Secure a Compromised Gmail Account

Stephanie Obodda - 2023-04-28 - Comments (0) - General Security

> If you believe that your account has been compromised, please complete the following recommended steps for its recovery as soon as possible to secure your compromised account, protect others who may respond to spam sent from you from becoming compromise as well, and to safeguard yourself from being compromised again in the future.

FIRST: Change your passwords!

Change your Brown password immediately. You can do this by

1. going to https://myaccount.brown.edu
2. click **Login and Manage Account**
3. sign in
4. click on **Change Brown Password** on the left-hand side
5. submit a password change

You should also change the password for any other accounts that use the same password and passwords for accounts that you think may no longer be secure.

> OIT suggests using different passwords for your online accounts. If you're on Chrome, you can use Google's password generator to generate complex passwords that will be stored within Chrome. You can also use Brown-authorized services like LastPass.

SECOND: Check your Duo settings

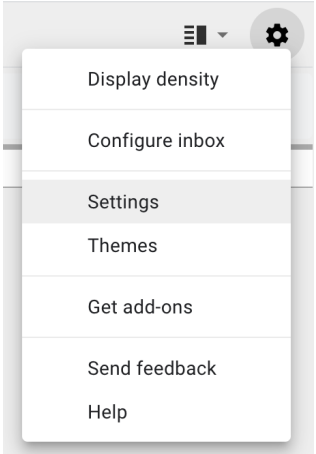
1. In https://myaccount.brown.edu
2. click the menu option for **Two-Step Verification**
3. Review all of the devices listed on the page and confirm they are yours
4. If you have any Duo bypass codes, click the button to expire them and generate brand new codes if truly necessary.

Be sure to never allow access to systems you are not personally trying to access when you receive any notifications from Duo.

NEXT: The Security Checklist

These steps require you sign into Gmail.com with your Brown email account while on a computer.

Go into your Gmail account's settings by clicking on the cog/gear at the top, right-hand corner of Gmail and then clicking Settings.



General tab

Signature: Make sure that your signature is either set to **No signature** or it's something that you've created.

Vacation responder: This should be either be set to **Vacation responder off** or have a response you've created.

Accounts tab

Send mail as: This should be set as your name and Brown email address. If needed, you can correct it by clicking on **edit info**, make your edit, and click **Save changes**.

Filters and Blocked Address tab

Filters: Filters are rules applied to your email. Delete any rules you did not create; like ones that delete your email.

Blocked addresses: Unblock any email addresses that should be allowed to email you.

Forwarding and POP/IMAP tab

Forwarding: This should either be set to **Disable forwarding** or set to forward to an address you approve.

POP download: This should be disabled unless you know used for an email client (e.g. Outlook, Thunderbird, etc.).

IMAP access: This should be disabled unless you know used for an email client (e.g. Outlook, Thunderbird, etc.).

> Make sure to click on **Save changes** if you made any corrections to your settings.

Sign out all other web sessions

Click on the word **Details** located at the bottom right-hand corner of Gmail. You may need to scroll down if you've got a lot of email. Clicking this will open a new window.

In the new window, click on **Sign out all other web sessions**. You can also view the last 10 times your account was accessed on this page. You can close out the window you receive notice that all other sessions have been signed out.

Third-party apps with account access

1. Sign into https://myaccount.google.com with your Brown Gmail account.
2. Click on Security on the left-hand side.
3. If any third-party apps have access to your account, you should see the **Third-party apps with account access** section. If you don't have this option, you can ignore the next few steps.
4. If you do see this option, click on **Manage third-party access** to review all the apps that have access to your account.
5. To remove an app's access to your account, click on the app and click **Remove Access.**

Additional items to check out

- Check your **Sent** mail to review any email that went out of your account while it was compromised.
- Check your **Google Drive** documents to check your sharing permissions.
- Check your computer for **malware/viruses**.

Add an Extra Layer of Protection

Protect your new passwords with Two-Step Verification. Visit the Two-Step section of the IT Knowledgebase for an overview and how to get started.

It is also recommended that if fraudulent emails were sent to your contacts from your account, please consider communicating to them that your email account was compromised and that the messages were not sent by you.

If you had been in previous contact with the IT Service Center, notify them when you have completed these steps.

If you discovered that confidential or restricted information may have been compromised as well, please notify the Information Security Group at ISG@brown.edu.

Attachments

- Secure a Compromised Gmail Account-2019-08-07.html (4.00 KB)