Gartner peerinsights customers' choice™

Most 5-Star Ratings

as reviewed by customers

AVANAN

Credential Harvesting as a Service

How this Darkweb Organization Steals Your Credentials

Michael Landewe

Co-Founder, Chief Privacy Officer

michael@avanan.com

SPAM-EGY: Office 365 Credential Harvesting

Office 365 Credential Harvesting as a Service

WWW.SPAM-EGY.GA

SPAM-EGY.GA

Office 365 Microsoft

Your payment method for Office 365 Business has been changed.
Invoice is ready.

Sign in to the Office 365 Admin Center to pay your invoice.

View this message in the Office 365 Message Center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message Center preferences.

Edit Release Preferences. Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

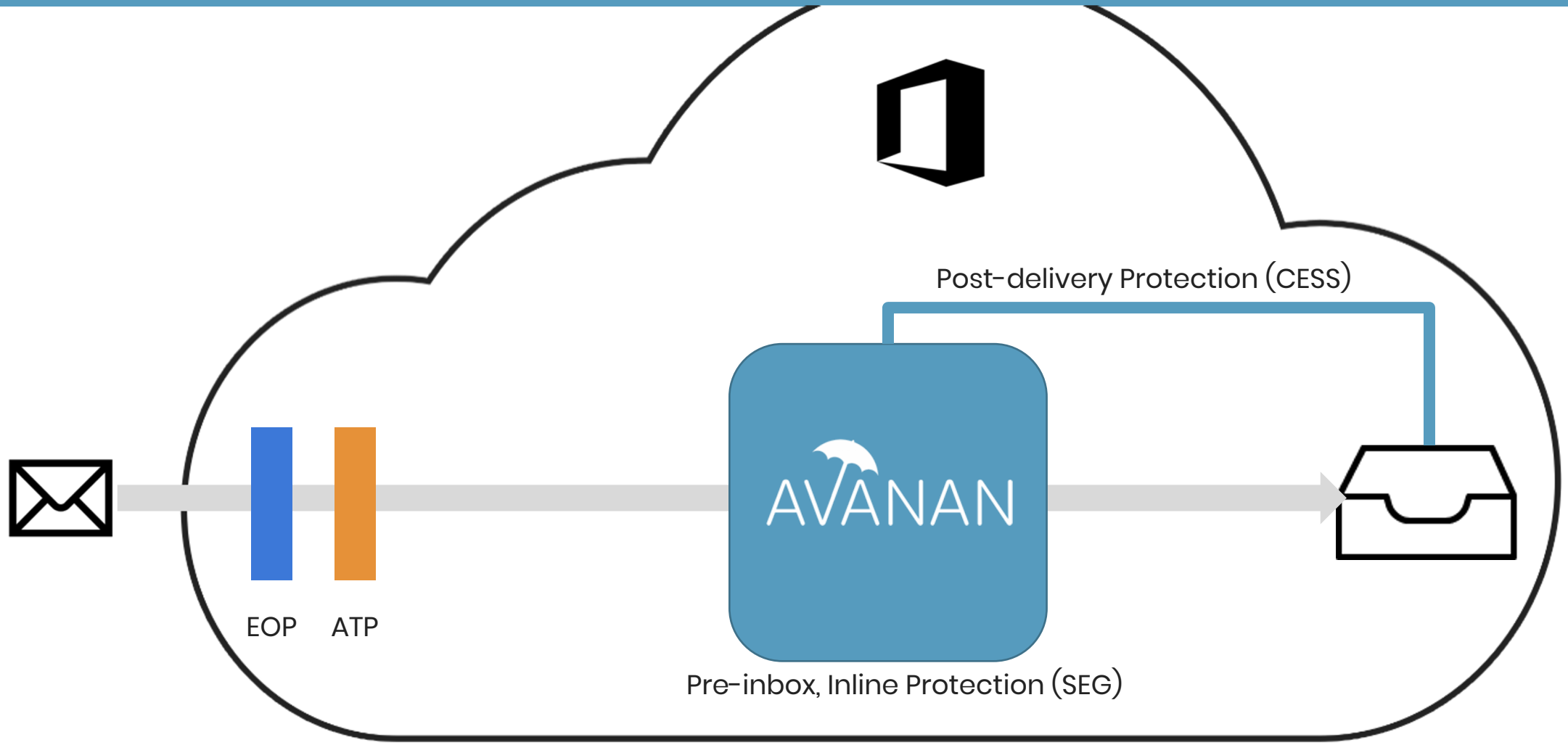
Unsubscribe

Microsoft

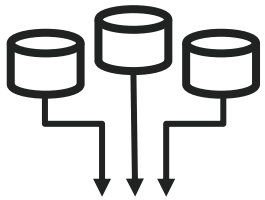
Unsubscribe | Privacy Statement

Most 5-Star Ratings
as reviewed by customers

Integrated Cloud Email (ICE) Security Architecture



Layers of Defense

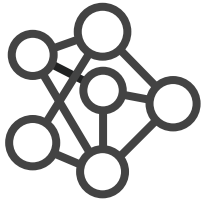


Known Threat Feeds

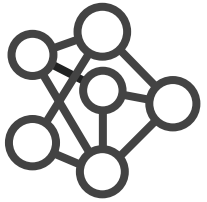
File and URL Sandboxing Tools

Office 365 | G Suite Indicators of Attack

Customer Specific Internal/BEC ML



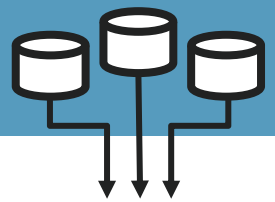
Customer Specific False Positive ML



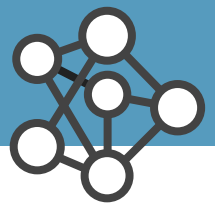
Customer Specific SaaS Events

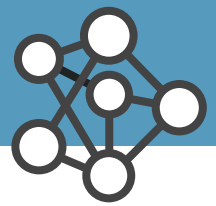
Most 5-Star Ratings
as reviewed by customers

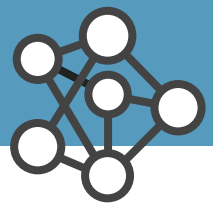
AVANAN

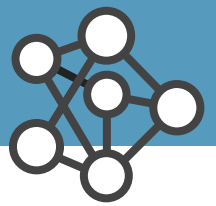

Known Threat Feeds

File and URL Sandboxing Tools


Office 365 | G Suite Indicators of Attack


Customer Specific Internal/BEC ML


Customer Specific False Positive ML


Customer Specific SaaS Events

- Bypass EOP
- Bypass ATP
- EMAIL Message
- ✗ URL

How did this known malicious URL bypass ATP?

BaseStriker
avanan.com/attacks

```
<!DOCTYPE html>
<html>
<head>
    <base href="https://domain.com">
</head>
<body>
But by splitting the URL, the <a href="malicious/link">link</a> gets through.
</body>
</html>
```

This becomes a highly-correlated indicator of attack.

Most 5-Star Ratings
as reviewed by customers

AVANAN

Known Threat Feeds

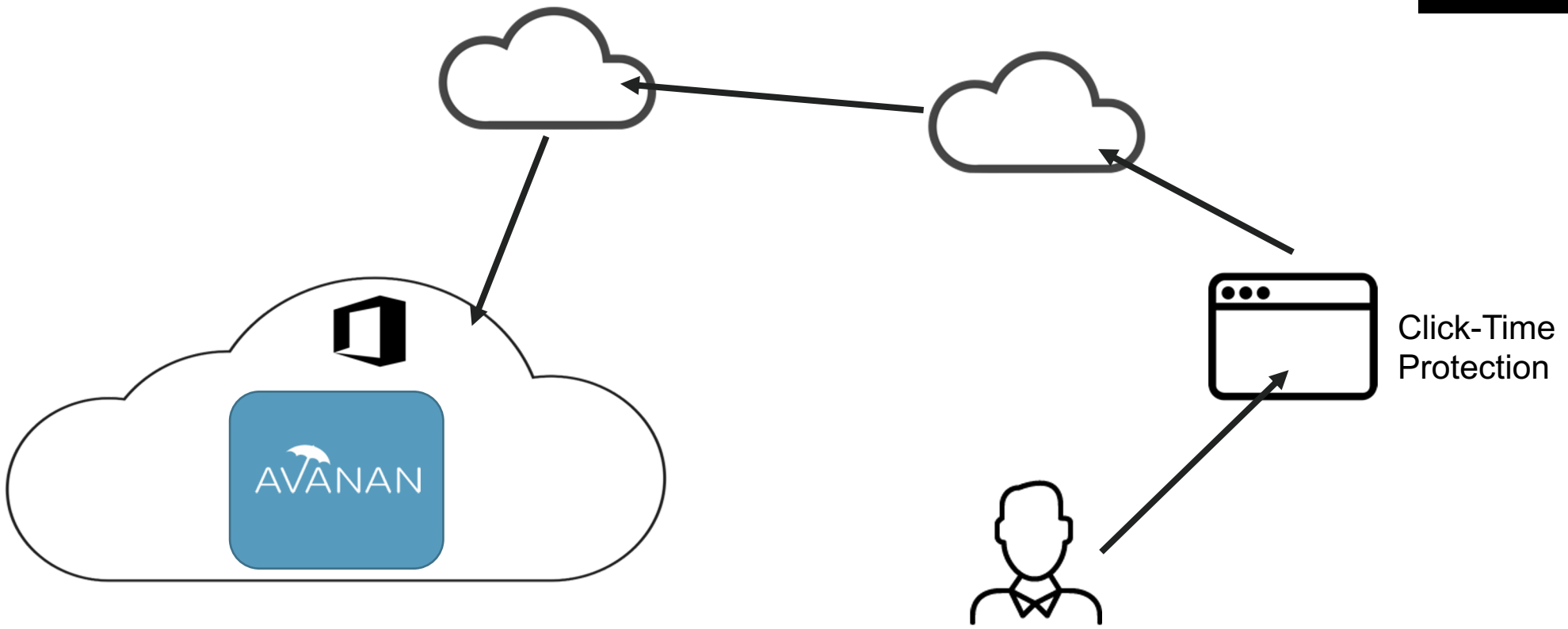
File and URL Sandboxing Tools

Office 365 | G Suite Indicators of Attack

Customer Specific Internal/BEC ML

Customer Specific False Positive ML

Customer Specific SaaS Events



The Business of Credential Harvesting

Bypass EOP

Bypass ATP

✅ Convincing EMAIL

Convincing Webpage

Password/Login Handler

SPAM-EGY Office 365 "True Login" Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont		▶BaseStriker	▶ZeroFont.v2		▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					

office page.html
Mail - mike@abletool.com
file:///C:/Users/lord/Desktop/old/office%20page.html
Apps
Russian Keyboard Or
ADD free Nome
Freenom - A Name fo
Temp Email Address
Free Website Hosting
Sign up for a free 00
TempMailAddress | D
Russian Keyboard Or

Office 365 Page true login (cloud) 2019 By Spam-Egy

Work in cloud html code

Office true login

Responsive design

Price:300$

my icq: 724397262

office page.html | Mail - mike@abletool.com

https://outlook.office.com/owa/?realm=abletool.com&exsvurl=1&ll-cc=1033&modurl=0&path=/mail/inbox

Apps | Russian Keyboard Or | ADD free Nome | Freenom - A Name f | Temp Email Address | Free Website Hostin | Sign up for a free 00 | TempMailAddress | D | Russian Keyboard Or

Office 365 | Outlook

Search Mail and People

New | Delete | Archive | Junk | Sweep | Move to | Categories | ... | Undo

Folders

- Favorites
  - Inbox 17
  - Sent Items
  - Drafts 1
  - Vendor PO's
  - Vendor Quotes
  - Confirmations
  - Deleted Items 1
- Mike Trovillo
  - Inbox 17
    - .Misc.
    - Able
      - Alexander
      - Buy Castings.com
      - Confirmations

Focused | Other | Filter

Next: No more events for today or tomorrow | Agenda

Other: New conversations 4
AMTS 2018; Vulcan Spring; Design 2 Part Trade S...

Security !
Action Needed: Verify Your Account 6:33 AM
This mail is from a trusted sender. fzJi3vOfzJi3vffzJi3...

GunBroker.com
Wells Fargo + Gun Manufacturers, Exclusive 6:06 AM
Don't miss the GunBroker.com Weekly! ...

info@winstonht.com
WINSTON HEAT TREATING, INC., seq#46 Sh 6:03 AM
(No message text)

Yesterday

BTS Docs
Electronic Documents 167547 Fri 9:03 PM
MIKE TROVILLO, Below are invoice details from : Inv...

Shars Tool Company
Meet ParaKeep, our newest line of Made in Fri 5:32 PM

This message was sent with high importance.

This mail is from a trusted sender.

Office 365

You Have 23 Undelivered / Pending Messages

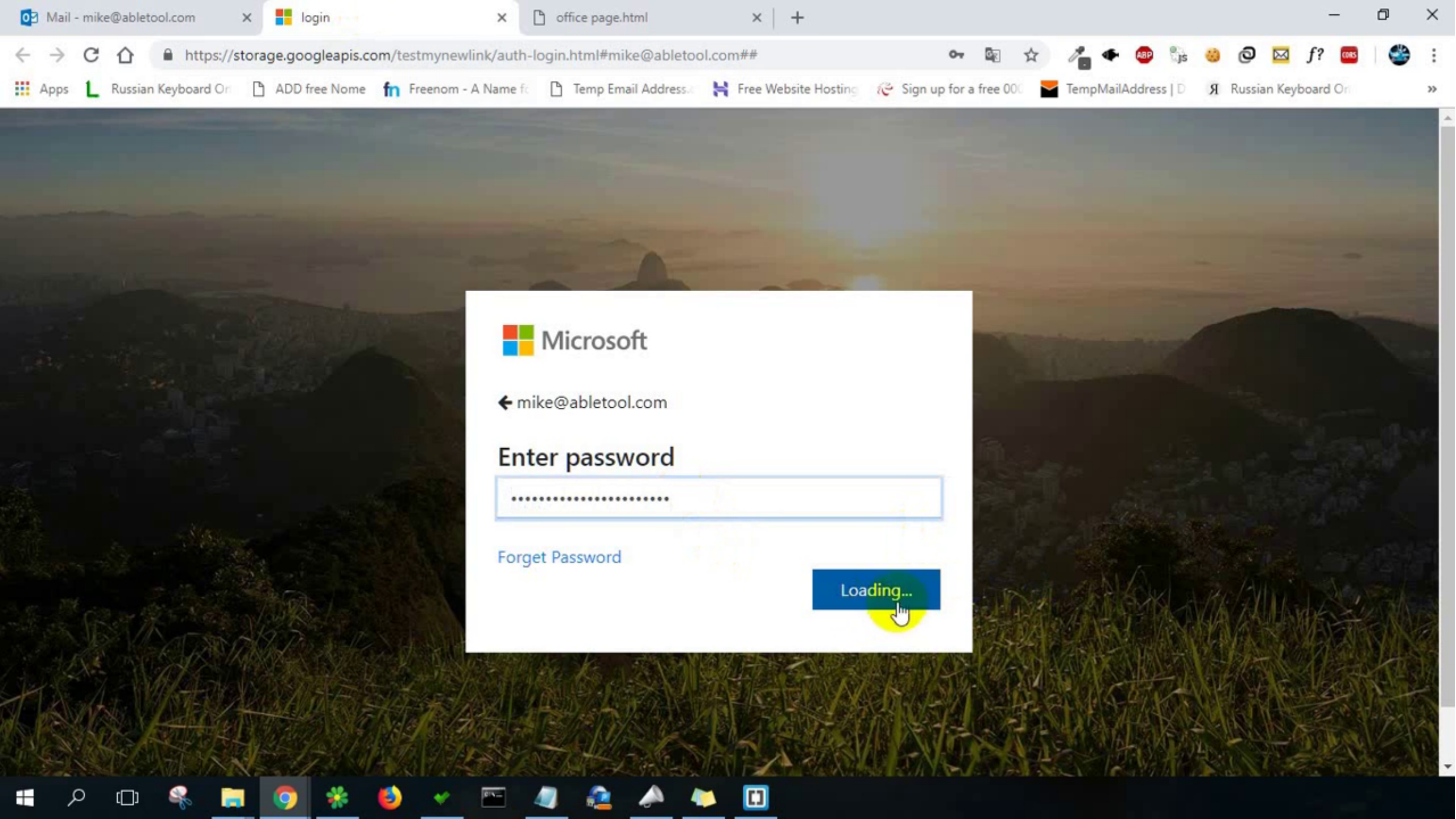
Dear mike@abletool.com

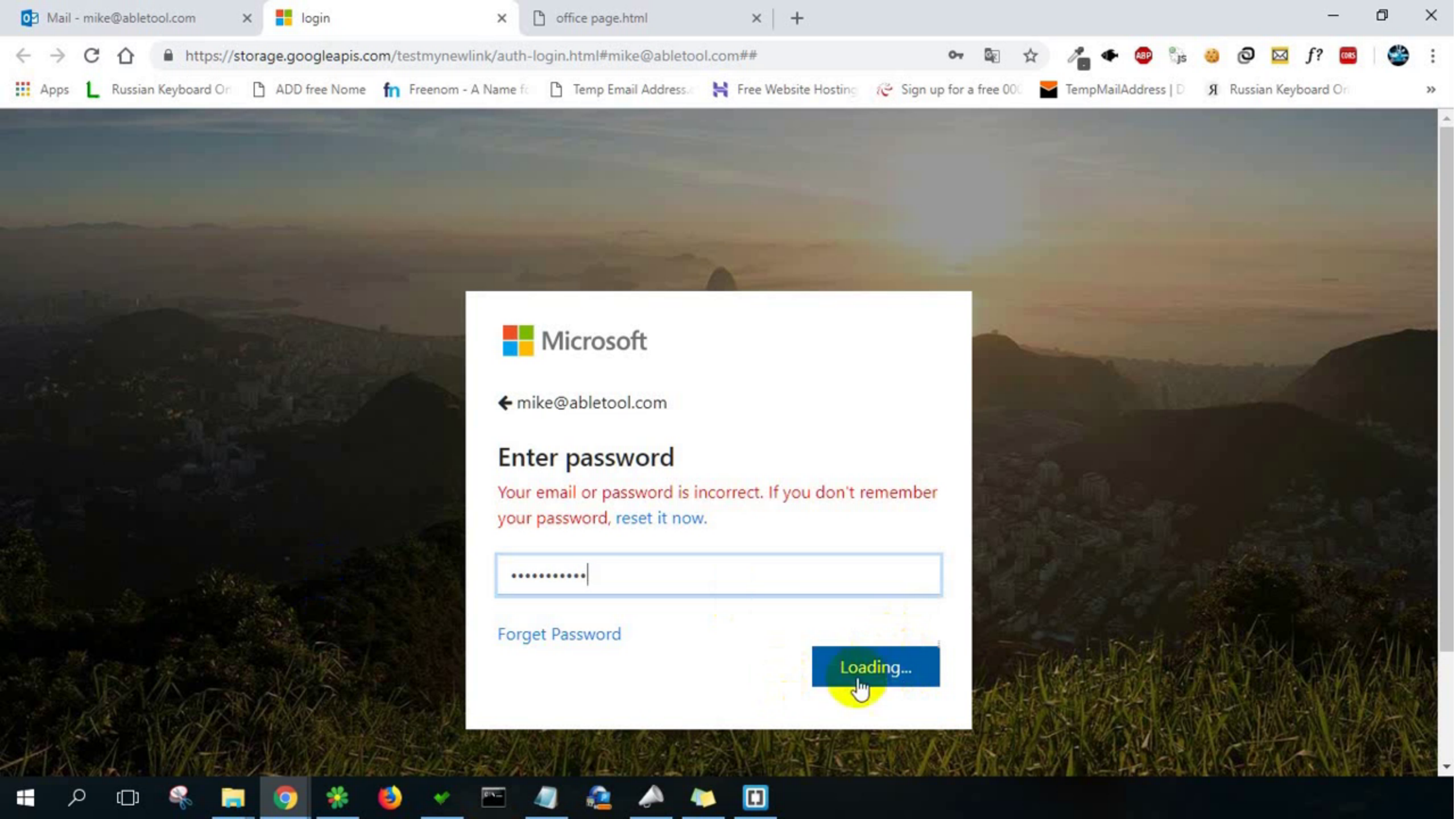
Microsoft Office 365 mail server has detected about (23) clustered messages undelivered/ pending to your mailbox as of Oct 10, 2018 06:00 AM. They are awaiting your approval to be delivered.

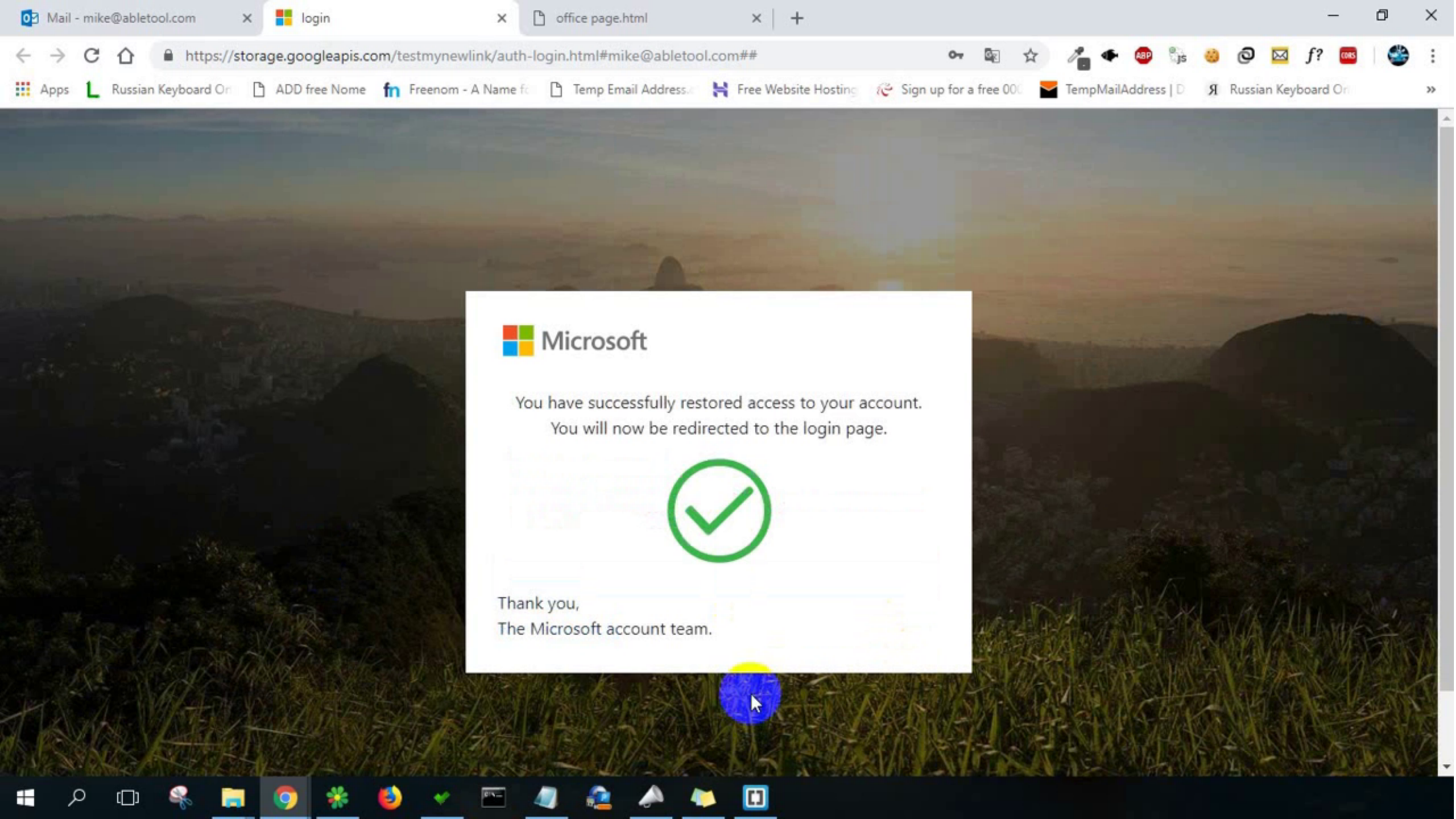
Please review them here and restore delivery of pending messages.

Review Messages

Best regards,

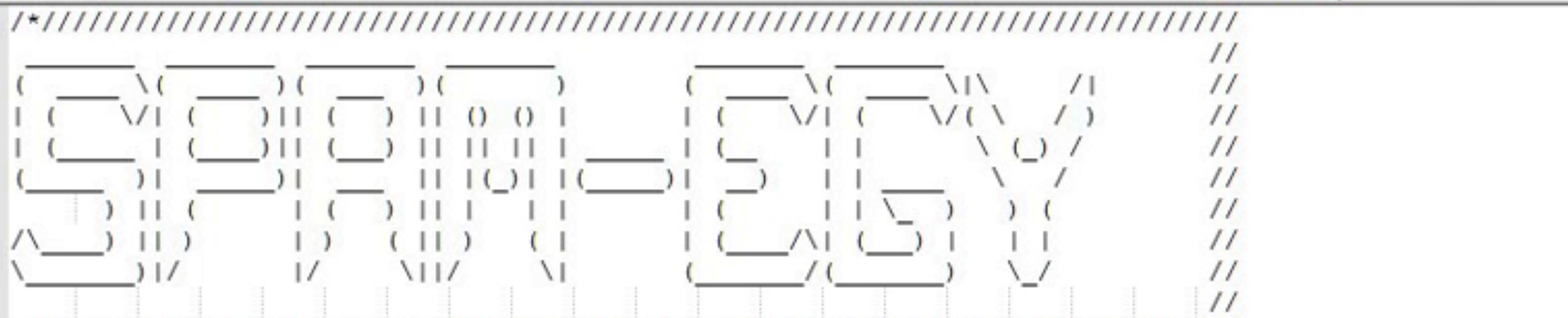

Mail - mike@abletool.com
login
office page.html
https://storage.googleapis.com/testmynewlink/auth-login.html#mike@abletool.com##
Apps
Russian Keyboard Or
ADD free Nome
Freenom - A Name f
Temp Email Address
Free Website Hostin
Sign up for a free 00
TempMailAddress | D
Russian Keyboard Or
Microsoft
mike@abletool.com
Enter password
Forget Password
Loading...


Mail - mike@abletool.com
login
office page.html
https://storage.googleapis.com/testmynewlink/auth-login.html#mike@abletool.com##
Apps
Russian Keyboard Or
ADD free Nome
Freenom - A Name fo
Temp Email Address
Free Website Hosting
Sign up for a free 00
TempMailAddress | D
Russian Keyboard Or
Microsoft
mike@abletool.com
Enter password
Your email or password is incorrect. If you don't remember your password, reset it now.
Forget Password
Loading...


Mail - mike@abletool.com
login
office page.html
https://storage.googleapis.com/testmynewlink/auth-login.html#mike@abletool.com##
Apps
Russian Keyboard Or
ADD free Nome
Freenom - A Name fo
Temp Email Address
Free Website Hosting
Sign up for a free 00
TempMailAddress | D
Russian Keyboard Or
Microsoft
You have successfully restored access to your account.
You will now be redirected to the login page.
Thank you,
The Microsoft account team.

SPAM-EGY Office 365 "True Login" Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont		▶BaseStriker	▶ZeroFont.v2		▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					



```
##################################
build and crypt letter by SPAM-EGY

build letter and crypt  inbox 10000%

Price : privet

my icq :724397262

telegram:  https://t.me/spamegy

Facebook : https://www.facebook.com/Segy6

##################################
```

Office 365

Update your mailbox.

within the next 24 hours, [] will be blocked
from incoming and outgoing messages from other users
because you failed to update your mailbox.
Please note this will be the last reminder before your mailbox
will blocked from our system.

UPDATE HERE

Office-365 hope to serve you better.
Regards,
The Mail Team

Microsoft respects your privacy.
To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052.

Hassan Hassan | Mail - gregoryfane@fanewoodin | SPAM-EGY
https://s4egy.com/make/new.php
Apps | Russian Keyboard On | ADD free Nome | Freenom - A Name fo | Temp Email Address | Sign in | Free Website Hosting | Sign up for a free 00 | TempMailAddress | D

SPAM-EGY

http://image.email2.office.com/lib/fe81137272620d7a7d/m/1/logo_office365_large_corrected.png

Update your mailbox.

within the next 24 hours, [] will be blocked
from incoming and outgoing messages from other users
because you failed to update your mailbox.
Please note this will be the last reminder before your mailbox
will blocked from our system.

https://mail.yandex.com/

UPDATE HERE

Office-365 hope to serve you better.
Regards,

Hassan Hassan | Mail - gregoryfane@fanewoodin | SPAM-EGY

https://s4egy.com/make/new.php

Apps | Russian Keyboard On | ADD free Nome | Freenom - A Name fo | Temp Email Address | Sign in | Free Website Hosting | Sign up for a free 00 | TempMailAddress | D

https://mail.yandex.com/

UPDATE HERE

Office-365 hope to serve you better.
Regards,
The Mail Team

Microsoft respects your privacy.
To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Make Now

You can make **5005** letter

Hassan Hassan | Mail - gregoryfane@fanewoodin | Update your mailbox. 173360

https://s4egy.com/make/post.php

Apps | Russian Keyboard On | ADD free Nome | Freenom - A Name fo | Temp Email Address | Sign in | Free Website Hosting | Sign up for a free 00 | TempMailAddress | D

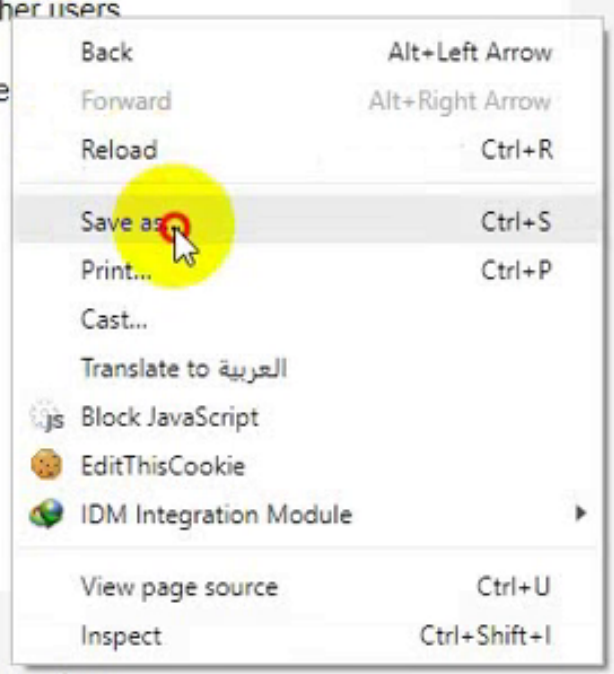
Office 365

Update your mailbox.

within the next 24 hours, [] will be blocked
from incoming and outgoing messages from other users
because you failed to update your mailbox.
Please note this will be the last reminder before
will blocked from our system.

UPDATE HERE

Office-365 hope to serve you better.
Regards,
The Mail Team



Microsoft respects your privacy.
To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052.

C:/Users/lord/Desktop/doc/Update your mailbox. 173360.html (Getting Started) - Brackets

File Edit Find View Navigate Debug Help Emmet

Working Files

lettr.html
index.php
Update your mailbox. 360887.html
Update your mailbox. 173360.html

Getting Started

screenshots
quick-edit.png
index.html
main.css

```
43                  <div style="text-align: center;background-color: #DDD;padding:5px;" class="text">
44
45              U<font id="xv">XOCgGZ</font>p<font id="xv">XOCgGZ</font>d<font id="xv">XOCgGZ</font>a<font id="xv">XOCgGZ</font>t<font
                id="xv">XOCgGZ</font>e<font id="xv">XOCgGZ</font> <font id="xv">XOCgGZ</font>y<font id="xv">XOCgGZ</font>o<font
                id="xv">XOCgGZ</font>u<font id="xv">XOCgGZ</font>r<font id="xv">XOCgGZ</font> <font id="xv">XOCgGZ</font>m<font
                id="xv">XOCgGZ</font>a<font id="xv">XOCgGZ</font>i<font id="xv">XOCgGZ</font>l<font id="xv">XOCgGZ</font>b<font
                id="xv">XOCgGZ</font>o<font id="xv">XOCgGZ</font>x<font id="xv">XOCgGZ</font>.<font id="xv">XOCgGZ</font> <font
                id="xv">XOCgGZ</font>
46
47                  <br>
48  </div>
49
50                   <p>  <br>
51  <font id="xv">nX0Z7U</font><br><font id="xv">nX0Z7U</font>w<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>t<font
    id="xv">nX0Z7U</font>h<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>t<fo
    id="xv">nX0Z7U</font>h<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font>e<fo
    id="xv">nX0Z7U</font>x<font id="xv">nX0Z7U</font>t<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>2<font id="xv">nX0Z7U</font>4<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>h<font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>u<font id="xv">nX0Z7U</font>r<fo
    id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font>,<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>[E-mail Address]<font
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>w<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>l<font id="xv">nX0Z7U</font>l<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>b<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>b<fo
    id="xv">nX0Z7U</font>l<font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>c<font id="xv">nX0Z7U</font>k<font id="xv">nX0Z7U</font>e<fo
    id="xv">nX0Z7U</font>d<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>
52  <font id="xv">nX0Z7U</font><br><font id="xv">nX0Z7U</font>f<font id="xv">nX0Z7U</font>r<font id="xv">nX0Z7U</font>o<font
    id="xv">nX0Z7U</font>m<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font>c<fo
    id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>m<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font>g<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font>d<font id="xv">nX0Z7U</font> <fo
    id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>u<font id="xv">nX0Z7U</font>t<font id="xv">nX0Z7U</font>g<font id="xv">nX0Z7U</font>o<fo
    id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>n<font id="xv">nX0Z7U</font>g<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>m<fo
    id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>g<fo
    id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>f<font id="xv">nX0Z7U</font>r<fo
    id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>m<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>t<fo
    id="xv">nX0Z7U</font>h<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>r<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>u<fo
    id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>r<font id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font> <fo
    id="xv">nX0Z7U</font>
53  <font id="xv">nX0Z7U</font><br><font id="xv">nX0Z7U</font>b<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>c<font
    id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>u<font id="xv">nX0Z7U</font>s<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font> <fo
    id="xv">nX0Z7U</font>y<font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>u<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>f<fo
    id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>l<font id="xv">nX0Z7U</font>e<font id="xv">nX0Z7U</font>d<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>t<font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>u<fo
    id="xv">nX0Z7U</font>p<font id="xv">nX0Z7U</font>d<font id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>t<font id="xv">nX0Z7U</font>e<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>y<font id="xv">nX0Z7U</font>o<font id="xv">nX0Z7U</font>u<font id="xv">nX0Z7U</font>r<fo
    id="xv">nX0Z7U</font> <font id="xv">nX0Z7U</font>m<font id="xv">nX0Z7U</font>a<font id="xv">nX0Z7U</font>i<font id="xv">nX0Z7U</font>l<fo
```

Getting Started

Line 53, Column 178 — 124 Lines

INS UTF-8 HTML

ZeroFont

```
<style>
    #xv
            color: transparent;
            display: none;
            height: 0;
            max-height: 0;
            max-width: 0;
            opacity: 0;
            overflow: hidden;
            mso-hide: all;
            visibility: hidden;
            width: 0;
  }
```

nx0Z7UUnx0Z7Upnx0Z7Udnx0Z7Ua nx0Z7Ut nx0Z7Uenx0Z7Uynx0Z7Uo nx0Z7Uu nx0Z7Ur nx0Z7U m nx0Z7Ua nx0Z7Uinx0Z7Ulnx0Z7Ubnx0Z7Uo nx0Z7Ux

ZeroFont

Microsoft's Natural Language Filters see:

nx0Z7UUnx0Z7Unx0Z7Udnx0Z7Ua nx0Z7Ut nx0Z7Uenx0Z7Uynx0Z7Uo nx0Z7Uu nx0Z7Ur nx0Z7U m nx0Z7Ua nx0Z7Uinx0Z7Ulnx0Z7Ubnx0Z7Uo nx0Z7Ux

You see:

Update Your Mailbox

SPAM-EGY Office 365 “True Login” Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	“True Login” $300	“Build&Crypt” Subscription			“Sender Inbox”			“Office 365 Page 2020” Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					

ATP Updates

- 2018 October Release
- 2018 December 31
- 2019 February 2
- 2019 April 23
- 2019 April 29
- 2019 June 9
- 2019 June 29
- 2019 August 3
- 2019 November 3

ATP Updates: ZeroFont

```
    <br>
    <br>
    <br>
    <p>© 2019 Mi<font id="xv">[[Company]]</font>cro<font id="xv">[[Company]]</font>sof<font id="xv">[[Company]]</font>t Corp<font id="xv">
[[Company]]</font>orat<font id="xv">[[Company]]</font>ion. All rights reserved. |Ac<font id="xv">[[Company]]</font>cept<font id="xv">[[Company]]
</font>able Use Po<font id="xv">[[Company]]</font>li<font id="xv">[[Company]]</font>cy | Pr<font id="xv">[[Company]]</font>iv<font id="xv">
[[Company]]</font>acy No<font id="xv">[[Company]]</font>ti<font id="xv">[[Company]]</font>ce </p>
  </div>

</html>
```

ATP Updates: CiteUnseen

Random Text in <cite> code

<cite>n9UDBNakdai</cite>O
<cite>n9UDBNakdai</cite>f
<cite>n9UDBNakdai</cite>fi
<cite>n9UDBNakdai</cite>c
<cite>n9UDBNakdai</cite>e
<cite>n9UDBNakdai</cite> 36
<cite>n9UDBNakdai</cite>5

Microsoft Sees:

n9UDBNakdaiOn9UDBNakdaifn9UDBNakdaifin9UDBNakdaicn9UDBNakdaien9UDBNakdai36n9UDBNakdai5

You See:

Office 365

ATP Updates: CiteUnseen

Introduction of email and company name makes each email unique.

<cite>n9UDBNakdai-user@company.com&Company</cite>O
<cite>n9UDBNakdai-user@company.com&Company</cite>f
<cite>n9UDBNakdai-user@company.com&Company</cite>fi
<cite>n9UDBNakdai-user@company.com&Company</cite>c
<cite>n9UDBNakdai-user@company.com&Company</cite>e
<cite>n9UDBNakdai-user@company.com&Company</cite> 36
<cite>n9UDBNakdai-user@company.com&Company</cite>5

ATP Updates: CiteUnseen

⬅ character &#8207 converts reading direction right-to-left

<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite>O
<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite>f
<cite> ⬅ 9UDBNakdai-user@company.com&Company</cite>fi
<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite>c
<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite>e
<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite> 36
<cite> ⬅ n9UDBNakdai-user@company.com&Company</cite>5

ATP Updates: BaseStriker

```
<!DOCTYPE html>
<html lang="en">
<head>

</head>
<body>
This malicious <a href="https://domain.com/malicious/link">link</a> is blocked. </body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
    <base href="https://domain.com">
</head>
<body>
But by splitting the URL, the <a href="malicious/link">link</a> gets through.
</body>
</html>
```

ATP Updates: Signature

From: "Redacted.com"

To: David.Smith@redacted.com

Subject: David Smith Urgent: Your Account Termination Request

<!DOCTYPE html> <head> <!---------- This Letter By SPAM -EGY ICQ: @SPAMEGY ---------- -->

<body>

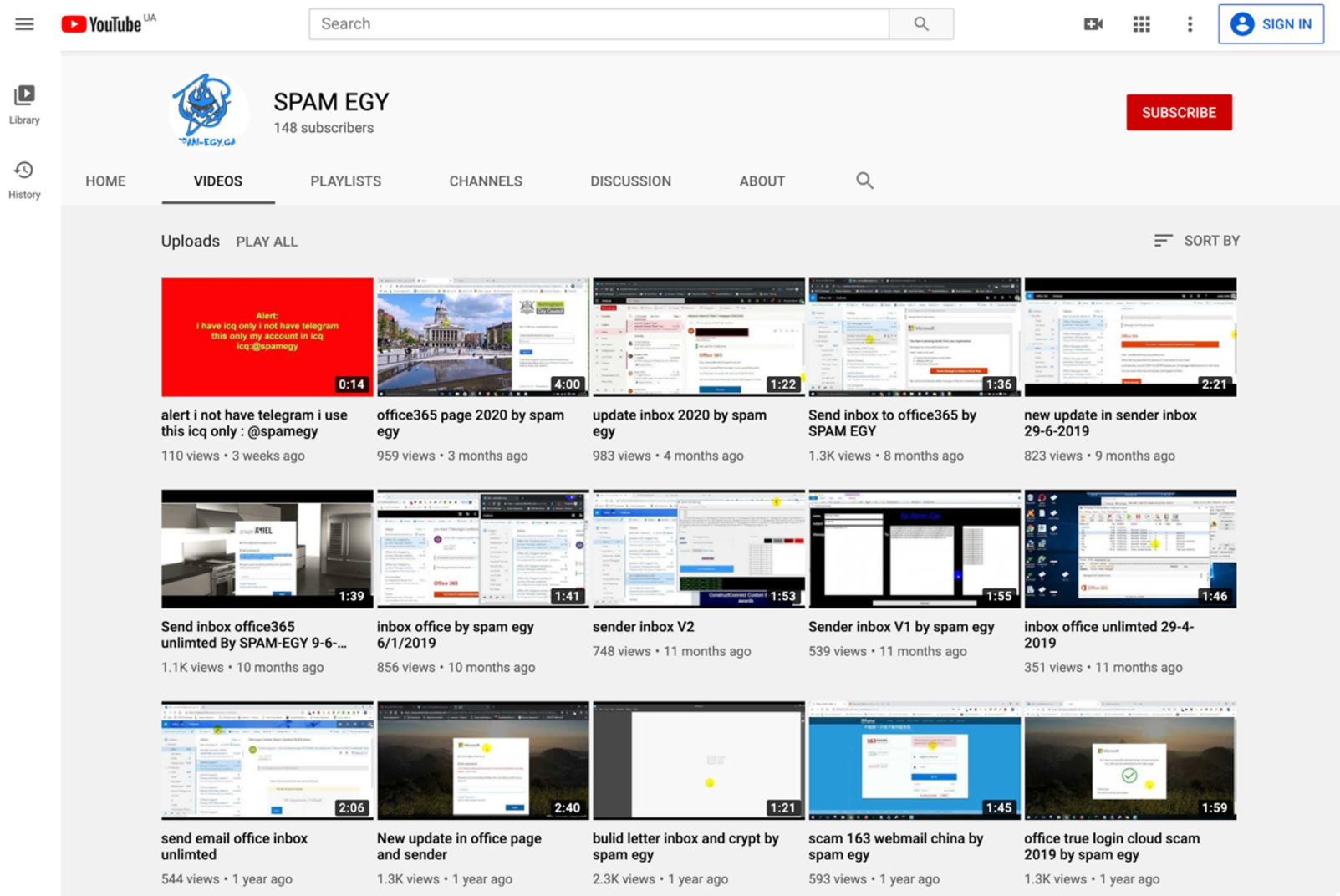
Most 5-Star Ratings
as reviewed by customers

AVANAN

SPAM-EGY Release Video Channel

Video Proof Of New Bypass Techniques

Demonstration of New Features



Mail - andrea@lsnf.org

https://outlook.office365.com/owa/?realm=lsnf.org&exsvurl=1&ll-cc=3073&modurl=0&path=/mail/inbox

Incognito

PHP File Manager | Russian Keyboard... | ADD free Nome | Freenom - A Name... | Temp Email Addres... | TempMailAddress |... | Russian Keyboard... | Azure - Sign up

Legal Services of North Florida

Outlook

Andrea Roberts AR

Search Mail and People | New | Delete | Archive | Junk | Sweep | Move to | Categories | ... | Undo | Try the new Outlook

Folders

Drafts 72
Sent Items 1
Deleted Items 123
Archive
Conversation Histo
Family Law
Important Tax ListS
Infected Items
Junk Email 170
Junk E-Mail
Notes 15
OVW Grant
RSS Feeds
Scheduled

Groups

Inbox Filter

Next: No more events for today or tomorrow. Agenda

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM
this message sent from trusted sender Oandreafan...

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM
this message sent from trusted sender Oandreafan...

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM
this message sent from trusted sender Oandreafan...

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM
this message sent from trusted sender Oandreafan...

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM
this message sent from trusted sender Oandreafan...

Office 365<Support-andrea-5... !
you Have 7 Messages undelivered 6:58 AM

Andrea Roberts

This message was sent with high importance.

this message sent from trusted sender

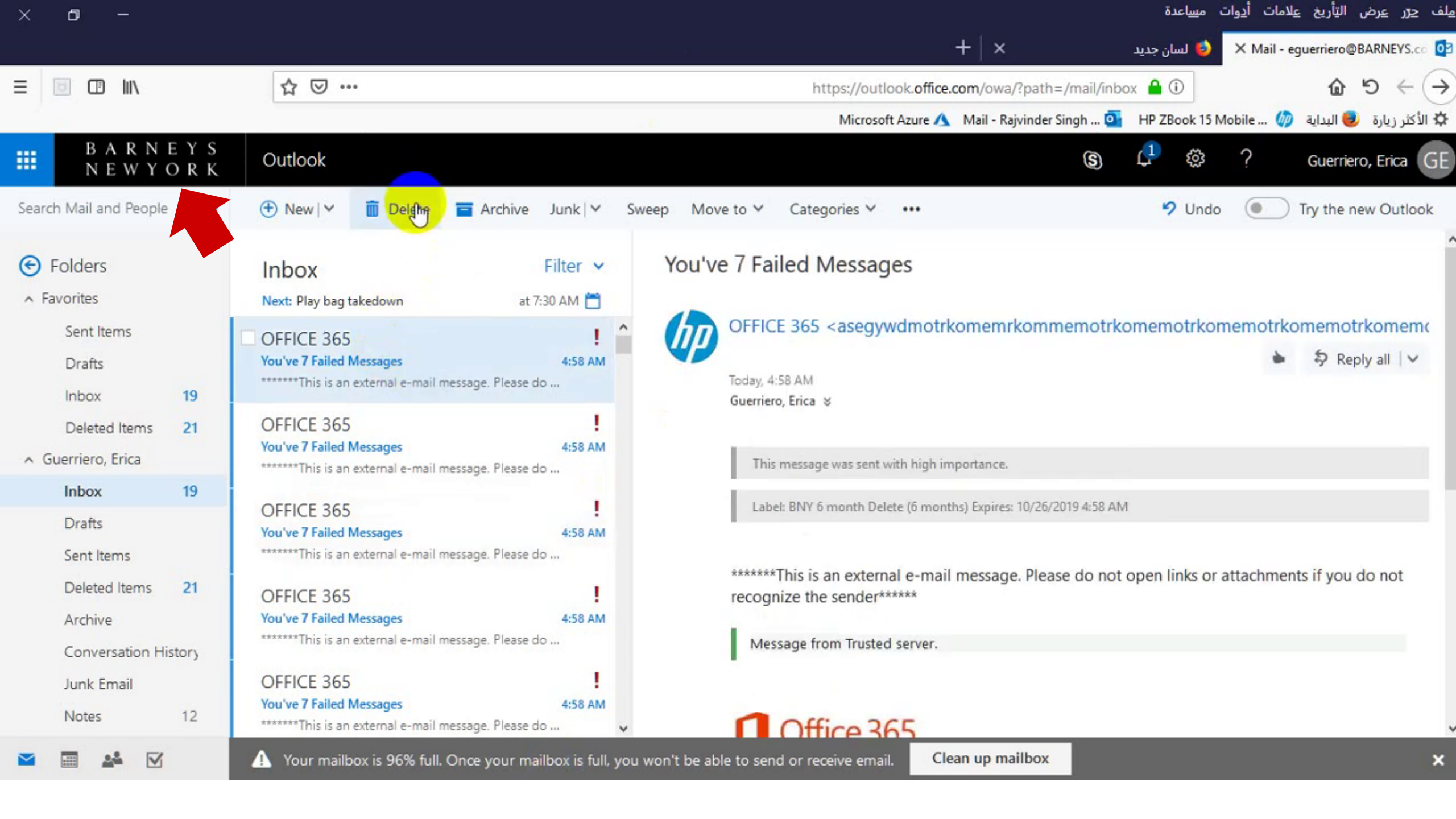
Office 365

You have (7) undelivered/pending mails

Dear : andrea@lsnf.org
We noticed your emails failed to sync 7 messages
to your inbox as of 6/1/2019.
This is due to a server error on your mailbox.
Review these messages and choose what happens to them.

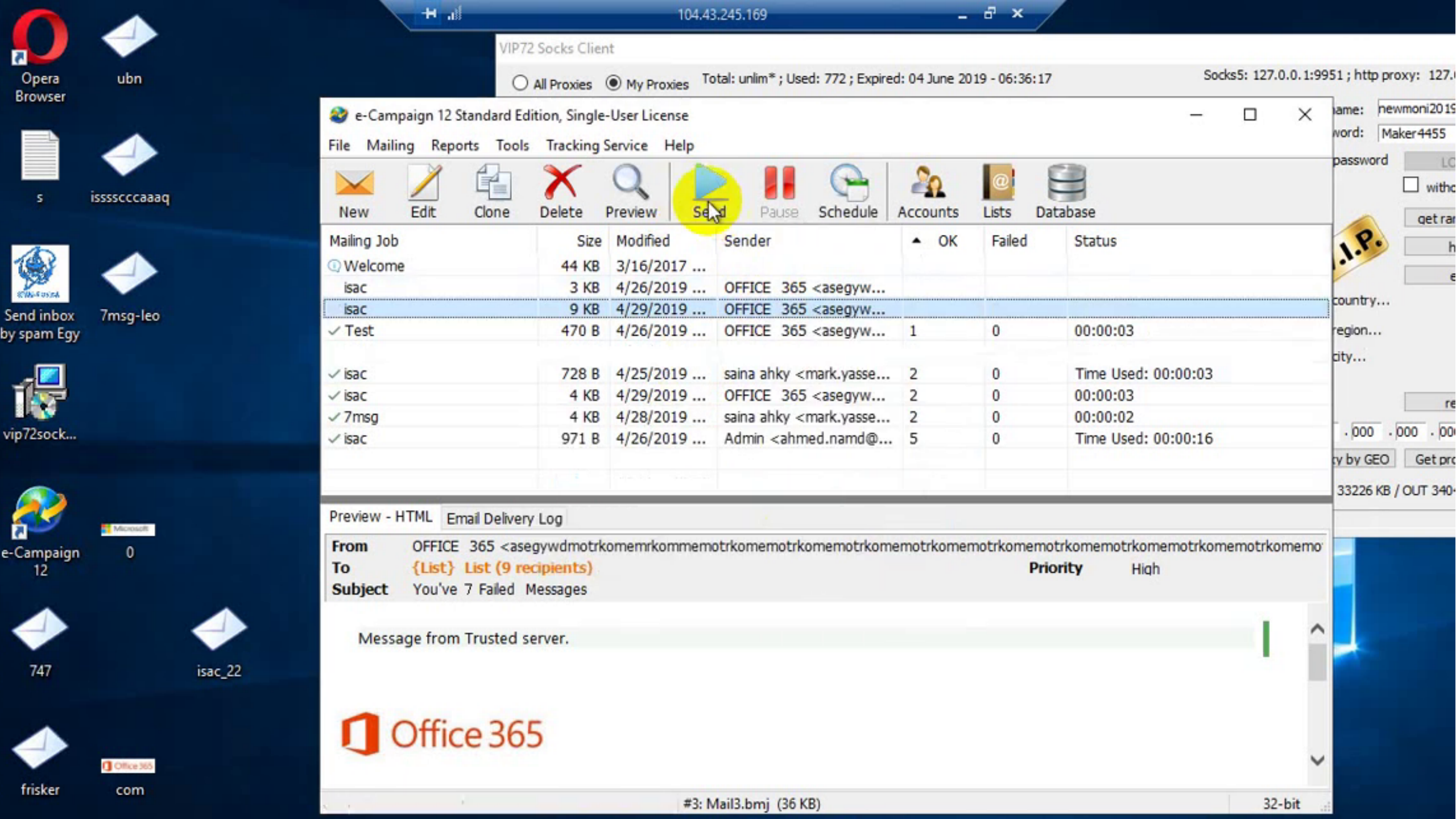
Review Message

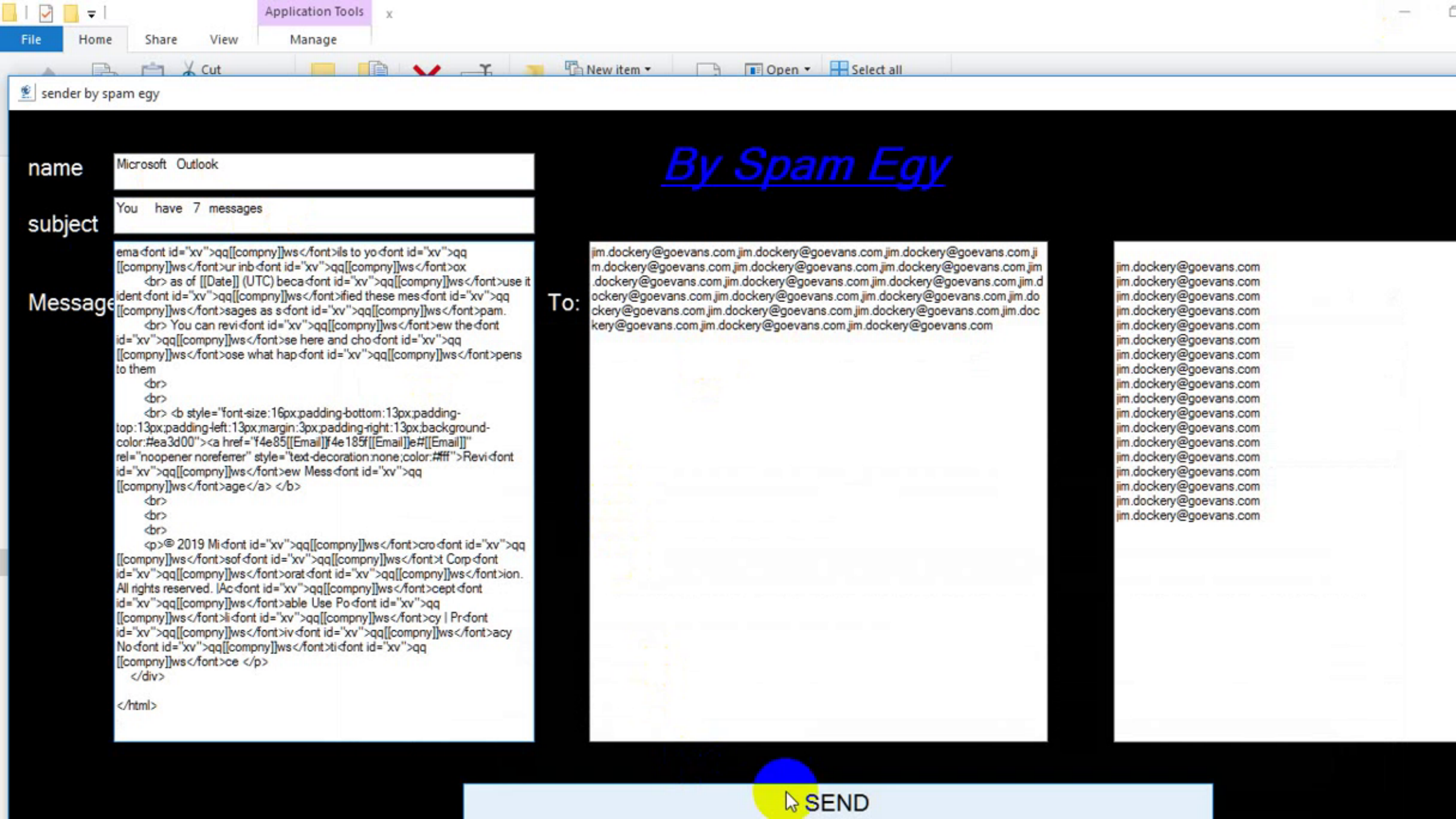
Activate Windows
Go to Settings to activate Windows.


BARNEYS NEWYORK
Outlook
Guerriero, Erica
Search Mail and People
New
Delete
Archive
Junk
Sweep
Move to
Categories
Undo
Try the new Outlook
Folders
Favorites
Sent Items
Drafts
Inbox 19
Deleted Items 21
Guerriero, Erica
Inbox 19
Drafts
Sent Items
Deleted Items 21
Archive
Conversation History
Junk Email
Notes 12
Inbox
Filter
Next: Play bag takedown at 7:30 AM
OFFICE 365
You've 7 Failed Messages 4:58 AM
*******This is an external e-mail message. Please do ...
You've 7 Failed Messages
OFFICE 365 <asegywdmotrkomemrkommemotrkomemotrkomemotrkomemotrkomemo
Reply all
Today, 4:58 AM
Guerriero, Erica
This message was sent with high importance.
Label: BNY 6 month Delete (6 months) Expires: 10/26/2019 4:58 AM
*******This is an external e-mail message. Please do not open links or attachments if you do not recognize the sender******
Message from Trusted server.
Office 365
Your mailbox is 96% full. Once your mailbox is full, you won't be able to send or receive email.
Clean up mailbox

SPAM-EGY Office 365 “True Login” Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	“True Login” $300	“Build&Crypt” Subscription			“Sender Inbox”			“Office 365 Page 2020” Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
✅ EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					


104.43.245.169
VIP72 Socks Client
All Proxies
My Proxies
Total: unlim* ; Used: 772 ; Expired: 04 June 2019 - 06:36:17
Socks5: 127.0.0.1:9951 ; http proxy: 127.
e-Campaign 12 Standard Edition, Single-User License
File Mailing Reports Tools Tracking Service Help
New Edit Clone Delete Preview Send Pause Schedule Accounts Lists Database
Mailing Job Size Modified Sender OK Failed Status
Welcome 44 KB 3/16/2017 ...
isac 3 KB 4/26/2019 ... OFFICE 365 <asegyw...
isac 9 KB 4/29/2019 ... OFFICE 365 <asegyw...
Test 470 B 4/26/2019 ... OFFICE 365 <asegyw... 1 0 00:00:03
isac 728 B 4/25/2019 ... saina ahky <mark.yasse... 2 0 Time Used: 00:00:03
isac 4 KB 4/29/2019 ... OFFICE 365 <asegyw... 2 0 00:00:03
7msg 4 KB 4/28/2019 ... saina ahky <mark.yasse... 2 0 00:00:02
isac 971 B 4/26/2019 ... Admin <ahmed.namd@... 5 0 Time Used: 00:00:16
Preview - HTML
Email Delivery Log
From OFFICE 365 <asegywdmotrkomemrkommemotrkomemotrkomemotrkomemotrkomemotrkomemotrkomemotrkomemotrkomemo
To {List} List (9 recipients)
Priority High
Subject You've 7 Failed Messages
Message from Trusted server.
Office 365
#3: Mail3.bmj (36 KB)
32-bit
Opera Browser
ubn
s
issssccaaaq
Send inbox by spam Egy
7msg-leo
vip72sock...
e-Campaign 12
0
747
isac_22
frisker
com


Application Tools
File
Home
Share
View
Manage
Cut
New item
Open
Select all
sender by spam egy
name
Microsoft Outlook
subject
You have 7 messages
Message
emaqq[[compny]]wsils to yoqq
[[compny]]wsur inbqq[[compny]]wsox

 as of [[Date]] (UTC) becaqq[[compny]]wsuse it
identqq[[compny]]wsified these mesqq
[[compny]]wssages as sqq[[compny]]wspam.

 You can reviqq[[compny]]wsew theqq[[compny]]wsse here and choqq
[[compny]]wsose what hapqq[[compny]]wspens
to them

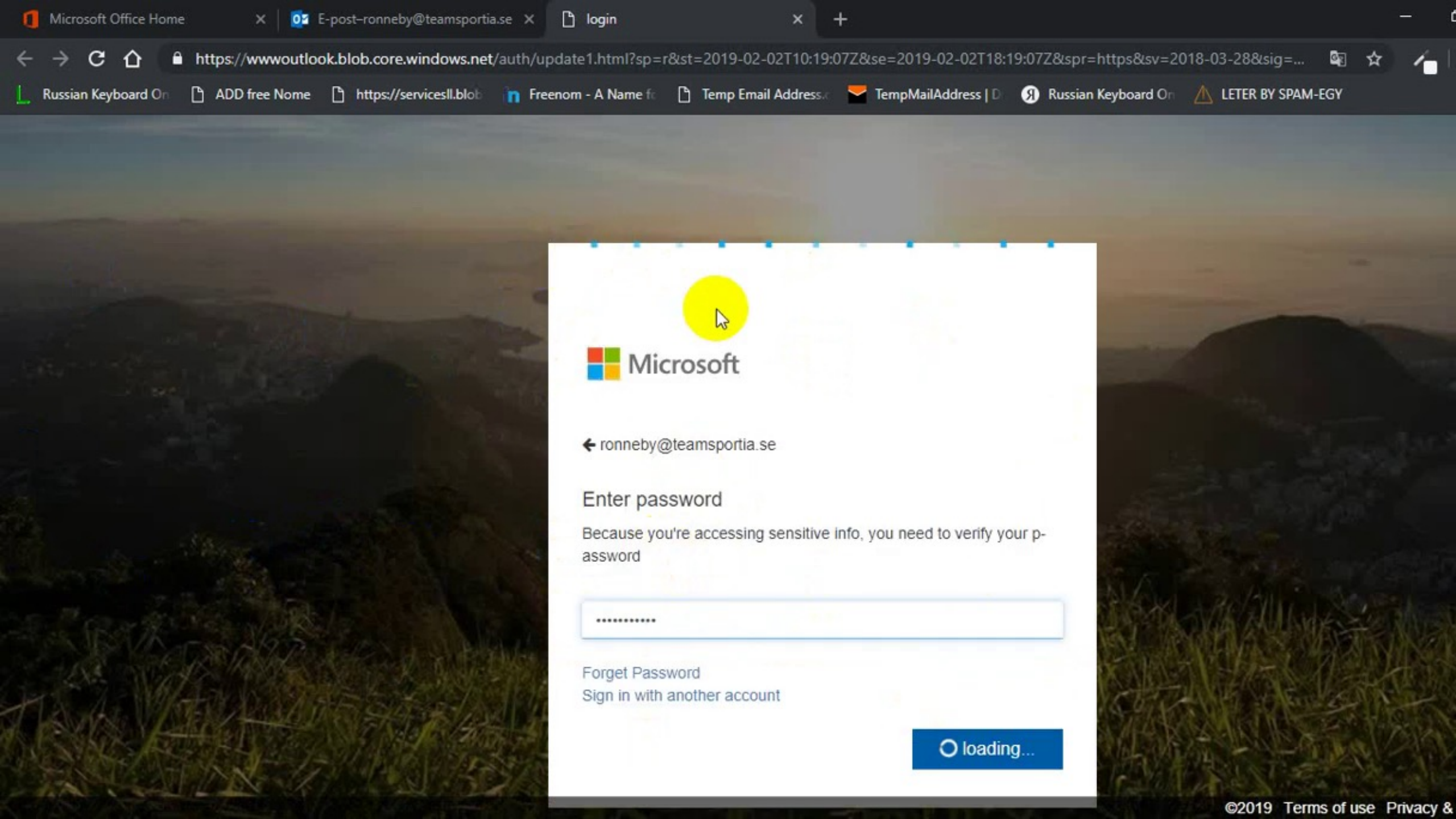
 <b style="font-size:16px;padding-bottom:13px;padding-
top:13px;padding-left:13px;margin:3px;padding-right:13px;background-
color:#ea3d00"><a href="f4e85[[Email]]f4e185f[[Email]]e#[[Email]]"
rel="noopener noreferrer" style="text-decoration:none;color:#fff">Reviqq[[compny]]wsew Messqq
[[compny]]wsage

© 2019 Miqq[[compny]]wscroqq
[[compny]]wssofqq[[compny]]wst Corpqq[[compny]]wsoratqq[[compny]]wsion.
All rights reserved. |Acqq[[compny]]wsceptqq[[compny]]wsable Use Poqq
[[compny]]wsliqq[[compny]]wscy | Prqq[[compny]]wsivqq[[compny]]wsacy
Noqq[[compny]]wstiqq
[[compny]]wsce

</html>
By Spam Egy
To:
jim.dockery@goevans.com,jim.dockery@goevans.com,jim.dockery@goevans.com,

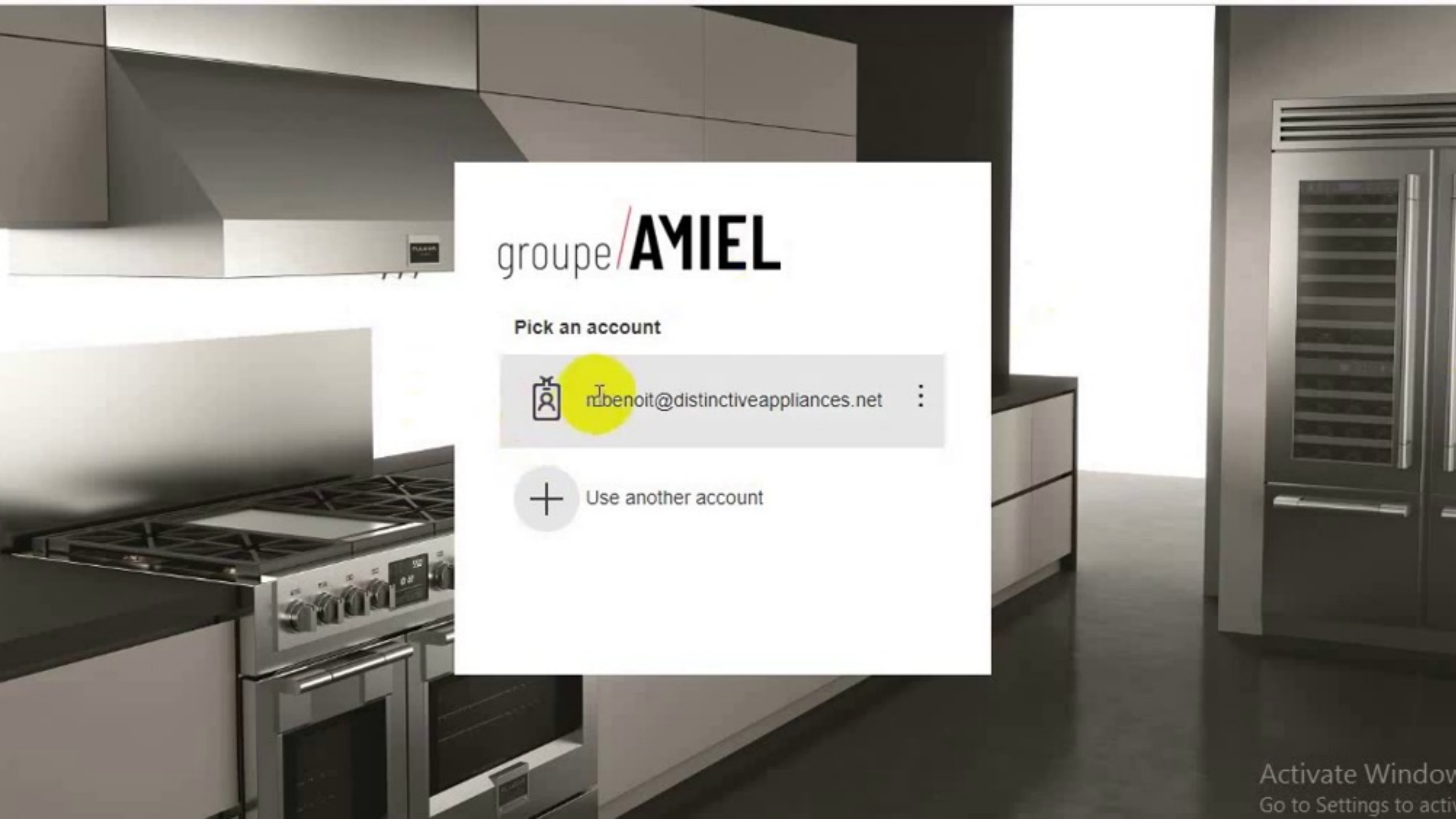
SPAM-EGY Office 365 “True Login” Release History

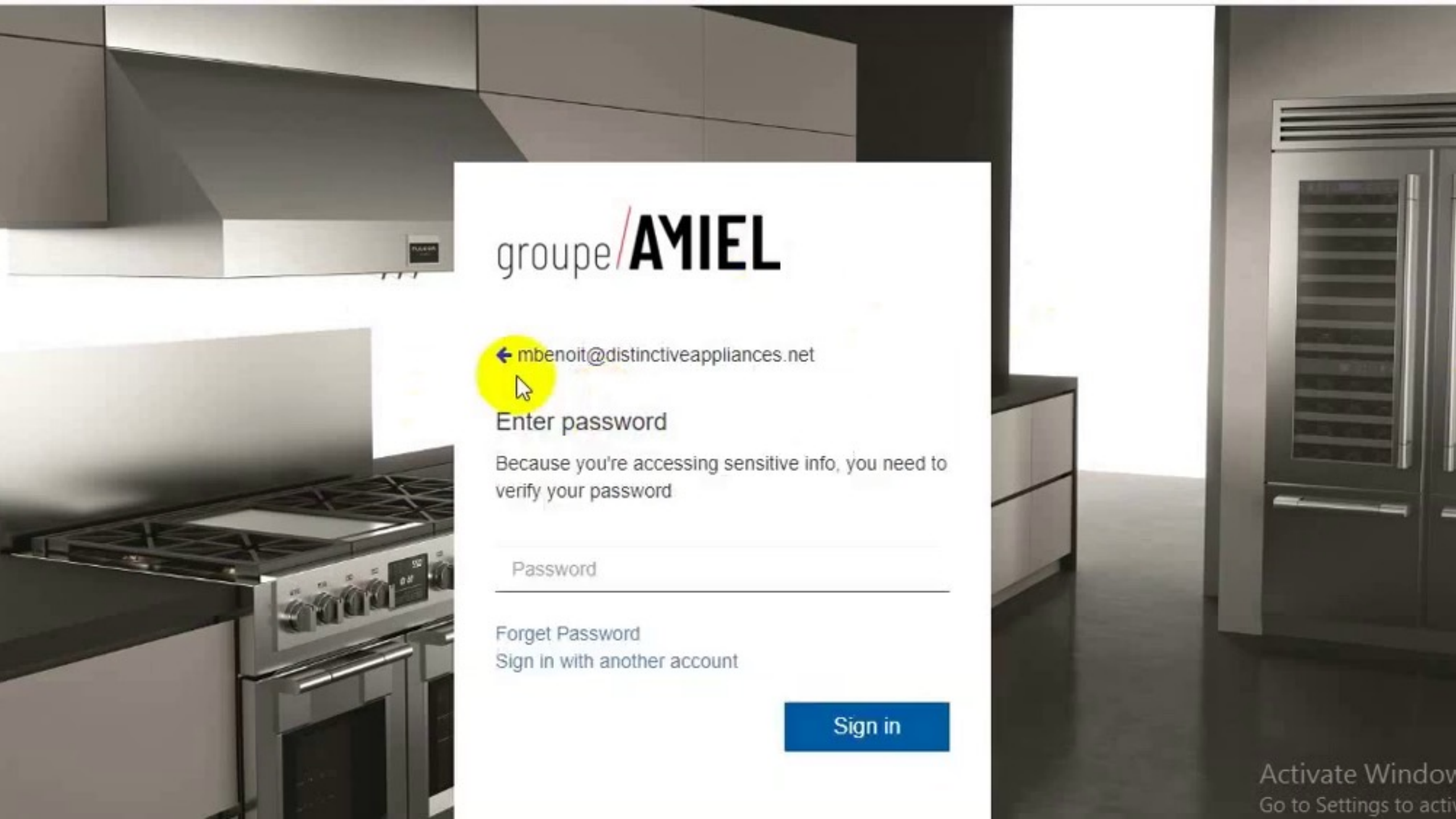
	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	“True Login” $300	“Build&Crypt” Subscription			“Sender Inbox”			“Office 365 Page 2020” Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					


Microsoft Office Home
E-post–ronneby@teamsportia.se
login
https://wwwoutlook.blob.core.windows.net/auth/update1.html?sp=r&st=2019-02-02T10:19:07Z&se=2019-02-02T18:19:07Z&spr=https&sv=2018-03-28&sig=...
Russian Keyboard On
ADD free Nome
https://servicesll.blob
Freenom - A Name fo
Temp Email Address
TempMailAddress | D
Russian Keyboard On
LETER BY SPAM-EGY
Microsoft
ronneby@teamsportia.se
Enter password
Because you're accessing sensitive info, you need to verify your p-assword
Forget Password
Sign in with another account
loading...
©2019 Terms of use Privacy &

SPAM-EGY Office 365 "True Login" Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					


groupe/AMIEL
Pick an account
rbenoit@distinctiveappliances.net
Use another account


groupe/AMIEL
mbenoit@distinctiveappliances.net
Enter password
Because you're accessing sensitive info, you need to verify your password
Password
Forget Password
Sign in with another account
Sign in
Activate Windov
Go to Settings to acti

SPAM-EGY Office 365 "True Login" Release History

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					

SPAM EGY

Office 365 page 2020 by spam egy

before start i need say this page not for sell

lets Go :D

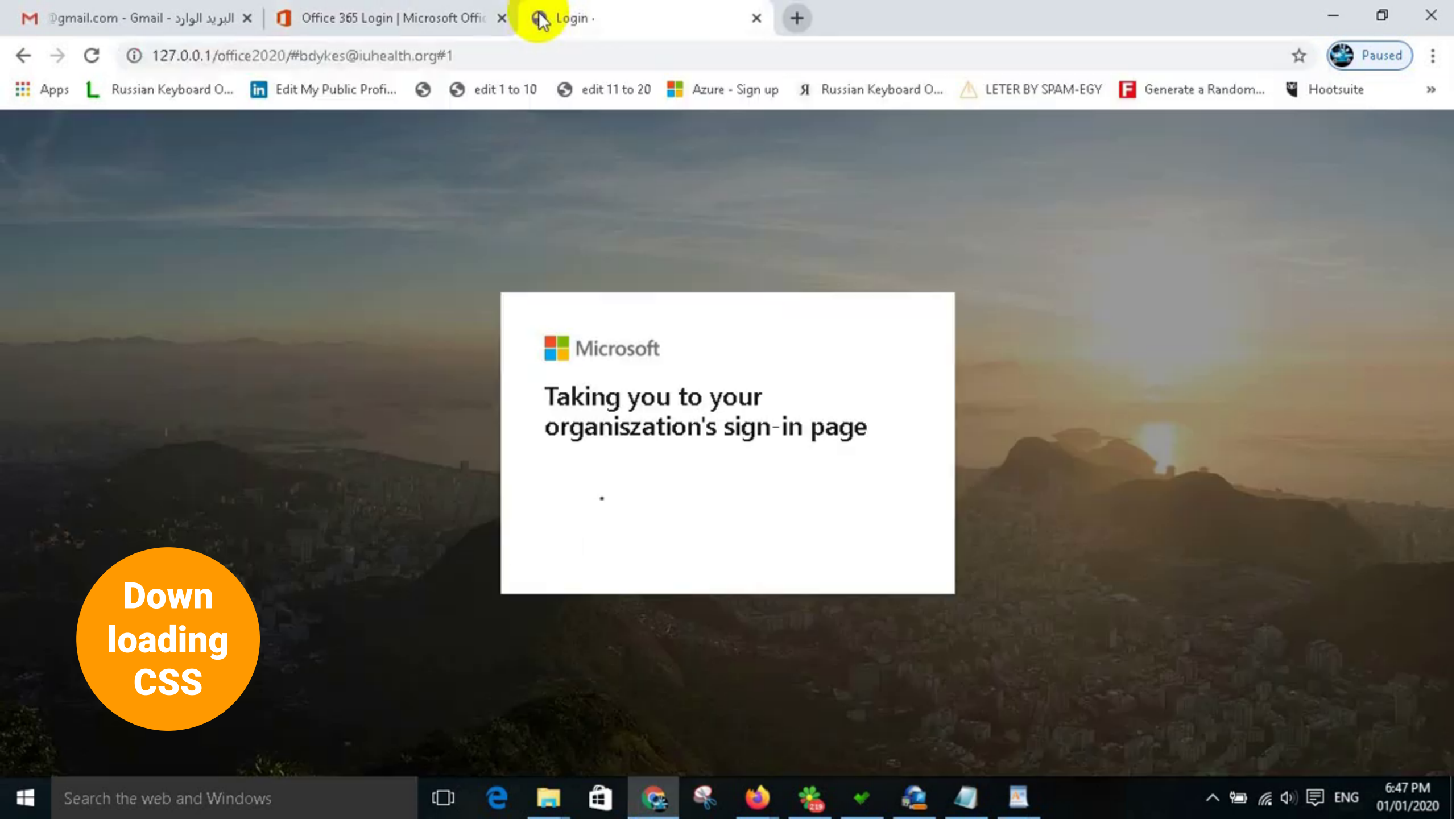
http://127.0.0.1/office2020/#adykes@iuhealth.org#1

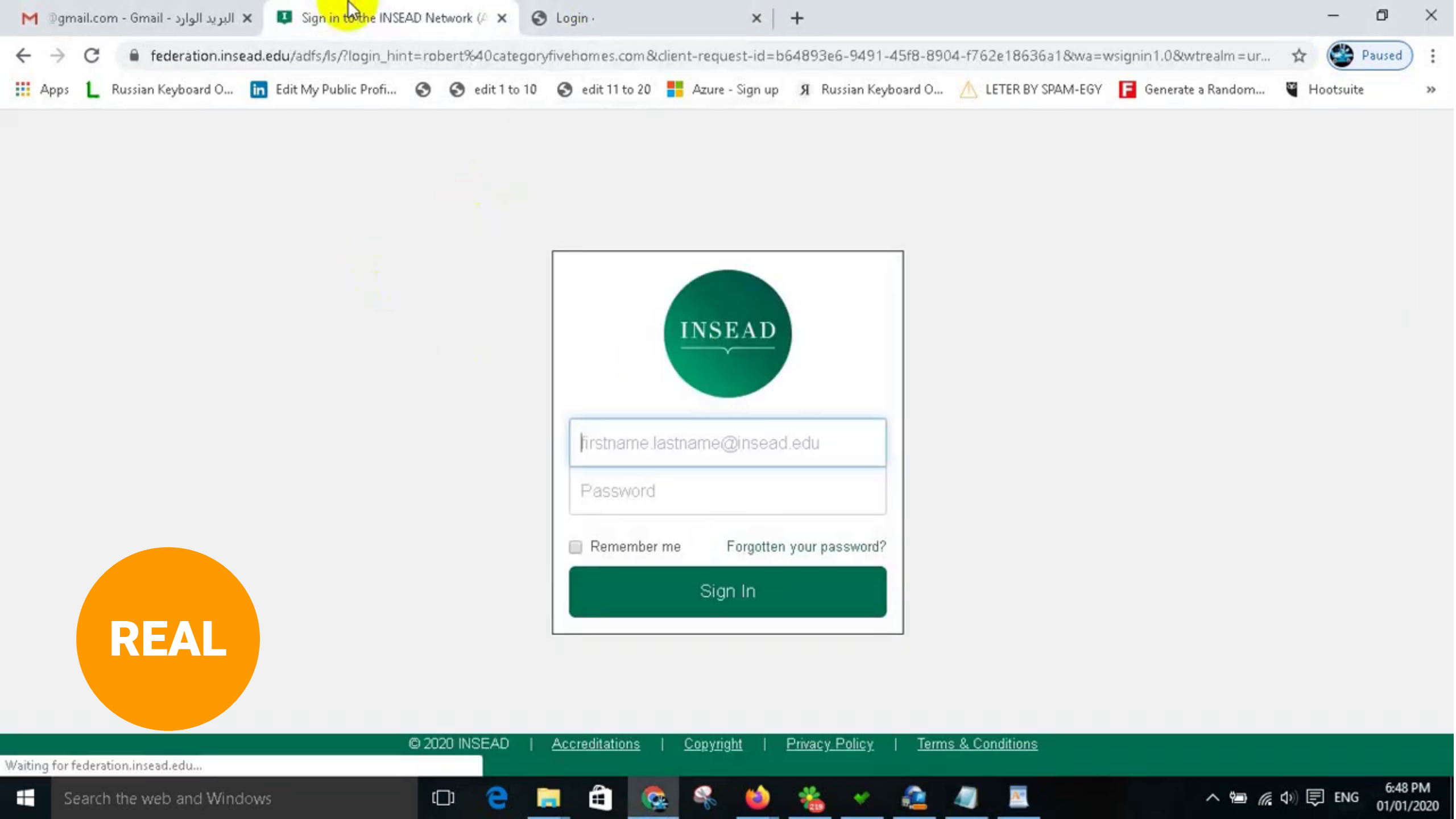
The page is advanced and smart

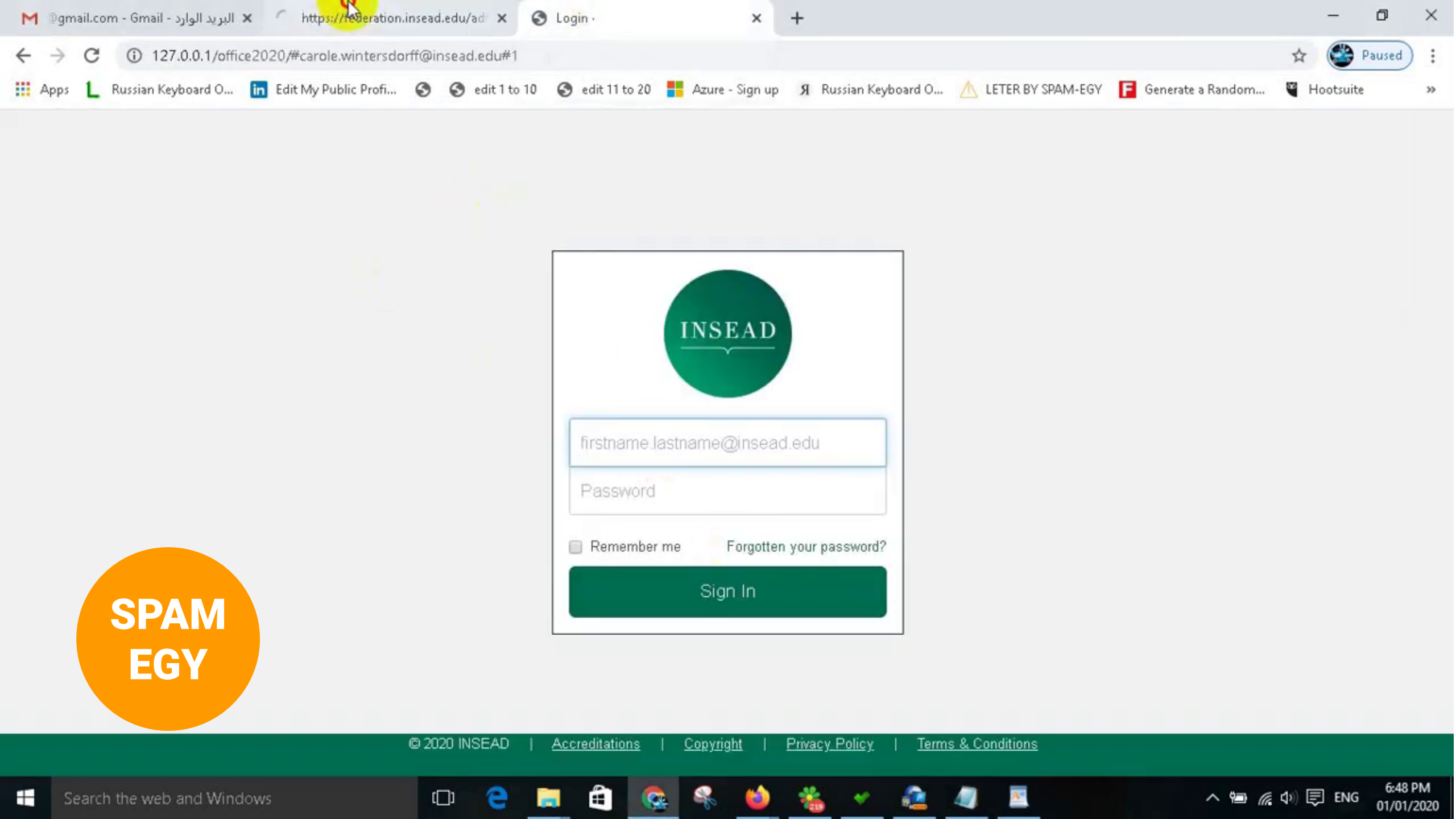
1- this page all lang

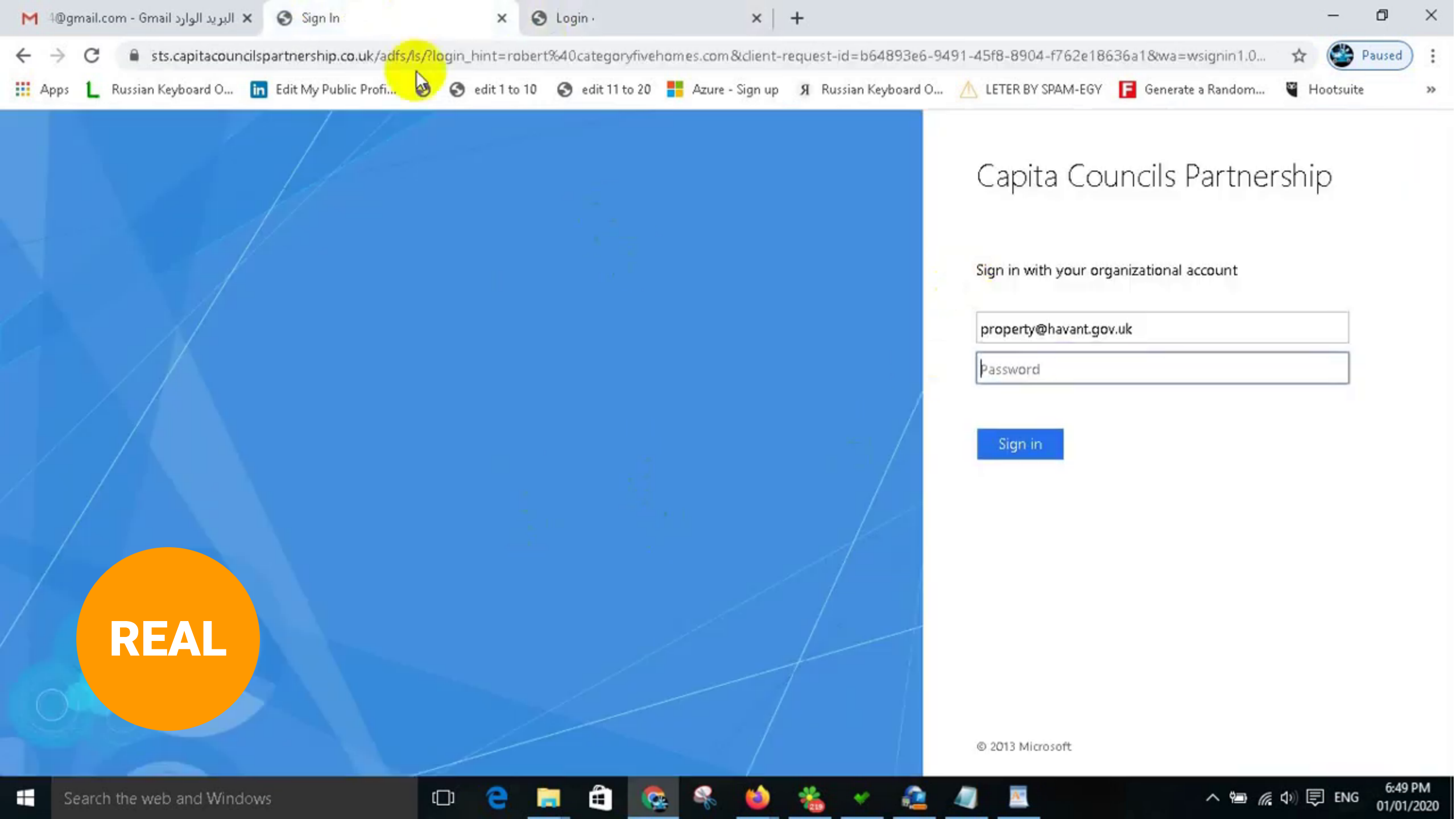
2-this page get same Real office login

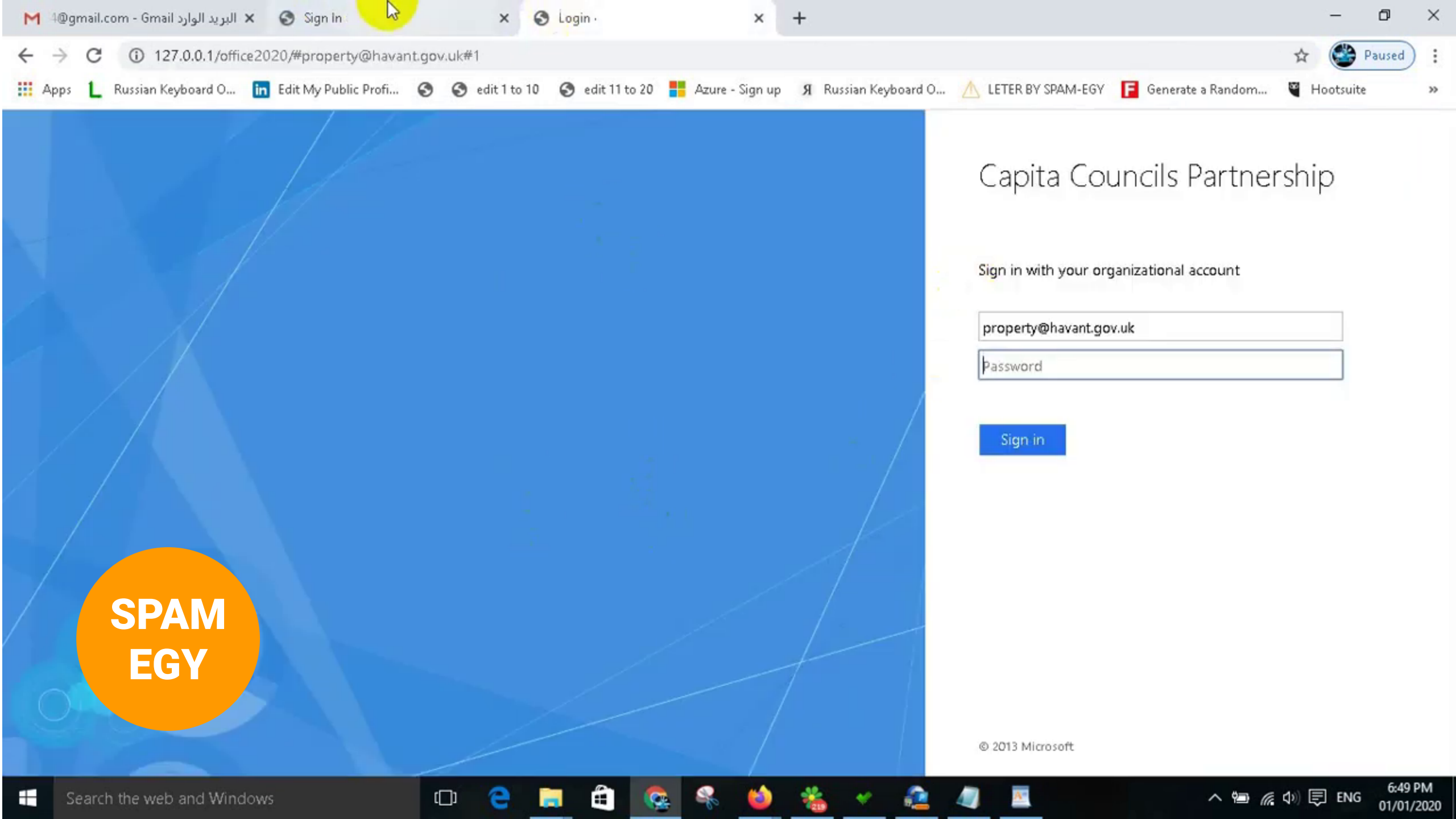
3-true login

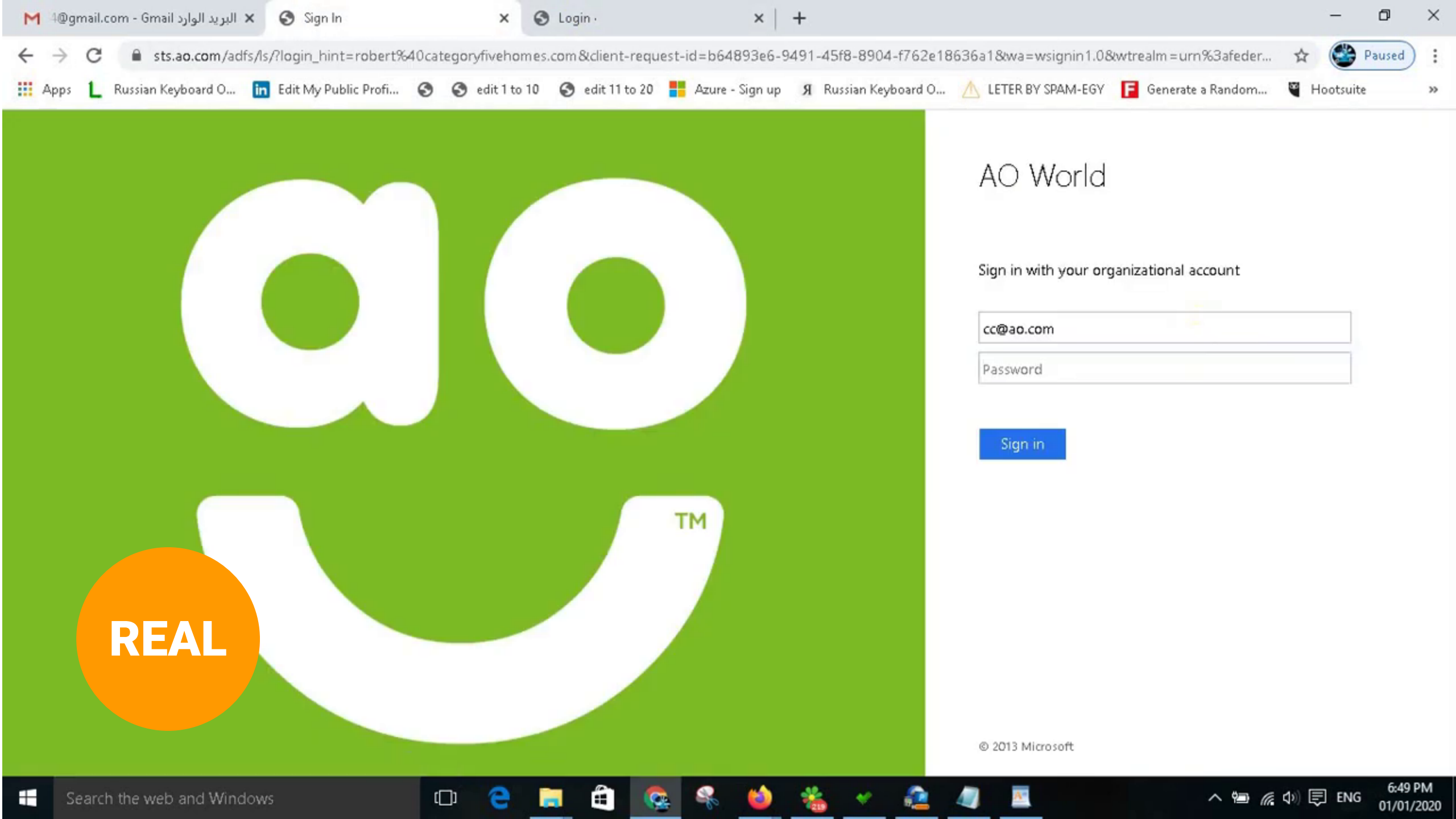

@gmail.com - Gmail - البريد الوارد
Office 365 Login | Microsoft Offic
Login
127.0.0.1/office2020/#bdykes@iuhealth.org#1
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
Microsoft
Taking you to your organiszation's sign-in page
Down loading CSS
Search the web and Windows
ENG
6:47 PM
01/01/2020

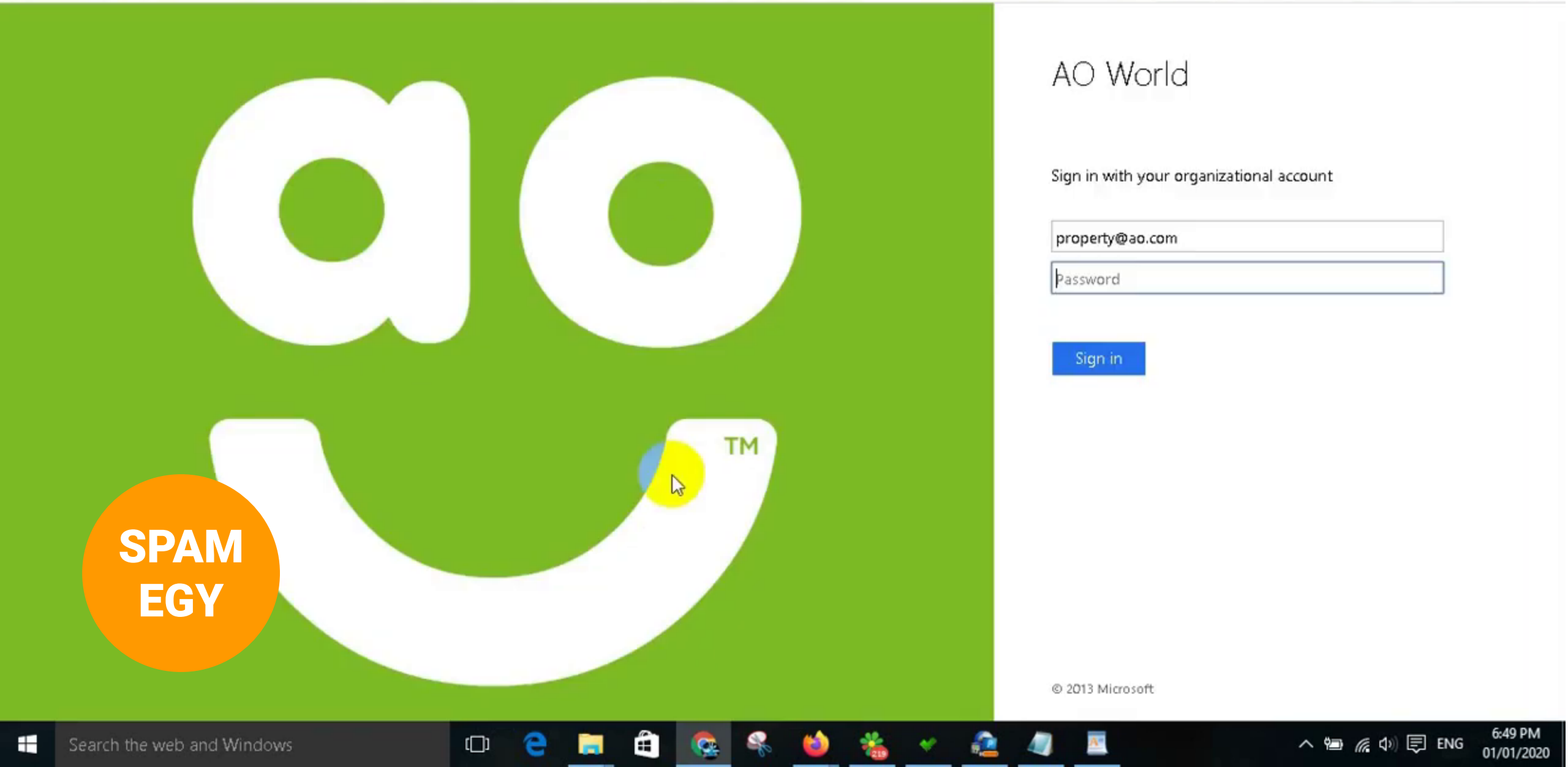

gmail.com - Gmail - البريد الوارد
Sign in to the INSEAD Network
Login
federation.insead.edu/adfs/ls/?login_hint=robert%40categoryfivehomes.com&client-request-id=b64893e6-9491-45f8-8904-f762e18636a1&wa=wsignin1.0&wtrealm=ur...
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
INSEAD
firstname.lastname@insead.edu
Password
Remember me
Forgotten your password?
Sign In
REAL
© 2020 INSEAD | Accreditations | Copyright | Privacy Policy | Terms & Conditions
Waiting for federation.insead.edu...
Search the web and Windows
ENG
6:48 PM
01/01/2020

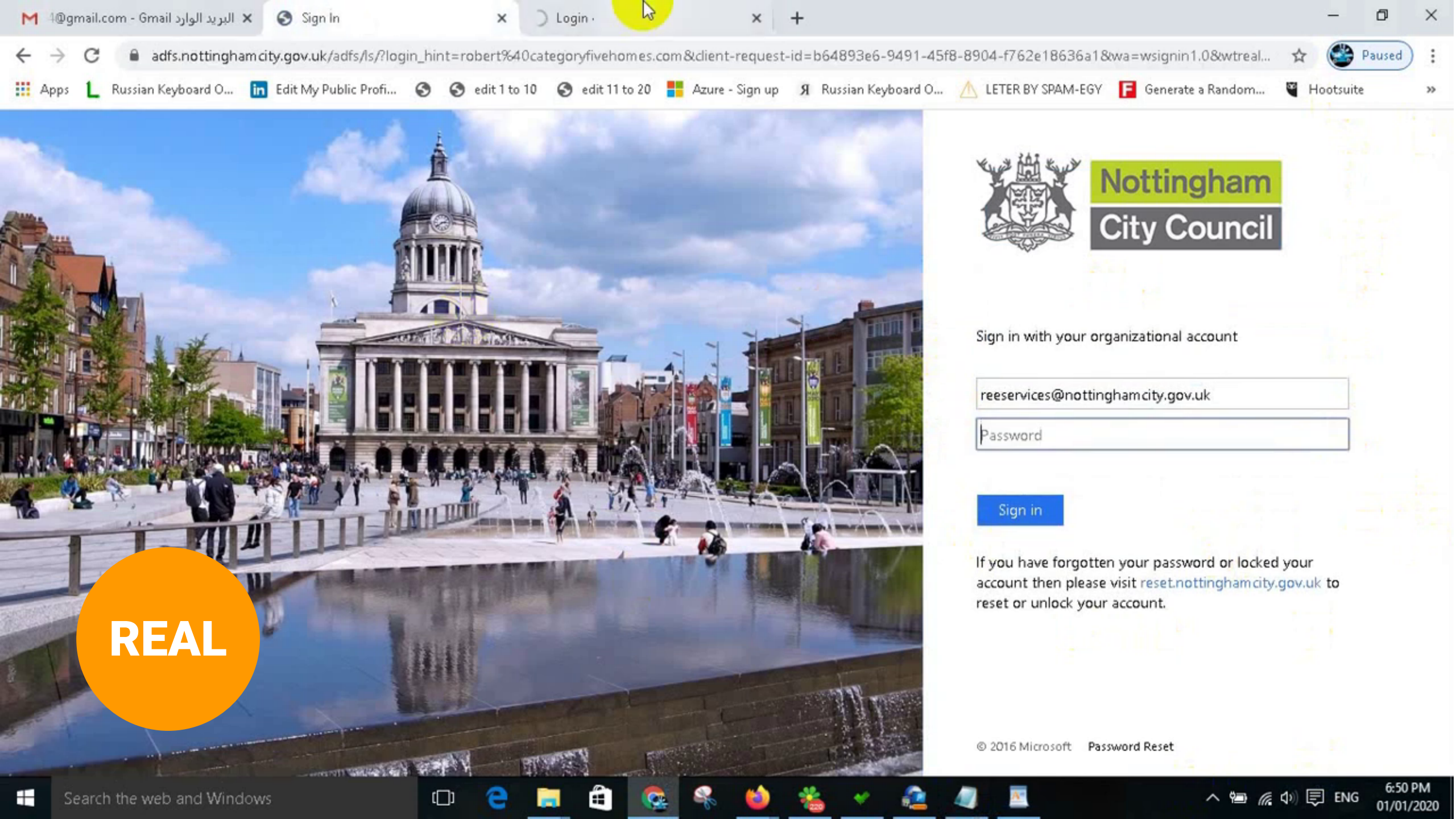

@gmail.com - Gmail - البريد الوارد
https://federation.insead.edu/ad
Login
127.0.0.1/office2020/#carole.wintersdorff@insead.edu#1
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
INSEAD
firstname.lastname@insead.edu
Password
Remember me
Forgotten your password?
Sign In
SPAM EGY
© 2020 INSEAD | Accreditations | Copyright | Privacy Policy | Terms & Conditions
Search the web and Windows
ENG
6:48 PM
01/01/2020


4@gmail.com - Gmail البريد الوارد
Sign In
Login ·
sts.capitacouncilspartnership.co.uk/adfs/ls/?login_hint=robert%40categoryfivehomes.com&client-request-id=b64893e6-9491-45f8-8904-f762e18636a1&wa=wsignin1.0...
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
REAL
Capita Councils Partnership
Sign in with your organizational account
property@havant.gov.uk
Password
Sign in
© 2013 Microsoft
Search the web and Windows
ENG
6:49 PM
01/01/2020


@gmail.com - Gmail البريد الوارد
Sign In
Login
127.0.0.1/office2020/#property@havant.gov.uk#1
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
Capita Councils Partnership
Sign in with your organizational account
property@havant.gov.uk
Password
Sign in
© 2013 Microsoft
SPAM EGY
Search the web and Windows
ENG
6:49 PM
01/01/2020


4@gmail.com - Gmail البريد الوارد
Sign In
Login ·
sts.ao.com/adfs/ls/?login_hint=robert%40categoryfivehomes.com&client-request-id=b64893e6-9491-45f8-8904-f762e18636a1&wa=wsignin1.0&wtrealm=urn%3afeder...
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
TM
REAL
AO World
Sign in with your organizational account
cc@ao.com
Password
Sign in
© 2013 Microsoft
Search the web and Windows
ENG
6:49 PM
01/01/2020


@gmail.com - Gmail البريد الوارد
Sign in to your account
Login ·
127.0.0.1/office2020/#property@ao.com#1
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
AO World
Sign in with your organizational account
property@ao.com
Password
Sign in
© 2013 Microsoft
SPAM EGY
Search the web and Windows
ENG
6:49 PM
01/01/2020


4@gmail.com - Gmail البريد الوارد
Sign In
Login ·
adfs.nottinghamcity.gov.uk/adfs/ls/?login_hint=robert%40categoryfivehomes.com&client-request-id=b64893e6-9491-45f8-8904-f762e18636a1&wa=wsignin1.0&wtreal...
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite
REAL
Nottingham City Council
Sign in with your organizational account
reeservices@nottinghamcity.gov.uk
Password
Sign in
If you have forgotten your password or locked your account then please visit reset.nottinghamcity.gov.uk to reset or unlock your account.
© 2016 Microsoft
Password Reset
Search the web and Windows
ENG
6:50 PM
01/01/2020

4@gmail.com - Gmail البريد الوارد
Sign in to your account
Login
127.0.0.1/office2020/#proreeservices@nottinghamcity.gov.uk#1
Paused
Apps
Russian Keyboard O...
Edit My Public Profi...
edit 1 to 10
edit 11 to 20
Azure - Sign up
Russian Keyboard O...
LETER BY SPAM-EGY
Generate a Random...
Hootsuite

Nottingham City Council

Sign in with your organizational account

proreeservices@nottinghamcity.gov.uk

Password

Sign in

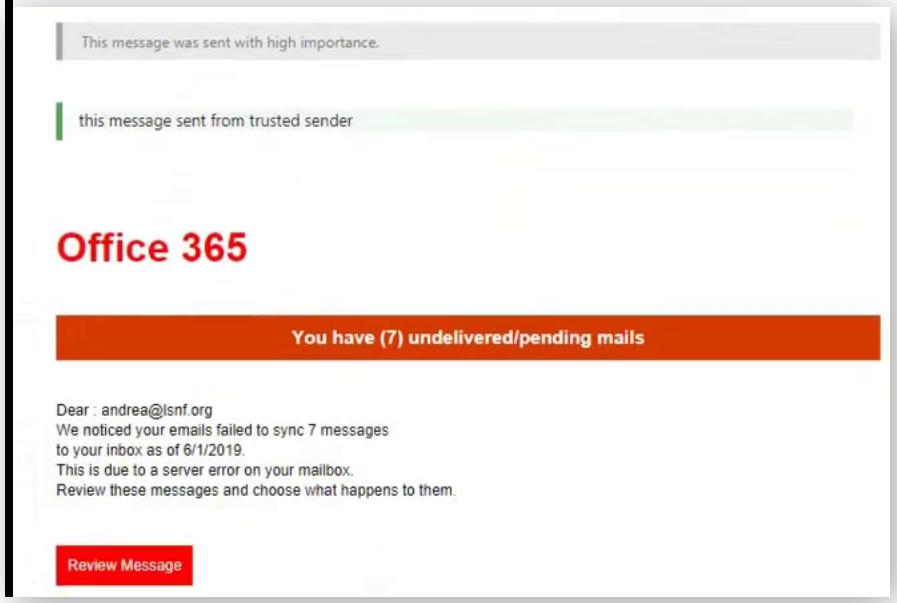
If you have forgotten your password or locked your account then please visit reset.nottinghamcity.gov.uk to reset or unlock your account.

© 2016 Microsoft Password Reset

Search the web and Windows
ENG
6:50 PM
01/01/2020

Evolution of an Attack

Oct 2018 | Jan 2019 | Feb 2019 | Apr 2019 | May 2019 | Jun 2019 | Aug 2019 | Jan 2020



This message was sent with high importance.

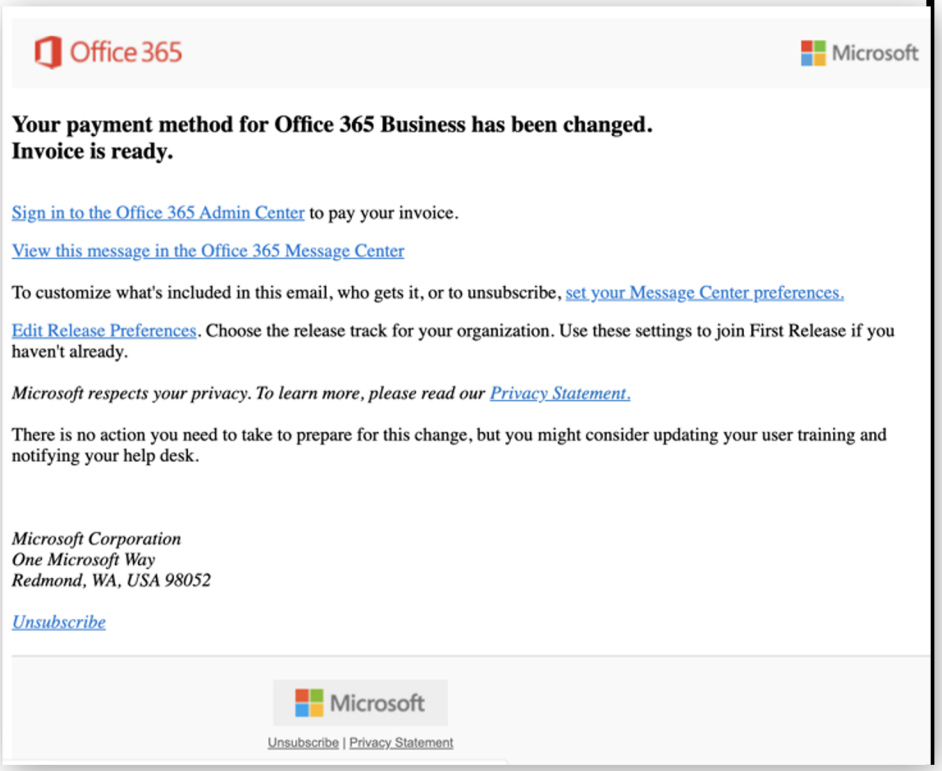
this message sent from trusted sender

Office 365

You have (7) undelivered/pending mails

Dear : andrea@lsnf.org
We noticed your emails failed to sync 7 messages
to your inbox as of 6/1/2019.
This is due to a server error on your mailbox.
Review these messages and choose what happens to them.

Review Message



Office 365 Microsoft

Your payment method for Office 365 Business has been changed.
Invoice is ready.

Sign in to the Office 365 Admin Center to pay your invoice.

View this message in the Office 365 Message Center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message Center preferences.

Edit Release Preferences. Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

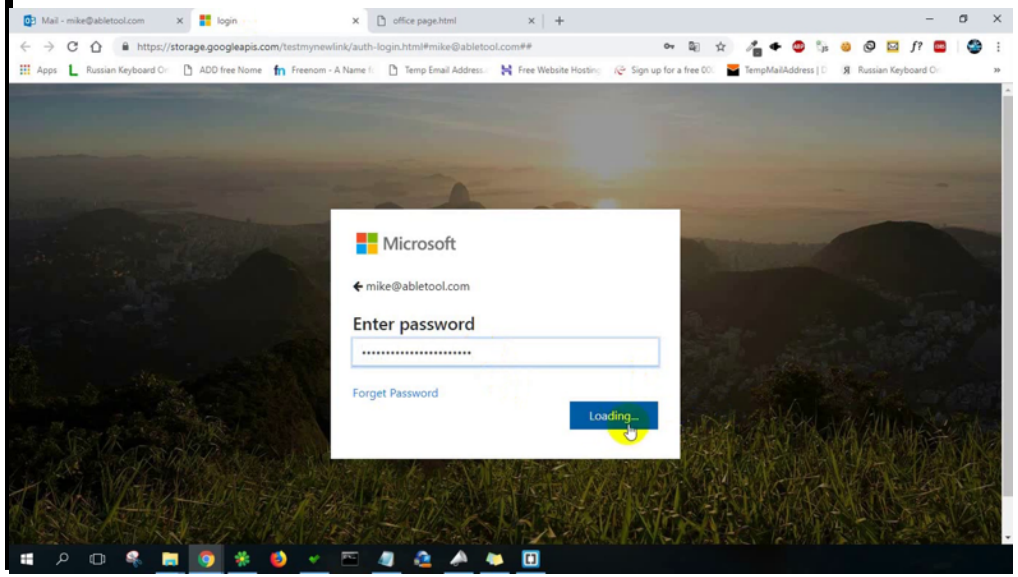
Unsubscribe

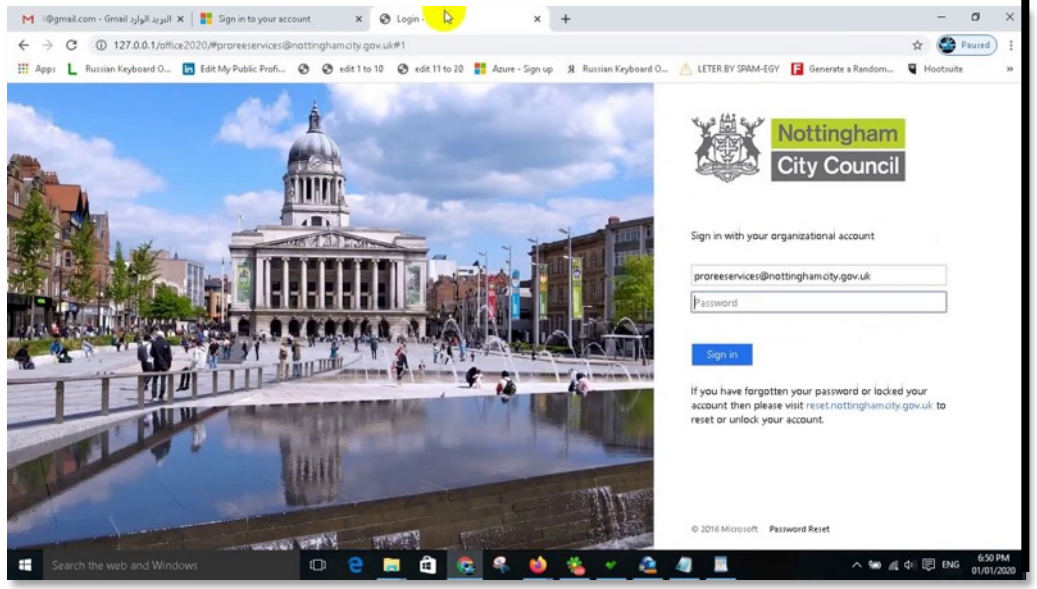
Microsoft

Unsubscribe | Privacy Statement

Evolution of an Attack

Oct 2018 Jan 2019 Feb 2019 Apr 2019 May 2019 Jun 2019 Aug 2019 Jan 2020



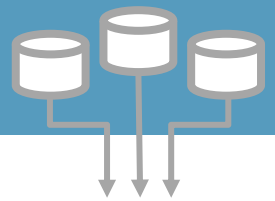


SPAM-EGY Office 365 "True Login" Release History

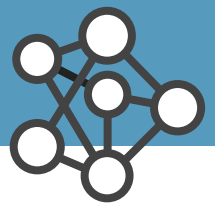
	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					

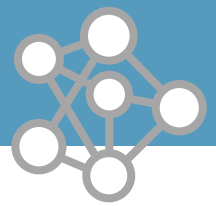
Most 5-Star Ratings
as reviewed by customers

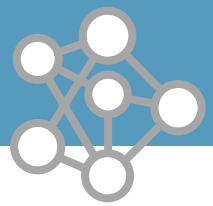
AVANAN

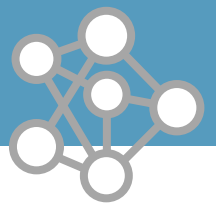

Known Threat Feeds

File and URL Sandboxing Tools


Office 365 | G Suite Indicators of Attack


Customer Specific Internal/BEC ML


Customer Specific False Positive ML


Customer Specific SaaS Events

	Oct 2018	Jan 2019	Feb 2019	Apr 2019	May 2019	Jun 2019	Aug 2019	Jan 2020
	"True Login" $300	"Build&Crypt" Subscription			"Sender Inbox"			"Office 365 Page 2020" Not For Sale
EOP					▶Sender Bot			
ATP		▶ZeroFont	▶	▶BaseStriker	▶ZeroFont.v2	▶	▶CiteUnseen	
EMAIL	▶Office Alert	▶HaaS						
WEB	▶Email Autofill		▶Animation			▶Real Logo and Background		▶Auto Customization
LOGIN	▶Validator		▶Remote Attack and Logoff					

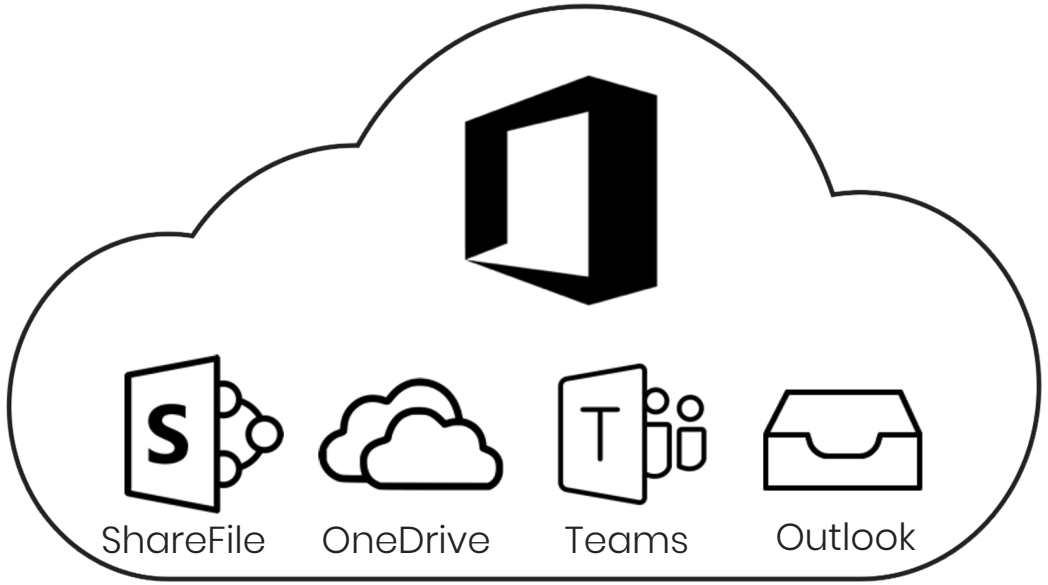
Gartner peerinsights customers' choice™

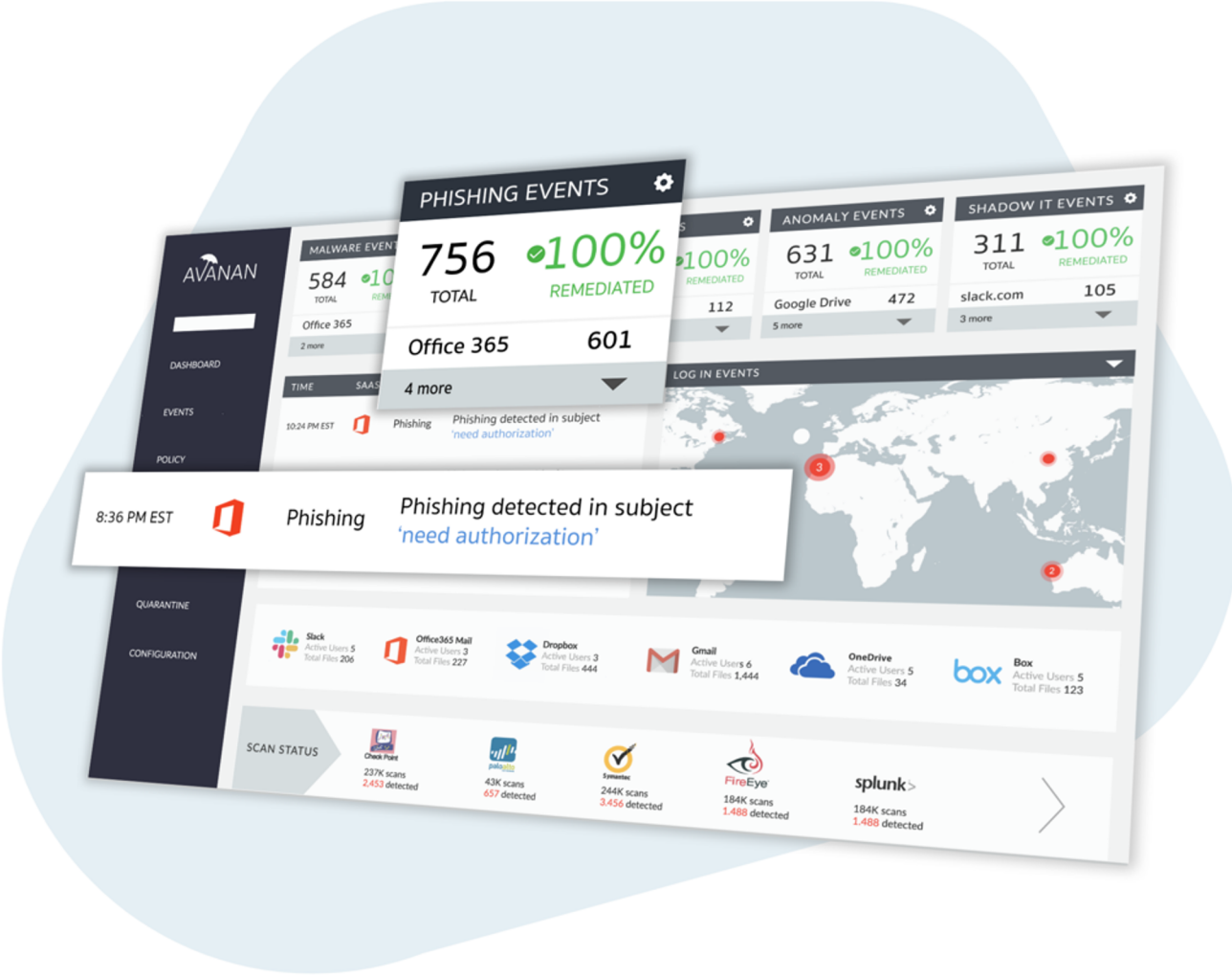
Best Email Security

as reviewed by customers

AVANAN

Protects the Entire Suite
Not just Email





Gartner peerinsights customers' choice™

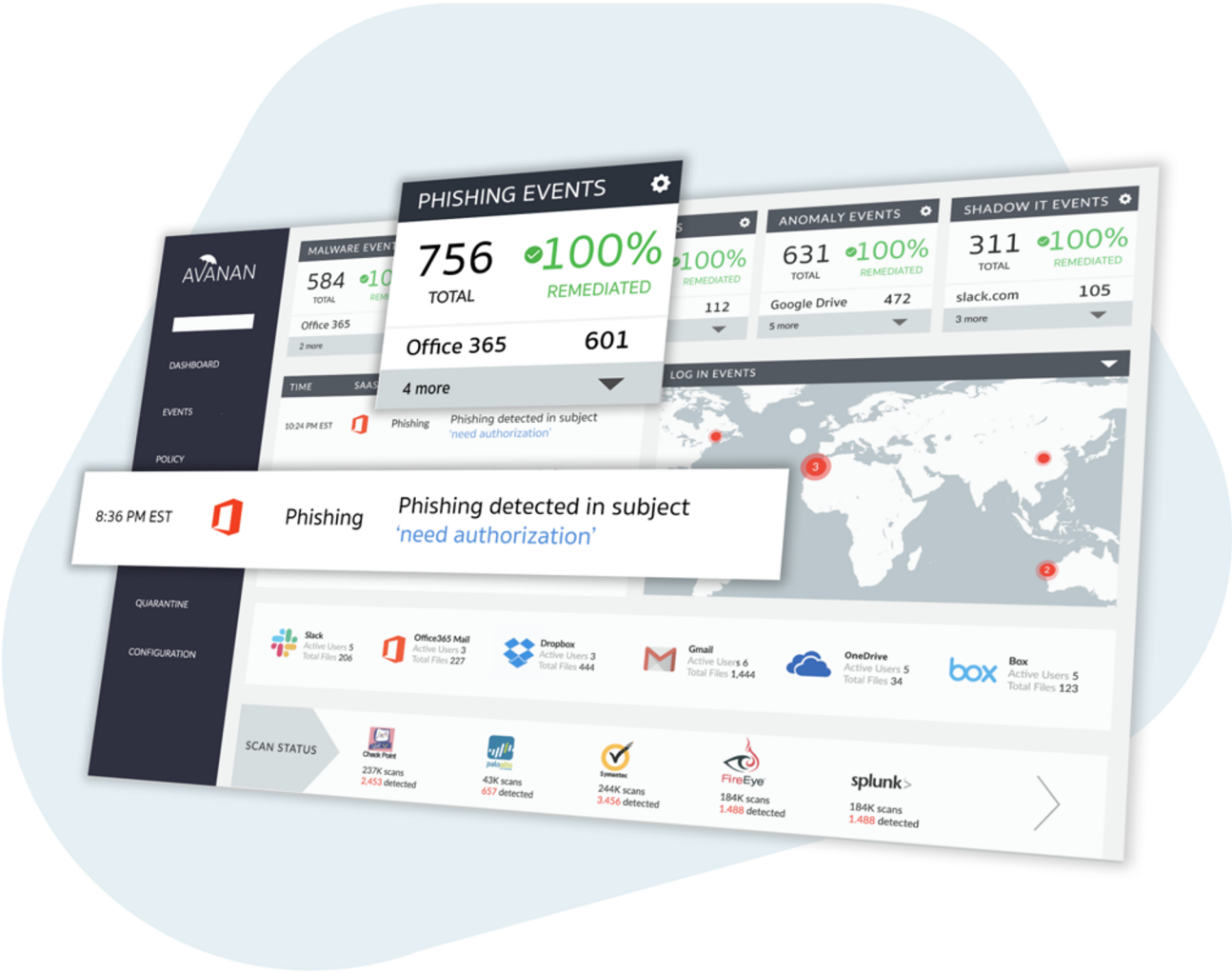
Best Email Security

as reviewed by customers

AVANAN

Has a SPAM-EGY customer visited your inbox? Request a free trial.

avanan.com/spam-egy



Gartner peerinsights customers' choice™

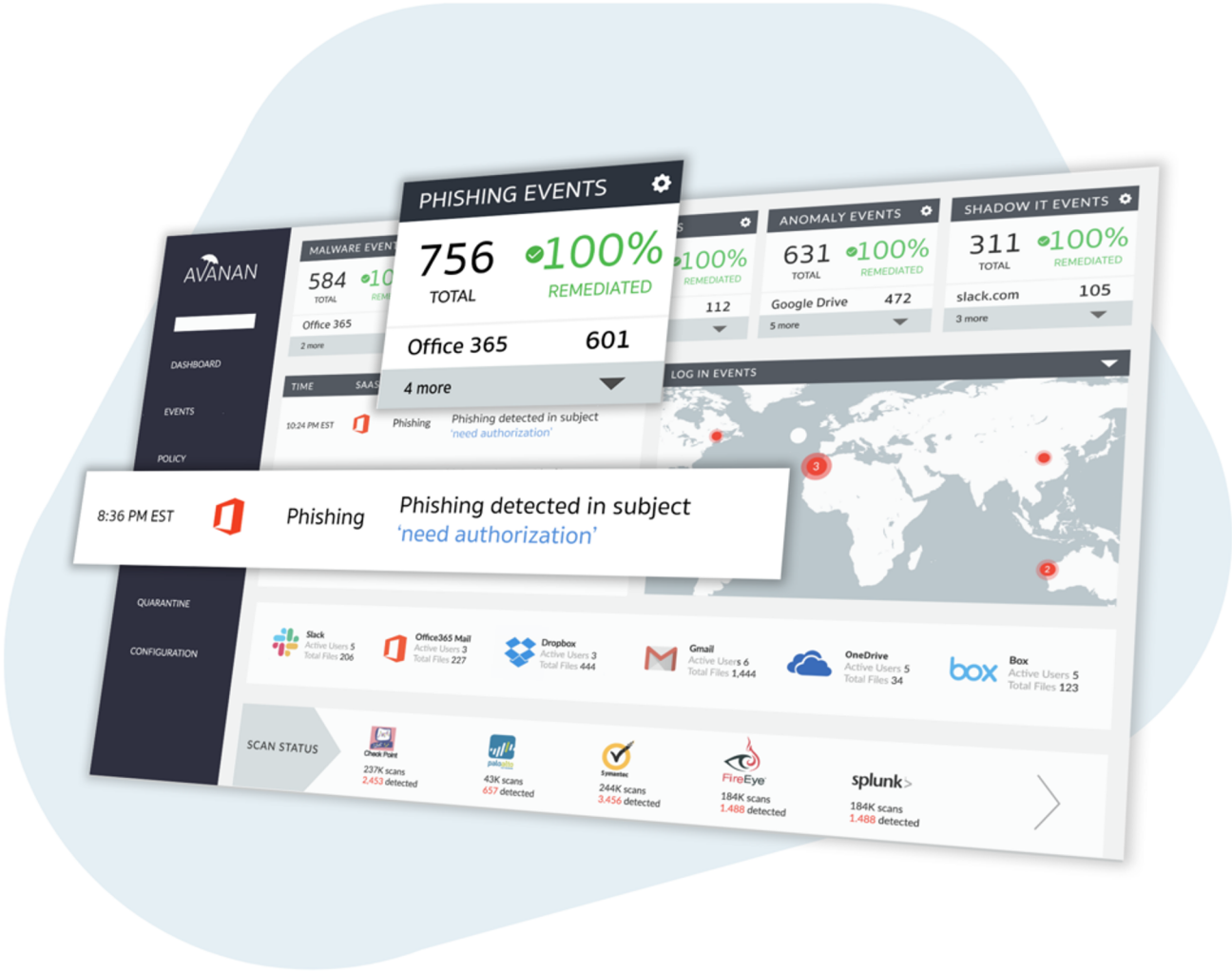
Best Email Security

as reviewed by customers

AVANAN

Request a free trial.

avanan.com/spam-egy



Michael Landewe

Co-Founder, Chief Privacy Officer

michael@avanan.com