WordCrypt®
NON-STORED PASSWORD MANAGEMENT

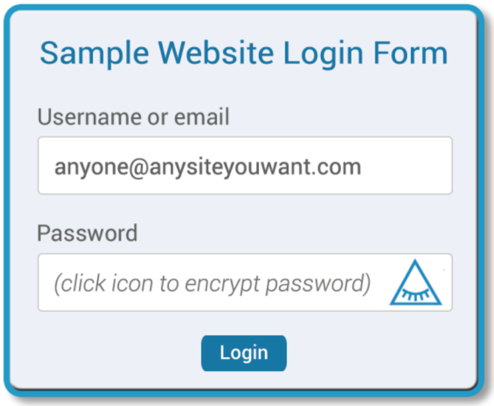
Executive Summary

Problem: Everyone has a problem with passwords

- **40%** of help desk calls are just to reset lost or forgotten passwords
- **83%** of the public are using the same password on more than one site
- **59%** are using the **same** password on **every** site
- **81%** of data breaches, ransomware attacks and identity theft are due to poor password management

Solution: A web server-based password encryptor that eliminates the need for users to ever see, save, remember or reset their passwords.

Our website plugin embeds our icon in the password field as an option to typing in a saved password. Clicking our icon launches a popup encryptor that is only visible to the user.



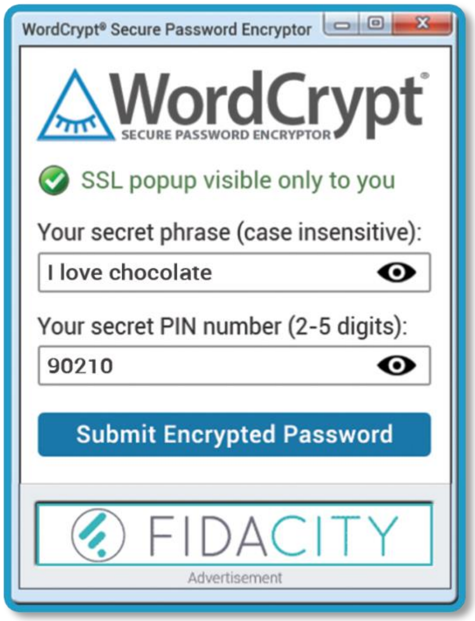
Sample Website Login Form

Username or email

anyone@anysiteyouwant.com

Password

(click icon to encrypt password)



WordCrypt® Secure Password Encryptor

WordCrypt
SECURE PASSWORD ENCRYPTOR

✓ SSL popup visible only to you

Your secret phrase (case insensitive):

I love chocolate

Your secret PIN number (2-5 digits):

90210

Our secure, SSL popup encryptor combines the values of the domain name with the user's own secret phrase and secret PIN number to generate an encrypted password. Inputting the same secret phrase and PIN number will always generate the same encrypted password for a given domain.

Benefits: Our exclusive features and benefits that no other password manager on the market can claim

Users are completely anonymous
Users never register or login to WordCrypt so we never see their identities

Passwords are never stored by us or revealed to users
Passwords are regenerated as needed so there is no need to store them anywhere except the site you log into

There is nothing for users to install on any device
WordCrypt is installed on websites, not users' devices so it works on any device right off the shelf

No skeleton key password required
There is no unsecured master password needed to launch WordCrypt as with other password managers

No stored login credentials for hackers to steal
Even under subpoena we couldn't possibly reveal any users' identities or their passwords

Business Model: WordCrypt will be offered in three versions to accommodate every business's needs

- **Free Version**: Our popup password encryptor features CPM banner ads earning .1c-.2c per impression.
- **Ad-Free**: Businesses can opt to remove or replace our banner ad with their own at the same CPM rate.
- **Local Hosted**: Financial institutions, medical facilities, government agencies, any business with sensitive data could host our server's software on their own internal servers to eliminate all external password encryptions and submissions for a modest per-server package fee and the same Ad-Free CPM rate.

Competition: We truly have no competitors. Unlike traditional password managers, WordCrypt doesn't store any user data or passwords whatsoever and there is nothing for users to register or install on any device. In-depth studies conducted in 2014 by the University of California at Berkeley and in 2019 by white hat Independent Security Evaluators exposed "critical vulnerabilities" and "security flaws" in every one of the top 5 password managers. Consider also that it takes an unsecured password to first launch a password manager, 65% of those polled don't trust them, and less than 15% of us are using one. I'd like to add that LastPass was sold to private equity firms in 2019 for **$4.3 billion** and they only rank 2nd or 3rd in a long list of contenders.

Market Analysis: It is estimated that there are currently more than 5 billion Internet users worldwide. Just one password per user per day at .1c per ad impression could earn $50 million daily or $2 billion annually, equal to the amount that all password managers combined earn now, and yet remain free for all to use.

Websites and businesses would welcome an non-stored password management solution such as WordCrypt:

- Eliminates constant password resets and 40% of help desk calls due to lost or forgotten passwords
- Every password would be exclusive, stored only on their site and never even revealed to members
- No more two-factor authentication necessary or forced password updates every 60 or 90 days
- Eliminates credential stuffing and 81% of data breaches, ransomware attacks and identity theft
- Passwords can't be reverse-engineered to reveal users' secret phrase or PIN number – not even by us

Team: I am the sole owner of WordCrypt and its intellectual properties including US Patent #9,647,839. I have no partners and have personally invested over $150,000 to design and develop wordcrypt.com, the prototype plugins and code, all marketing materials, and to secure the patent. Unfortunately, my lead developer is in Ukraine and currently defending his country and family from invading Russian forces.

MVP: We have developed a working WordPress plugin and PHP code for non-WordPress sites as a Minimum Viable Product. Both are available for download and testing from wordcrypt.com and demonstrated on anysiteyouwant.com. The next steps would be to modify our plugin to accommodate any WordPress theme or template and then to include ASP.net, Ruby, Java and Scala based sites. However, further development was suspended due to the war in Ukraine and WordCrypt's patent and other intellectual properties are now being offered for sale as an unmarketed 'virgin product' for a cybersecurity company to claim as their own.

Funding: I am seeking to sell outright to a company that can leverage their collective development and marketing expertise to perfect and launch this simpler and safer password management standard; a new global standard that would render present user-installed and browser-based password managers obsolete and eliminate the 80% of data breaches, ransomware attacks and identity theft caused by poor password management. For more information please contact me directly at jim@wordcrypt.com.