

IS YOUR BUSINESS BROWSER PROTECTING WHAT IT SAVES?

Business Browser Security Checklist — IT Club

DEVICE

- ☐ Supported Windows version installed and up to date
- ☐ Automatic screen lock configured — short inactivity timeout
- ☐ Windows Hello configured — PIN, fingerprint or facial recognition
- ☐ BitLocker / device encryption enabled where appropriate
- ☐ Each user has their own Windows account — no shared logins

USER

- ☐ Each person uses their own Windows account
- ☐ Windows Hello set up for each user on each device
- ☐ Shared Windows logins reviewed and eliminated

BROWSER

- ☐ Current supported version of Chrome installed
- ☐ Automatic Chrome updates enabled
- ☐ Use Windows Hello when filling passwords — reviewed and enabled
- ☐ Verify it's you to autofill payment methods — reviewed and enabled
- ☐ Saved payment cards reviewed — unnecessary cards removed
- ☐ Saved card security codes reviewed
- ☐ Unnecessary browser extensions removed
- ☐ Extension permissions reviewed

CREDENTIAL

- ☐ Unique passwords used for all accounts
- ☐ A password manager in use
- ☐ Weak or reused passwords reviewed and replaced
- ☐ Passkeys used where the service supports them

ACCOUNT

- ☐ Google Account MFA or passkeys enabled
- ☐ Account recovery methods reviewed and current
- ☐ Work and personal Chrome profiles reviewed

BUSINESS

- ☐ Company payment card access restricted to staff who need it
- ☐ Browser policies documented
- ☐ Shared Windows accounts avoided

Chrome Autofill Verification — Both Settings

Two separate settings. Both need to be enabled.

PASSWORDS

Use Windows Hello when filling passwords

Protects: filling, revealing, copying, editing saved passwords

Chrome > Passwords and autofill > Google Password Manager > Settings

PAYMENT CARDS

Verify it's you to autofill payment methods

Protects: saved payment cards — screen lock must be configured

Chrome > Settings > Autofill and passwords > Payment methods

Turn on one and you have not necessarily turned on the other. Both may need configuring.

THE IT CLUB BROWSER SECURITY MODEL

DEVICE

Lock screen · Patching · Encryption

USER

Individual accounts · Windows Hello

BROWSER

Managed Chrome · Autofill controls · Extension management

CREDENTIAL

Password manager · Passkeys

ACCOUNT

MFA · Recovery methods · Account monitoring

KEY REMINDERS

- Windows Hello autofill settings are off by default — enable them deliberately.
- These are device-level settings — configure them on each PC.
- Windows Hello verification does not carry over to other synced devices.
- Both settings apply only where a screen lock is configured.
- Central enforcement via Chrome Enterprise policy is not confirmed — verify current availability.
- Good local authentication reduces one risk. MFA protects the account itself.
- Browser security needs an Operational Heartbeat — review versions, extensions and credentials regularly.

Security settings only count if they are actually enabled on the devices people use.