Sun City Computer Club

Cyber Security SIG

September 2, 2021

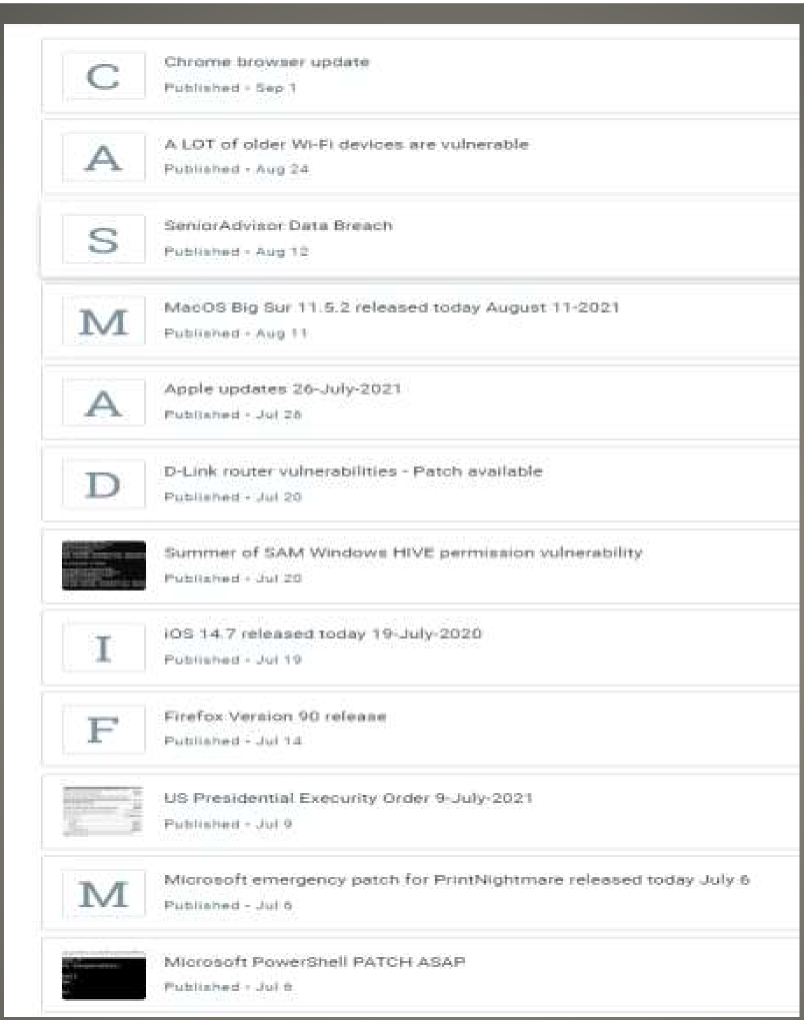
Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law



Chrome browser update
Published - Sep 1

A LOT of older Wi-Fi devices are vulnerable
Published - Aug 24

SeniorAdvisor Data Breach
Published - Aug 12

MacOS Big Sur 11.5.2 released today August 11-2021
Published - Aug 11

Apple updates 26-July-2021
Published - Jul 26

D-Link router vulnerabilities - Patch available
Published - Jul 20

Summer of SAM Windows HIVE permission vulnerability
Published - Jul 20

iOS 14.7 released today 19-July-2020
Published - Jul 19

Firefox Version 90 release
Published - Jul 14

US Presidential Execurity Order 9-July-2021
Published - Jul 9

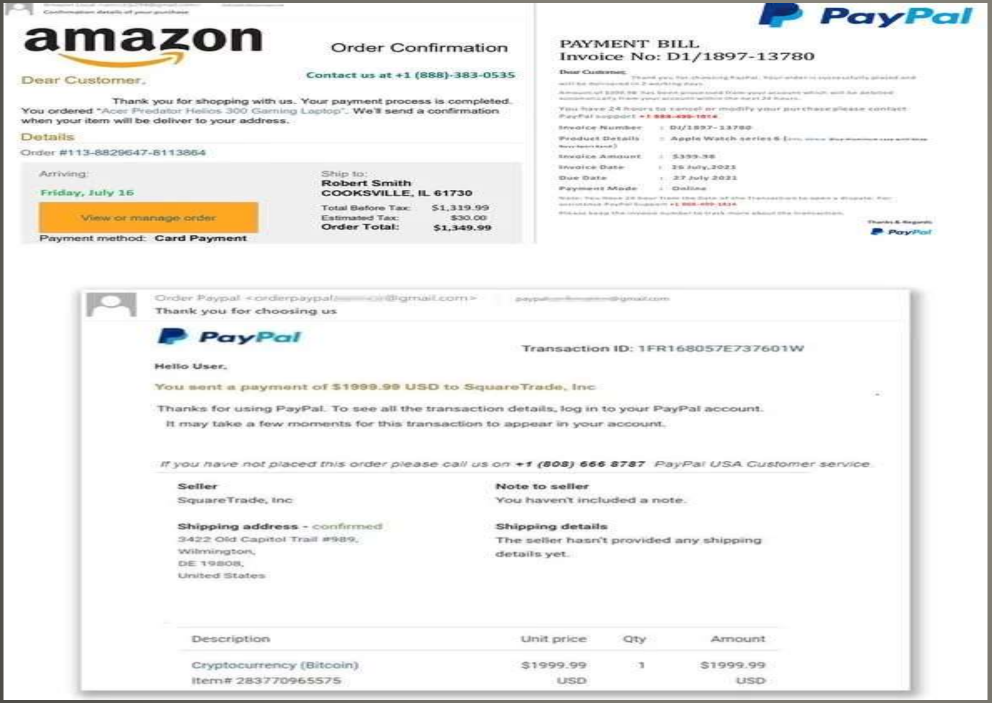
Microsoft emergency patch for PrintNightmare released today July 6
Published - Jul 6

Microsoft PowerShell PATCH ASAP
Published - Jul 6

News Archive

Current Issues

- Making the news - again
- Convincing eMails, SMS, popups



[illegible]

Confirmation details of your purchase

amazon

Order Confirmation

Contact us at +1 (888)-383-0535

Dear Customer,

Thank you for shopping with us. Your payment process is completed. You ordered "Acer Predator Helios 300 Gaming Laptop". We'll send a confirmation when your item will be deliver to your address.

Details

Order #113-8829647-6113864

Arriving:

Friday, July 16

View or manage order

Payment method: Card Payment

Ship to:
Robert Smith
COOKSVILLE, IL 61730

Total Before Tax:	$1,319.99
Estimated Tax:	$30.00
Order Total:	**$1,349.99**

PayPal

PAYMENT BILL
Invoice No: D1/1897-13780

Dear Customer,

Thank you for choosing PayPal. Your order is successfully placed and will be delivered in 2 working days.

Amount of $399.98 has been processed from your account which will be debited automatically from your account within the next 24 hours.

You have 24 hours to cancel or modify your purchase please contact PayPal support +1 888-499-1814

Invoice Number	: D1/1897-13780
Product Details	: Apple Watch series 6 ([illegible])
Invoice Amount	: $399.38
Invoice Date	: 26 July,2021
Due Date	: 27 July 2021
Payment Mode	: Online

Note: You have 24 hour from the Date of the Transaction to open a dispute. For assistance PayPal Support +1 888-499-1814

Please keep the invoice number to track more about the transaction.

Thanks & Regards

PayPal

Order Paypal <orderpaypal[redacted]@gmail.com> paypal[redacted]@gmail.com

Thank you for choosing us

PayPal

Transaction ID: 1FR168057E737601W

Hello User,

You sent a payment of $1999.99 USD to SquareTrade, Inc

Thanks for using PayPal. To see all the transaction details, log in to your PayPal account.
It may take a few moments for this transaction to appear in your account.

*If you have not placed this order please call us on **+1 (808) 666 8787** PayPal USA Customer service*

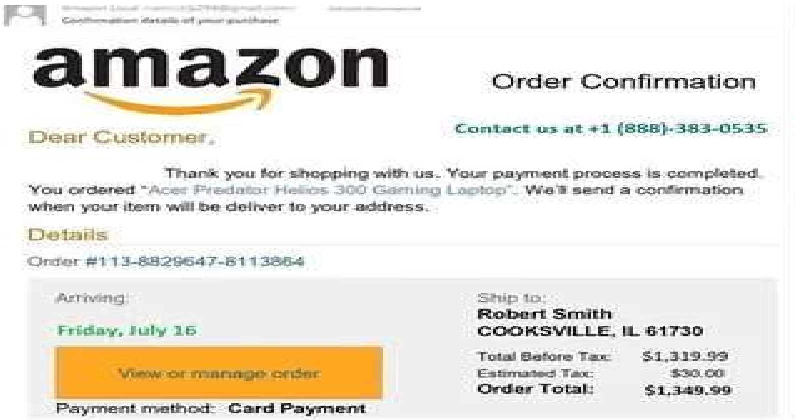
Seller
SquareTrade, Inc

Note to seller
You haven't included a note.

Shipping address - confirmed
3422 Old Capitol Trail #989,
Wilmington,
DE 19808,
United States

Shipping details
The seller hasn't provided any shipping details yet.

Description	Unit price	Qty	Amount
Cryptocurrency (Bitcoin) Item# 283770965575	$1999.99 USD	1	$1999.99 USD



[illegible] <[illegible]@gmail.com>

Confirmation details of your purchase

Order Confirmation

Dear Customer,

Contact us at +1 (888)-383-0535

Thank you for shopping with us. Your payment process is completed. You ordered "Acer Predator Helios 300 Gaming Laptop". We'll send a confirmation when your item will be deliver to your address.

Details

Order #113-8829647-8113864

Arriving:

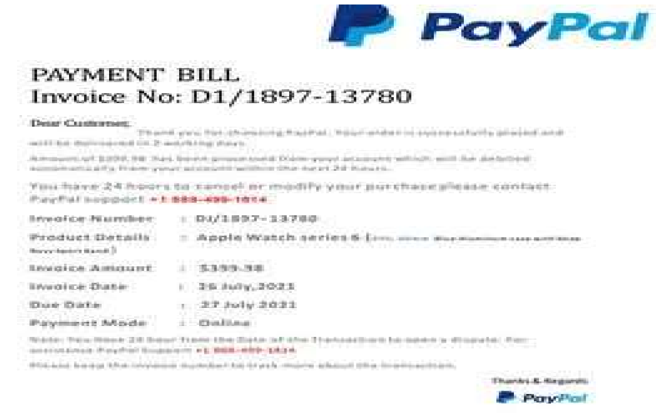
Friday, July 16

View or manage order

Payment method: Card Payment

Ship to:
Robert Smith
COOKSVILLE, IL 61730

Total Before Tax:	$1,319.99
Estimated Tax:	$30.00
Order Total:	$1,349.99



PAYMENT BILL
Invoice No: D1/1897-13780

Dear Customer,

Thank you for choosing PayPal. Your order is successfully placed and will be delivered in 2 working days.

Amount of $399.98 has been processed from your account which will be debited automatically from your account within the next 24 hours.

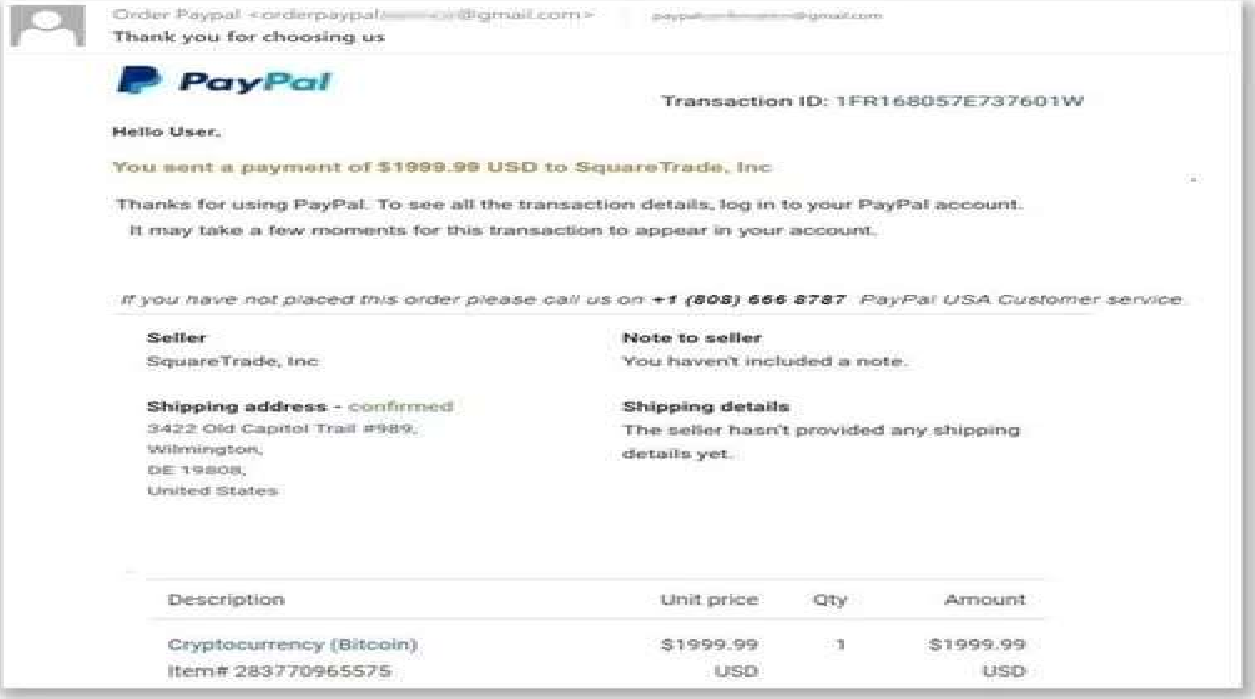
You have 24 hours to cancel or modify your purchase please contact PayPal support +1 888-499-1814

Invoice Number	:	D1/1897-13780
Product Details	:	Apple Watch series 6 ([illegible])
Invoice Amount	:	$399.98
Invoice Date	:	26 July,2021
Due Date	:	27 July 2021
Payment Mode	:	Online

Note: You Have 24 hour from the Date of the Transaction to open a dispute. For assistance PayPal Support +1 888-499-1814

Please keep the invoice number to track more about the transaction.

Thanks & Regards
PayPal



Order Paypal <orderpaypal[redacted]@gmail.com> paypalconfirmation@gmail.com

Thank you for choosing us

Transaction ID: 1FR168057E737601W

Hello User,

You sent a payment of $1999.99 USD to SquareTrade, Inc

Thanks for using PayPal. To see all the transaction details, log in to your PayPal account.
It may take a few moments for this transaction to appear in your account.

If you have not placed this order please call us on ***+1 (808) 666 8787*** *PayPal USA Customer service*

Seller
SquareTrade, Inc

Note to seller
You haven't included a note.

Shipping address - confirmed
3422 Old Capitol Trail #989,
Wilmington,
DE 19808,
United States

Shipping details
The seller hasn't provided any shipping details yet.

Description	Unit price	Qty	Amount
Cryptocurrency (Bitcoin) Item# 283770965575	$1999.99 USD	1	$1999.99 USD

Vishing

- Substantial potential loss
- Convincing phone interaction
- Campaign, then wait for phone call(s)
- “WE apologize, give us your credit card so we can re-imburse this mistake”

Current Issues

- US Census Bureau

  Jan 2020 incident report

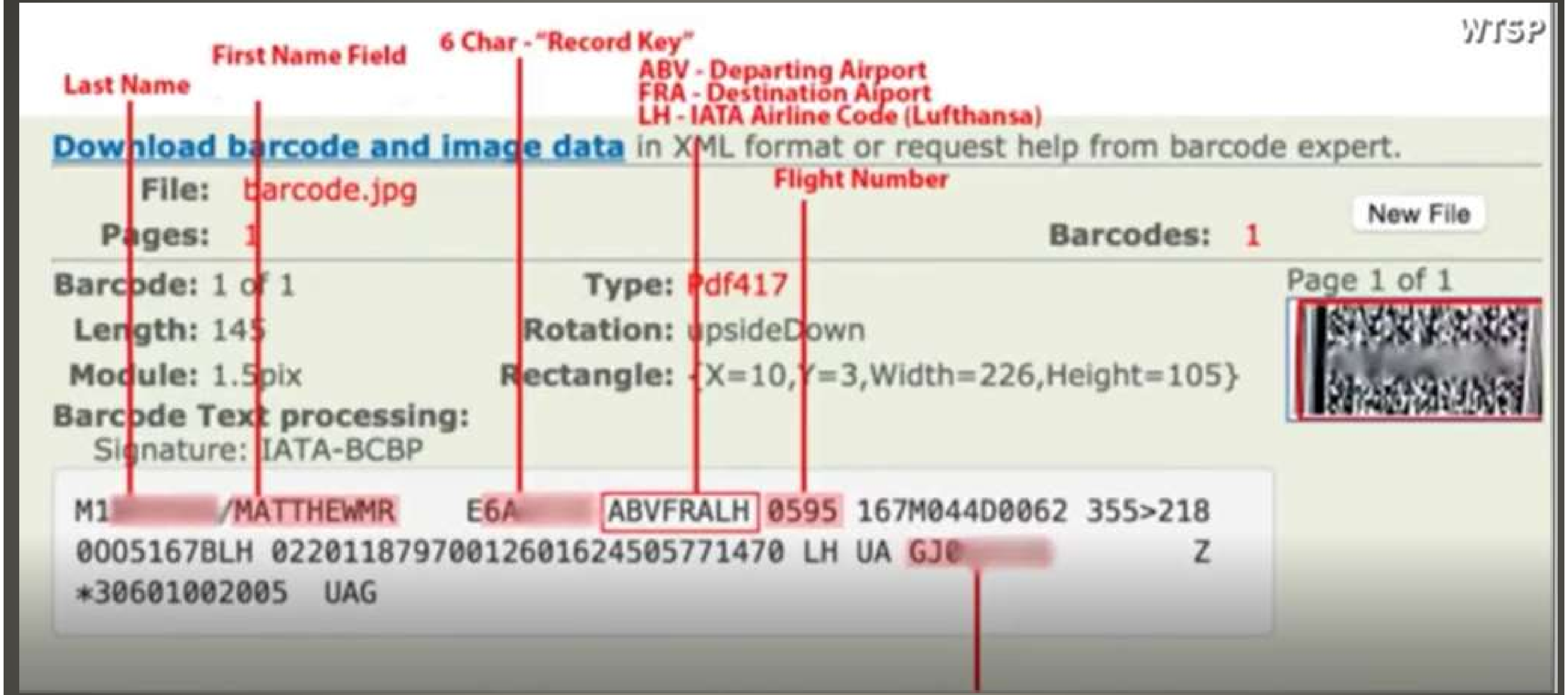
  missed opportunities to mitigate critical vulnerability

  Exploitation of vital servers

  Failure to maintain vital logs

  Operating unsupported servers

  failure to discover and report incident
- Abbott Labs Covid test inventory destroyed
- US DoD protection of data Afghanistan withdrawal
- More zero-click spyware for iMessage app
- Malware using GPU to avoid detection



Last Name

First Name Field

6 Char - "Record Key"

ABV - Departing Airport
FRA - Destination Aiport
LH - IATA Airline Code (Lufthansa)

Flight Number

Download barcode and image data in XML format or request help from barcode expert.

File: barcode.jpg

Pages: 1

Barcodes: 1

New File

Barcode: 1 of 1

Type: Pdf417

Length: 145

Rotation: upsideDown

Module: 1.5pix

Rectangle: {X=10,Y=3,Width=226,Height=105}

Page 1 of 1

Barcode Text processing:

Signature: IATA-BCBP

```
M1[redacted]/MATTHEWMR     E6A[redacted] ABVFRALH 0595 167M044D0062 355>218
0005167BLH 02201187970012601624505771470 LH UA GJ0[redacted]          Z
*30601002005   UAG
```

Boarding Pass   QR code

- Paper boarding passes had similar info
- QR scan accelerates copy of information
- Protect ANY PII as if it was PII
- Barcode scanner experience at convention

Boarding Passes

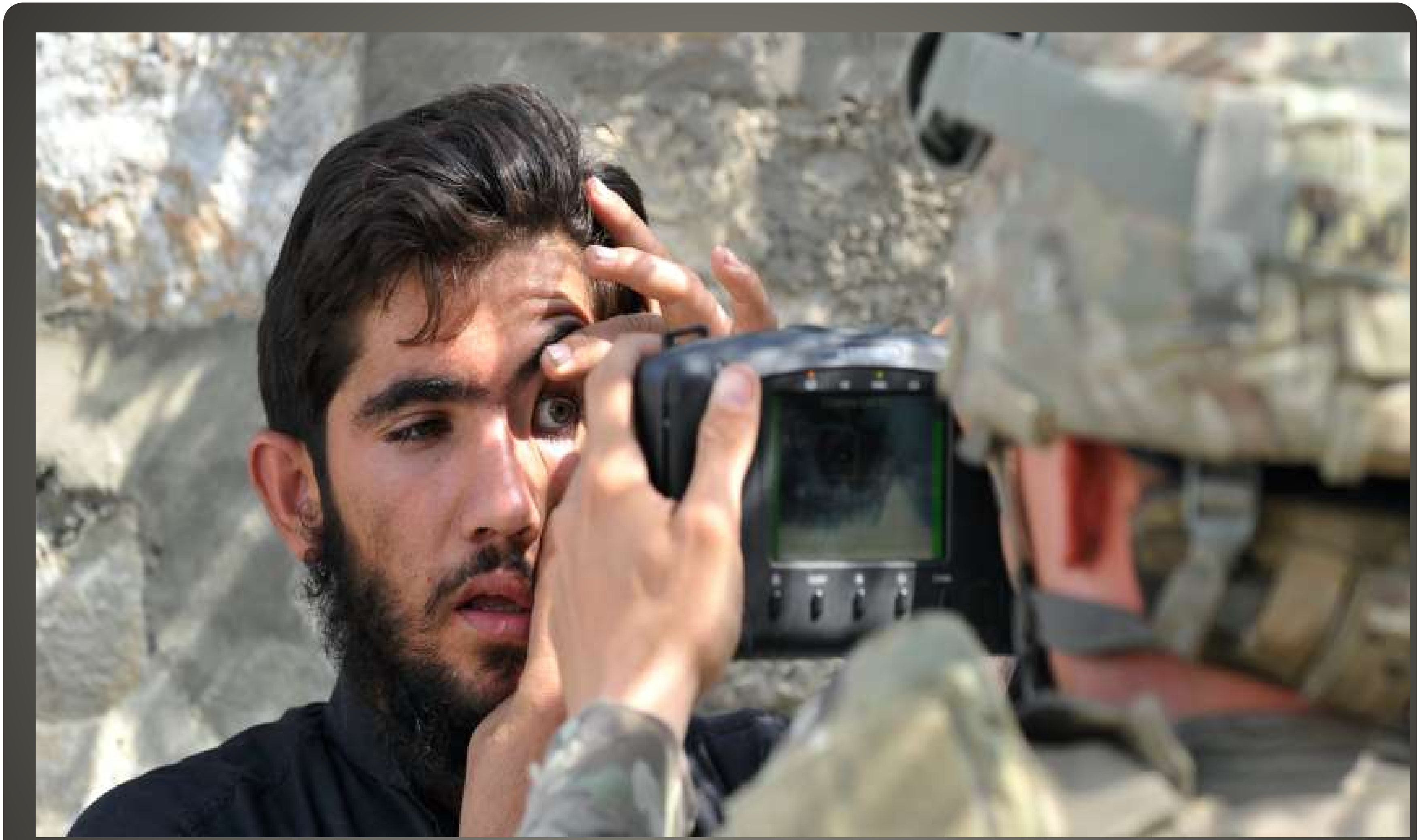
- “they all look alike”
- Once scanned …
- BUT

QR scanner with preview function

good cyber hygiene

No scripting, etc.

QR codes



HIIDE Fingerprints, faces, irises

- HIIDE Handheld Interagency Identity Detection Equipment 80% of country
- And UN Refugee agency
- Install a USB mouse – Gain SYSTEM

  Razer Synapse

  SteelSeries keyboards, ……..
- Microsoft Power Apps platform

  38 million records

  Open permissions by default
- Joker Android malware

  Subscribe to pay services

  Drain bank accounts
- Coinbase accounts drained
- Realtek Wi-Fi devices – News Blog

Current Issues

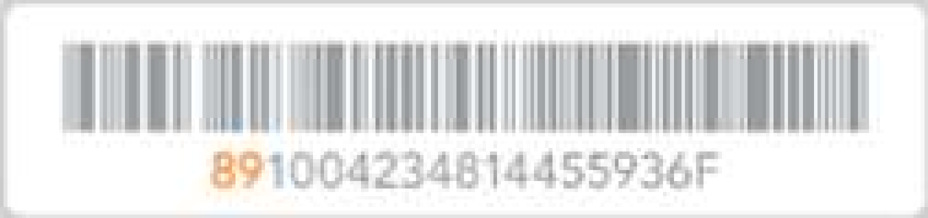
- PIN
- T-Mobile, AT&T, ???
- Stolen - Reset
- Convince T-Mobile I am you
  Hacker has more info on you than you do
- SIMjacking
- NEW PHONE – Different carrier
- "recovery" phone – eMail
- THEN …
- Same browser - browser saved accounts
  AND passwords (passphrases)

Convenience ours -> Convenience theirs

Personal Identification Number

Cellular numbers

- Integrated Circuit Card ID ICCID
  SIM card Identifier
  18-22 digit
  country code
  mobile network code
  unique code per SIM



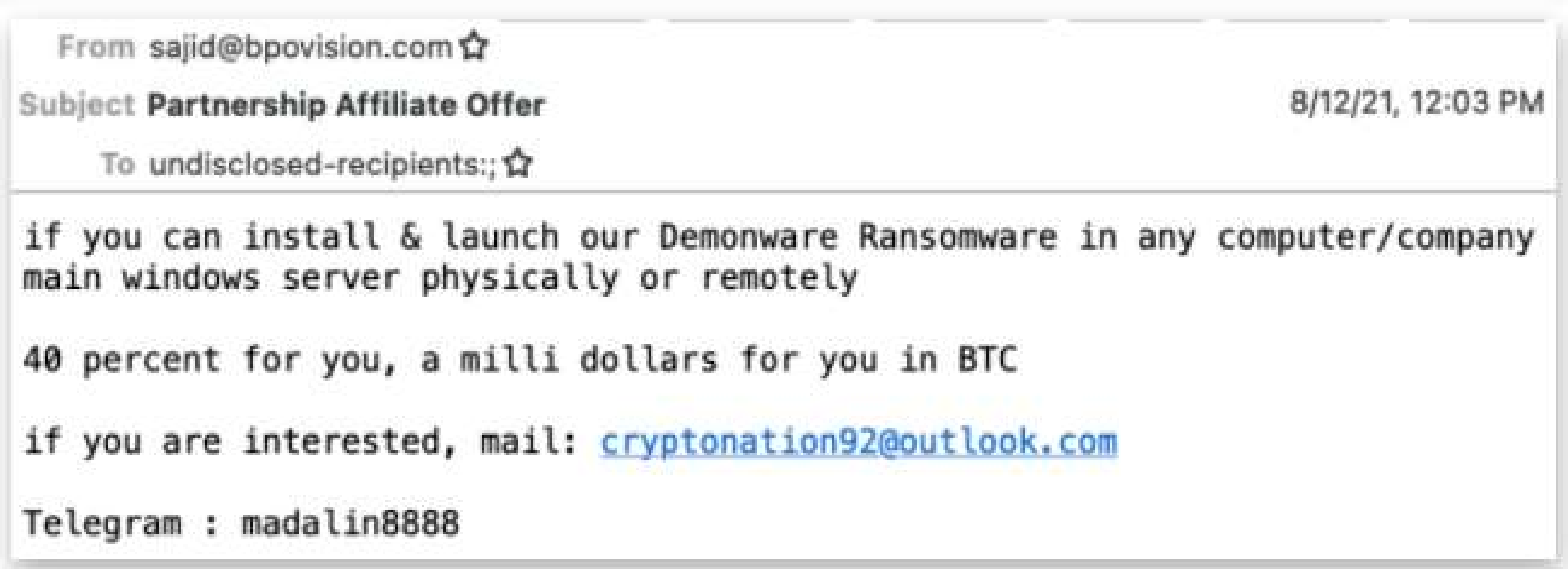
8910042348144559 36F

Cellular numbers

- International Mobile Equipment Identity
  IMEI
  15 digit
  “burned” into device
  blocked or blacklisted

- International Mobile Subscriber Identity
  IMSI
  64 bit
  Sent to cellular network
  home location register
  visitor location register
  protection against tracking
  TMSI
  4 octet (NOT FF)
  I want to be found, but not tracked

Cellular numbers



From sajid@bpovision.com ✩

Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM

To undisclosed-recipients:; ✩

```
if you can install & launch our Demonware Ransomware in any computer/company
main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888
```

Insider Threat

IDentity theft

- T-Mobile
- Metro by T-Mobile
- 5 reported breaches in 4 years
- WSJ interview

  Lousy security   Unsecure router
  No detection   No data segregation
  No encryption
  Firewall & IDS facing wrong way
- IDentity theft - misnomer
- AT&T
- NOT just current customers
- *Inquired about T-Mobile home Internet?*
- Reset PIN

- 40+ “other”
- Innovus, ChexSystems, Certegy
- LexisNexis

  Customer Risk

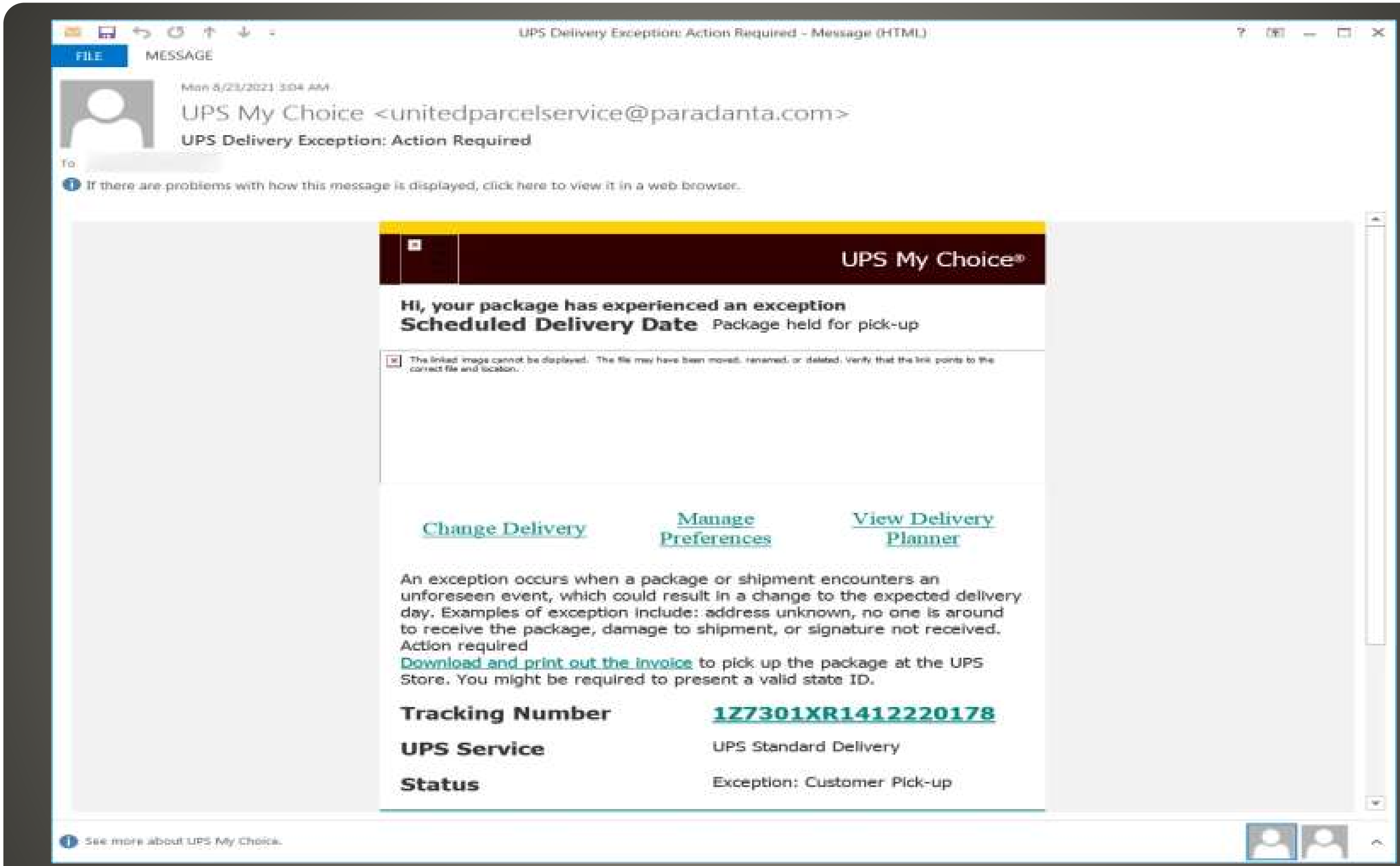
  92 page report

  Address Characteristic records
- Must provide all information you are trying to protect
- Freeze – Federal mandated – free

Other Credit Reporting Agencies

- Freeze credit

  GAIN and GUARD the PIN
- Credit monitoring services
- IDentity theft monitoring
- Password health & safety
- Act before the next reported breach
- Lock vs Freeze
- 10 day unlock



UPS Delivery Exception: Action Required - Message (HTML)

Mon 8/23/2021 3:04 AM

UPS My Choice <unitedparcelservice@paradanta.com>

UPS Delivery Exception: Action Required

To [redacted]

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

UPS My Choice®

Hi, your package has experienced an exception

Scheduled Delivery Date Package held for pick-up

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Change Delivery | Manage Preferences | View Delivery Planner

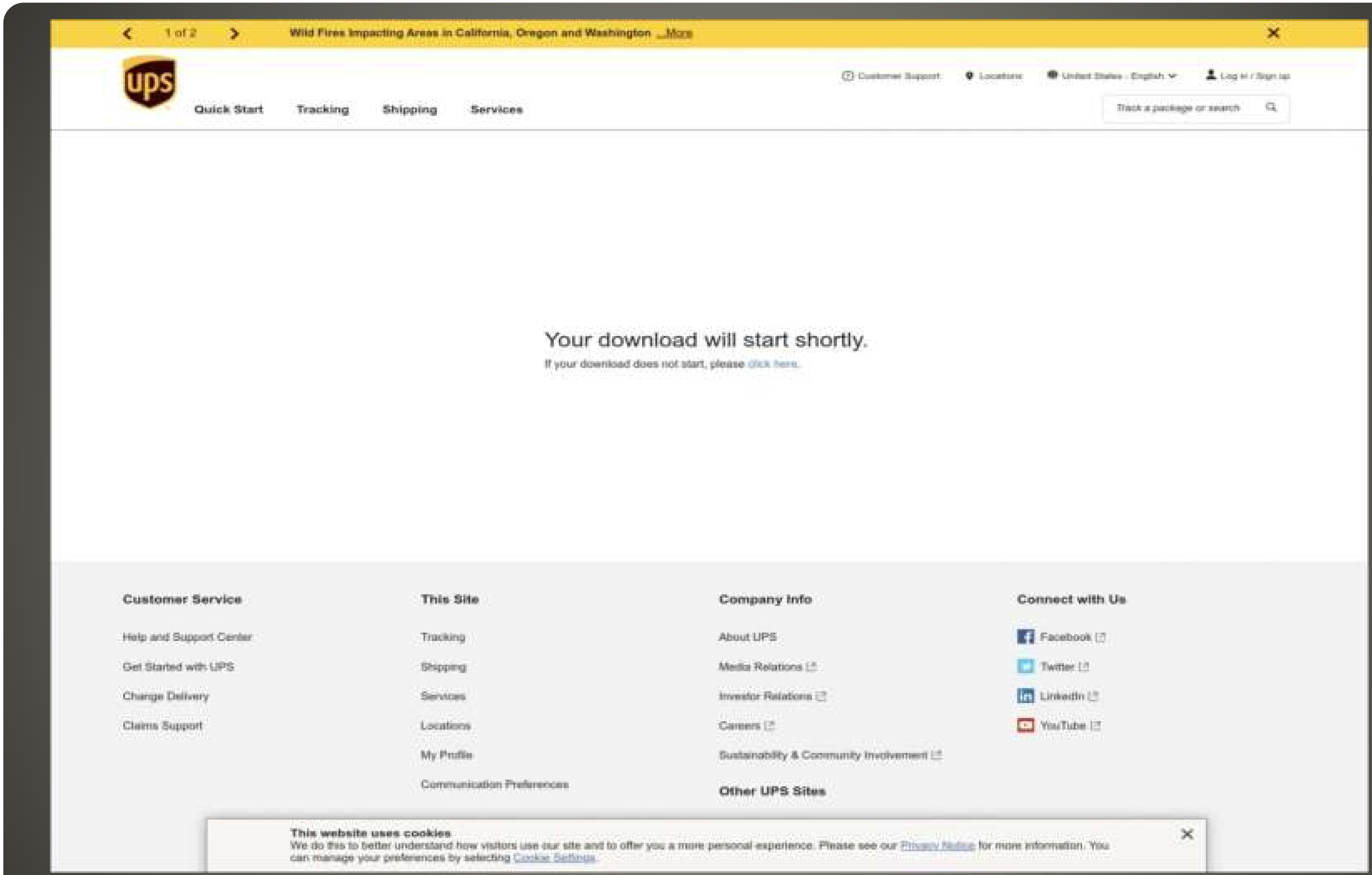
An exception occurs when a package or shipment encounters an unforeseen event, which could result in a change to the expected delivery day. Examples of exception include: address unknown, no one is around to receive the package, damage to shipment, or signature not received. Action required

Download and print out the invoice to pick up the package at the UPS Store. You might be required to present a valid state ID.

Tracking Number	1Z7301XR1412220178
UPS Service	UPS Standard Delivery
Status	Exception: Customer Pick-up

See more about UPS My Choice.

UPS XSS campaign



Wild Fires Impacting Areas in California, Oregon and Washington ...More

Your download will start shortly.

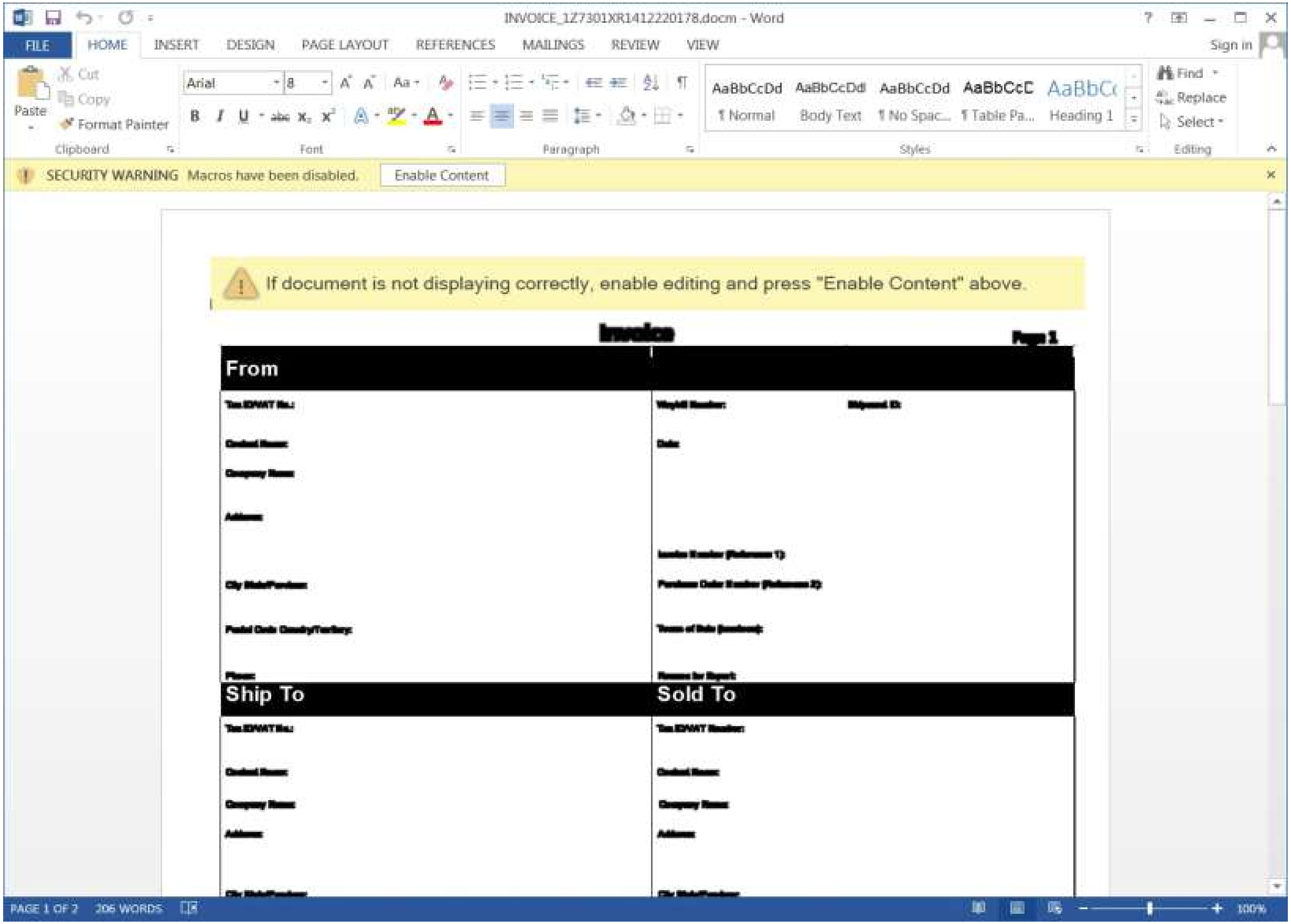
If your download does not start, please click here.

This website uses cookies
We do this to better understand how visitors use our site and to offer you a more personal experience. Please see our Privacy Notice for more information. You can manage your preferences by selecting Cookie Settings.

UPS XSS campaign

- Legitimate URLs
- Distribute malicious files convincingly

UPS XSS campaign



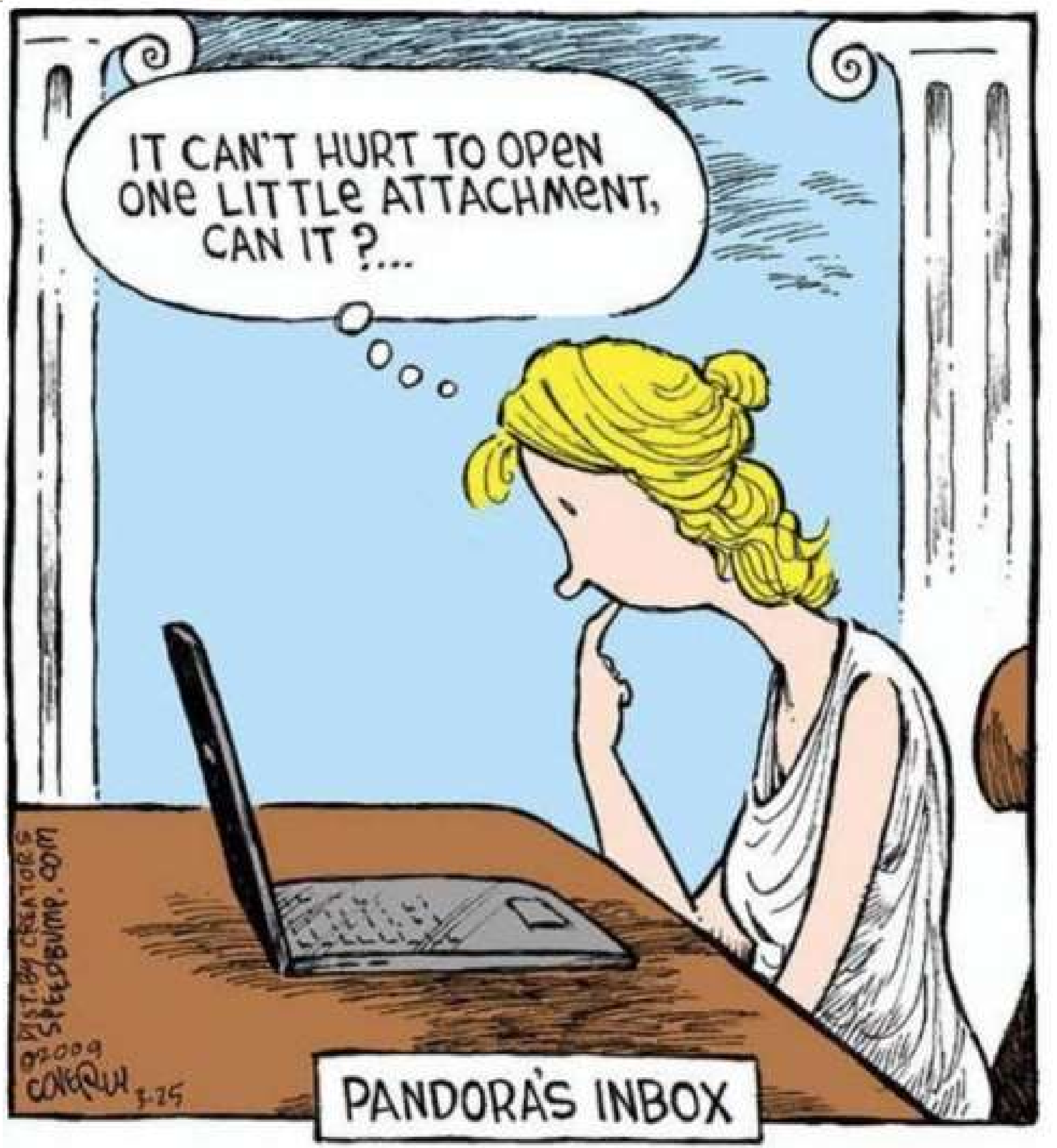
SECURITY WARNING Macros have been disabled. Enable Content

If document is not displaying correctly, enable editing and press "Enable Content" above.

Invoice

Page 1

From	
Tax ID/VAT No.:	Waybill Number: Shipment ID:
Contact Name:	Date:
Company Name:	
Address:	
	Invoice Number (Reference 1):
City State/Province:	Purchase Order Number (Reference 2):
Postal Code Country/Territory:	Terms of Sale (Incoterm):
Phone:	Reason for Export:
Ship To	**Sold To**
Tax ID/VAT No.:	Tax ID/VAT Number:
Contact Name:	Contact Name:
Company Name:	Company Name:
Address:	Address:
City State/Province:	City State/Province:

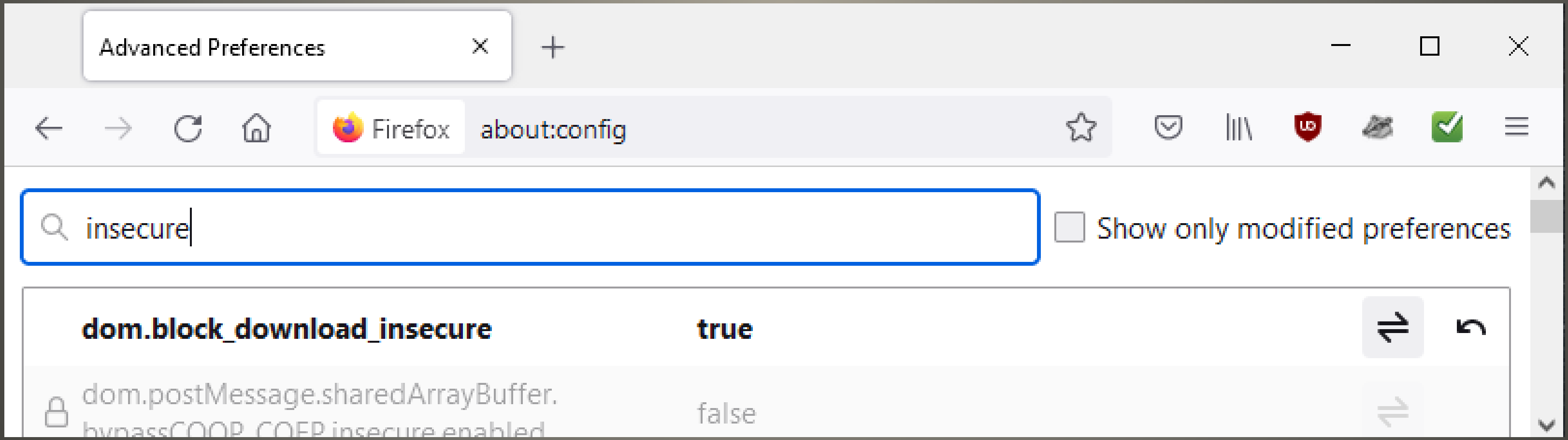

IT CAN'T HURT TO OPEN ONE LITTLE ATTACHMENT, CAN IT?...
PANDORA'S INBOX
©2009 DIST. BY CREATORS SPEEDBUMP.COM
COVERLY 3-25

Current Issues

- Open Banking

  Quicken, YNAB, Banktree, Money Dashboard, Moneydance
- Firefox mixed content download block

  Version 92



insecure

□ Show only modified preferences

dom.block_download_insecure **true**

dom.postMessage.sharedArrayBuffer.bypassCOOP_COEP.insecure.enabled false

Current Issues

- Yet another Microsoft Exchange server vulnerability
  - ProxyLogon, ProxyShell, ProxyToken
  - LockFile ransomware
- Web shell
  - Trivial to plant
  - Very difficult to detect
- Remotely disable “looted” smart TVs
  - what could possibly go wrong?
- Netflow data for sale
  - yeahbut were do they get it?
  - Team Cymru
- UK person suing cyber currency thieves' parents

Current Issues

- Fake takeout sites increase

  Double check URL, Certificate, ability

  Credit vs Debit

  Once bitten …
- Cosmos DB Microsoft Azure cloud

  2019 tool Jupyter Notebook

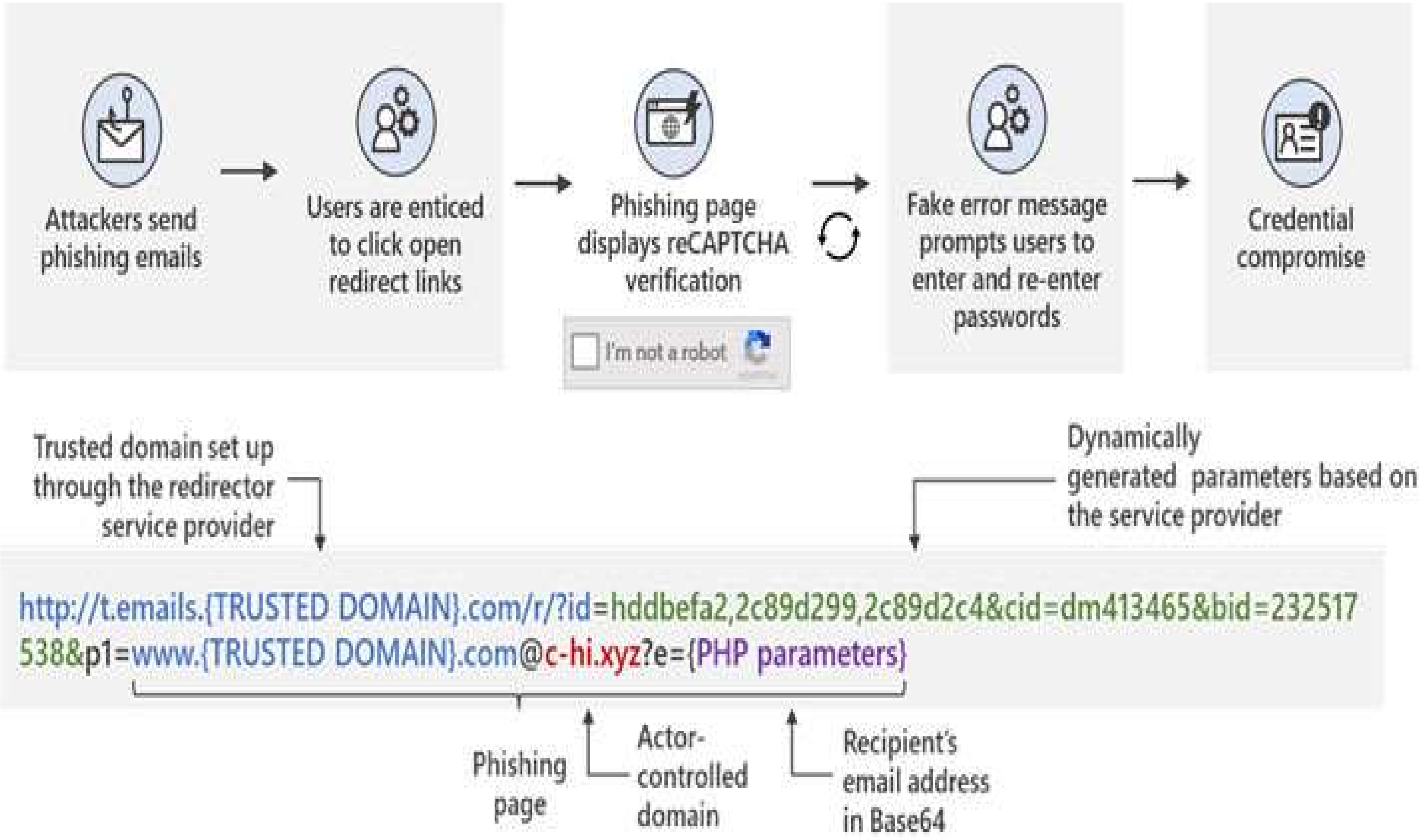
  Microsoft request customer key change
- August 25 White House Cyber Summit

  NIST standards
- F5 fixes for 13 High Severity device bugs
- FBI alert for Hive ransomware

  Disk backup copies, snapshots, volume shadow copies
- SSD “binning” practices -> bait-and-switch
- Cryptocurrency clipboard attack
- Labor day CISA & FBI warning

- Credential phishing with long leadup
- Open redirector links
- “fool” security solutions
- Several redirects
- With captcha
- large number of domains
- Double check certificate whenever asked for credentials

New cybercrime campaign



Attackers send phishing emails → Users are enticed to click open redirect links → Phishing page displays reCAPTCHA verification → Fake error message prompts users to enter and re-enter passwords → Credential compromise

Trusted domain set up through the redirector service provider

Dynamically generated parameters based on the service provider

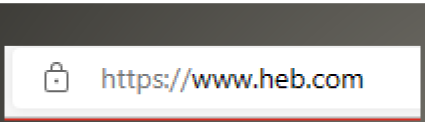
```
http://t.emails.{TRUSTED DOMAIN}.com/r/?id=hddbefa2,2c89d299,2c89d2c4&cid=dm413465&bid=232517
538&p1=www.{TRUSTED DOMAIN}.com@c-hi.xyz?e={PHP parameters}
```

Phishing page

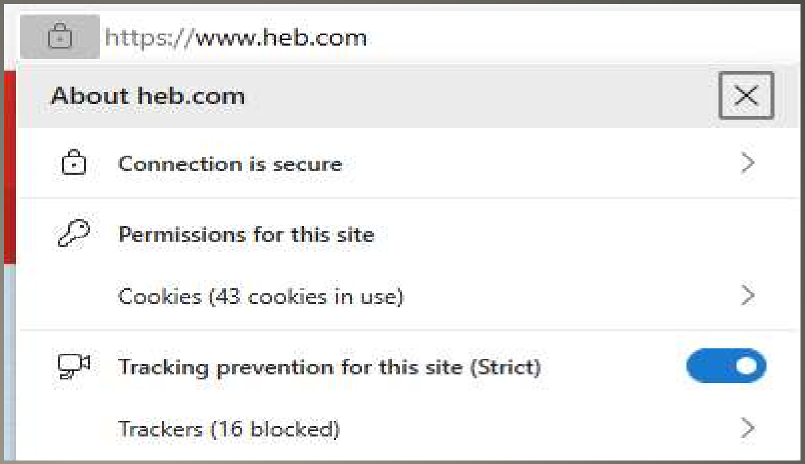
Actor-controlled domain

Recipient's email address in Base64

Certificate check Edge



https://www.heb.com



https://www.heb.com

About heb.com

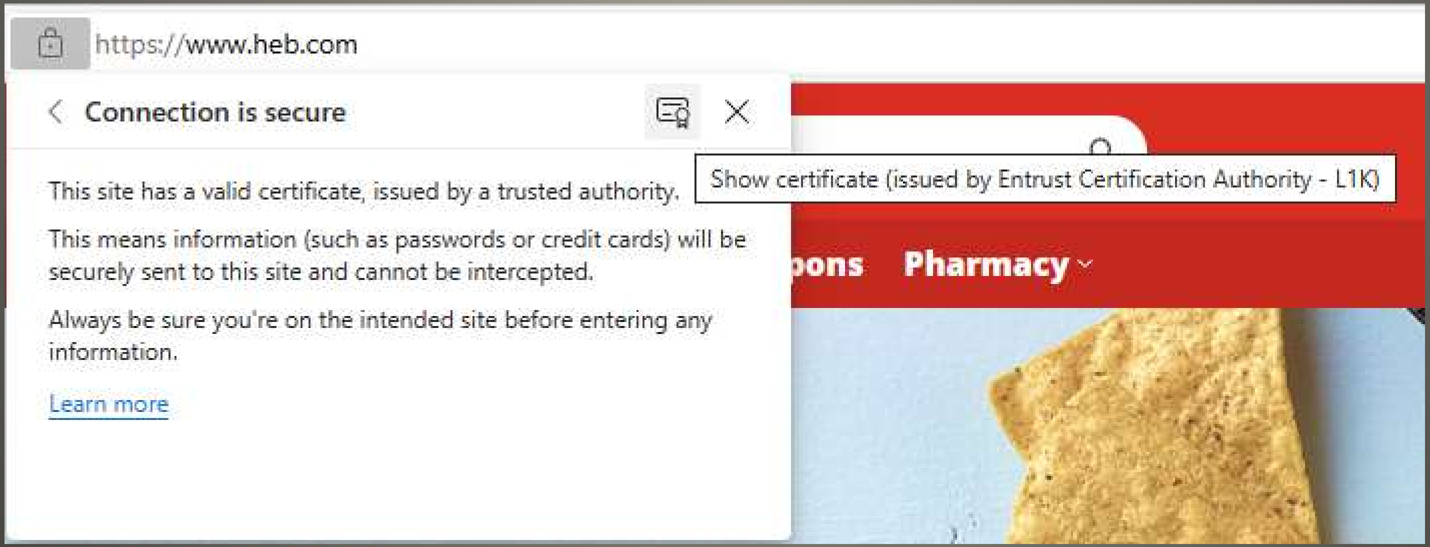
Connection is secure

Permissions for this site

Cookies (43 cookies in use)

Tracking prevention for this site (Strict)

Trackers (16 blocked)



https://www.heb.com

Connection is secure

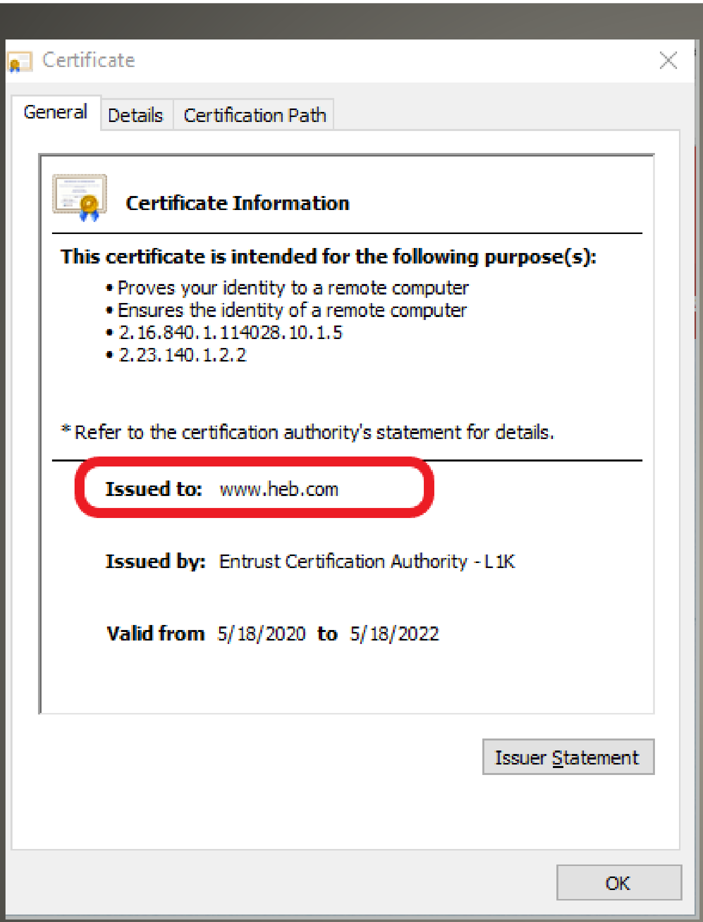
This site has a valid certificate, issued by a trusted authority.

This means information (such as passwords or credit cards) will be securely sent to this site and cannot be intercepted.

Always be sure you're on the intended site before entering any information.

Learn more

Show certificate (issued by Entrust Certification Authority - L1K)



Certificate Information

This certificate is intended for the following purpose(s):

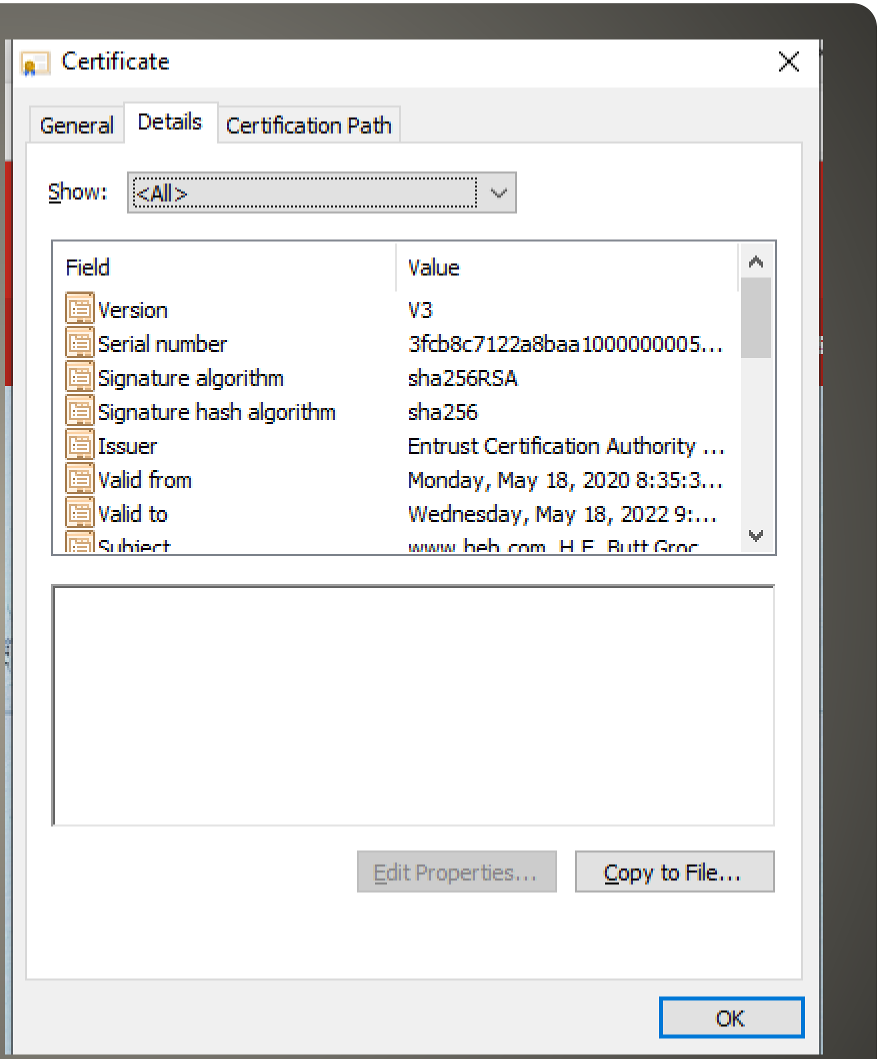
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114028.10.1.5
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: www.heb.com

Issued by: Entrust Certification Authority - L1K

Valid from 5/18/2020 **to** 5/18/2022



Show: <All>

Field	Value
Version	V3
Serial number	3fcb8c7122a8baa1000000005...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Entrust Certification Authority ...
Valid from	Monday, May 18, 2020 8:35:3...
Valid to	Wednesday, May 18, 2022 9:...
Subject	www.heb.com, H-E-Butt Groc...

Certificate Check Edge

Parallels

- Parallels Desktop

  High severity privilege escalation bug
  “inconvenience”
  Reduce product functionality
  CVE-2021-34864 8.8 low complexity
  upgrade to Parallels Desktop version 17
  Alternatives Boot Camp, VirtualBox, VMWare

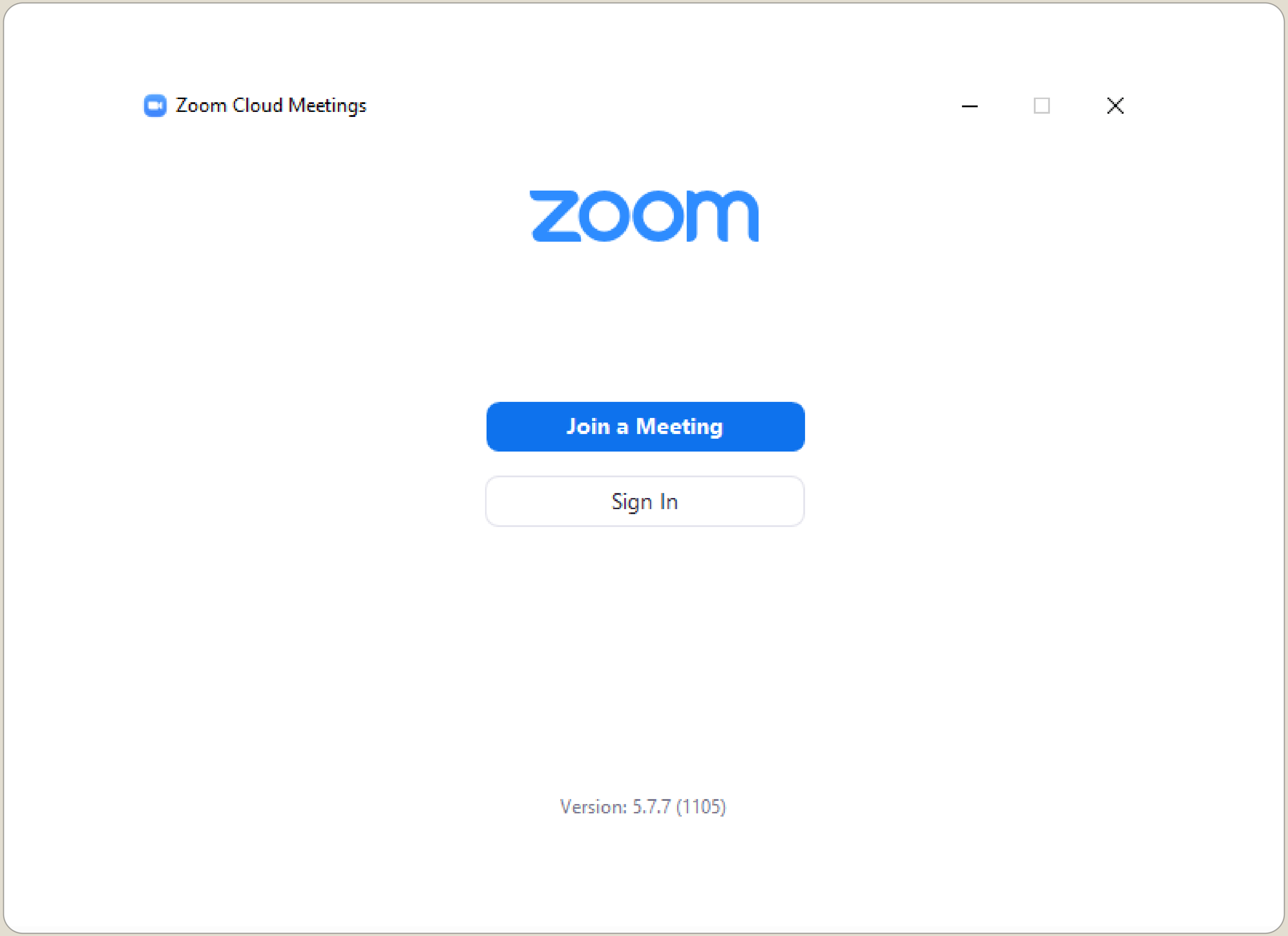
- Zoom via web – no login no update action
- Zoom updates

  Function fixes

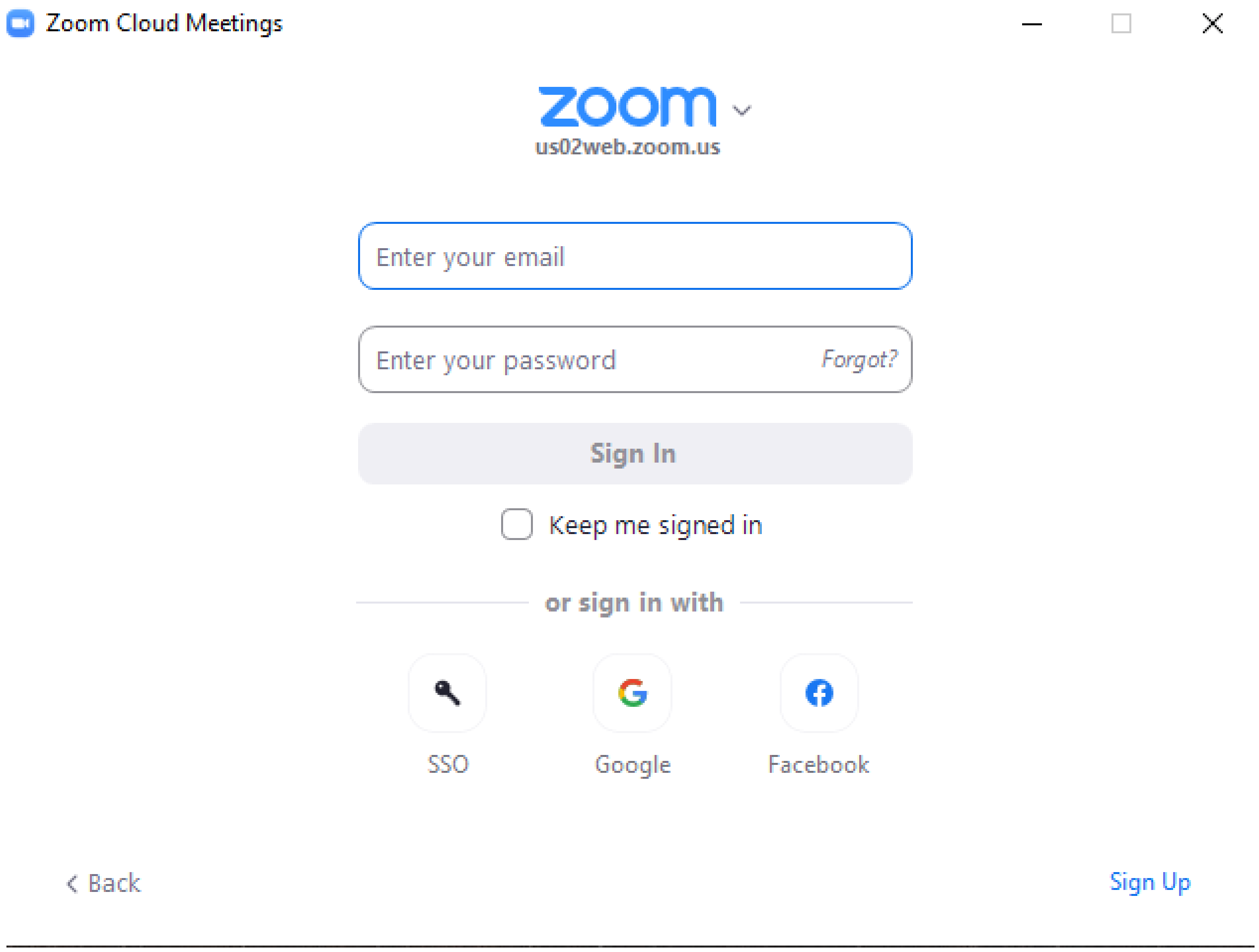
  Security Issues

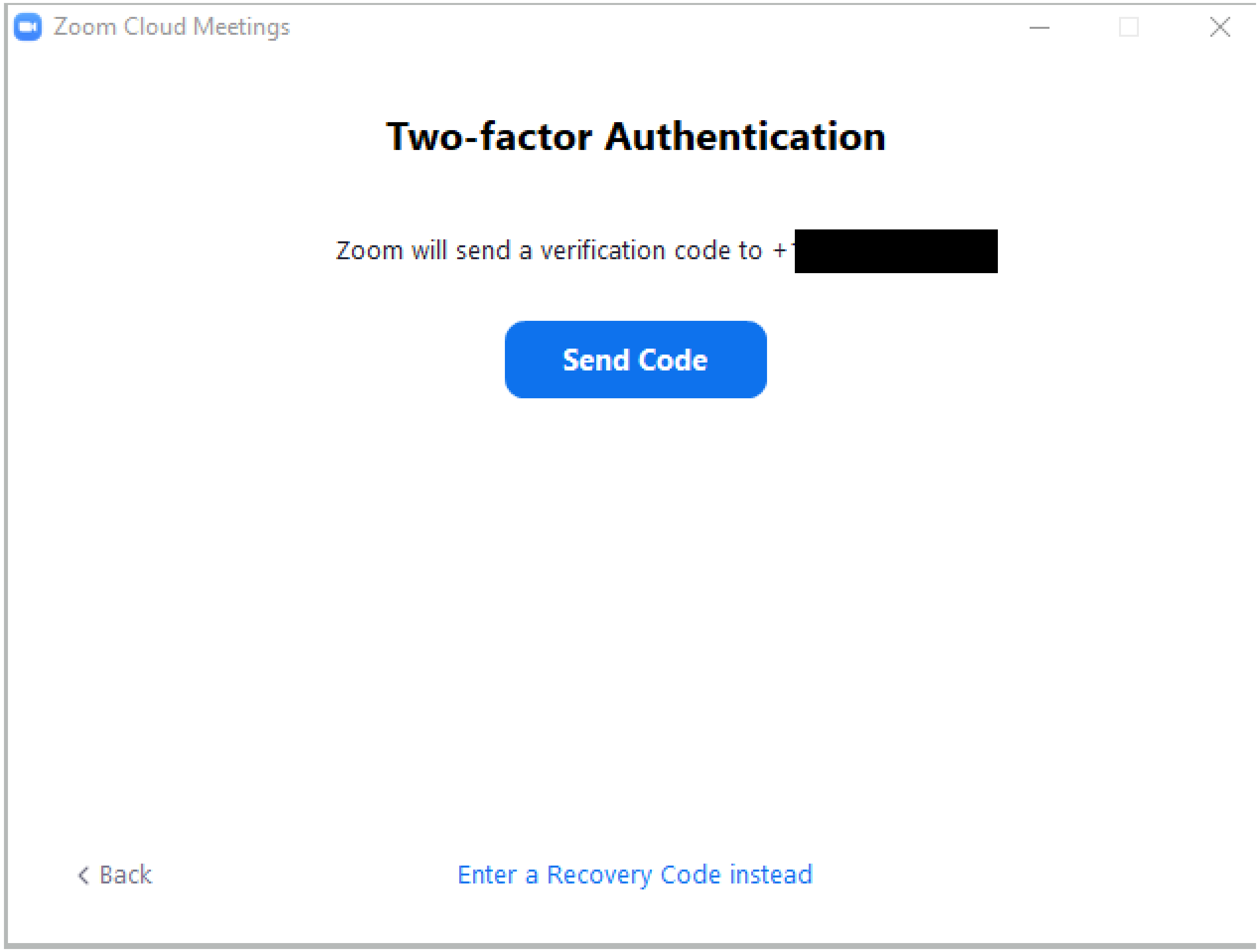
- Zoom psychology

Zoom updates



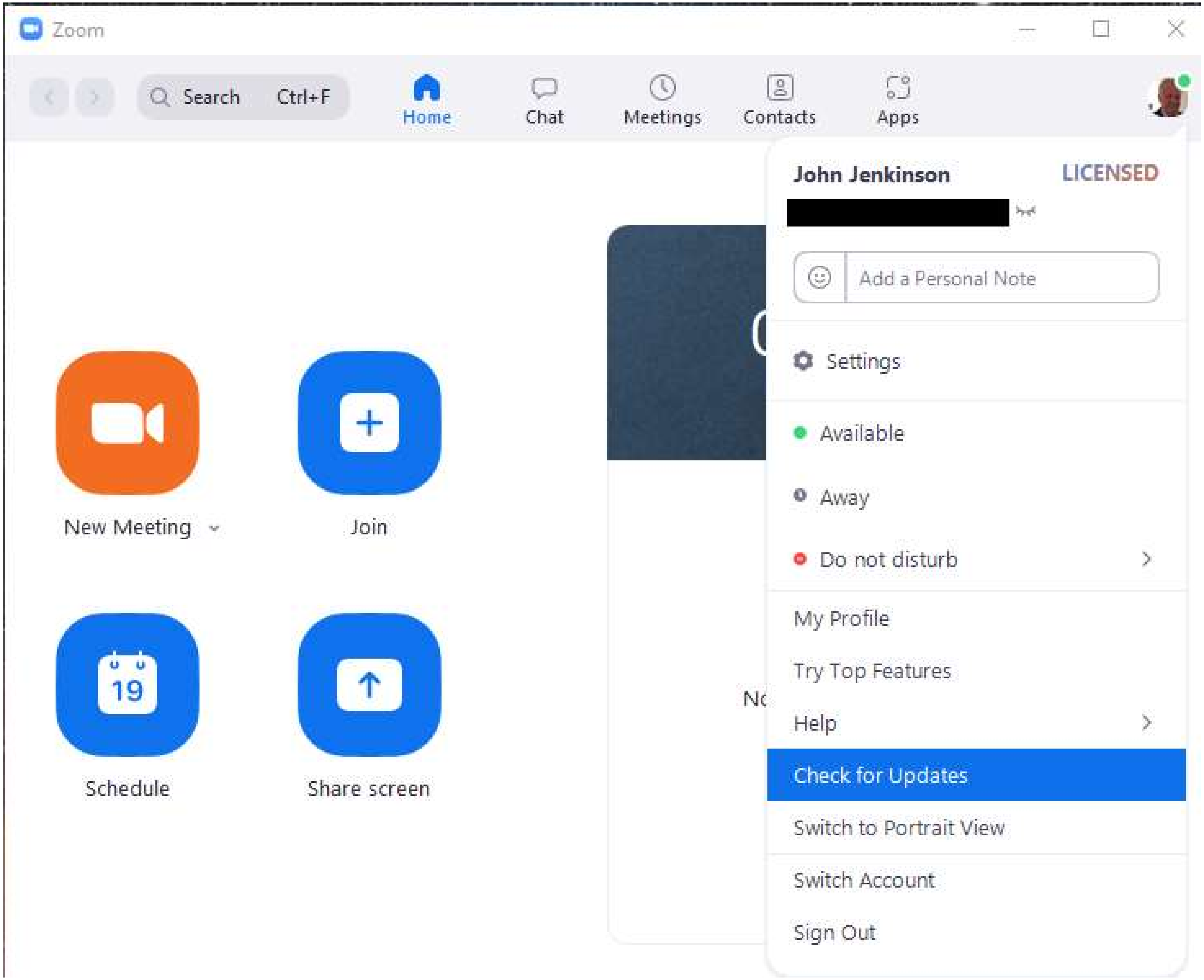
Version: 5.7.7 (1105)

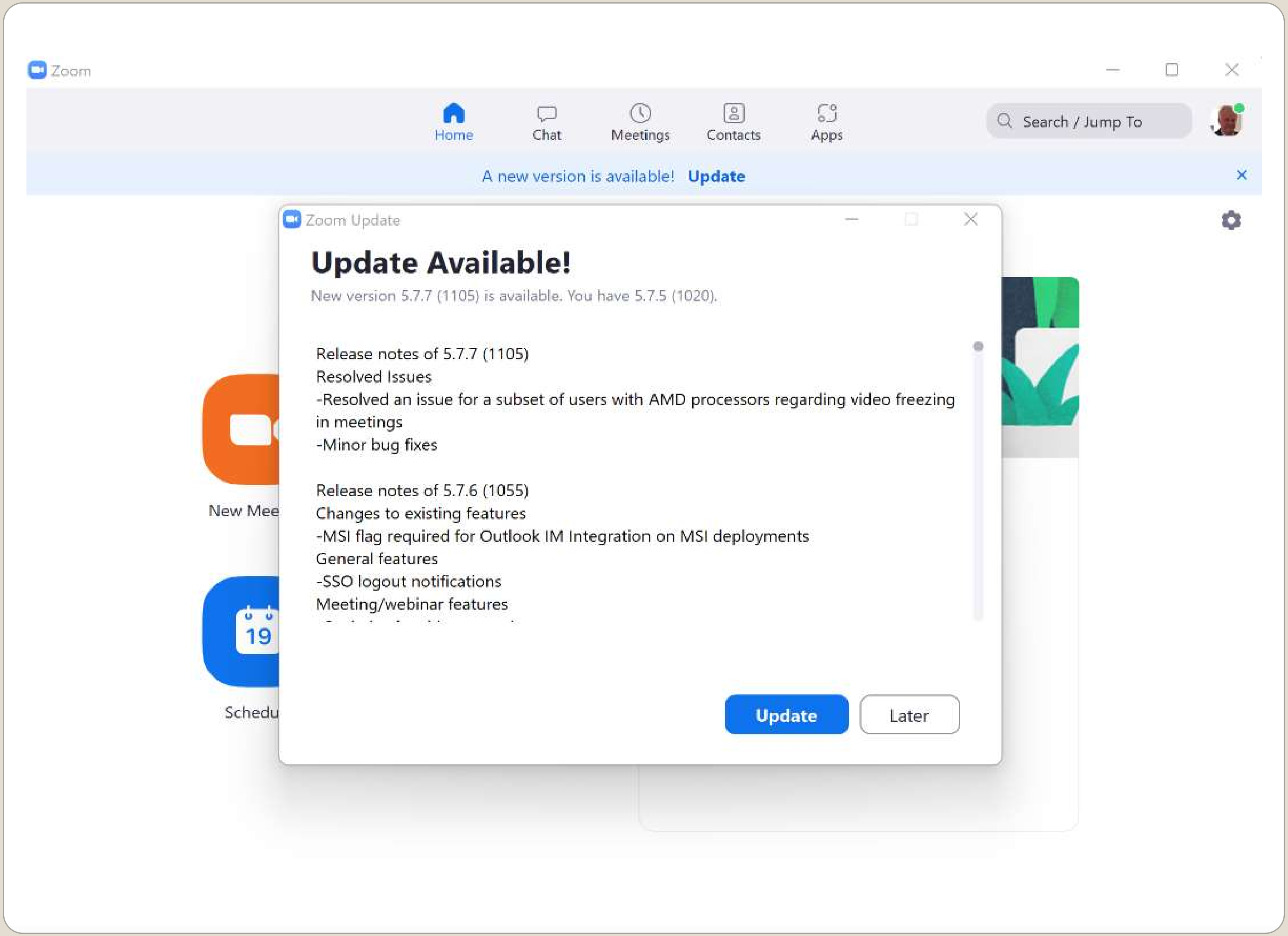

Zoom Cloud Meetings
zoom
us02web.zoom.us
Enter your email
Enter your password
Forgot?
Sign In
□ Keep me signed in
or sign in with
SSO
Google
Facebook
Back
Sign Up



Two-factor Authentication

Zoom will send a verification code to +[redacted]


Zoom
Search
Ctrl+F
Home
Chat
Meetings
Contacts
Apps
John Jenkinson
LICENSED
[redacted]
Add a Personal Note
Settings
Available
Away
Do not disturb
My Profile
Try Top Features
Help
Check for Updates
Switch to Portrait View
Switch Account
Sign Out
New Meeting
Join
19
Schedule
Share screen



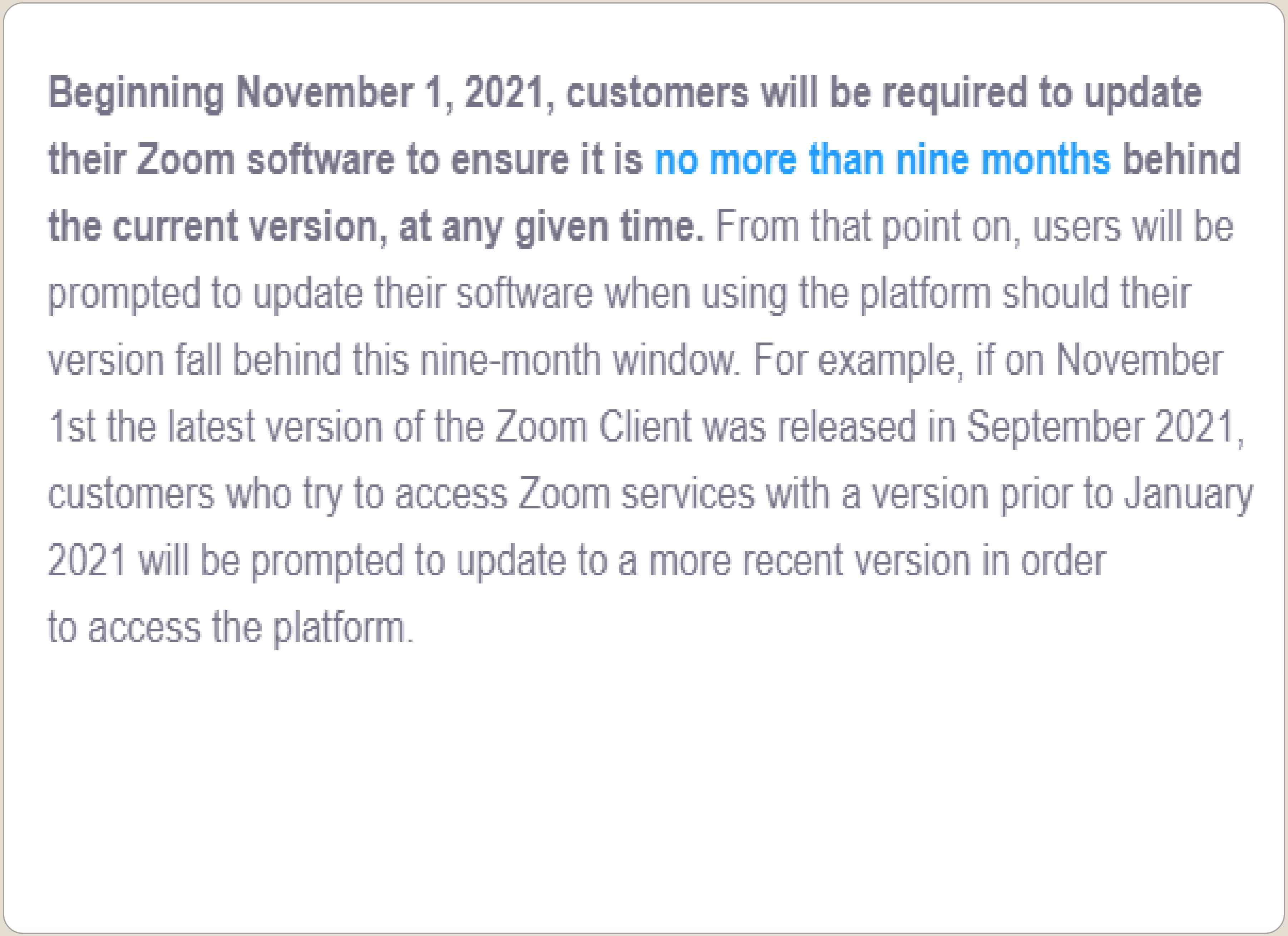
A new version is available! **Update**

Update Available!

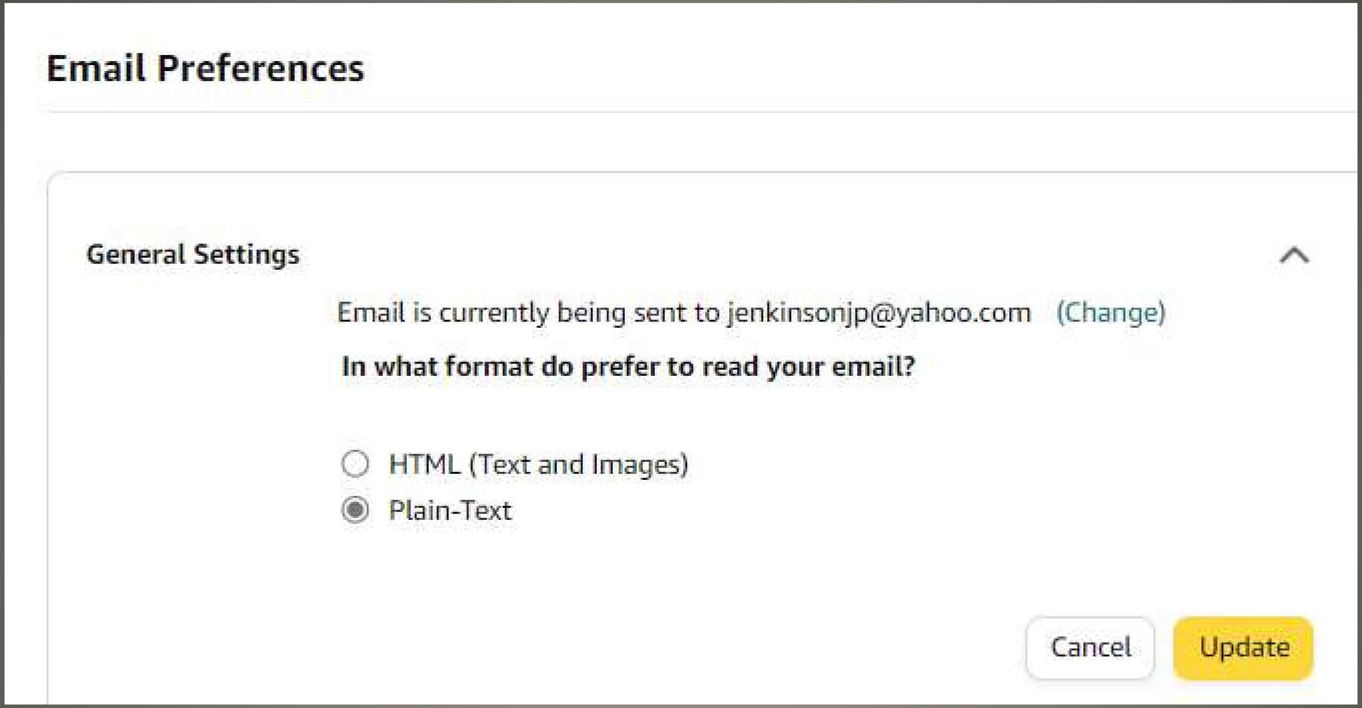
New version 5.7.7 (1105) is available. You have 5.7.5 (1020).

Release notes of 5.7.7 (1105)
Resolved Issues
-Resolved an issue for a subset of users with AMD processors regarding video freezing in meetings
-Minor bug fixes

Release notes of 5.7.6 (1055)
Changes to existing features
-MSI flag required for Outlook IM Integration on MSI deployments
General features
-SSO logout notifications
Meeting/webinar features



Beginning November 1, 2021, customers will be required to update their Zoom software to ensure it is no more than nine months behind the current version, at any given time. From that point on, users will be prompted to update their software when using the platform should their version fall behind this nine-month window. For example, if on November 1st the latest version of the Zoom Client was released in September 2021, customers who try to access Zoom services with a version prior to January 2021 will be prompted to update to a more recent version in order to access the platform.



Email Preferences

General Settings

Email is currently being sent to jenkinsonjp@yahoo.com (Change)

In what format do prefer to read your email?

○ HTML (Text and Images)

● Plain-Text

Textual eMail sender

- Microsoft 365 Office 365

  Pseudonymize data from 1-September-2021

  BUT global administrators can override

  Privacy laws

- Internet shutdown research

  Egypt 2011

  Russia July 2021

  Number of cases down

  Duration increased

- 8 states

  Arizona, Georgia, Connecticut, Iowa, Kentucky, Maryland, Oklahoma, Utah

  Digital driver license/ID to Apple Wallet

  TSA

  Tap function

  view w/o unlock or handing device to someone

Current Issues

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com