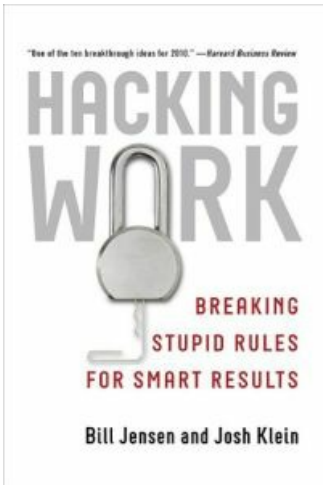

Book Hacking Work

Breaking Stupid Rules for Smart Results

Bill Jensen and Josh Klein
Portfolio, 2010

Recommendation

This lively book is not a manual or a how-to guide; it's a rallying cry for the community of "benevolent hackers" and an attitude adjustment for those who want to join. Bill Jensen, CEO of the Jensen Group, and Josh Klein, a skilled hacker, offer an enthusiastic spirit and an all-embracing outlook – at times to make up for being reserved about specificity, so as not to enable bad hackers – that clearly deliver their message: Courage and flexibility matter much more than technical expertise when it comes to changing oppressive work conditions. The authors walk a tightrope: They imply that you can alter software, networks and processes, but they never demonstrate how outright, and they advocate hacking only within ethical limits. Their obvious joy at circumventing restrictive or idiotic corporate practices, and their welcome conversational tone, makes this a tremendously fun read – one that will open some readers' eyes to possibilities they might not have considered. *BooksInShort* suggests this gleeful tome to those who feel that work procedures are dampening their productivity and creativity, and to anyone who likes to tweak the nose of authority.

Take-Aways

- "Hacking" means altering a system to your advantage.
- "Benevolent hackers" are employees who subvert company practices that make their work harder. They transparently demonstrate and share hacking ethics.
- A benevolent hack may make it simpler for you to do your best, give you power over your tasks, make your "work smarter" and provide some fun.
- You can and should work – or hack – around inefficient company rules and procedures.
- For your first hack, figure out which annoyance to tackle; learn about the problem and create a simple, harmless circumvention – all the time with your final goal in mind.
- "Hard Hacks" alter mechanical systems. "Soft Hacks" deal with relationships.
- The best time for your first hack is when you're newly hired, but before you start work.
- Hacking has 10 commandments: "Be cool," hack only when necessary, "do no harm," play nice and protect people's data are the first five.
- The remaining commandments are: "Pay it forward"; use buzz; be yourself; learn from hacking and "practice, practice, practice," because "hard work trumps talent."
- Explain your hacks to everybody and take responsibility. People will follow you.

Summary

"Benevolent Hackers"

Workers are fomenting a quiet revolution. They subvert established company policies whenever those rules and regulations make their jobs harder or less efficient. This revolution takes the form of circumventing or replacing outmoded or silly procedures. It enables workers to be faster and more productive, and it allows them to fine-tune work circumstances to suit their own natures, rather than bending to idiotic bureaucracy. The members of this ever-growing community of under-the-radar revolutionaries are called benevolent hackers.

> "There is an underground army of benevolent hackers out there who are saving business from itself and having fun along the way."

"**Broken Businesses"** Old business models and processes no longer work. Rigid managers and top-down directives make a company less productive. Yet in uncertain times, most firms tend to be more fearful, more controlling, more rigid and less concerned with employee happiness. But hard times demand courage, not timidity. Workers are fighting back. Evers Pearce's bosses at Oxford cut his project's funding to nearly nothing and told him to throw out its furniture and other detritus. Instead, he sold the supposed garbage on eBay and funneled £37,000 back into the project. Such workers are taking control. Well-meaning "rulebreakers" are making sure their employers thrive in spite of self-destructive policies. The workplace has changed, but few firms have kept pace with these changes. Workers must drag their employers into the present first, and then into the future. Lots of that forward-motion is taking place underground, right under managers' noses.

You Can Hack

If you've ever convinced your boss to extend a deadline despite the rules, or if you've used email to send "a company file to yourself at a personal address so you could work on it at home," then you understand hacking. It requires only curiosity, imagination and drive. Ask what would happen if you tried something new. Don't listen to anyone who says you "can't." Doing a "benevolent hack" may make it simpler for you to work at your best, give you power over your tasks, make your "work smarter" and provide some kicks. Even the word "hacking" derives from fun. In the 1960s, a small group of students who called themselves "hackers" altered electric trains to make them run faster. Then they did the same to the main computer at their college, the Massachusetts Institute of Technology, and gave birth to a name and a movement.

> "Today's top performers are taking matters into their own hands."

With the right hack, you can make your company a place where people work better, feel more creative and generate higher quality work for less money, thus fulfilling the modern rallying cry, "morebetterfastercheaper." Firms that force people to follow top-down processes are the same ones who legally hack and track your Web interactions to find more, better, faster and cheaper ways to market to you. Are you ready to fight back? Four basic steps can lead to "your first hack":

1. **What three things at work annoy you most?** – Find the restrictive rules, the inefficient procedures, and the corporate customs that impede your work and get in your way.
2. **Research and learn** – If you must do X, find out how X works and why you were forced to do it in the first place. Ask who might benefit or suffer if you find an alternative way.
3. **The first hack is the simplest** – Your first "work-around" must be simple and harmless.
4. **Know your goal** – You're not taking action just to mess with the system. You're taking action to achieve a narrow, specific result. Be aware of that goal before you hack.

"Soft and Hard Hacks"

Hard Hacks alter any "nonliving system." Using instant messaging in a meeting to communicate work-related insights while a dull speaker drones on is a Hard Hack. You don't need expertise to perform 99% of Hard Hacks. Instructions for most hacks exist online; just search for them. If security keeps you from sending colleagues information, try "open source Web tools" or Google Docs. If you can't obtain the needed data, some office geek doubtless can find it.

> "Hacking is...understanding a system well enough to take it apart, play with its inner workings and do something better with it."

Soft Hacks alter "relationships or work agreements," like asking a colleague or boss about working in a nonprocedural way to mutual benefit. Because Soft Hacks involve other people, they are as complex as any other relationships. The best time for your first hack is when you're newly hired but before you start work. Use the "Negotiating the Deal" Soft Hack to arrange the terms of your employment, such as persuading the boss to let you work from home or to give you the perks and pay you what you want no matter what others earn. Soft Hack every aspect of your job, hours, bonuses and compensation. Don't accept the status quo. Most compensation deals benefit companies, not employees, but managers know which staffers are worth paying to keep. If you are one of them, hack a pay package that reflects your worth. After you've been working awhile, identify the aspect of your job that demands the most energy for the least progress. Seek the simplest possible change, even if it is as small as "using your own email" instead of the firm's.

> "Technology changes continuously."

"Changing the Relationship" Soft Hacks might involve being allowed to work with an excellent manager or to make work contacts via your social network. Since everyone wants something, Soft Hack your target's desires to your advantage: Coach, manipulate, horse-trade, wheedle, bargain, persuade or help someone in a way that ensures they'll help you in return. The start of a new project is hack-time supreme. By then you'll know which communications or processes hamper your work. Hack around them as you set project parameters. Once you make a deal, hold up your end. Then you can Soft Hack again. Pick your moments wisely; use any leverage you can devise.

"The Ten Commandments of Benevolent Hacking"

When you hack successfully, tell others. Give them the advantage you created for yourself. Sharing fulfills the reason you hacked in the first place: to make work faster, better, more efficient, less restricted and more fun. The 10 core rules of benevolent hacking are:

1. "**Be cool"** – You'll know you're not cool when no one wants to play with you. Don't be a jerk. Share, clean up, be fair, apologize if you're wrong, keep your word and try hard.
2. **Try not to hack** – If you can fix a problem without hacking, do. Don't waste a hack.
3. **"Do no harm**" – "Don't hack for any of the seven deadly sins (no porn, no greed...no revenge or wrath, no lack of diligence or getting out of virtuous work, no enhancing your own vanity)." Don't do anything to a system that changes how others use it. Improve your situation; do not damage anyone else's.
4. **"Never compromise other people's information"** – Keep customer data and "corporate intellectual property" where it belongs. Don't share information with anyone who is not authorized. Check your hack to make sure you have not exposed anything to anyone.
5. **Play nice** – Collaborate; create a work-group. Respect other people's skills.

6. **"Pay it forward"** –Your transparency regarding your hacks will help others and will teach them to be open about their gains.
7. **Honor "the Law of Attraction"** – If a YouTube video gets 100,000 hits, those hits will garner 100,000 more. The buzz grows, the mainstream notices and lives change. Letting your audience know you work within ethical guidelines will earn you a larger following.
8. **You can only be yourself** – If hacking is not for you, tell your idea to those who can hack. If hacking is in your blood, be a hacking consultant. Consider all your options.
9. **Hard work trumps talent** – Practice your skills, stick to a routine, be disciplined and work like a dog.
10. **Let hacking teach you who you are** – Think through hacking's "ethical dilemmas." "What really matters to you?" Are you "doing your best? What do you stand for? What would you compromise to keep your job? How much is too much compromise?"

What's Broken and Needs Hacking?

"Business just doesn't get it." Central commands function against efficiency and individuality; they serve the company, not its people. IBM's 2008 "Global Human Capital Study" found that the most significant barriers to good performance were the company's own "tools and processes." Any procedure you must enact, any manual you must read, any guidelines your boss must follow get in the way of simple, common-sense behavior. The very managers who should set you free to do your best work instead work overtime to control you. Corporate tools and procedures, by their nature, limit and restrict you. Awesome anomalies exist, of course. Zappos will pay you $2,000 to quit right away if its corporate culture, the "Zappos way," doesn't suit you.

No Safety in a Paycheck

Working for someone else has become "a high-risk profession." In a tough economy, companies do not protect their employees. They cut salaries, and some firms – like British Airways – ask people to work a month for free. To keep your job, you must sacrifice. "Loyalty and performance" once counted, but now, no matter how hard or well you work, you could be fired in a heartbeat. Nothing stands between you and the vagaries of the market. However, you can do a few things to protect yourself:

- **"Be lucky"** – Find a forward-thinking, sharing company and get a job there.
- **"Accept the risk"** – Find the best work situation you can; hang on tooth and nail.
- **Hack** – Change what you can to your own advantage.

Fight "FUD: Fear, Uncertainty, Doubt"

You must address FUD: the fear, uncertainty and doubt that hold you back. This term derives from a 1970s IBM sales strategy. Salesmen would try to plant FUD in the minds of potential customers so they would regard buying from IBM as the safest course. Knowing that any twitch in the global market could mean the instant end of your job, how can you fight FUD? Conquer your fear of these conflicting forces: You want your work to help you develop as a person. You also want to serve your firm, its shareholders and the world, but every system serves "company priorities." If your priorities become the least important aspect of your work, you'll be unhappy, unproductive and unhealthy. Change the paradigm; make the systems default to your priorities.

> "Whenever business finally embraces the age of co-creation, the hackers among us will be our best advisers."

Don't be afraid to hack. Everyone around you is hacking, so join the party. "Benevolent hackers do not get fired." The hacking universe offers a continuum of risk. Don't aim too high or too low. The "Life Changing" hack offers high risk but great reward. Creating Facebook was a Life Changing hack for Mark Zuckerberg. The "Career Changing" hack offers less risk but still confers a high reward. The "Work Changing" hack dodges some minor obstacles to make your day easier, but it does not bring you more money. The "Getting By" hack offers no risk and little reward. It might change one small aspect of your work life, but even that is a good place to start.

> "Hackers believe that if you don't know whether or not you're being cool...you probably aren't."

To carry out work-around hacks, behave as if you are a leader who has the power to make the changes you create. If you act like you're in charge, people will follow. Be brazen and never craven. "Design from the bottom up, not the top down." If you want to hack, start gathering and mastering tools that fit your purpose. When you hack well, you may be surprised that co-workers who once opposed you suddenly become your allies and backers. If you show them a better way, "nonbelievers become sponsors."

Deliver the Results You Promise

Hack well, deliver what you promise – even if you made the pledge only to yourself – and success will find you. If you achieve company goals before "your boss and your boss's bosses" figure out their own routes to meeting those goals, you will be a hero. Once your results are certain, tell your manager how you achieved them. Explain your hack clearly. Show that you haven't damaged anything. Share your method. Remember you are personally accountable for your hacks. Take responsibility for your actions. Make no excuses. Behave like a leader. More folks than you think are out there hacking. Someone a cubicle away is changing the world in tiny increments. Hacking gives you the power to bring about change. The hack comes from your willingness to embrace the possibility that things could be different. When you find the courage to start changing the world, just remember: Do no harm.

About the Authors

Bill Jensen is the CEO of the Jensen Group. Consultant **Josh Klein** is an expert hacker.