Honeypot Protection

Magic Login Pro · https://handyplugins.co/docs/honeypot-protection/

Honeypot Protection adds a lightweight, no-CAPTCHA spam protection layer to Magic Login forms.

It helps reduce automated login requests by adding hidden form fields and timing checks that real users do not see or interact with. Bots often submit forms too quickly, skip required hidden payloads, or fill fields that should remain empty. When that happens, Magic Login can detect the request before sending a login link.

What Honeypot Protection Does

When enabled, Magic Login adds a hidden validation layer to supported forms. This layer checks:

- Whether the hidden honeypot field was filled
- Whether the signed form payload is present and valid
- Whether the form was submitted too quickly
- Whether the form payload is too old

For normal users, nothing changes. They can request a magic login link as usual.

For suspicious automated requests, Magic Login blocks the request silently or returns a generic error depending on the flow.

Why Use Honeypot Protection?

Honeypot Protection is useful when you want extra protection without adding friction to the login experience.

Unlike CAPTCHA services, honeypot protection does not require users to solve a challenge, click a checkbox, load third-party scripts, or connect an external service.

It is a good fit for sites that want to:

- Reduce bot-generated login link requests
- Avoid unnecessary login emails
- Add a quiet security layer to public login forms
- Keep passwordless login fast and simple
- Avoid external CAPTCHA services for basic spam protection

Supported Forms

In Magic Login, Honeypot Protection applies to:

- Magic login request forms
- Code login forms
- The default WordPress login screen when Magic Login is added there

In Magic Login Pro, Honeypot Protection also applies to:

- Registration forms

How Suspicious Requests Are Handled

For magic login link requests, Magic Login uses a generic success-style response for suspicious submissions.

This helps avoid giving bots useful feedback and reduces account enumeration signals. In other words, the response does not clearly reveal whether a matching user account exists.

For code login and registration flows, invalid honeypot submissions return a generic error message.

How to Enable Honeypot Protection

1. Go to your WordPress admin dashboard.
2. Open **Magic Login > Settings**.
3. Go to the **Spam Protection** section.
4. Enable **Honeypot Protection**.
5. Save your settings.

No API key or external account is required.

Default Timing Checks

By default, Magic Login checks whether the form was submitted too quickly or after too much time has passed.

The default timing values are:

- Minimum form age: 2 seconds
- Maximum form age: 1 hour

These defaults help catch simple automated submissions while staying out of the way for real users.

Developer Customization

Developers can customize honeypot timing with the magic_login_honeypot_config filter.

Example:

```
add_filter( 'magic_login_honeypot_config', function ( $config ) { $config['min_render_age'] = 3; $config['max_render_age'] = 30 * MINUTE_IN_SECONDS; return $config; } );
```

Available config values:

- min_render_age: Minimum number of seconds before a form submission is accepted.
- max_render_age: Maximum number of seconds before a rendered form payload expires.

Only adjust these values if your site has a specific need. Setting the minimum too high may affect very fast legitimate users, while setting the maximum too low may affect users who keep a page open before submitting.

Honeypot vs CAPTCHA

Honeypot Protection is not the same as CAPTCHA.

A CAPTCHA asks the user to complete a visible challenge or verification step. Honeypot Protection works silently in the background.

For many sites, honeypot protection is enough to reduce basic automated form spam. For high-risk or heavily targeted sites, Magic Login Pro can also be used with stronger CAPTCHA-based protections such as reCAPTCHA, Cloudflare Turnstile, or Friendly Captcha.

Recommended Use

We recommend enabling Honeypot Protection on public Magic Login forms, especially if your site receives repeated login link requests or bot traffic.

It is lightweight, private, and invisible to real users, making it a practical first layer of protection for passwordless WordPress login forms.