A Style Guide for Writing about WordPress and Security

1. Security, Vulnerability, and Trust in Open Source

We sell a security product, but the product is not *security*.

As part of the Open Web, WordPress is a commons, and so is WordPress security. It's both a resource and a responsibility. To be honest, it can be quite a pain, and a big burden.

Security is both a feeling (that might be wrong) and an objective situation. The feeling of security and actually being secure may not be aligned with each other much of the time. Giving that problem much thought is likely to make a person feel uncertain and insecure. Only the experience of a security breach is truly grounded in reality. There is no question then — you know. You're not secure. *You've been compromisd.*

Paranoia and overconfidence are both things we want to discourage.

Security is never absolute, which is to say, *security always comes with vulnerability*.

We are always vulnerable in some way, however small. We are never completely invulnerable.

Open source leads by refusing to pretend software can ever be perfect — especially by hiding the source code.

Open source means working in the open — together.

That's never easy. We must constantly resist our inclination to hide defects and vulnerabilities — to create a mask of invulnerability based on obscurity and deception.

We are confident in the security of our systems when we believe our trust is well-founded in our tools, partners, experts, and other authorities we rely on for advice and insight.

Our confidence and trust require maintenance, learning, and growth in cooperative relationships. Together, we take care of our shared tools, knowledge, and relationships — with colleagues, partners, customers, and even competitors.

Because our security and vulnerability are shared collectively, so is responsibility. If responsibility is shared, so is the quality, security, and trust it generates in our customers and marketplace.

2. In/vulnerability: Dilemma and Opportunity

Writing about security, especially in open source, is a tricky rhetorical situation. There are several dilemmas presented to anyone with “bad news” facing an audience of superiors, peers, customers, and competitors, especially in contexts where “professionalism” is often misconstrued as a performance or mask of invulnerability, if not omniscience.

Admitting errors, defects, new risks, and security failures may cause individuals, organizations, and brands to lose trust. But denying, hiding, or lying about security failures always fails harder in the end. It’s devastating to brands, products, reputations, and careers. We see this happen time and again.

Maximizing security — and trust — in open source requires exposing all our work (warts and all) to everyone for review (or exploitation) by anyone.

3. Writing about Security and Vulnerabilities in WordPress

Be realistic about threats and empower people to manage them.

Be as accurate as possible about threats — but focus on solutions. Don’t use fear, uncertainty, and doubt (FUD) to sell solutions. Dispel fear with knowledge, demonstrate how reasonable levels of risk can be managed, and foster confidence in the tools, information, and relationships that empower WordPress users to secure their web properties. Empower people with knowledge, teach rational risk management, and show how we work together and care about each other’s welfare in open source.

Don’t minimize threats, overstate them, or tell an open-ended story of dark and scary unknowns. There is almost always an upside. What is it? What knowledge, tools, resources, and relationships will most effectively and efficiently reduce risks and increase security? There is always helpful action that can be taken now. Always lead with that. There is always something to be learned from bad situations — what is it? At the same time, don’t minimize the downside or exploit a problem to oversell our solution as a cure-all.

Make security interesting and engaging — even better, empowering — from the perspective of a new WordPress user who knows nearly nothing. 99.9% of all vulnerabilities and successful attacks exploiting WordPress sites are a result of their users’ carelessness with 1) weak, guessable, and/or reused passwords across the web, 2) obsolete versions of WordPress core, 3) outdated nulled/pirated, or low-quality, insecure third-party plugins or other add-ons, 4) an outdated, insecure, poorly maintained server environment and hosts that tolerate any of these conditions. Just because this isn’t news (to you) doesn’t mean it’s not important to repeat or impossible to make our key messages interesting — it’s new to the people that need to hear it. Always try to see things from their perspectives.

Place responsibility where it belongs, where it can be helpful. If it's not part of a solution, it's just blame. What's on us, and what is on our users' plates? Level with them, but don't condescend or push away.

4. Audience, Voice, and Tone

Our audiences include:

The voice you use should convey and support the brand's personality and values: *confidence, candor, consistency, honesty, openness, expertise, and real people who are accessible.*

Your tone should convey and support the brand's attitude and emotional, affective qualities: *being realistic about problems, optimistic about solutions, and down-to-earth.*

5. An Inclusive Culture Brings Outsiders In

Always explain jargon and WordPress terminology. If possible, avoid jargon and explain technical terms the first time you use them. Spell out acronyms the first time you use them. Helping people learn the lingo means helping them enter the community.

WordPress Ways of Speaking

Admin Bar, Admin Dashboard = "The Admin [interface["
"Paid" / "Pro" plugins/features

Our Own On-Brand Terms and Phrases

Technical Vocabulary: Key Words and Concepts

Models to use:

- Brianne Hughes https://www.encyclopediabriannica.com/?cat=36
    - https://bishopfox.com/resources/cybersecurity-style-guide
    - Cybersecurity Style Guide: https://cybersecuritystyleguide.com
    - Cyberdic (Spellcheck augmenter) https://github.com/bishopfox/cyberdic
    - Chaos in the Machine: Why Security Needs a Style Guide: https://youtu.be/YI-4BWKpC28
    - https://cmosshoptalk.com/2018/05/15/brianne-hughes-talks-about-the-cybersecurity-style-guide/
    - https://www.the-parallax.com/cybersecurity-style-guide-write-hacker/
    - https://stancarey.wordpress.com/2018/03/02/cybersecurity-style-guide-a-useful-editing-tool/
- https://sandralmuller.com/copywriting-style-guide-examples/