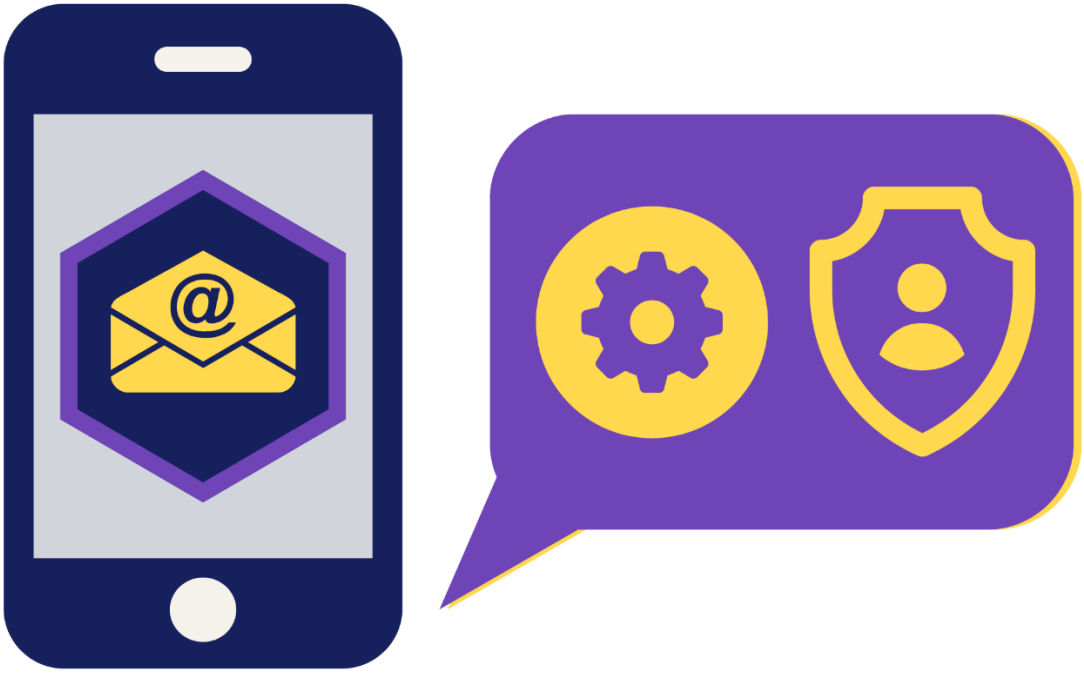
Tech Safe BC

Outlook Account Security Guide for Survivors of Intimate Partner Violence

Compiled by Tech Safe BC



Last Updated: January 27, 2026

Symbols and What They Mean in This Guide:

Course of action may be visible to your former or current partner.
You may want to consult with a staff of an anti-violence program in your community before removing your former or current partner's access.

Evidence documentation checkpoint. Take screenshots, pictures with a different device, or screen recordings of your former or current partner's unauthorized access.

If you have an Outlook account (previously called Hotmail) and suspect that your account and/or device has been compromised, this guide will help you review important settings and increase the security on your account. The instructions are based on accessing your Outlook account on a web browser. It is easiest to follow these instructions on a laptop or desktop computer. Note that Microsoft does not endorse nor sponsor this toolkit.

Before taking any steps such as removing access to suspicious accounts or turning off location sharing, it is important to consider collecting evidence and discussing any potential safety concerns as a result of these changes with your support worker.

If something in this guide is no longer up to date, or difficult to understand, please reach out to techsafe@bcsth.ca with your concerns.

If You Suspect There is Unauthorized Access to Your Account

Before taking these steps, consider creating a new, secure email address with an email provider such as Google, Microsoft, Yahoo Mail or Proton Mail on a secure device. You can use this email address for secure communication and to store important documents, as well as an account recovery email.

In addition to following these steps to secure your email account, you will want to secure other accounts (social media, ride share, food delivery, banking), as well as secure your devices (iCloud/iPhone, Android). Guides to do this can be found here.

☐ Check Recovery Email and Phone Number

Safety Tip:

If your former/current partner has access to the email or phone associated with the account, it is possible for your former/current partner to access your account.

Before updating your information to include a secure phone number or email address, consider discussing any safety concerns with your support worker.

To check your recovery email and phone number:

1. Go to the https://account.microsoft.com and log in.
2. On the left vertical bar, click the **Security icon** (shield).
3. Under the 'Account Security' heading, click the **Manage how I sign in** button.
4. Review recovery email and phone numbers.

Source: Microsoft Support

☐ Reviewing Log-Ins and Recent Account Activity

Safety Tip:

Be sure to take screenshots/recordings of the unauthorized log-ins. Before removing unauthorized access, consider discussing potential safety concerns with your support worker.

If you suspect someone has logged in to your account without your consent, review your login history.

To review your login history and recent account activity:

1. Go to https://account.microsoft.com and log in.
2. On the left vertical bar, click the **Security icon** (shield).
3. Under the 'Account Security' heading, click **View my sign-in activity**.
    a. You will see the date and time of each sign-in, location (IP address & region), device or platform used and whether the sign-in was successful or unsuccessful.
4. Scroll down further to the 'Recent activity' heading to review if any suspicious or unrecognized activity has occurred.

☐ Check the Mobile Devices List (the devices that you are synching your mailbox with)

Safety Tip:

Before signing out all devices, consider collecting evidence and discussing potential safety concerns with your support worker.

To check your mobile devices that are synched with your mailbox:

1. Go to https://outlook.live.com/mail and log in.
2. On the top right, click the **Setting icon** (gear). 
3. On the left menu bar, click **General**.
4. Click **Mobile Devices**.
5. Make sure you recognize the devices that appear on that list.

Source: Microsoft Support

☐ Check Rules

To check the rules:

1. Go to https://outlook.live.com/mail and log in.
2. On the top right, click the **Setting icon** (gear). 
3. On the left menu bar, click **Mail**.
4. In the middle menu bar, click **Rules**.
5. Make sure that the list is empty or that you recognize the rules that appear on that list.

Source: Microsoft Support

☐ Check Forwarding

To check forwarding:

1. Go to https://outlook.live.com/mail and log in.
2. On the top right, click the **Setting icon** (gear). 
3. On the left menu bar, click **Mail**.
4. In the middle menu bar, click **Forwarding and IMAP**.

5. Make sure that the list is empty or that you recognize the rules that appear on that list.

Source: Microsoft Support

☐ Changing Passwords

If your former/current partner has or is logged into your Outlook account, changing your password can prevent them from logging into your account again. To make a secure password, refer to How to Create and Maintain Strong Passwords in this library.

Safety Tip:

Changing your password will log all sessions out of your account. Consider discussing any potential safety concerns with your support worker before proceeding.

To change your password:

1. Go to https://account.microsoft.com and log in.
2. On the left vertical bar, click the **Security icon** (shield).
3. Under the 'Account Security' heading, click the **Manage how I sign in** button.
4. Under the heading 'Enter password,' click **Change password**.
5. Follow prompts to change your password to a new, secure password.

☐ Turning on 2-Factor Authentication (2FA)

Turning on 2FA can protect your account from future unauthorized logins, check the resource in this library to understand why 2FA is important.

Safety Tip:

Before enabling 2FA, make sure the password to your account is secure, and that you are the only one who has access to the email and/or phone number connected to your account. If 2FA is enabled on an account your current/former partner has access to, they will be notified of attempted logins through verification codes.

To turn on 2FA:

1. Go to https://account.microsoft.com and log in.
2. On the left vertical bar, click the **Security icon** (shield). 
3. Under the 'Account Security' heading, click the **Manage how I sign in** button.
4. Under the 'Additional security' heading, find the 'Two-step verification' sub-heading, and click **Turn on**.
5. Follow the prompts.

If you are experiencing tech abuse, you are not alone. Find support in your community by connecting with a BC Society of Transition Houses Member Program or check out our other safety resources at techsafebc.bcsth.ca.