

JOINT CYBERSECURITY ADVISORY

Co-authored by:

TLP: CLEAR

Product ID: 20240927-001



National Cyber
Security Centre

a part of GCHQ

Iranian Cyber Actors Targeting Personal Accounts to Support Operations

The Federal Bureau of Investigation (FBI), U.S. Cyber Command - Cyber National Mission Force (CNMF), the Department of the Treasury (Treasury), and the United Kingdom's National Cyber Security Centre (NCSC) are disseminating this joint Cybersecurity Advisory (CSA) to highlight continued malicious cyber activity by cyber actors working on behalf of the Iranian Government's Islamic Revolutionary Guard Corps (IRGC¹). This IRGC cyber activity is targeted against individuals with a nexus to Iranian and Middle Eastern affairs; such as current or former senior government officials, senior think tank personnel, journalists, activists, and lobbyists. Additionally, FBI has observed these actors targeting persons associated with US political campaign activity, likely in support of information operations.

The authoring agencies believe the group and the cyber techniques remain an ongoing threat to various sectors worldwide, including but not limited to entities in their respective countries.

This advisory provides observed tactics, techniques, and indicators of compromise (IOCs) that the authoring agencies assess are likely associated with cyber actors working on behalf of IRGC. The authoring agencies urge individuals in targeted groups to apply the recommendations listed in the **Mitigations** section of this advisory to diminish risk of compromise from these cyber-actors. For more information on Iranian state-sponsored malicious cyber activity, see the FBI's [Iran Threat](#) webpage.

¹ The IRGC is an Iranian Government agency tasked with defending the Iranian Regime from perceived internal and external threats.

U.S. organizations: All organizations should report incidents and anomalous activity to FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

United Kingdom organizations: Report significant cyber security incidents to ncsc.gov.uk/report-an-incident (monitored 24 hours).

This document is marked TLP: CLEAR. Disclosure is not limited. Sources may use TLP: CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP: CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tlp](https://www.cisa.gov/tlp) (<https://www.cisa.gov/tlp>)

TLP: CLEAR

TECHNICAL DETAILS

Threat Actor Activity

The cyber actors working on behalf of the IRGC gain access to victims' personal and business accounts using social engineering techniques, often impersonating professional contacts on email or messaging platforms. In addition, these actors might attempt to impersonate known email service providers to solicit sensitive user security information on email or messaging platforms. The targets usually have some nexus to Iranian and Middle Eastern affairs, such as current or former senior government officials, senior think tank personnel, journalists, activists, and lobbyists. More recently, FBI has observed these actors targeting persons associated with US political campaigns. The actors often attempt to build rapport before soliciting victims to access a document via a hyperlink, which redirects victims to a false email account login page for the purpose of capturing credentials. Victims may be prompted to input two-factor authentication codes, provide them via a messaging application, or interact with phone notifications to permit access to the cyber actors. Victims sometimes gain access to the document but may receive a login error.

Cyber actors working on behalf of the IRGC tailor instances of social engineering to include areas of interest or relevance to a target, including:

- Impersonations of known individuals, associates, and/or family members;
- Impersonations of known email service providers regarding account settings;
- Requests from impersonation accounts of well-known journalists for interviews;
- Conference invitations;
- Speaking engagement requests;
- Embassy events;
- Foreign policy discussions/opinions and article reviews; and,
- Current US campaigns and elections.

Indications of successful compromise include:

- Suspicious logins to victim accounts from foreign or domestic IP addresses;
- Creation of message handling rules to forward emails and prevent victims from receiving; notifications of the compromise;
- Connection of unknown devices, applications, or accounts to a victim account;
- Exfiltration and deletion of messages; and,
- Attempts to access other victim accounts.

Cyber actors working on behalf of the IRGC have used the following malicious domains:

Disclaimer: The below indicators are historical infrastructure associated with cyber actors working on behalf of IRGC. This data is being provided for informational purposes, to facilitate the identification of past cyber incidents, and to enable better tracking and attribution of these cyber actors. FBI does not recommend blocking the following domains based solely on their inclusion in this JCISA.

- 3dauth[.]live
- 3dconfirmation[.]com
- accesscheckout[.]online
- accessverification[.]online
- accunt-loqin[.]ml
- accurateprivacy[.]online
- atlantic-council[.]com
- bitly[.]org[.]il
- boom-boom[.]ga
- bytli[.]us
- continuetogo[.]me
- continue-to-your-account[.]000webhostapp[.]com
- covi19questionnaire[.]000webhostapp[.]com
- covid19questionnaire[.]freesite[.]vip
- css-ethz[.]ch
- cutly[.]biz
- cutly[.]vip
- daemon-mailer[.]com
- de-ma[.]online
- direct-access[.]info
- discovery-protocol[.]ml
- docfileview[.]org
- doctransfer[.]online
- dreamycareer[.]com
- dr-sup[.]live
- email-daemon[.]site
- email-protection[.]online
- file-access[.]com
- filetransfer[.]club
- freahman[.]online
- freshconnect[.]live
- gdrive-files[.]com
- gettogether[.]quest
- gl-sup[.]online
- gm-sup[.]com

TLP: CLEAR

- g-shorturl[.]com
- home[.]kg
- idccovid19questionnaire[.]000webhostapp[.]com
- ipsss[.]000webhostapp[.]com
- linkauthenticator[.]online
- litby[.]us
- lovetoflight[.]com
- lst-accurate[.]com
- ltf[.]world
- mailerdaemon[.]info
- mailer-daemon[.]live
- mailer-daemon[.]me
- mailer-daemon[.]net
- mailer-daemon[.]online
- mailer-daemon[.]org
- mailer-daemon[.]site
- mailer-daemon[.]us
- mailer-daemon-message[.]co
- mailer-support[.]online
- mfa-ic[.]ae
- mofa-ic[.]ae
- myconnect-support[.]com
- on-dr[.]com
- private-file-sharing[.]000webhostapp[.]com
- qmail[.]ml
- reactivate-disabled-accounts[.]000webhostapp[.]com
- redirect-drive[.]online
- safeshortl[.]jink
- shared-files-access[.]live
- sharefilesonline[.]live
- summit-files[.]com
- tinyurl[.]co[.]il
- tinyurl[.]jink
- tinyurl[.]live
- uani[.]us
- verificationservice[.]online
- washingtonInstitute[.]org
- workstation2020[.]000webhostapp[.]com
- www-myaccounts-support[.]000webhostapp[.]com
- youtransfer[.]live

TLP: CLEAR

MITIGATIONS

FBI, CNMF, Treasury, and UK NCSC recommend our partners remain vigilant and, if the behaviors outlined in this advisory are observed, US based individuals can contact their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be found at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov. Report UK-based significant cyber security incidents at ncsc.gov.uk/report-an-incident (monitored 24 hours). The authoring agencies recommend the following mitigation actions:

Social Engineering/Spoofing

- Be suspicious of unsolicited contact from any individual you do not know personally or contact from people you may know but are claiming to be using new accounts or phone numbers.
- Be suspicious of attempts to pass links or files via social media from anyone you do not know or from people you know who are using new accounts or phone numbers.
- Be suspicious of unsolicited requests to share files via online services, especially from people you do not know or people with whom you typically do not share files in this manner.
- Be suspicious of email messages conveying suspicious alerts for online accounts, including login notifications from foreign countries or other alerts indicating attempted unauthorized access to your accounts. FBI recommends logging into your accounts directly (versus using a link to do so) to review alerts.
- Be suspicious of emails purporting to be from legitimate online services (i.e. the images in the email appear to be slightly pixelated and/or grainy, language in the email seems off, sender email address looks suspicious, messages originate from an IP not attributable to that provider/company, etc.).
Be suspicious of unsolicited email messages that contain shortened links (i.e. via tinyurl, bit.ly, etc.).
- Refer to the guides in Appendix A for detecting malicious actor email rules enabling auto-forwarding or fetching from compromised email accounts.

Enterprise Mitigation

- Implement a user training program with phishing exercises to raise and maintain awareness among users about risks of visiting malicious websites or opening malicious attachments. Reinforce the appropriate user response to phishing and spear-phishing emails. Cyber hygiene awareness for personal accounts and company accounts is strongly recommended.
- Recommend using only official email accounts for official business, updating software, avoiding clicking on links or opening attachments from suspicious emails before confirming their authenticity with the sender, and turning on multi-factor authentication to improve online security and safety.
- Recommend users consider advanced account protection services and hardware security keys.
- Enable anti-phishing and anti-spoofing security features that block malicious email.
- Prohibit automatic forwarding of email to external addresses.

TLP: CLEAR

- Frequently monitor the company email server for changes in configuration and custom rules for specific accounts.
- Add an email banner to messages coming from outside your organization.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable alerts for suspicious activity, such as foreign IP address logins.
- Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.
- When available, use single sign on with either Passkeys, alternate Fast Identity Online (FIDO) authenticators, or Single Sign On backed by a phishing-resistant multi-factor authentication.
- Protect email in transit by enabling Transport Layer Security (TLS).

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. The FBI, CNMF, Treasury, and NCSC do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring.

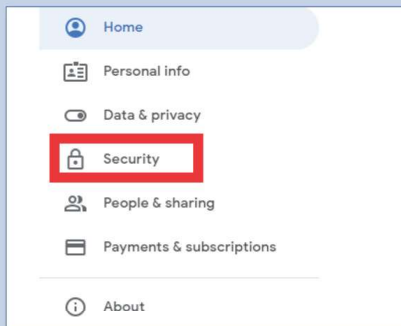
TLP: CLEAR

APPENDIX A: SECURING ONLINE ACCOUNTS

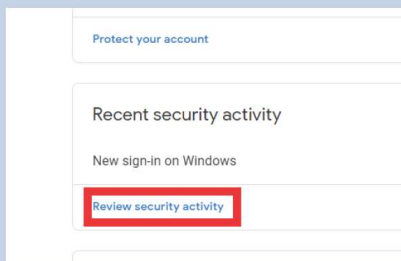


From a desktop computer, follow these steps to bolster your account's security:

1. Navigate to myaccount.google.com.
2. On the left side of the screen, select "Security."

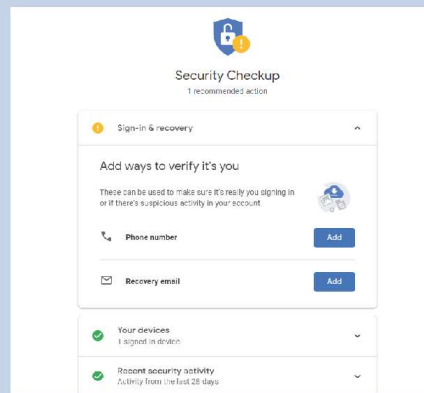


3. Under "Recent Security Activity," select "Review Security Activity."



4. If any activity seems suspicious to you, select the "Unrecognized Activity" button in red and choose "No, secure account."
5. Once confirming, a password reset option will present itself, click through and do so.

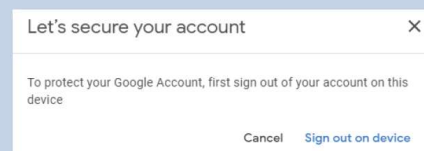
6. You will then be prompted to complete a security check-up, which will display your recovery phone and email. Ensure these are accurate.



7. Select "Continue to your Google Account" once the recovery information in step 6 is confirmed.
8. Still on the Security tab, under the "Your Devices" header, select "Manage Devices."



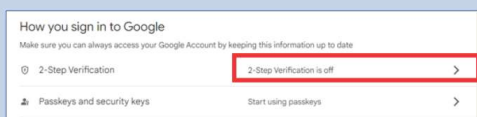
9. Similar to the Activity, if any devices look unfamiliar to you, select said device and choose "Don't Recognize Something?," at which point you can sign out of device using the button shown below:





Mitigation Guidance: A Practical Guide to Securing Your Google Account

10. Repeat step 9 for all unrecognized devices.
11. Moving forward, under the “How you sign in to Google” header in the Security tab, choose the option for “2-step Verification.”

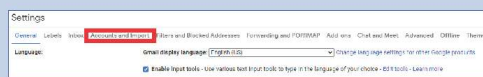


12. On the next page, click the “Get Started” button where you’ll be prompted for your password.
13. At this step, choose either the voice or text message options to set up your authentication method, which will then send out a key to your phone for confirmation.
14. If showing, check “Apps with Access to your Account,” or search “third” in the search bar at the top of the screen and select “Third-party apps.” Once again, disable connections with any unfamiliar links.



Now, strictly for your Gmail address:

1. Go to settings > see all settings
2. Select “Accounts & Import.”



3. Under “Send Mail As,” “Check Mail From Other Accounts,” and “Grant Access to your Account,” remove any accounts linked.
4. Under “Forwarding and POP/IMAP,” remove any listed accounts.



5. Under “Filters and Blocked Addresses,” select any suspicious showing and select “Delete.”



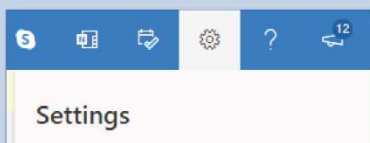
6. Lastly, under add-ons, ensure no add-ons are listed.



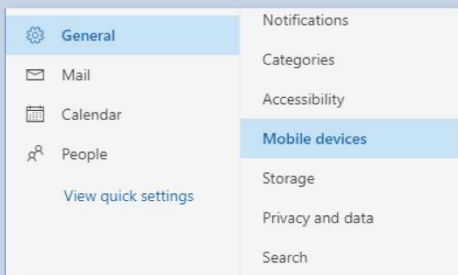
Mitigation Guidance: A Practical Guide to Securing Your Outlook Account


From a desktop computer, follow these steps to bolster your account's security:

1. Navigate to **outlook.live.com**.
2. At the top-right of the screen, click the gear icon.

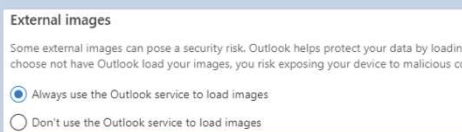


3. In the settings window, click "General" on the left side, and choose the "Mobile Devices" subcategory. If any unknown devices exist on this page, simply click the trash icon to remove them as seen in the example below:



Device	Phone number	Status	
ChatService		OK	
UniversalOutlook		OK	

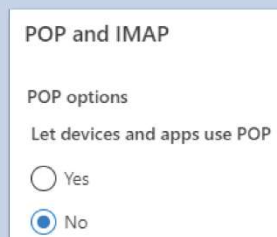
4. Under the "Privacy & Data" subcategory, ensure "Always use the Outlook service to load images" is checked.



5. Return to the "Mail" section from the left dialog menu. Then enter the "Rules" subcategory and remove all suspicious rules found there.



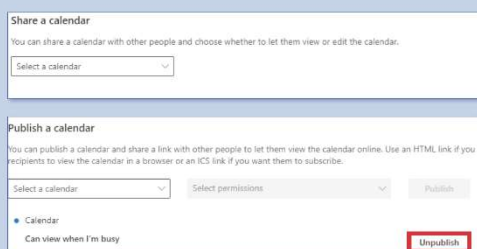
6. For the "Sync Email" subcategory, under "POP and IMAP," certify that "Let devices and apps use POP" is set to No.



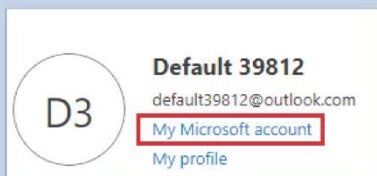
7. Under "Forwarding" subcategory, verify that the "Enable Forwarding" box is unchecked.

Mitigation Guidance: A Practical Guide to Securing Your Outlook Account

8. Click to the “Calendar” section from the left dialog menu. Within this section, under the submenu “Shared Calendars,” remove any connected accounts.

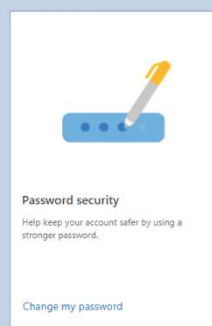


9. Once complete, migrate back to outlook.live.com once more. Click on your profile photo at the top-right, and select “My Microsoft Account” from the drop-down.

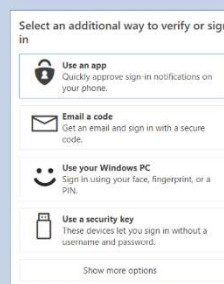


10. Check and remove any suspicious devices showing under the “Devices” header.
11. Select “Security” from the menu at the top of the screen.

12. Either near the top of the page, or on the second tile, select “Change Password.”



13. Once complete, select the third tile for “Advanced Security.” Under “Way to prove who you are,” remove any suspicious methods of sign-in. Then select “Add a new way to sign-in” and select any of the available app, email, biometric, or security key options shown to enable two-factor authentication.

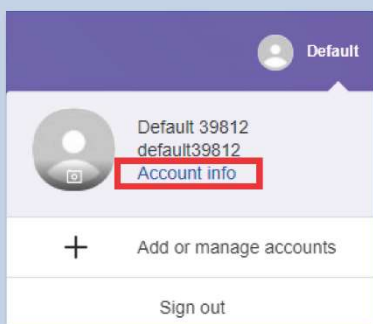


14. Migrate to the Privacy section from the top menu, scroll to the bottom, and select “Apps and Services,” Eliminate all those showing here by clicking edit > remove these permissions.
15. Finally, Near the bottom of the “Advanced Security” page we previously navigated to, select “Sign Out Everywhere.”

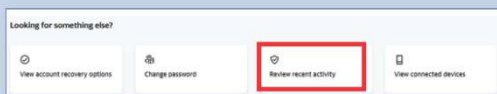
Mitigation Guidance: A Practical Guide to Securing Your Yahoo Account

From a desktop computer, follow these steps to bolster your account's security:

1. Navigate to mail.yahoo.com.
2. On the top-right of the screen, click on your profile name and image, and select "Account Info."



3. From the bottom panel, select "Recent Activity."

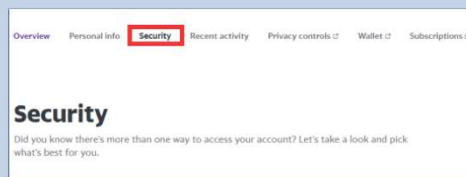


4. Review recent activity and account changes looking for any suspicious activity. If any devices seem suspicious, select "sign out."

5. Additionally, remove any devices or apps listed under "Review your connected devices and apps" as shown below:

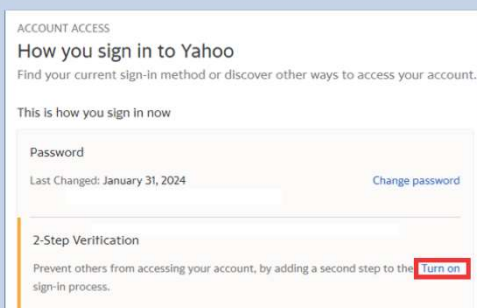


6. Once complete, shift back to the "Security" tab on the top menu (you may be requested to sign-in again).

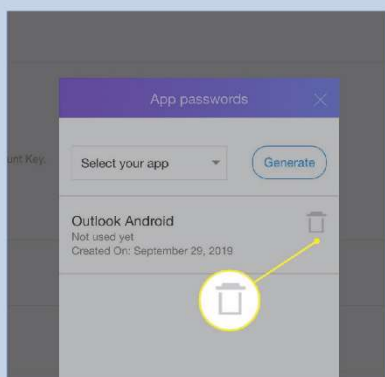


7. If you have not done so already, under the "How you sign into Yahoo" tab, select "Change Password" and proceed in creating a strong, new password for your account.
8. Once complete, in same section, select "Turn on" under 2-step Verification, click "Get Started" and select a method for enabling your second factor of authentication (visual accompaniment provided on back page).

Mitigation Guidance: A Practical Guide to Securing Your Yahoo Account

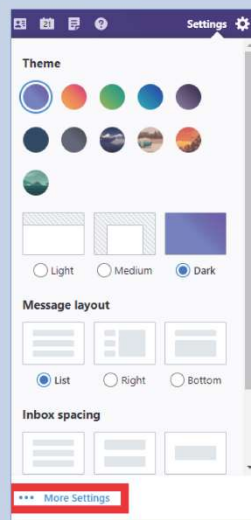


9. At this juncture, ensure that in the section below this labeled “App Passwords,” you remove any items that are shown:

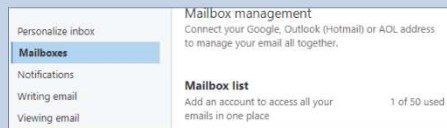


10. Moving further down the “Account Security” page, ensure both Recovery Emails and Recovery Phone Numbers are correct.

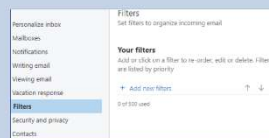
11. Going back to mail.yahoo.com, proceed to Settings > More Settings.



12. From here, choose “Mailboxes” from the dialog on the left, and select your email listed under “Mailbox List.” In the now-opened middle panel, remove any addresses shown as forwarding emails.



13. Lastly, select the “Filters” tab from the left dialog, and delete any filtering rules seen there.

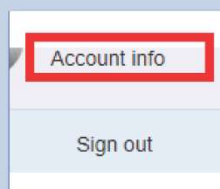




Mitigation Guidance: A Practical Guide to Securing Your AOL Account

From a desktop computer, follow these steps to bolster your account's security:

1. Navigate to **mail.aol.com**.
2. On the top-right of the screen, click on your profile image, then select "Account Info."



3. From the top panel, select "Recent Activity."

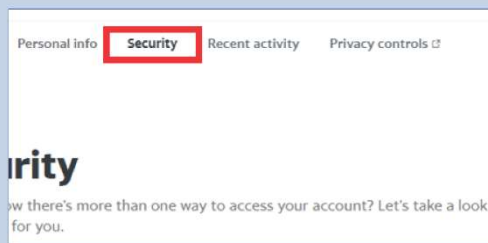


4. Review recent activity and account changes looking for any suspicious activity. If any devices seem suspicious, select either "View all Connected (Devices/Activity)" and select "Change your Password."

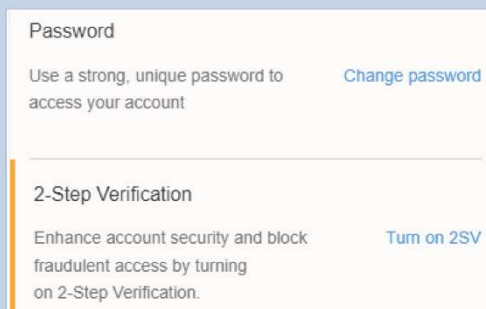
5. Additionally, remove any apps listed under "Apps connected to your account" as shown below:



6. Once complete, shift back to the "Security" tab on the top menu (you may be requested to sign-in again).

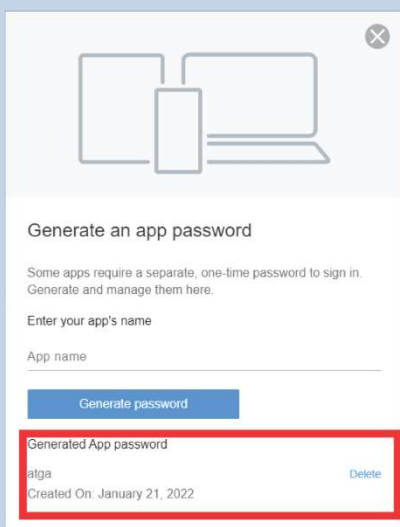


7. If you haven't done so already through previous steps, under the "How you sign into AOL" tab, select "Change Password" and proceed in creating a strong, new password for your account.
8. Once complete, in same section, select "Turn on" under the 2-step verification prompt., click "Get Started" and select a method for enabling your second factor of authentication.



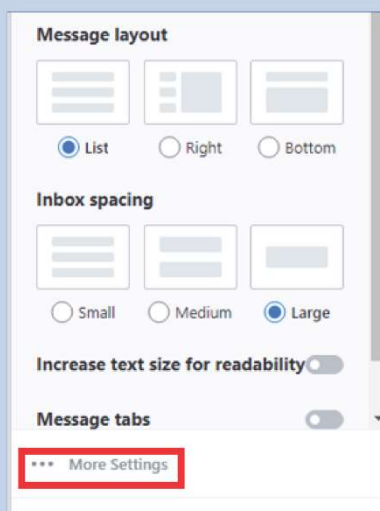
Mitigation Guidance: A Practical Guide to Securing your AOL Account

9. At this juncture, ensure that in the section below this labeled "App Passwords," you remove any items that are shown:



10. Moving further down the "Account Security" page, ensure both Recovery Emails and Recovery Phone Numbers are correct.

11. Going back to mail.aol.com, we can proceed on the right to Settings > More Settings



12. Lastly, select the "Filters" tab from the left dialog, and delete any filtering rules seen there by clicking the X on each filter showing.

