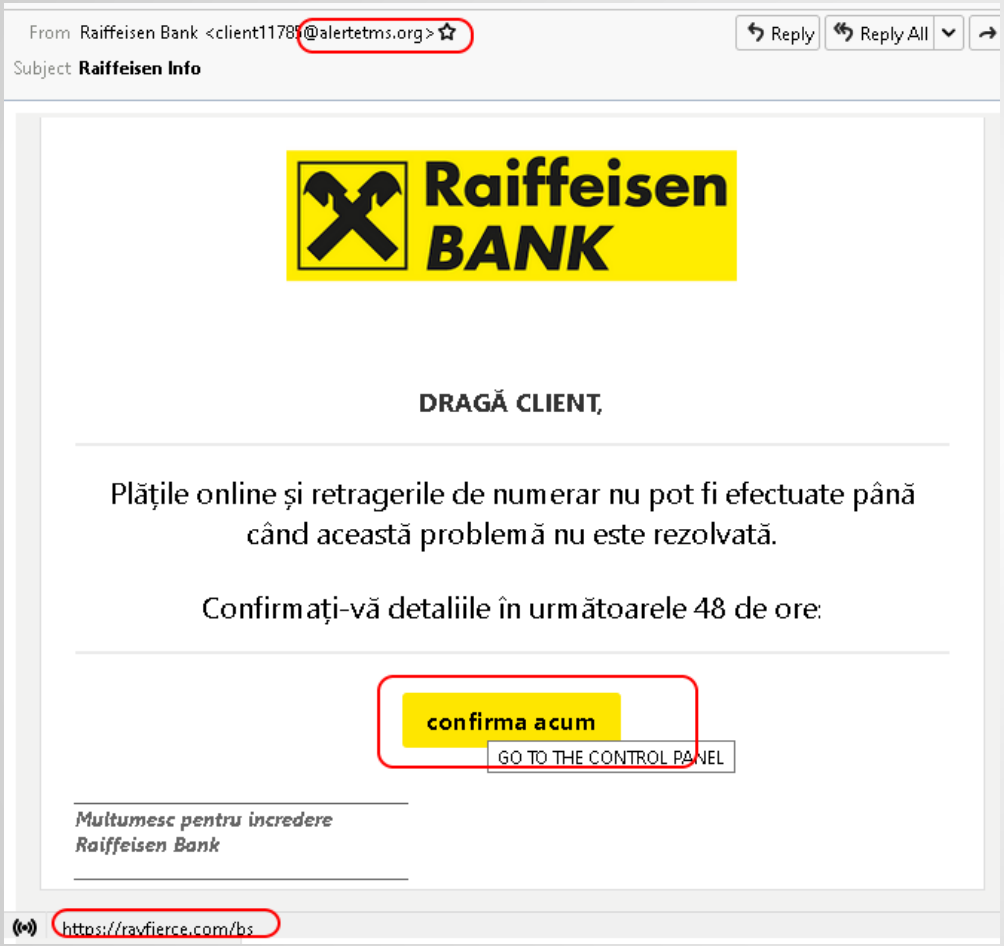
Email



Băncile nu vă vor cere niciodată pe e-mail să vă logați în contul vostru. În imaginea alăturată avem un exemplu de mesaj malițios. Indiciile falsității mailului sunt:

- Numele afișat: *ING.romania*
- Domeniul adresei de e-mail: *colormymedia.ch*
- Adresa din spatele butonului spre care vă trimite mesajul conținut, vizibilă prin plasarea cursorului (*fără accesare prin click*) asupra butonului, nu are nicio treabă cu denumrea reala a domeniului ING/Homebank. Atenție! E posibil ca în loc de buton să aibă scris un link semi-credibil, exact ca în această poză, dar care să aibă în spate un alt link la care sunteți trimiși dând click, link vizibil prin plasarea cursorului deasupra celui vizibil (*fără accesare prin click*).
- Exprimare nenaturală, de multe ori tradusă cu Google Translate.

Email



Aici aveți un al doilea exemplu de înselătorie în care este folosită identitatea unei entități bancare.
Ce se poate întâmpla dacă accesați linkul:

- Furt de identitate
  - Extragere/golire bani din cont
  - Plăți către conturi „greșite”
  - Transmitere de malware la contactele din agenda

Email

Obiectivul principal pentru propagarea unor astfel de mesaje este să provoace curiozitatea utilizatorului pentru a intra în conversație pe aplicația WhatsApp cu cei care se află în spatele numărului afișat.
De obicei infractorii cibernetici se folosesc de această metodă pentru a atrage potențiale victime să ofere date sensibile, sub pretextul nevoii deschiderii unor conturi pentru participarea într-un sistem piramidal de câștig bazat pe invitarea unor noi 'clienți', la care adaugă ulterior o componentă de investiții în criptomonedă. Astfel, pe termen mediu există pericolul ca atacatorii să extragă nu doar date personale, ci și date financiar-bancare de la utilizatori.

Email

From Universitatea din București <magdalena.platis@unibuc.ro>

Reply | Forward | Archive | Junk | Delete | More

Subject **Cerere de ofertă (Universitatea din București)**

To undisclosed-recipients:;

BUCUREȘTI
VIRTUTE ET SAPIENTIA

Salutări de la Universitatea din București

Am primit comentarii bune despre marea dvs. companie: Noi, Universitatea din București, dorim să vă invităm să participați la solicitarea bugetului școlii noastre pentru 2021 (atașat).
Vă rugăm să ne dați cel mai bun preț. Asigurați-vă că oferta dvs. ajunge înainte de 18 iunie 2021.
Găsiți un atașament, vă rugăm să ne informați imediat dacă aveți nevoie de mai multe informații..

Mulțumesc și salutări.

prorector profesorul Magdalena Iordache Platis
E-Mail: magdalena.platis@unibuc.ro

UNIVERSITATEA DIN BUCUREȘTI
Abordare: Șoseaua Panduri 90, București 050663, Romania
Telefon: +40213077300
E-mail: magdalena.platis@unibuc.ro
Site web: https://unibuc.ro

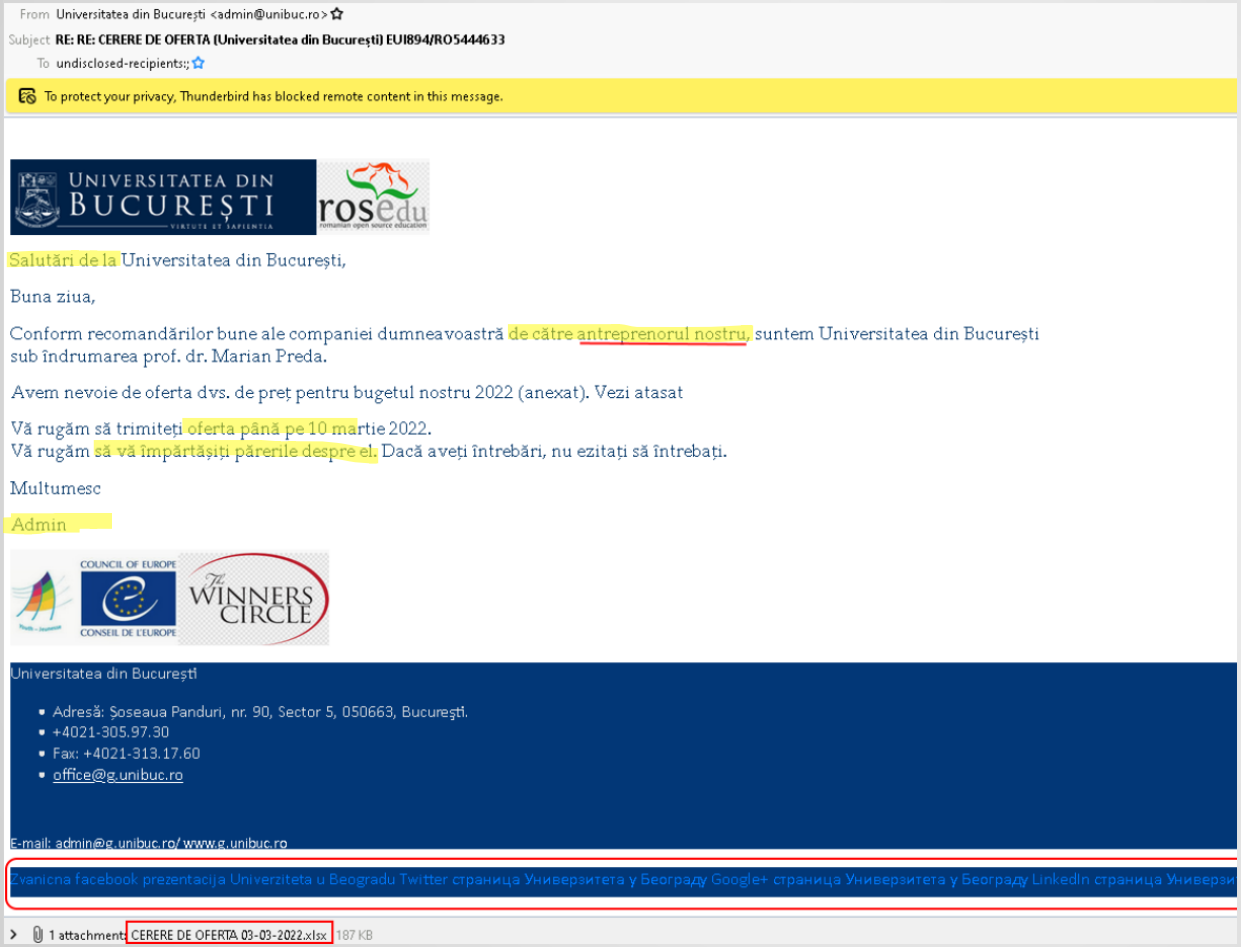
Take care of Earth! Please do not print this email unless absolutely necessary!
This message (including all attachments) contains confidential information intended for an individual and a specific purpose, and is protected by law. If you are not the intended recipient, you must delete this message and inform you that any disclosure, copying or distribution of this message, or any action in this regard, is strictly prohibited.

1 attachment: Cerere de ofertă 14-06-2021-pdf.zip 121 KB — Save

Cerere de ofertă 14-06-2021-pdf.zip 121 KB

De data aceasta avem o adresă de email care cel mai probabil a fost hackuită. După un search pe Google veți afla ca această doamnă profesor este reală, dar cu o altă înfățișare.
În afară de aceasta, alte elemente care arată că acesta este un mesaj spam e textul scris greșit/nenatural, cât și atașamentul trimis ca un așa-zis PDF arhivat în format ZIP.

Email


From Universitatea din București <admin@unibuc.ro>

Subject RE: RE: CERERE DE OFERTA (Universitatea din București) EUI894/RO5444633

To undisclosed-recipients:;

To protect your privacy, Thunderbird has blocked remote content in this message.

UNIVERSITATEA DIN BUCUREȘTI

rosedu

Salutări de la Universitatea din București,

Buna ziua,

Conform recomandărilor bune ale companiei dumneavoastră de către antreprenorul nostru, suntem Universitatea din București sub îndrumarea prof. dr. Marian Preda.

Avem nevoie de oferta dvs. de preț pentru bugetul nostru 2022 (anexat). Vezi atasat

Vă rugăm să trimiteți oferta până pe 10 martie 2022.
Vă rugăm să vă împărtășiți părerile despre el. Dacă aveți întrebări, nu ezitați să întrebați.

Multumesc

Admin

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

The WINNERS CIRCLE

Universitatea din București

- Adresă: Șoseaua Panduri, nr. 90, Sector 5, 050663, București.
- +4021-305.97.30
- Fax: +4021-313.17.60
- office@g.unibuc.ro

E-mail: admin@g.unibuc.ro/ www.g.unibuc.ro

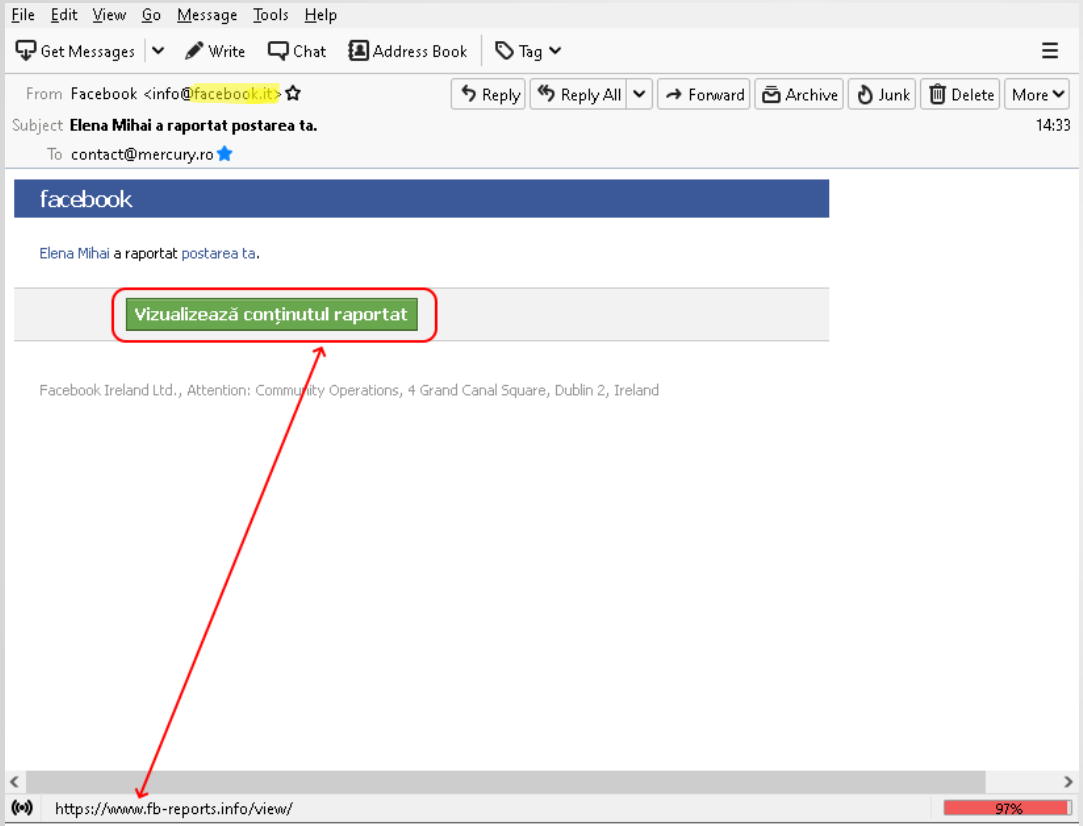
Zvanicna facebook prezentacija Univerziteta u Beogradu Twitter страница Универзитета у Београду Google+ страница Универзитета у Београду LinkedIn страница Универзи

1 attachment: CERERE DE OFERTA 03-03-2022.xlsx 187 KB

Spamul de la Universitatea din București revine, de data aceasta fără furtul de identitate, ci cu o adresă de „admin”.
Sunt prezente elementele:

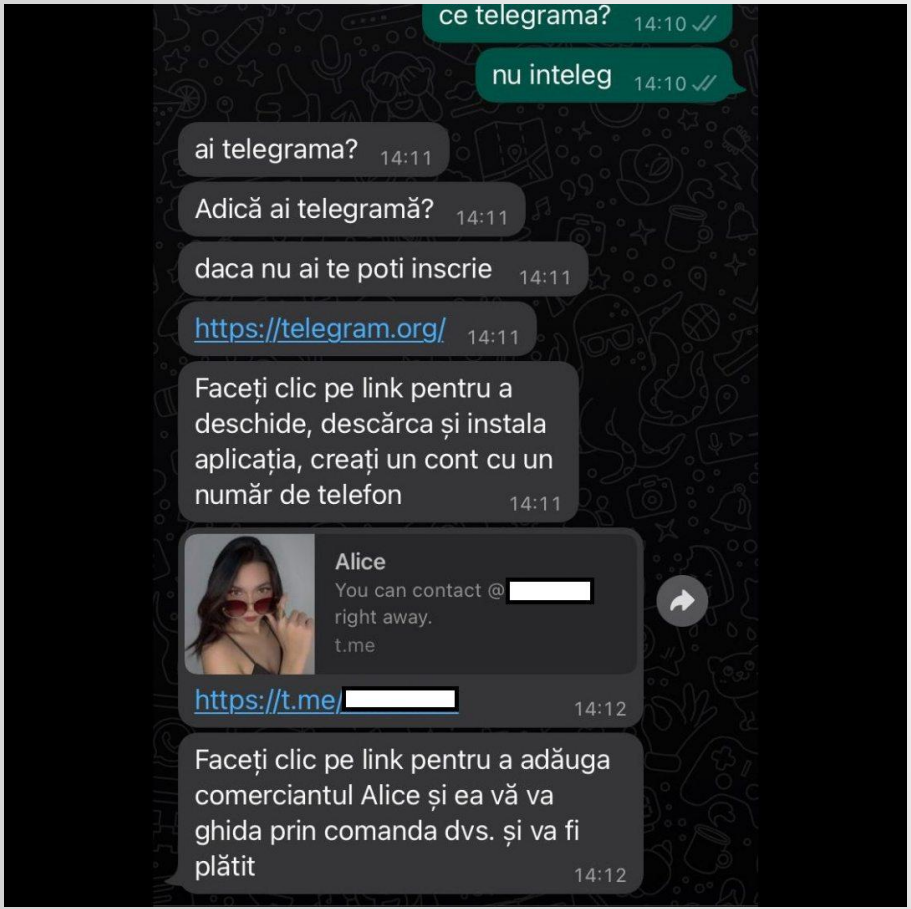
- Text scris nenatural, probabil tradus cu Google Translate
- Se semnează admin
- Text în subsol în altă limbă, unde confundă București cu Belgrad
- Fișier .xlsx în atașament, fișierele cu această extensie putând fi folosite pentru a răspândi malware sau pentru solicitarea de introducere a datelor de autentificare pentru contul Office365 si furtul acestora.

Email



Acesta este un exemplu tipic de phishing, în care pagina facebook.com a fost copiata pe un alt domeniu (fb-reports.info) unde ți se spune că trebuie să te loghezi cu contul și parola ta pentru a vedea cine ți-a raportat postarea.
După ce ai introdus datele tale, acestea ajung la cel care a lansat campania de phishing.
Pentru credibilitate, folosesc un domeniu dintr-o altă țară facebook.it, domeniu care nu apartine Facebook.

Mesagerie



Nu accesati mesaje primite de la numere sau persoane necunoscute care vă invită să folosiți alte aplicații, să accesați imagini/conținut video sau să accesați un link.

De cele mai multe ori vă puteți alege cu malware, sau cu datele personale compromise.

SMS


+31 6 53 92 20 04
Nu accesați link-uri primite prin SMS, din surse necunoscute!
Text Message
Today 10:23
Pachetul dvs. este pe drum, urmati-l aici: https://news.stepphase.com/3gpb0t.php?8n1s1o4aebq3

Info

- Elementele de identificare de pe slide-urile anterioare sunt comune pentru multe tentative de phishing, șantaj sau de răspândire malware.
- Identitățile asumate de către persoanele rău intenționate sunt, în multe cazuri, diverse companii mari/companii de hosting sau trimit mesaje în numele unor celebrități (ex. DHL, Posta Romana, Cpanel, Fan Courier, Elon Musk etc.)
- Pe slide-urile următoare sunt câteva exemple suplimentare.

* De unde ne putem informa:
https://dnsc.ro/
https://www.facebook.com/DNSC.RO
https://www.facebook.com/groups/certro

Fwd:Noua ta actualizare la inceputul lui 2022. - N'6953991803 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Reply All | Reply | Forward | Tag

From BRD <terry@islandtelecom.com>

Subject **Fwd:Noua ta actualizare la inceputul lui 2022. - N'6953991803**

Reply | Forward | Archive | Junk | Delete | More

1:30 PM

To protect your privacy, Thunderbird has blocked remote content in this message. Options

Dragă client,

Sistemul nostru recunoaște că nu ați activat încă noul serviciu de securitate **YOU BRD**, astfel încât să vă puteți verifica cu ușurință contul BRD:

Codul SMS va fi șters la începutul anului 2022 din cauza securității și a timpilor lungi de răspuns pentru tranzacțiile online. Utilizați noua securitate gratuită "**YOU BRD**" pentru a vă gestiona achizițiile directe online fără a pierde timpul.

Acum urmați instrucțiunile pentru a activa "YOU BRD".

1. Identificați-vă cu informațiile dvs. bancare.
2. Confirmați ultimele 4 cifre ale cardului dvs. bancar.
3. Introduceți codul SMS primit la numărul dvs. de telefon.

Toate cele bune
Echipa de service BRD

Detaliu!

Acest serviciu de securitate inovator și sigur se bazează pe un sistem de autentificare care este

https://t.co/YE9ICTHDe0

93%

From HostSevr <info@digestfile.com>

Subject **Your e-mail verification code.**

To contact@mercury.ro

Reply | Reply All | Forward

Hi contact,

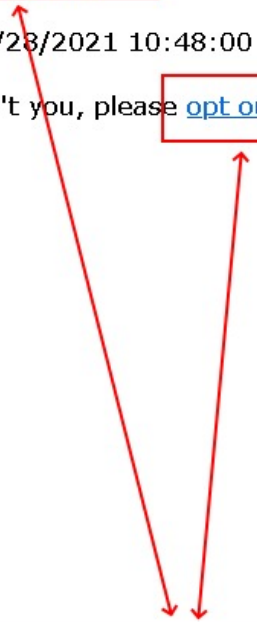
Your verification code to verify contact@mercury.ro
is ceexay36.

Device : Check

Where: IP Location

When: 11/28/2021 10:48:00 p.m.

If this wasn't you, please opt out from this email.
Thanks.



http://aybdqws.eviosys.biz/#Y29udGFjdEBtZXJjdXJ5LnJv

AWB 23410028317313 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

From FAN Courier <inbo[illegible]@km.hr.court.gov.ua>

Reply | Forward | Archive | Junk | Delete | More

Subject **AWB 23410028317313** 06:07

To undisclosed-recipients:;

FAN Courier has asked to be notified when you read this message. Send Receipt | Ignore Request

Stimate client,

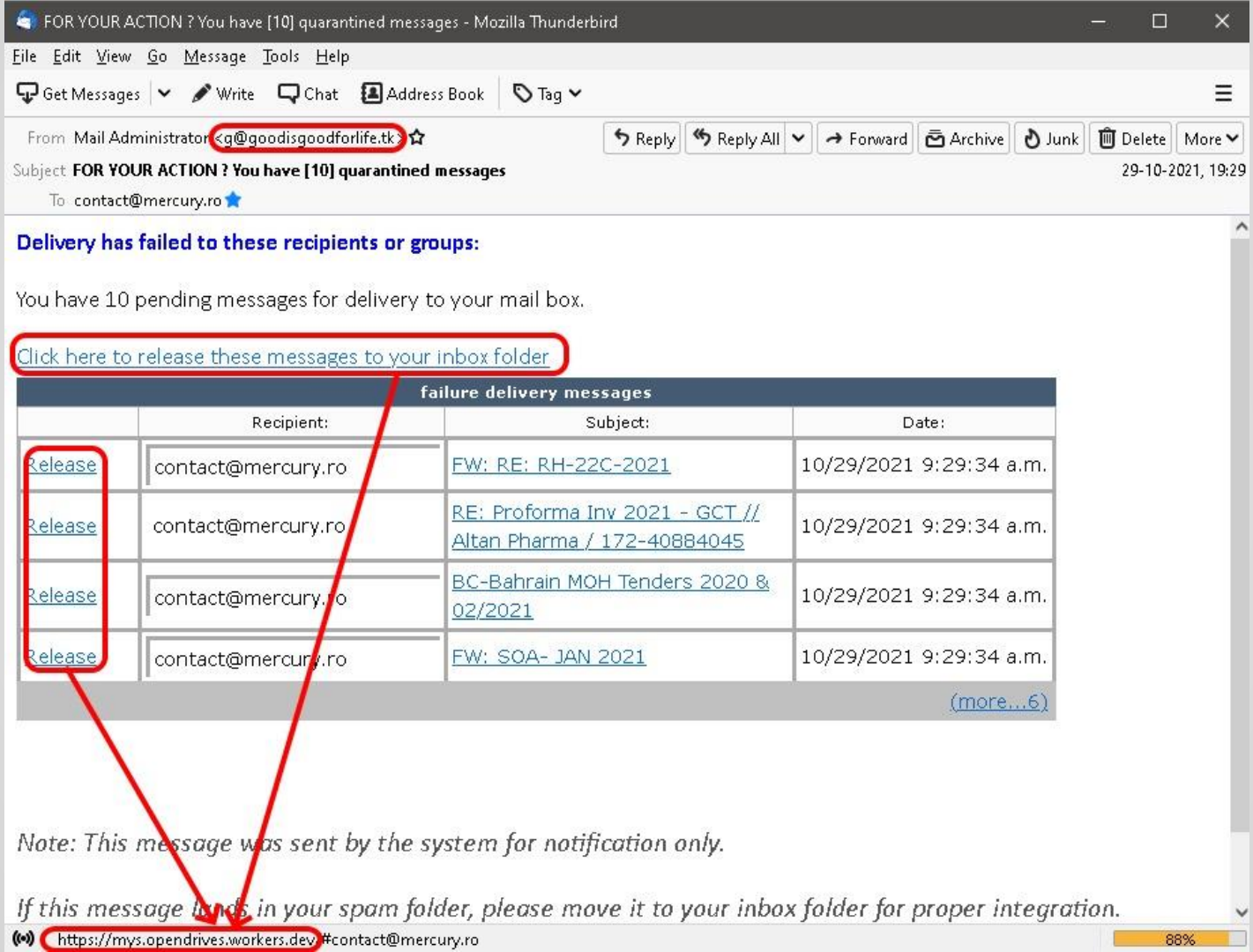
Vă informăm că livrarea cu numărul AWB 23410028317313 a fost livrată.

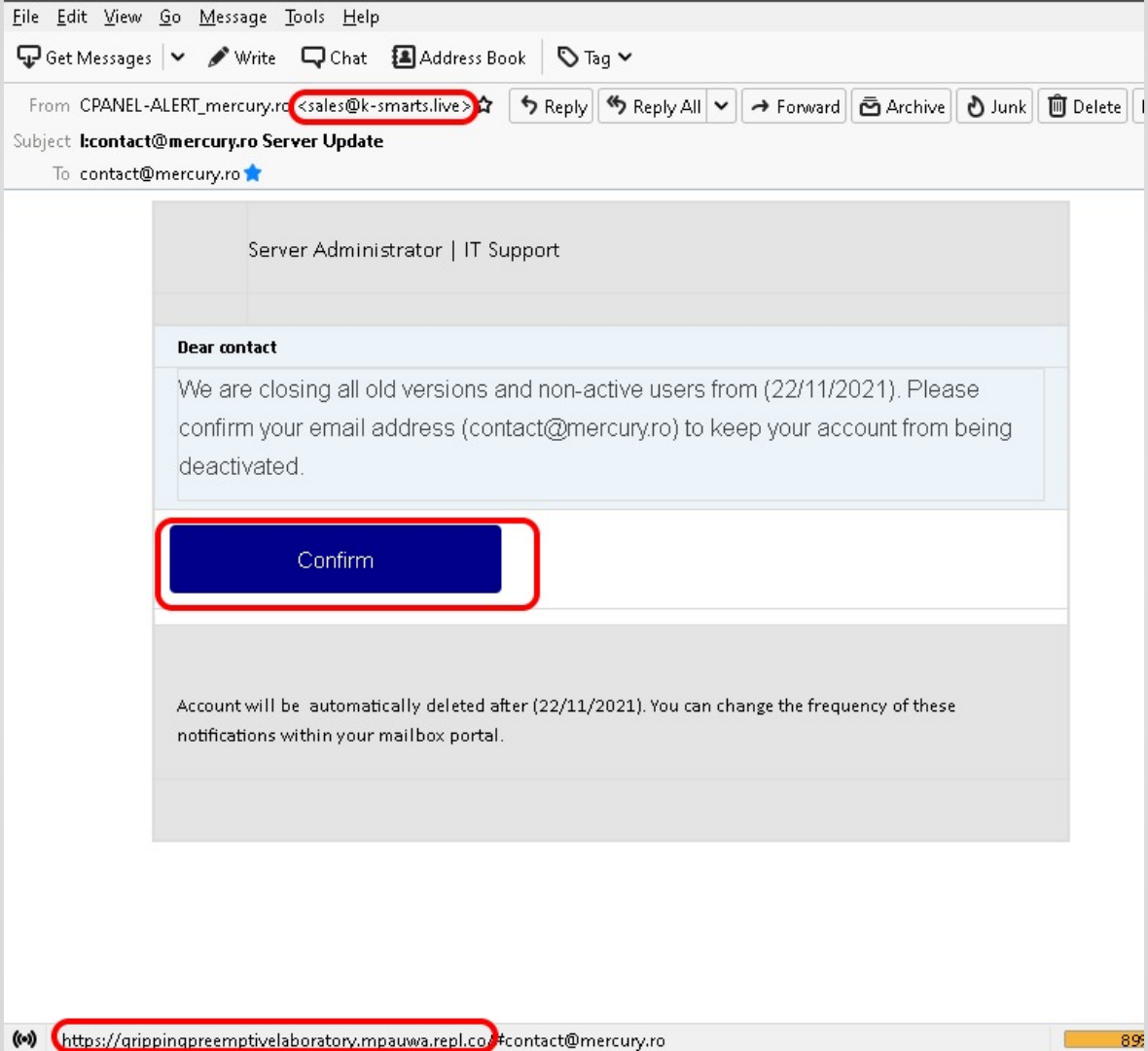
Vă rugăm să faceți clic aici pentru a descărca chitanța

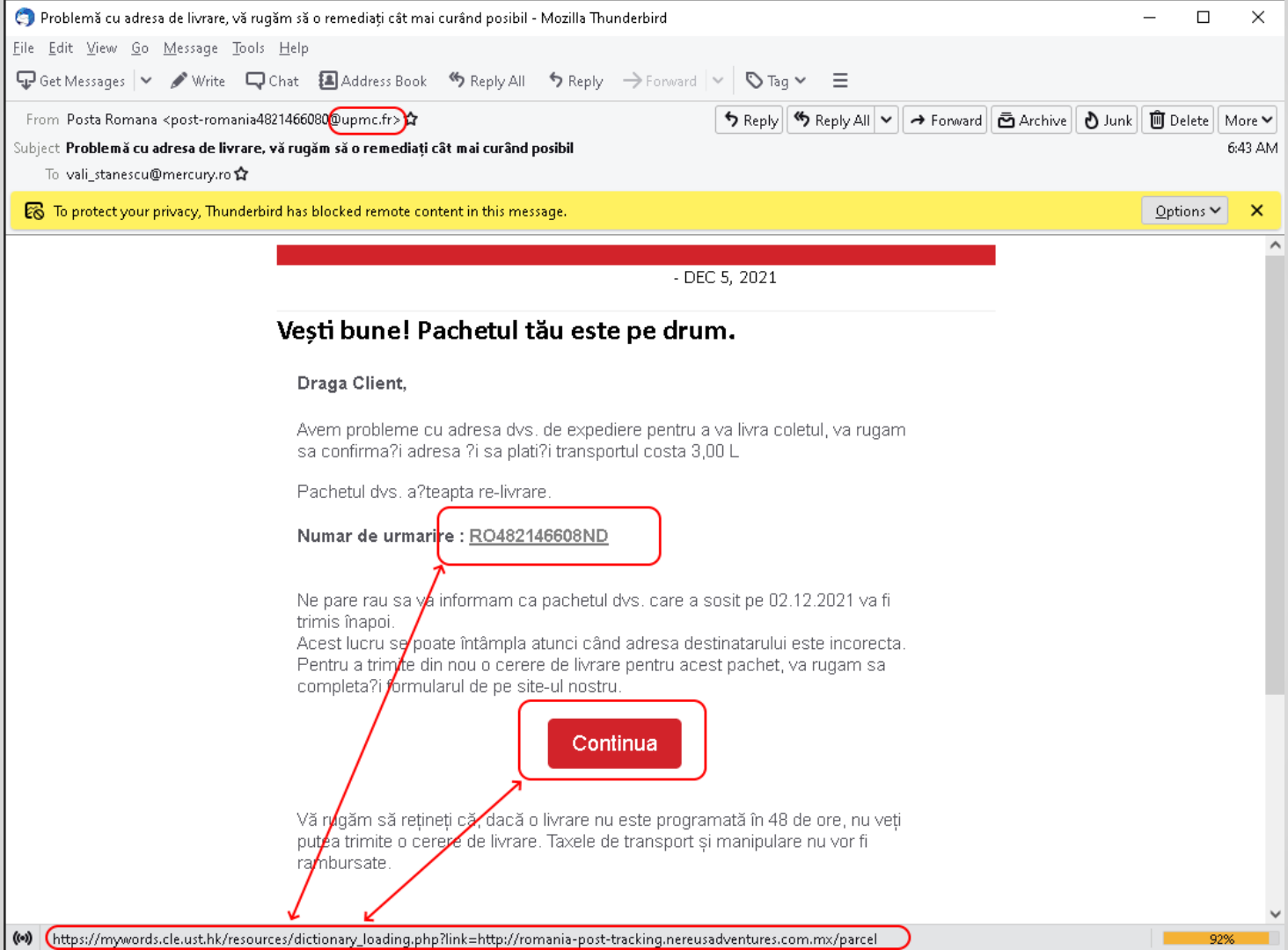
Acesta este un e-mail generat automat, vă rugăm să nu trimiteți e-mail la această adresă, deoarece nu este monitorizat.
Pentru a comunica cu FAN Courier vă rugăm să utilizați adresele de e-mail cunoscute.

Mulțumesc,
FAN Courier
Sediul central București
021-9336

https://www.mediafire.com/file/izkmf11a47k0ifh/23410028317313.tgz/file 87%


FOR YOUR ACTION ? You have [10] quarantined messages - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
From Mail Administrator <g@goodisgoodforlife.tk>
Subject FOR YOUR ACTION ? You have [10] quarantined messages
To contact@mercury.ro
Reply Reply All Forward Archive Junk Delete More
29-10-2021, 19:29
Delivery has failed to these recipients or groups:
You have 10 pending messages for delivery to your mail box.
Click here to release these messages to your inbox folder
failure delivery messages
Recipient:
Subject:
Date:
Release contact@mercury.ro FW: RE: RH-22C-2021 10/29/2021 9:29:34 a.m.
Release contact@mercury.ro RE: Proforma Inv 2021 - GCT // Altan Pharma / 172-40884045 10/29/2021 9:29:34 a.m.
Release contact@mercury.ro BC-Bahrain MOH Tenders 2020 & 02/2021 10/29/2021 9:29:34 a.m.
Release contact@mercury.ro FW: SOA- JAN 2021 10/29/2021 9:29:34 a.m.
(more...6)
Note: This message was sent by the system for notification only.
If this message lands in your spam folder, please move it to your inbox folder for proper integration.
https://mys.opendrives.workers.dev/#contact@mercury.ro
88%


File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
From CPANEL-ALERT_mercury.ro <sales@k-smarts.live>
Reply
Reply All
Forward
Archive
Junk
Delete
Subject !:contact@mercury.ro Server Update
To contact@mercury.ro
Server Administrator | IT Support
Dear contact
We are closing all old versions and non-active users from (22/11/2021). Please confirm your email address (contact@mercury.ro) to keep your account from being deactivated.
Confirm
Account will be automatically deleted after (22/11/2021). You can change the frequency of these notifications within your mailbox portal.
https://grippingpreemptivelaboratory.mpauwa.repl.co/#contact@mercury.ro


Problemă cu adresa de livrare, vă rugăm să o remediați cât mai curând posibil - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Reply All Reply Forward Tag
From Posta Romana <post-romania4821466080@upmc.fr>
Subject Problemă cu adresa de livrare, vă rugăm să o remediați cât mai curând posibil
To vali_stanescu@mercury.ro
Reply Reply All Forward Archive Junk Delete More
6:43 AM
To protect your privacy, Thunderbird has blocked remote content in this message.
Options
- DEC 5, 2021
Vești bune! Pachetul tău este pe drum.
Draga Client,
Avem probleme cu adresa dvs. de expediere pentru a va livra coletul, va rugam sa confirma?i adresa ?i sa plati?i transportul costa 3,00 L
Pachetul dvs. a?teapta re-livrare.
Numar de urmarire : RO482146608ND
Ne pare rau sa va informam ca pachetul dvs. care a sosit pe 02.12.2021 va fi trimis înapoi.
Acest lucru se poate întâmpla atunci când adresa destinatarului este incorecta.
Pentru a trimite din nou o cerere de livrare pentru acest pachet, va rugam sa completa?i formularul de pe site-ul nostru.
Continua
Vă rugăm să rețineți că, dacă o livrare nu este programată în 48 de ore, nu veți putea trimite o cerere de livrare. Taxele de transport și manipulare nu vor fi rambursate.
https://mywords.cle.ust.hk/resources/dictionary_loading.php?link=http://romania-post-tracking.nereusadventures.com.mx/parcel
92%

From Netflix <info@mailer.netflix.com>
Subject **Reminder: payment information to update**
To cz

Reply All | Reply | Forward

NETFLIX

⚠ Reminder: payment information to update.

Reminder: payment information to update

Hi,

We're having trouble with your billing information. We will try again, but you may need to update your payment details.

update the account

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix.

From 04038939 <delia.ginga@catalyst.ro>
Subject **Re: Răspuns**
Reply to jomi1626@comcast.net
To contact@mercury.ro

Reply | Reply All | Forward | Junk | Delete
03-09-2019, 22:3

Presupun că vă întrebați de ce primiți acest e-mail corect?

Ar fi extrem de benefic pentru confidențialitatea dvs. dacă nu o ignorați.

Am plasat un program Malware pe un site web pentru adulți (... P ... 0 ... r ... n site) și pe măsură ce ați vizitat și vizionat video dispozitivul dvs. a fost afectat, plasând un program spyware pe mașina dvs. Ceea ce v-a înregistrat atât cu captura de cameră foto cât și pe ecran, în timp ce aveți „timpul distractiv", permițându-mi să văd exact ce vedeți.

Acest lucru a afectat și smartphone-ul dvs. printr-un exploit. Așadar, nu credeți că puteți evita o clipă acest lucru reinstalând sistemul de operare. Ați fost deja înregistrat.

După aceea, malurile noastre au colectat toate mesagerele, e-mailurile și contactele rețelelor sociale.

Cred că nu este o veste bună, nu?
Dar nu vă faceți griji prea mult, există o modalitate prin care putem rezolva această problemă de confidențialitate. Tot ce îmi trebuie este o plată Bitcoin de **£7,360.00 GBP**, ceea ce cred că este un preț corect, având în vedere circumstanțele.

Adresa Bitcoin pentru efectuarea plății este: 1AWFrDW1LMpzVRJnakhHDrtuAMED2rkt2N

NOTĂ: AȚIȚIȚI-VĂ A RECONFIRMA ADRESUL BITCOINULUI CU NOI ÎNAINTE DE A FACE PLATĂ PENTRU A EVITA A FĂRĂ DE două ori plata.

Dacă nu înțelegeți bitcoin, accesați YouTube și căutați „cum să cumpărați bitcoin" sau Google pentru „bitcoins locale", este destul de ușor să îl faceți.

Aveți la dispoziție doar 48 de ore de la citirea acestui e-mail pentru a trimite plata (fiți avertizat, știu când ați deschis și citiți acest e-mail, am plasat o imagine de pixel în interiorul acesteia. Ceea ce îmi permite să știu când ați deschis mesajul exact ce zi și ce oră)

Dacă decideți să ignorați acest e-mail, nu vom avea de ales decât să redirecționăm videoclipul tuturor contactelor colectate pe care le aveți pe contul de e-mail, precum și să postați pe conturile de social media și să trimiteți ca mesaj personal tuturor contactelor Facebook . și bineînțeles, faceți videoclipul disponibil public pe internet, prin YouTube și site-uri web pentru adulți. având în vedere reputația ta, ne îndoim că îți dorești să fii expus familiei / prietenilor / colegilor tăi în această perioadă curentă.

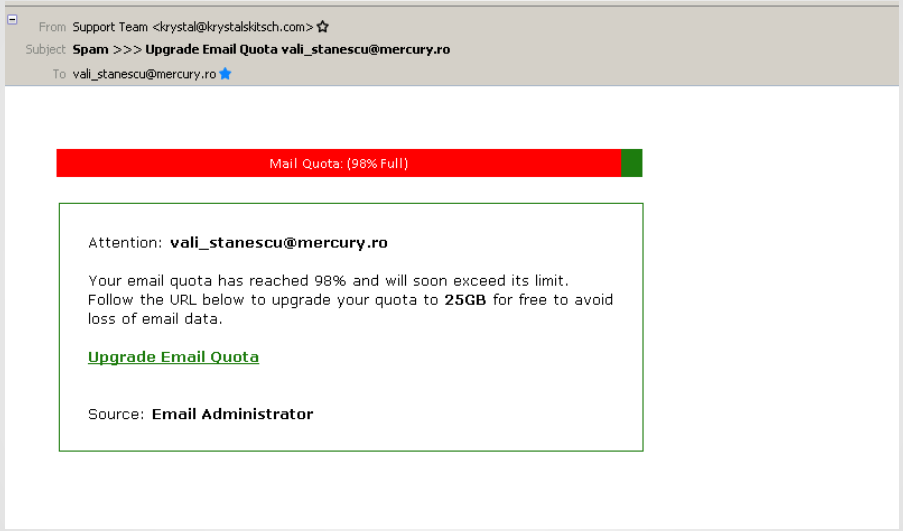
Puteți efectiv să mergeți la poliție, dar acești oameni nu vor face probabil nimic, cele mai semnificative lucruri pe care le pot face este să-mi închid portofelul și veți privi ceilalți de posibilitatea de a-mi plăti. Deci, gândiți-vă de două ori înainte de a face lucruri nechibzuite.

Dacă primim plata, tot materialul va fi distrus și nu veți mai auzi niciodată de la mine. Dacă nu primim fondurile mele din vreun motiv, cum ar fi incapacitatea de a trimite bani către un portofel cu lista neagră - reputația ta va fi naufragiată. Așa că faceți-o repede.

Amintiți-vă aici este adresa Bitcoin pentru a efectua plata către: 1AWFrDW1LMpzVRJnakhHDrtuAMED2rkt2N

Nu încercați să luați contact cu noi, deoarece folosim un e-mail al victimei care a fost hacked și expus. Răspundeți doar pentru a-mi anunța că ați făcut plata sau aveți întrebări despre efectuarea plății, apoi dați clic pe Răspuns.

Dacă nu credeți și nu doriți dovada, răspundeți doar la acest e-mail cu „PROOF" și vă voi trimite videoclipul la 5 dintre contactele dvs. prin e-mail și postați pe peretele Facebook. În care nu veți putea elimina pentru totdeauna. Asta vrei tu? Dacă nu procedați și efectuați plata fără întârziere


From Support Team <krystal@krystalskitsch.com>
Subject Spam >>> Upgrade Email Quota vali_stanescu@mercury.ro
To vali_stanescu@mercury.ro
Mail Quota: (98% Full)
Attention: vali_stanescu@mercury.ro
Your email quota has reached 98% and will soon exceed its limit.
Follow the URL below to upgrade your quota to 25GB for free to avoid loss of email data.
Upgrade Email Quota
Source: Email Administrator

From DHL Express <recepcija@solarisresort.com>

Subject **DHL Shipment Notification : 093207971605**

To Recipients <recepcija@solarisresort.com>

FYI

PDF DHL-Shipment_09...

VIEW | DOWNLOAD PDF

Thank you for using our services.

Yours Sincerely,
Customer Service
DHL Express Team.


PROFI
CADOURI
PENTRU
FEMEILE IUBITE
Ce produse cumperi mai des?
PRODUSE COSMETICE
ALIMENTE
PRODUSE DE UZ CASNIC
ALTE
PROFI
CADOURI
PENTRU
FEMEILE IUBITE
Ce messenger folosești cel mai mult?
FACEBOOK
WHATSAPP
@ 2022 Toate drepturile rezervate

FRAUDĂ

Mulțumim pentru atentie!