

WordCrypt

SERVER-SIDE PASSWORD MANAGER

Note that the anonymous users' password encryption and submission processes ③-⑥ occur in a microsecond 'blink of an eye' .

HOST SITE'S FRONTEND



1. Our plugin embeds our icon in the password field and monitors our CallBack URL (domain.ext/wc).



USER'S BROWSER

6. Users sign in securely with a unique and complex password they never need to see, save, remember or reset. The only place their password is ever saved is on that one site they're logging into.

2. Clicking our icon generates a random One Time Key (OTK) and sends a URL request to launch our SSL popup encryptor in that browser.

3. The user's secret phrase and PIN are submitted directly to our secure server with the OTK while the host's URL is checked against our database of registered domains. The user's phrase and PIN are never revealed to the host site and the user's email or username are never seen by us.

SSL ENCRYPTED

Demo the WordCrypt plugin on <https://anysiteyouwant.com>



5. Our plugin monitors the CallBack URL and compares the OTK received with the OTK generated in Step 2. If equal, simple asterisks are inserted into the frontend login form, the password is inserted into the backend login script, then both the password & OTK are permanently deleted.

4. We generate an encrypted password by combining the values of the domain, phrase and PIN utilizing a one-way Secure Hash Algorithm (SHA-256) and send the password and OTK to the host site's CallBack URL.



WORDCRYPT'S SECURE SERVER

WordCrypt would be available in three different versions to accommodate every business's needs and security standards:

FREE

Our popup password encryptor features a revenue generating CPM banner ad making it possible for every website and user around the world to participate for free.



AD-FREE



Businesses can feature their own logo or banner ads at the same CPM rate of \$1-\$2 per 1000 impressions or .1c to .2c per encrypted password.

LOCALHOST



Financial institutions, medical facilities, govt agencies, any business with sensitive data could pay to host WordCrypt on their own internal servers.