# Kim Crawley unveils new strategies to reclaim digital privacy amid rising AI and corporate control



In an age increasingly defined by the complexities of technology and the encroaching threats of authoritarianism, cybersecurity expert Kim Crawley is set to release her forthcoming book, *Digital Safety in a Dangerous World*. Her insights, alongside contributions from fellow experts, lawyers, and activists, aim to empower individuals to navigate the intricate landscape of digital safety and privacy. The book emerges from a belief that the average consumer can take proactive, lawful steps towards safeguarding their digital lives.

Crawley's impetus for writing this book stems from her personal experiences and concerns regarding the pervasive influence of technology giants. She expresses a firm stance against the growing reliance on generative AI, asserting that these systems often propagate mass plagiarism and threaten the authenticity of human thought. The transition from mainstream platforms to alternatives that prioritise privacy—such as GrapheneOS and Kubuntu—illustrates her commitment not only to digital safety but also to personal agency in an era where data control is increasingly under the grip of major corporations.

The narrative draws parallels with historical precedents, setting the stage for discussions on the role of military research in technology. Crawley intends to explore how many foundational computer technologies have roots in US government projects dating back to World War II. Such context is essential, as it highlights how the digital tools and systems that many now take for granted are deeply entwined with state interests and military R&D. This perspective is a natural evolution from her previous works, which primarily catered to enterprise-level cybersecurity, including *The Pentester Blueprint* and *8 Steps to Better Security*.

Crawley's collaborations with experts in the fields of privacy law and cybersecurity enrich the content of her book. Engaging with prominent figures—such as Dell Cameron from Wired and Evan Greer from Fight for the Future—has allowed her to incorporate crucial insights that resonate with the realities many face today. The intersections of their varied backgrounds form a comprehensive approach, addressing both theoretical and practical considerations in digital safety.

The challenges of translating technical terminology into accessible language for a general audience are not lost on Crawley. Her target readership includes individuals who may not be tech-savvy but are increasingly aware of the risks posed by digital platforms. She emphasises the importance of explaining complex concepts without diluting their significance, offering easily digestible advice on operational security and harm reduction strategies. These insights are particularly timely as many find themselves grappling with emerging threats in their daily lives.

One of the book's core messages is a call for scepticism—urging readers to critically assess the intentions of tech and government entities alike. Crawley notes that, while certain tools like commercial VPNs can enhance security to some degree, trusting the motives of corporations that control such tools is fraught with uncertainty. This caution underscores the critical need for individuals to become savvier consumers of technology while forging communal ties for support and advocacy.

As she navigates the evolving landscape of cybersecurity, Crawley aims not only to inform but also to inspire a proactive stance among her readers. While the daunting reality of a digitally interconnected, often perilous world can feel overwhelming, the narrative she crafts champions resilience, self-reliance, and accountability. Ultimately, *Digital Safety in a Dangerous World* seeks to arm readers with knowledge and strategies that affirm their right to privacy and personal security in an ever-dangerous digital frontier.

### Reference Map

1. First paragraph
2. Second paragraph
3. Third paragraph
4. Fourth paragraph
5. Fifth paragraph
6. Sixth paragraph
7. Seventh paragraph

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

* <https://www.helpnetsecurity.com/2025/05/15/kim-crawley-digital-safety-in-a-dangerous-world-book/> - Please view link - unable to able to access data
* <https://www.helpnetsecurity.com/2025/05/15/kim-crawley-digital-safety-in-a-dangerous-world-book/> - In this interview, cybersecurity expert Kim Crawley discusses her upcoming book, 'Digital Safety in a Dangerous World,' which offers advice on protecting safety and privacy in challenging times. The book features insights from various experts, including lawyers and activists, and addresses topics such as the influence of big tech and rising authoritarianism. Crawley emphasizes the importance of self-reliance and critical thinking in the digital age, advocating for alternative operating systems and applications to enhance digital safety.
* <https://www.barnesandnoble.com/w/8-steps-to-better-security-kim-crawley/1139590533> - Kim Crawley's '8 Steps to Better Security: A Simple Cyber Resilience Guide for Business' provides a practical roadmap to enhance cybersecurity within organizations. Drawing from her experience with major tech companies like Sophos, AT&T, and BlackBerry Cylance, Crawley outlines steps to foster a strong security culture, build effective security teams, comply with regulatory requirements, and conduct thorough security testing. The book is designed to be accessible to both technical and non-technical readers, offering valuable insights for businesses of all sizes.
* <https://neurosec.captivate.fm/episode/neurodiversity-in-cybersecurity-kim-crawley> - In this podcast episode, Kim Crawley discusses the intersection of neurodiversity and cybersecurity. She shares her personal journey of self-education in the field, highlighting the challenges faced by neurodiverse individuals in the industry. Crawley emphasizes the importance of self-advocacy and the need for allies to support neurodiverse professionals. She also addresses the subtle forms of ableism present in the workplace and offers advice for neurodiverse individuals aspiring to enter the cybersecurity field.
* <https://www.tripwire.com/profile/kim-crawley> - Kim Crawley is a cybersecurity researcher and writer with experience in consumer tech support and information security. She has contributed articles to publications such as CIO, CSO, Computerworld, SC Magazine, and 2600 Magazine. Crawley specializes in various aspects of information security, including malware analysis, social engineering, and advanced persistent threats. Her work focuses on making cybersecurity knowledge accessible to a broad audience, emphasizing the importance of understanding and mitigating cyber threats.
* <https://medium.com/hackernoon/7-surprising-ways-people-became-infosec-professionals-3a6596032a5a> - In this article, Kim Crawley explores unconventional paths to becoming an information security professional. She shares stories of individuals who transitioned into the field from diverse backgrounds, such as politics and retail. The article highlights the importance of curiosity, self-education, and perseverance in pursuing a career in cybersecurity. Crawley emphasizes that a non-traditional background can offer unique perspectives and skills valuable to the information security industry.
* <https://www.helpnetsecurity.com/2025/05/15/kim-crawley-digital-safety-in-a-dangerous-world-book/> - In this interview, cybersecurity expert Kim Crawley discusses her upcoming book, 'Digital Safety in a Dangerous World,' which offers advice on protecting safety and privacy in challenging times. The book features insights from various experts, including lawyers and activists, and addresses topics such as the influence of big tech and rising authoritarianism. Crawley emphasizes the importance of self-reliance and critical thinking in the digital age, advocating for alternative operating systems and applications to enhance digital safety.