Additional Information on SSL

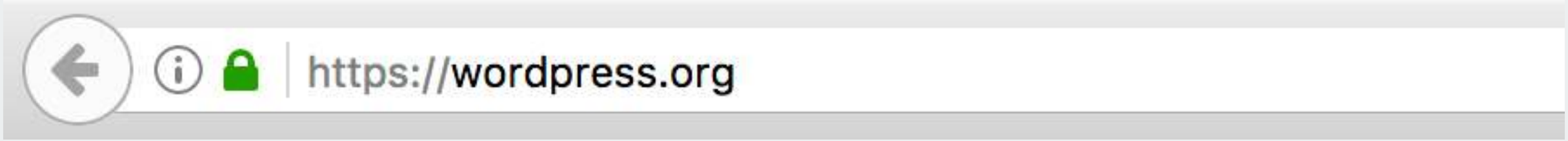
Basic Steps for Adding SSL (without Let's Encrypt)

1. Generate a CSR (certificate signing request) at your web host
2. Buy a certificate from a vendor
3. Validate your domain/certificate
4. Send the CSR, certificate, and bundle files to your web host
5. Configure your site to use SSL
6. Every year, repeat steps #1-4

Why Would You Want to Go Through That?

In some cases, you might want a paid certificate instead of Let’s Encrypt.

1. Establish more trust with a higher-level certificate. Just because a site has SSL doesn't mean it's trustworthy.
2. Limit your downside with a warranty. I've seen up to $1.75M.
3. Cover all of your subdomains with one certificate.

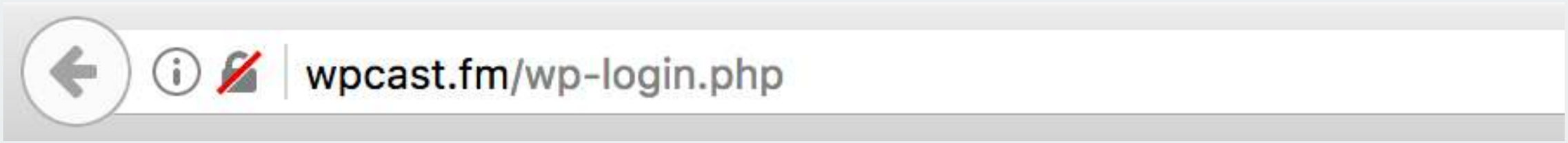


Basic Types of SSL Certificates

- **Domain Validation:** Proves domain ownership
- **Organization Validation:** Also validates organization/company
- **Extended Validation:** Also verifies the business is legitimate
  - Shows the company name in the address bar
  - Used to have a green bar, now it seems to just be green text
  - Requires a longer vetting process
  - Usually somewhere around $100-200/year
- **Common Options:**
  - Wildcard certificate (for subdomains)
  - Multi-domain certificate

Additional Points

- Adding SSL isn't the same as securing your site. It just encrypts information sent to/from your website.
- If you're using WordPress Multisite, SSL can only be used on the parent site and subdomains (with a wildcard certificate), but not on mapped domains.
- Firefox now shows a lock with a red line through it on non-SSL pages with login forms.



THANKS!

Doug Yuen

Email: doug@efficientwp.com

Twitter: @Doug_Yuen

Website: EfficientWP.com