



Account Security & Optimization Checklist

This checklist is designed for Hotmail and Outlook users who want to secure their digital identity and streamline their email workflow. It helps prevent lockouts, protects against hacking attempts, and turns a chaotic inbox into an organized tool. Use this list immediately after regaining access to your account to ensure long-term safety.

Phase 1: Securing Access and Recovery

- Verify that the browser address bar shows a lock icon before entering credentials.
- Update the recovery phone number in the security settings immediately.
- Add a secondary recovery email address that is currently active.
- Generate a unique Recovery Code from the Microsoft security dashboard.
- Print the Recovery Code and store it in a physical safe or lockbox.
- Remove any old or unrecognized devices from the "Trusted Devices" list.
- Clear browser cache and cookies if login issues persist.

Phase 2: Fortifying Account Defense

- Enable Two-Factor Authentication (2FA) in the advanced security options.
- Download an authenticator app instead of relying solely on SMS codes.
- Create a strong, unique password that is not used for any other service.
- Check the "Recent Activity" log for any successful logins from foreign locations.
- Disable the "Keep me signed in" option on all shared or public computers.
- Review connected apps and revoke access to services no longer in use.

Phase 3: Optimizing Workflow and Efficiency

- Download the official Outlook mobile app for better synchronization.
- Enable "Focused Inbox" to automatically filter out marketing spam.
- Create a "Follow Up" folder for emails requiring action within 24 hours.
- Set up a "Sweep" rule to auto-delete newsletters older than 30 days.
- Configure the email signature with a professional name and contact info.



- Customize the display density settings to reduce visual clutter.
- Test the search function to ensure old emails are being indexed correctly.

Phase 4: Ongoing Maintenance Habits

- Review the spam folder weekly to ensure legitimate mail is not lost.
- Unsubscribe from at least three newsletters every Friday.
- Update the email password once every six to twelve months.
- Export important contacts to a local file for backup once a year.