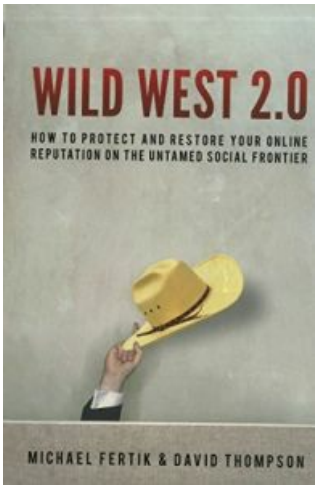

Book Wild West 2.0

How to Protect and Restore Your Reputation on the Untamed Social Frontier

Michael Fertik and David Thompson
AMACOM, 2010
Listen now

- play
- pause

00:00
00:00

Recommendation

Although the Internet is the greatest information resource and connectivity medium the world has ever seen, it is still remarkably wild and woolly. Millions of shady characters inhabit it, lurking to steal your shirt and sell it back to you at twice the original price. Some online con artists set up phony rating sites where they publish scathing reviews of companies' products and then extort heavy fees from those firms to remove the negative reviews. Malevolent liars use the Internet anonymously to ruin people's reputations or corporations' standings with blog attacks and negative postings. Reputation management consultants Michael Fertik and David Thompson examine these fraudulent activities and more in this disturbing but timely book, and they outline steps you can take to protect your online reputation or the good name of your business. Though the book is somewhat repetitive, Fertik and Thompson have created a solid, useful manual on safeguarding your good name online. *BooksInShort* recommends it to anyone who has to fight back against online slurs, and to anyone who has a good reputation and wants to keep it.

Take-Aways

- The Internet is like the untamed "Wild West" where anything goes.
- This freedom is based on the structure of the Internet, which does not include screening for accuracy.
- Malicious people can anonymously use the Internet to destroy the reputation of any person or business, and still remain unaccountable.
- Your Internet reputation will quickly become your offline reputation as well.
- Negative online reports can expand exponentially due to Google's "self-reinforcing cycle," which calculates Web sites' popularity based on their number of links.
- Conduct an "online reputation audit" to see what people say about you or your firm.
- Look for damage to your personal, social and professional reputations, and try to determine who may have searched for your name or posted data about you.
- Going on the defensive will not sufficiently protect your reputation. Take the offensive.
- Develop positive, broadly linked Web content about yourself everywhere possible. Get your friends to comment, and post widely on sites like Twitter and Facebook.
- Take charge of your identity online by securing all the domain names and usernames someone could appropriate to pretend to be you.

Summary

The Virtual Territory of the Digital Desperadoes

The Internet is a dangerous "digital frontier" where anything goes. Malicious online criminals can trash your reputation by spreading vile lies and outrageous smears without having to worry about the consequences. Anonymous attacks against you or your business can spread from Web site to Web site like wildfire, viewable by

anyone with Internet access. Lawmakers have not yet controlled the Internet's wild side, and law enforcement can do little to apprehend unknown, unnamed, unseen perpetrators. Since the Internet is still evolving, complete social norms have not yet formed to dictate what is acceptable to do or say online.

> "Smears that would once have been limited to a bathroom stall or a hand-passed note can now be seen by employers, friends, families, dates, clients and anyone else with access to the Web."

The Internet strongly resembles the "Wild West," a raw, lawless land where hardy settlers had to fend for themselves. The Internet's tradition of self-policing matches the Old West's customs and attitudes. Online pornography and betting quickly became popular during the birth of the Internet, just as prostitution and gambling thrived in the early days of the American West.

> "Your reputation can be created or destroyed in just a few clicks."

Primary online players such as Google generally have a hands-off policy about the ways bitter or unhinged people can use their powerful online applications for nefarious purposes, such as ruining your reputation or your business, so it's easy to post vicious slanders that search engines will retrieve. Miscreants on the Web can undermine your reputation because:

- **"Everyone can create"** – Anyone can become an online publisher and build blogs, social media pages, Twitter accounts, Web sites, and more.
- **"Everyone is (almost) equal"** – Anyone can set up a page that looks like a legitimate business just by purchasing a reputable domain name.
- **"Everything is online somewhere"** – The Internet has no limits. Data about everything – including you – can appear on countless Web sites.
- **"Everything is instant"** – People can access all sorts of information immediately, including negative reports about you.
- **"Everything is permanent"** – Once information hits the Internet, it can bounce around cyberspace forever. Cache technology saves copies of the Web pages that people open.
- **"Everything is powerful"** – For instance, face-recognition software now exists that can identify you in an obscure group photo posted online.

> "People suspected of wrongdoing are run out of town on an electronic rail, often before there is time to figure out whether they are really guilty or innocent."

You can't track people who post data online. Such anonymity, one of the Internet's most insidious characteristics, protects illicit operations. Virtual-world covertness stands in sharp contrast to the real world, where it is difficult to hide who you are. People are less inclined to engage in outrageous behavior if they know they can be identified and caught. Many perpetrators engage in online activities anonymously that they would never attempt openly in the offline world. Internet protocols and most legal systems encourage online anonymity, but that translates to a total lack of accountability.

> "Anything that is said online may be available forever, no matter how hard anyone tries to delete it."

Attackers may target you, your business or another person because of:

- **"Jealousy, envy and revenge"** – Such negative feelings apparently account for more than 50% of online attacks against individuals' reputations.
- **"Bullying"** – This is so common it has a name: "cyberbullying."
- **"Vigilante justice"** – People who wrongly see you as a villain may try to destroy you.
- **"Politics"** – Already dirty enough in the real world, political battles can grow particularly noxious in cyberspace, where anonymity cloaks false accusations.
- **"Greed"** – Unethical competitors may damage your company's reputation.
- **"Extortion"** – Cyber criminals may smear you online and ask you to pay them to stop.
- **"Social gossip"** – The Internet has become the world's rumor mill.
- **"Sociopathy"** – The Web is a powerful tool for those seeking to humiliate and hurt others.

> "Powerful anonymity combined with outdated laws has allowed a complete lack of accountability for online content."

Many people trust the Internet and believe everything online is accurate. Thus, readers may assume that false or negative reports about you are true. This is particularly likely if you already have a negative "Google trail," that is, if a series of search hits depict you unfavorably. The Web has no built-in accuracy gatekeeper, a major concern if you have an online reputation to protect.

> "Every day, thousands of innocent victims find that they have been smeared, slandered and dragged through the mud online by one or more attackers."

A good reputation is an incredibly valuable asset that tells others you deserve their trust so they will work with you, value your opinion and respect you. Conversely, a bad reputation can cause others to avoid you and refuse to do business with you. To protect yourself, you must understand that your online reputation will quickly become your offline reputation, too. And, since your reputation depends entirely on other people's perceptions, negative online comments can shape how others see you.

> "Dangerous information is often like an iceberg: What you see at the top of a Google search is often the tip of what is available online."

Online attacks vary in "content" and in "format," or mode of distribution. Content concerns the material an online nemesis posts, such as compromising data or manipulated photos. Distribution methods vary, from single e-mails to mass e-mailed bombardments to untrue Web site entries. Other harmful tactics include setting up insulting Internet sites and spreading attacks on social networks. For example, JuicyCampus, a Web site which is now defunct, served as a prime rumor and scandal hub for college students. You can become the victim of "Googlebombing," the fraudulent distribution of smears to searchers who actually are looking for something else, or "Googlestuffing," "the act of spreading false and negative content in an attempt to fill ('stuff') the first 10 links in a search engine search." In other words, the intent of Googlestuffing is to be sure a searcher finds only negative information about a given subject.

"Self-Reinforcing Cycles"

Online information is powerful because the Internet is a popular research medium. Searching for data via a search engine is much easier than using standard journalistic sources, like reputable newspapers and magazines that verify the information they publish. As the world's leading search engine, Google can seriously damage your reputation. This is due, in part, to its carefully guarded search algorithm, which generates self-reinforcing cycles of data. Google prioritizes its Web search findings based on the popularity of individual sites, as indicated by their number of links. So, when someone searches for your name or your company, Google returns all the Web pages that mention you or your business, including sites with harmful information. Because of the salacious nature of these sites, more people tend to look for them, comment on them and link them to other sites. Google interprets such activity as increased popularity and, thus, moves the negative Web sites further forward in its search rankings. Then, more people see them and link to them, further increasing their popularity. Such search engine cycles can slam your reputation.

Determining the Extent of Reputation Damage

An online attack can damage your individual reputation on three levels: personal, social and professional. Damage to your personal reputation may affect your relationships with friends, relatives and colleagues. Your social reputation reaches a broader arena, including your community. Your professional reputation is the intangible asset that enables you to make a living.

> "The Internet has...democratized extortion, just as it has democratized information."

To calculate how much damage an online smear may have done, use the "Libel Index" formula: "potential harm equals audience size multiplied by the closeness of the audience." Negative data distributed to an extremely large audience that does not touch your life in a meaningful way (like people in a distant country) generally harms your reputation less than smears sent to a smaller, but closer audience (your neighbors or colleagues). Consider where smears appear. Bad data that pops up on the initial pages of search engine findings is more damaging than data on later pages.

Your "Online Reputation Audit"

Perform an online audit, or hire a professional reputation management firm to do it for you. An audit can determine what you are dealing with online by cataloguing the results of extensively searching for your name. Begin by developing a "reputation road map" detailing exactly who – what audiences – might search the Web for data about you or your work. Listing your roles (business owner, board member, volunteer, parent) will help you identify your constituencies. Consider how people might search for data about you. Your audit will help you determine how much damage your reputation has sustained from online smears. Dig deep. Scroll through at least the first 10 pages of Google search results to see what is available about you. Treat your search returns like an iceberg: What you don't see or pay attention to can sink you and your reputation.

> "Several people...have discovered fake MySpace profile pages created about them, often with insulting or embarrassing fake content."

Audit all aspects of your "online profile." Use the same search terms people in your various audiences may use to search for you. If you find something negative, run more keywords that are close to your original search term. Google your name thoroughly and then conduct a survey using other search engines such as Yahoo Search, Ask and Bing. Don't neglect minor engines like Spock, a Web site designed to find information about people. Investigate social sites as well.

Go On the Offensive

Once you assess the online damage your reputation has sustained, develop a strategy to restore your good name or your company's standing. If possible, determine where the smears originated. The Internet is rife with cases of mistaken identity, so if a site has posted incorrect information, you may be able to get its Webmaster to remove the untrue data.

> "Wikipedia is a massive free online encyclopedia. It can be edited by anyone, which creates a constant risk of vandalism and reputation attacks."

Purely defensive action isn't enough to protect your online reputation. You must go on the offensive, seeding positive references about yourself all over the Internet. Start a blog. Create an online persona on social media sites. Twitter extensively. Get friends to post positive news about you via blog comments, tweets, social site entries, and so on. Plant the information you want people to find when they search your name. Comprehensively link as much of this positive information together as you can to make it appear highly popular to Google's search algorithm. This will push good news about you higher up in the search rankings.

> "For many professionals, your image is your business."

Control your identity online so that those who wish to harm you or your company can't manage your Internet presence. Secure all user names, Web sites and URLs that might be relevant so you prevent others from taking them for nefarious purposes. You don't have to add content to each of these online components, though you can. Treat them as placeholders so others can't use them against you or misrepresent themselves as you. Of course, removing all harmful Internet content may be impossible. However, you can smother a lot of negative, mistaken information with good, truthful information by creating a protective "Google wall" of positive data.

> "A false appearance of controversy can be just as bad as actual guilt in some professions."

If someone has attacked your business online, contact other firms that have dealt successfully with such assaults. Find out what they did. Apply their tactics if they make sense. If you can identify your online attackers, despite the barricade of anonymity, deal with them immediately and notify them to cease and desist. Of course, uncovering who has harmed you is never easy, but try thinking like a detective. Can you attach a meaning to any clues the assailant may have left? Do the aggressors seem to know intimate details about your life? Have they posted photos only someone close to you could have taken? Narrow your choices to potential suspects if you can.

> "Your online reputation is your reputation. Period."

You may want to sue your attackers – if you identify them – but that has drawbacks. They may have limited resources, so you would receive nothing for your trouble, even if you expend the time and money to win a judgment. Once smears are on the Web, they assume a life of their own, so your suit would not correct any damage

that's already been done to you or your business. Would that matter? Or would you find it sufficiently satisfying just to sue those who tried to ruin your reputation? Discuss your options with a lawyer who practices in the area of "Internet-based defamation." Meanwhile, proactively control your online reputation by creating positive content.

About the Authors

Michael Fertik is founder and CEO of a reputation management consultancy where **David Thompson** is general counsel. Fertik also serves on the advisory board of The Internet Keep Safe Coalition, which protects the safety of children online.