

PASSWORD MANAGERS & BROWSER-MADE RISK.



A password saved in the browser is only as safe as the device it lives on — a password manager decides whether that credential survives when the device doesn't.

- PASSWORD MANAGER VAULTS
- BROWSER-MADE PASSWORDS
- ZERO-KNOWLEDGE ENCRYPTION
- CREDENTIAL MONITORING & MFA

01 THE MECHANISM



Password Manager Vault

Storing credentials in an **encrypted vault** unlocked only by a separate master password.



Browser-Saved Passwords

Storing credentials inside the browser profile, tied to the device and sync account.



Zero-Knowledge Encryption

Encrypting vault contents client-side so even the provider can't read stored credentials.

02 THE FLOW

The Vault-Protected Credential PROTECTED

1

A credential is generated and stored inside an **encrypted, zero-knowledge vault**.

2

The vault unlocks only with a **master password and a second factor**.

3

A stolen device or browser profile yields **no usable credentials without the vault key**.

The Browser-Saved Credential LIVE EVENT

1

A password is saved through the browser's built-in prompt, **tied to the device login**.

2

Infostealer malware on the device **extracts the saved-password store in bulk**.

3

Every device synced to that browser account **inherits the exposure instantly**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Password Manager Vaults	Encrypts and organizes credentials behind a master password separate from the OS or browser login.
Browser-Saved Passwords	Stores credentials inside the browser profile, tied to the device and browser-sync account.
Zero-Knowledge Encryption	Encrypts vault contents client-side so even the provider cannot read stored credentials.
Credential Monitoring & MFA	Flags reused, weak, or breached passwords and adds a second factor beyond the master password.

04 CREDENTIAL STORAGE APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Browser-Saved Passwords Only	No	Tied to the device and browser account, exposed in bulk by infostealers or session theft.
Reused Passwords Across Sites	No	One breach compromises every account sharing that password.
Password Manager Without MFA	No	A compromised master password alone can unlock the entire vault.
Manual Password Tracking Only	No	Doesn't scale and misses credentials saved outside the tracked list.
Password Manager + MFA + Zero-Knowledge Vault	Yes	Isolates credentials, enforces unique passwords, and survives device compromise.

PASSWORD MANAGERS & BROWSER-MADE RISK.

VAULT · GUARD · MONITOR

05 PROGRAM OPERATIONS

Password managers aren't a convenience feature — they're the boundary between one breach and every breach. Reused passwords turn a single leak into full account takeover.

Browser-saved passwords inherit the security of the weakest synced device. One compromised laptop exposes every credential across every synced browser.

Master passwords without MFA are a single point of failure. Anyone who obtains it gets the entire vault, not just one account.

Credential monitoring only works if the vault is the single source of truth. Passwords saved outside the vault never get flagged as weak, reused, or breached.

06 CONTROL MAPPING

NIST SP 800-63B

Digital identity guidelines defining password composition and authentication requirements.

CISA SECURE OUR WORLD

Baseline account hygiene guidance recommending password managers and multi-factor authentication.

OWASP ASVS

Authentication verification standard covering credential storage and vault requirements.

FIDO2 / WEBAUTHN

Passwordless authentication standard reducing reliance on stored credentials entirely.

07 WHAT THIS DOES NOT SOLVE

Domain-mismatch autofill

Autofill checks the exact domain, but a copied and pasted password still works on a look-alike site.

Master password compromise

A vault is only as strong as the master password protecting it, especially without MFA enabled.

Unlocked-device malware

Keyloggers and clipboard-scraping malware can capture credentials the moment the vault is unlocked.

Credentials outside the vault

Old accounts using passwords stored outside the vault stay invisible to breach and reuse monitoring.

08 MYTHS VS. REALITY

MYTH "Browser-saved passwords are basically the same as a password manager."	REALITY Browser storage lacks zero-knowledge encryption and independent vault protection.
MYTH "A strong master password is all the protection a vault needs."	REALITY Without MFA, a compromised master password unlocks the entire vault at once.
MYTH "Password managers are a bigger target, so browser storage is safer."	REALITY A zero-knowledge vault stays encrypted even if the provider itself is breached.
MYTH "Autofill means the password manager already prevents phishing."	REALITY Autofill blocks mismatched domains, but a pasted password still works on a fake site.
MYTH "Turning on browser sync is the same as using a password manager."	REALITY Sync spreads the same unencrypted exposure to every device signed into that account.

09 SPEAK THE PROGRAM — KEY TERMS

PASSWORD MANAGER

Encrypted software vault for generating, storing, and autofilling unique credentials.

MASTER PASSWORD

The single key that unlocks the vault; never stored or transmitted to the provider.

ZERO-KNOWLEDGE ARCHITECTURE

Encrypting data client-side so the provider itself cannot read it.

CREDENTIAL STUFFING

Automated attacks that test stolen username/password pairs across many sites.

INFOSTEALER MALWARE

Malicious software that harvests saved browser passwords and session tokens.

PASSKEY

A phishing-resistant, passwordless credential tied to a device and public-key cryptography.

SOURCES: NIST SP 800-63B · CISA · OWASP ASVS · FIDO2

PASSWORD MANAGERS & BROWSER STORAGE · FIELD REFERENCE