(Updated post in continuation to the one posted on 15th June 2022 on Auronet by Auroville Foundation)

In continuation to our previous post, we would like to inform all Aurovilians regarding updates on the auroville.org.in email system and sysop. This is especially important since a number of alarming posts full of lies, half-truths and fabrications have been posted by various factions to community members in order to sow hysteria and create some form of panic over user emails, online data and privacy.

Though currently a preliminary investigation is still ongoing, we nevertheless thought it best to post an update on this topic, as it had become evident through repeated and multiple posts that an atmosphere of panic was being drummed up quite purposefully, in order to draw users away from the current mailing system by labeling it "insecure", and spreading malicious misinformation that the Foundation Office (FO) and its staff were prying into people inboxes. Nothing could be further from the truth.

So in order to help members of the community to better understand the situation as it is being dealt with - here is a short sequence of events on the matter as they have transpired over the last few weeks.

Please read through to understand the issue at hand fully

Admin Access:

15/5/22: A police complaint is received at the Foundation Office alleging use and misuse of Auroville's email systems, google cloud apps and internal bulletin board of Auronet being used and abused to foster and spread anti-national and anti-government sentiments.

17/5/22: The FO reaches out to Sysop and the Webservices teams to request for the backend administrative access to these platforms in order to conduct an investigation. An initial email is sent around 2 PM and is then followed up with a reminder around 6 PM.

That same night, FO receives responses including from the FAMC, that no such access would be granted.

18/5/22: FO at this point reaches out directly to Google HQ to request for legal access to the Google workspace, while requesting mailbox operation does not suffer from any downtime allowing for smooth functioning of the email operations.

19/5/22: Upon the FO's request, Google disables access to all current and past workspace administrators accounts.

1st June 22: The Auroville Foundation is legally granted admin access by Google.

Sysop Action:

Sequence of events for 17th/18th and 19th May; as evident from the Sysop audit logs (investigation still ongoing):

Sysop receives two emails from Undersecretary Mr. Srinivasmurthy

Sysop then creates 3 new accounts and grants them admin privileges.

sysop17

sysop23

sysop56

Sysop then downgrades 3 existing admin accounts to regular member accounts:

da

ublass

sysop02

user bharathy remains to continue as an admin account.

User group details are downloaded from the server along with data and other google drive contents (without any authorization from FO).

A third party secure connection is then made to an obscure service through APIs to transfer confidential and private user data out; again without any authorization from FO.

Sysop then deletes certain specific folders, documents and drives as well as mailing groups.

On 19th of May, Sysop admins lose access to the Google workspace.

Technical Facts on Google Workspace and it's functions:

To address the fears that have been spread by various groups, the FO wants to let all mailbox users know that, in spite of all the hysteria that you may have come across repeatedly through shared posts, Google workspace is technically designed in such a manner that a system admin cannot explicitly read into a users mailbox and without your getting alerted to it. The only ways for a backend admin to gain access to your account is if:

- the admin forcefully resets or changes your existing password

- the admin changes and updates your current password/account recovery details to a different mobile number /email.

Also it is interesting to note that:

- the mailbox user (you, for example) can decide to forward a copy of the emails to another mailbox only via the front-end settings. A backend admin (workspace administrator) CANNOT set up such settings, since both sending and receiving mailboxes need to have a shared verification code for such forwarding to work with both users' consent.

In either case (whether you try to set up mail forwarding or a workspace administrator), the user is alerted of the same and system logs are generated for future audit purposes. So without your knowledge such a breach is simply not possible. This is how mailboxes are designed to keep both tech data and user data safe and secure from any prying eyes.

Securing your account and data/email:

We would like to take this opportunity to remind you to secure your accounts through 2-factor authentication (2FA) in your account settings, this mailbox feature allows for 2FA verification codes to be sent to a mobile number or other email address that you own and/or through Google Authenticator app by adding an extra layer of security to your account.

And should you still feel insecure about your emails, mail account and data privacy - please use end to end encryption tools and such PGP to send and receive encrypted emails such that only the intended recipient(s) read through the content of your emails through public and private keys.

In doing so, one can continue to use the same mailbox and email address without being worried over mails being 'read into' by unauthorized/unintended recipients while in transit or on delivery.

Preliminary Audit:

Our preliminary audits of the system admin logs reveal that the previous Sysop admins had been reading into mail headers of different user accounts for incoming or outgoing emails over the last months.

Email headers are provided to system administrators to help troubleshoot email issues; however largely, across organizations, reading of email headers for reasons other than for troubleshooting purposes is generally considered as both unethical and immoral, even though the legalities of the same are governed through non-disclosure agreements system admins.

The initial audits that have been conducted reveal that the email headers of a number of mailboxes of Auroville residents and Auroville working groups, units and services have been read into by Sysop over the last six months.

The mailbox users are being reached out individually to inform them of the same.

Criminal investigation for Cyber crimes:

The investigation also reveals that confidential Government of India data from auroville.org.in mailboxes/drives have been illegally transferred out to obscure server(s) without any prior authorisation, consent or approval from the FO. The matter is now awaiting investigation under the relevant cybercrime laws both through IT Act as well as the relevant IPC through the IT Cell.

The audit also has revelaed that the following Auroville working groups mailbox accounts had their email settings set to automatically “forward and delete” all incoming emails to an obscure domain of auroville.services - which is currently awaiting investigation by the cybercrime division.

AVC and AVC office

Workingcom and WCoffice

FAMC

Admin Famc

Applications FAMC

AV Security

Since the matter is now under investigation, this is a very delicate situation, and therefore we would like to inform you that the Auroville Foundation has taken great care to ensure no individual accounts experience any inconvenience or downtimes and continue to smoothly operate as before.

Anyone with questions and needing support with their emails/mailboxes and mailing groups etc can reach out to mailbox@auroville.org.in

Regards,

Auroville Foundation Office

(Annex from the previous post has been removed on user request)

Update on sysop and auroville email

By Auroville Foundation , 15 Jun 2022 / 06:44 pm

in Announcement

Tags auroville.org.in cybercrime Email sysop

7

In continuation to our previous post, we would like to inform all Aurovilians regarding updates on the auroville.org.in email system and sysop. This is especially important since a number of alarming posts full of lies, half-truths and fabrications have been posted by various factions to community members in order to sow hysteria and create some form of panic over user emails, online data and privacy.

Though currently a preliminary investigation is still ongoing, we nevertheless thought it best to post an update on this topic, as it had become evident through repeated and multiple posts that an atmosphere of panic was being drummed up quite purposefully, in order to draw users away from the current mailing system by labeling it "insecure", and spreading malicious misinformation that the Foundation Office (FO) and its staff were prying into people inboxes. Nothing could be further from the truth.

So in order to help members of the community to better understand the situation as it is being dealt with - here is a short sequence of events on the matter as they have transpired over the last few weeks.

Please read through to understand the issue at hand fully

Admin Access:

15/5/22: A police complaint is received at the Foundation Office alleging use and misuse of Auroville's email systems, google cloud apps and internal bulletin board of Auronet being used and abused to foster and spread anti-national and anti-government sentiments.

17/5/22: The FO reaches out to Sysop and the Webservices teams to request for the backend administrative access to these platforms in order to conduct an investigation. An initial email is sent around 2 PM and is then followed up with a reminder around 6 PM.

That same night, FO receives responses including from the FAMC, that no such access would be granted.

19/5/22: FO at this point reaches out directly to Google HQ to request for legal access to the Google workspace. And upon the FO's request, Google disables access to all current and past workspace administrators accounts.

1st June 22: The Auroville Foundation is legally granted admin access by Google.

Sysop Action:

Sequence of events for 17th-19th May as evident from the Sysop audit logs (investigation still ongoing):

Sysop receives email from Undersecretary Mr. Srinivasmurthy

Sysop then creates 3 new accounts and grants them admin privileges.

sysop17

sysop23

sysop56

Sysop then downgrades 3 existing admin accounts to regular member accounts:

da

ublass

sysop02 and user bharathy remains to continue as an admin account.

User group details are downloaded from the server along with data and other google drive contents (without any authorization from FO)

A third party secure connection is then made to an obscure service through APIs to transfer confidential and private user data out; again without any authorization from FO.

Sysop then deletes certain specific folders, documents and drives as well as mailing groups.

On 19th of May, Sysop admins lose access to the Google workspace.

Technical Facts on Google Workspace and it's functions:

To address the fears that have been spread by various groups, the FO wants to let all mailbox users know that, in spite of all the hysteria that you may have come across repeatedly through shared posts, Google workspace is technically designed in such a manner that a system admin cannot explicitly read into a users mailbox and without your getting alerted to it. The only ways for a backend admin to gain access to your account is if:

- the admin forcefully resets or changes your existing password

- the admin changes and updates your current password/account recovery details to a different mobile number /email.

Also it is interesting to note that:

- the mailbox user (you, for example) can decide to forward a copy of the emails to another mailbox only via the front-end settings. A backend admin (workspace administrator) CANNOT set up

such settings, since both sending and receiving mailboxes need to have a shared verification code for such forwarding to work with both users' consent.

In either case (whether you try to set up mail forwarding or a workspace administrator), the user is alerted of the same and system logs are generated for audit purposes. So without your knowledge such a breach is simply not possible. This is how mailboxes are designed to keep both data and user data safe and secure from any prying eyes.

Securing your account and data/email:

We would like to take this opportunity to remind you to secure your accounts through 2-Factor Authentication in your account settings, this mailbox feature allows for 2FA verification codes to be sent to a mobile number or other email address that you own and/or through Google authentication adding an extra layer of security to your account.

And should you still feel insecure about your mails, mail account and data privacy - please use end to end encryption tools and such PGP to send and receive encrypted emails such that only the intended recipient(s) read through the content of your emails through public and private keys.

In doing so, one can continue to use the same mailbox and email address without being worried over mails being ‘read into’ by unauthorized/unintended recipients while in transit or on delivery.

Preliminary Audit:

Our preliminary audits of the system admin logs reveal that the previous Sysop admins had been reading into mail headers of different user accounts for incoming or outgoing emails over the last months.

Email headers are provided to system administrators to help troubleshoot email issues; however largely, across organizations, reading of email headers for reasons other than for troubleshooting is generally considered as both unethical and immoral, even though the legalities of the same are governed through non-disclosure agreements system admins.

The initial audits that have been conducted reveal that the email headers of a number of mailboxes of Auronet residents and Auroville working groups and services have been read into by Sysop over the last 6 months.

The users are being reached out individually to inform them of the same.

Criminal investigation for Cyber crimes:

The investigation also reveals that confidential Government of India data from auroville.org.in mailboxes/drives have been illegally transferred out to obscure server(s) without any prior authorisation, consent or approval from the FO. The matter is now awaiting investigation under the relevant cybercrime laws both through IT Act of 2020 as well as the relevant IPC through the IT Cell.

The audit also has revelaed that the following Auroville working groups mailbox accounts had their email settings set to automatically “forward and delete” all incoming emails to an obscure domain of auroville.services - which is currently awaiting investigation by the cybercrime division.

AVC and AVC office

Workingcom

FAMC

Admin Famc

Applications FAMC

AV Security

Since the matter is under investigation, this is a very delicate situation, and therefore we would like to inform you that the Auroville Foundation has taken great care to ensure no individual accounts experience any inconvenience or downtimes and continue to smoothly operate as before.

Anyone with questions and needing support with their emails/mailboxes and mailing groups etc can reach out to mailbox@auroville.org.in

Regards,

Auroville Foundation Office