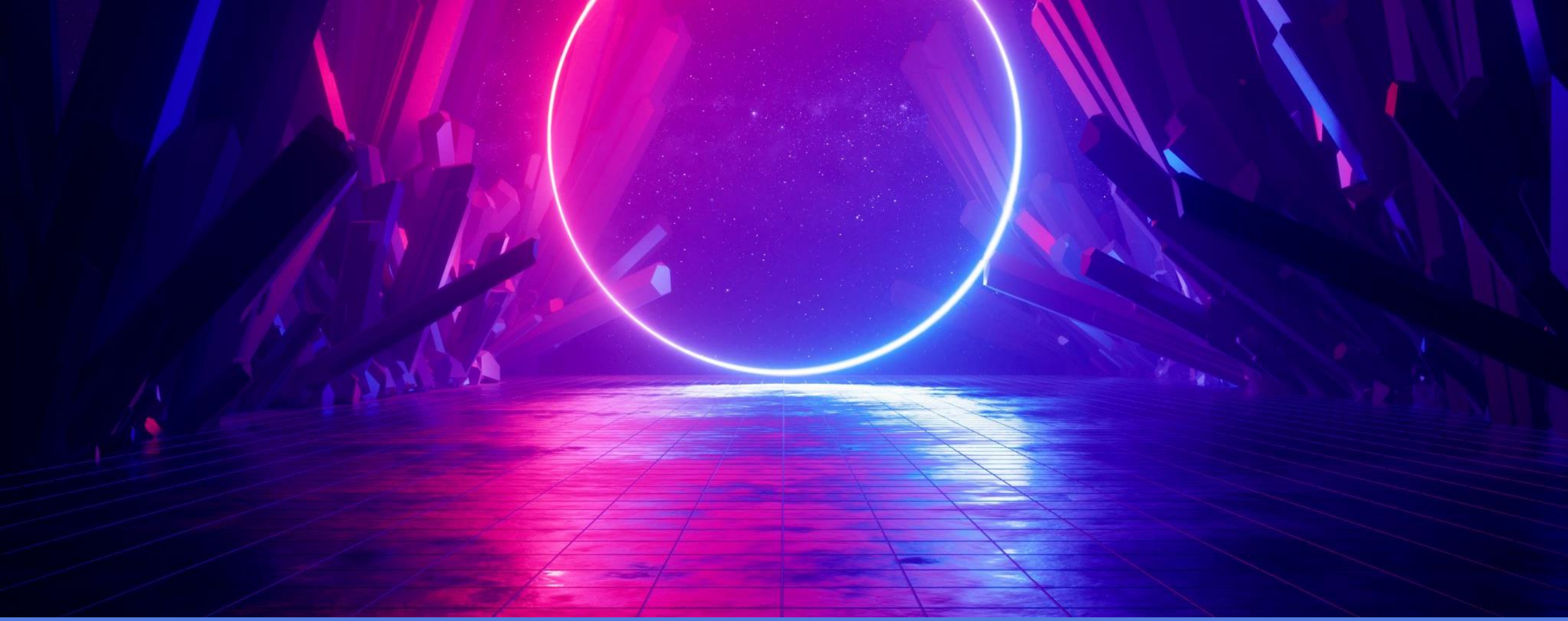


Practical Cybersecurity Awareness

Using The Internet

- Email, instant messaging, and personal websites now provide easy ways for everyone to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances.
- Many scammers target Americans ages 65 and older via emails and websites for charitable donations, online dating services, online auctions, buyer's clubs, health insurance, prescription medications, and health care.
- At home, at work, and in the community, our growing use of technology, coupled with increasing cyber threats and risks to our privacy, demands greater security in our online world.

Identity Theft:

The illegal use of someone else's personal information in order to obtain money or credit.

- DO NOT use the same password twice.
- Choose a password that means something to you and you only; use strong passwords with eight characters or more that uses a combination of numbers, letters, and symbols.
- Do not reveal personally identifiable information online such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or doctor's name.
- Be sure to shred bank and credit card statements before throwing them in the trash; talk to your bank about using passwords and photo identification on credit cards and bank accounts.

Tech Support Scams

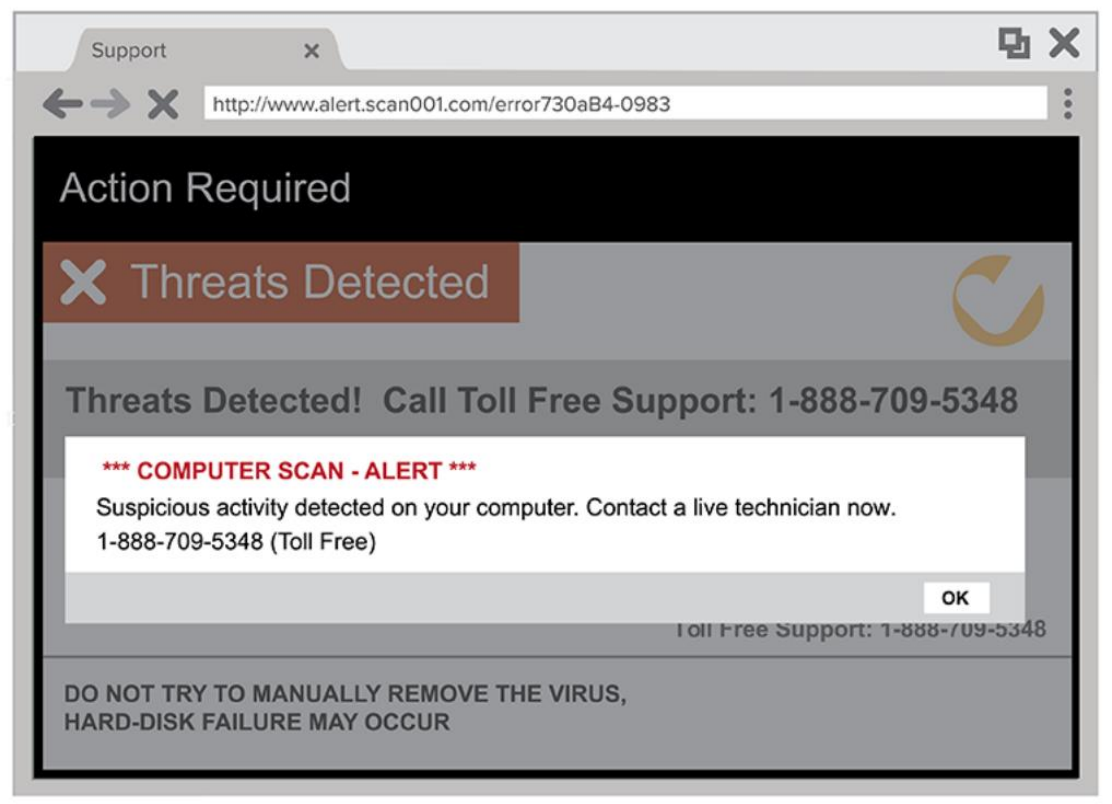
Tech Support Scam:

Type of fraud where someone pretends to be a tech support professional and tries to trick you into giving them remote access to your computer.

- Impersonating a tech company such as rnicrosoft and use technical terms to convince you there is a problem with your computer.
- Create fake error messages that popup on your screen with a phone number to call for “technical support”
- Once you call, they pressure you to install remote-access or screensharing software so they can access your computer.
- Often their goal is to get you to give them financial information or access to your financial information.

Tech Support Scam:

Type of fraud where someone pretends to be a tech support professional and tries to trick you into giving them remote access to your computer.



Fraud & Phishing

Fraud:

The intentional perversion of truth in order to induce another to part with something of value.

Phishing:

A scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

- Most organizations - banks, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies. *Use the "hover" method, hold your cursor over the link*
- Don't access your personal or banking accounts online from a public computer or kiosk.
- Beware of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your passwords often and avoid using the same password for multiple accounts.

SPAM EMAIL

SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

[redacted]

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

[redacted]

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

SPAM EMAIL

SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location apr device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

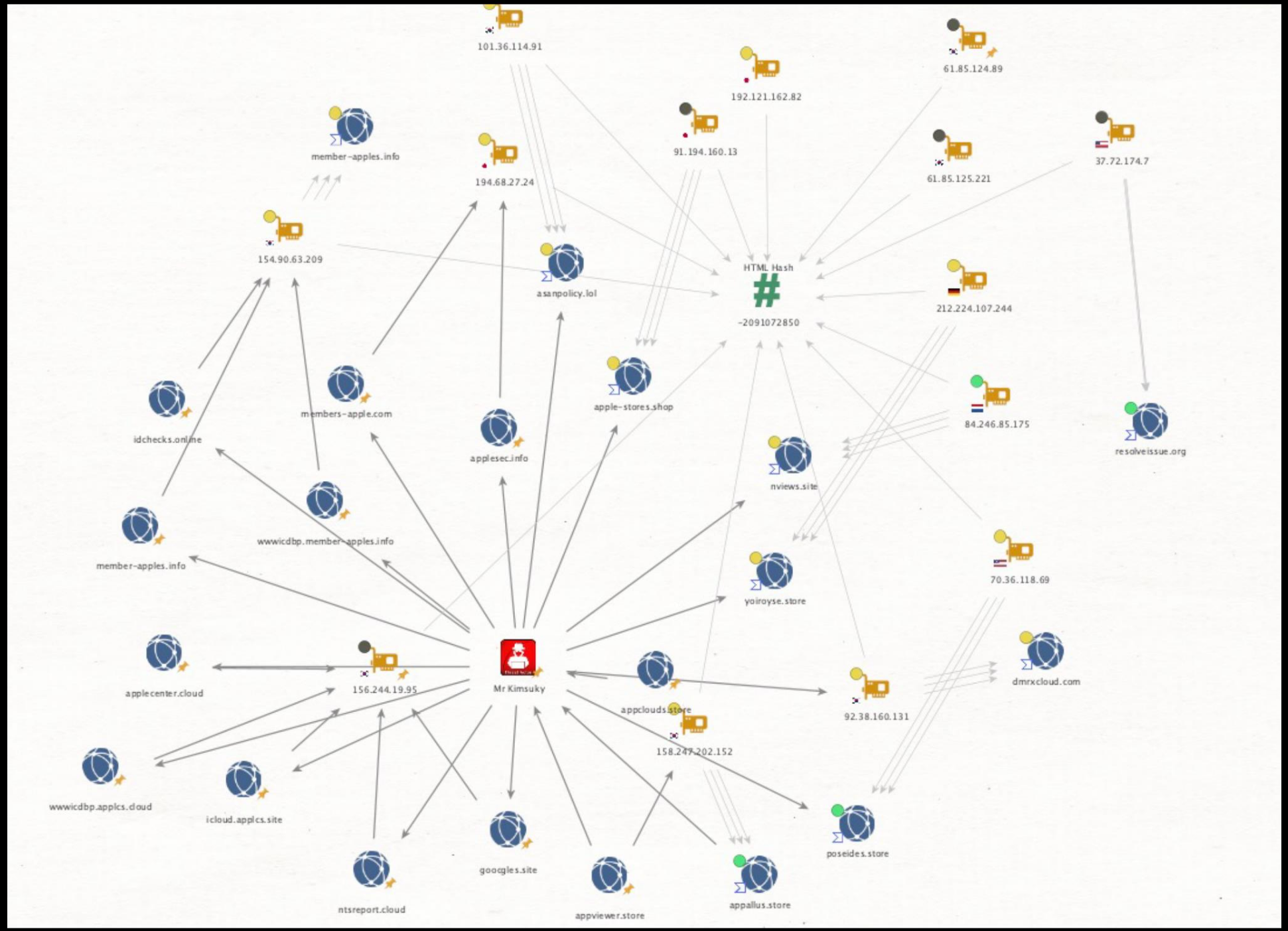
To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

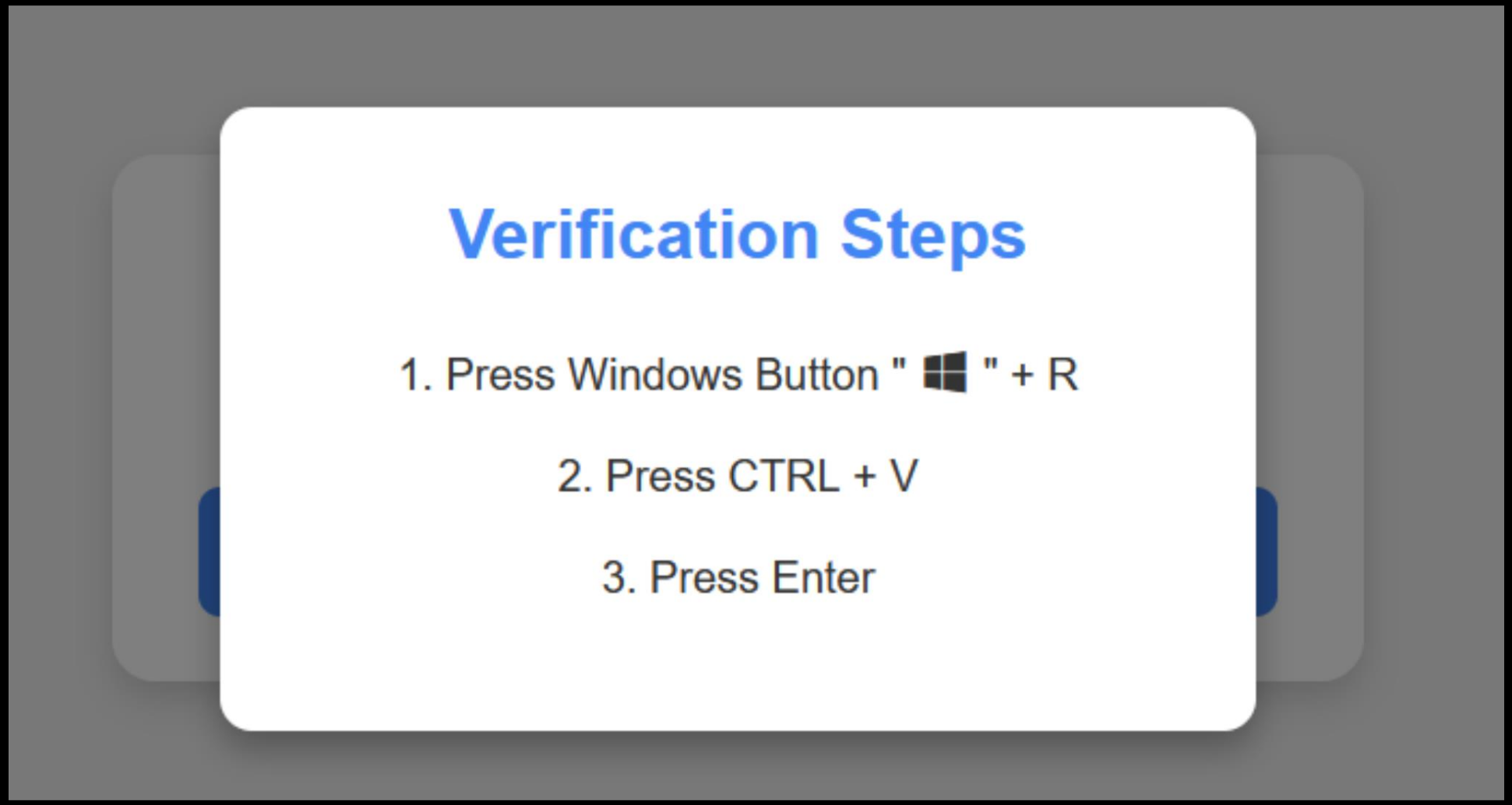
Review recent activity

Thanks,
The Microsoft Team

Note extra space in fake link

https: //www.apple.com


101.36.114.91
192.121.162.82
61.85.124.89
member-apples.info
91.194.160.13
194.68.27.24
61.85.125.221
37.72.174.7
154.90.63.209
asanpolicy.lol
HTML Hash
-2091072850
212.224.107.244
apple-stores.shop
84.246.85.175
resolveissue.org
members-apple.com
idchecks.online
applesec.info
nviews.site
wwwicdbp.member-apples.info
member-apples.info
70.36.118.69
yoiroyse.store
applecenter.cloud
156.244.19.95
Mr Kimsuky
appclouds.store
92.38.160.131
dmrxcloud.com
158.247.202.152
wwwicdbp.applcs.cloud
icloud.applcs.site
poseides.store
googles.site
ntsreport.cloud
appviewer.store
appallus.store



Tower Lakes HOA / 2024 REQUEST

Inbox ×

Bruce Messer <presidentb404@gmail.com>
to

Hi

Hope all is well!! Are you available? I am currently out of the office with limited phone accessibility. Urgently, I need your assistance in handling an administrative expense that is due on our behalf.

our treasurer Melanie Riggleman is currently unavailable to take care of it. Please let me know if you can process the payment through Zelle/PayPal. I'll promptly send you the vendor's payment information for either option that is most suitable for you. Your prompt attention to this matter is crucial, and I will ensure your reimbursement is processed as soon as the the treasurer becomes available.

President
Bruce Messer

Essentials

- Keep your PC up-to-date with the latest patches.
- Consider the use of password manager.
- Use common sense while online.
- Before you click on a link or download an attachment verify its authenticity.