

Account Remediation Checklist

Prepared by the Ottawa Area Cybersecurity Operations Center

Purpose

This worksheet is used to track completion of account security remediation after a security alert or suspected compromise. **Do not write passwords on this document.** This checklist is for tracking actions only.

How to Use This Checklist

- Start with your primary email account and any account that can reset other passwords.
- Mark each action as completed before moving on.
- Enable multi factor authentication wherever it is available.
- Verify recovery email addresses and phone numbers after changing passwords.

Account Remediation Tracking

Service or Website	Username or Email	Password Reset (✓)	MFA Enabled (✓)	Recovery Info Verified (✓)	Date Completed	Notes
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		
		☐	☐	☐		

Password Manager Guidance

When resetting passwords after a security alert, we recommend avoiding saving new passwords directly in your browser. Browser stored passwords are tied to that browser profile and may be accessible without an additional layer of protection. Using a dedicated password manager provides stronger security by storing passwords in an encrypted vault and requiring an extra step to access them.

Free password managers we recommend

- [Bitwarden](#)
- [Keeper](#)
- [NordPass](#)
- [Dashlane](#)