

The Fruit of the Poisoned Tree: Why Criminal Hackers Must Not Be Rewarded

M. E. Kabay, PhD, CISSP-ISSMP
Prof of Computer Information Systems
School of Business & Management, Norwich University

The original version of the following essay appeared in the Proceedings of the Third International Conference on Information Warfare in Arlington, VA (7-8 Sept 95). The “Great Hacker Debate” on the 7th of September 1995 pitted Robert Steele, President of Open Source Solutions Inc., against M. E. Kabay. The title of the event was “Hackers: National Resources or Criminal Kids?”

Our debate today concerns the proposition that hackers are a national resource and should be cultivated as valuable contributors to national and corporate security.

I utterly reject this proposition.

No, society must not reward criminal behavior. Criminal hackers—those who break the law by intruding into computer systems and networks without authorization and those who steal services from telecommunications companies—must not be rewarded for their criminality.

If you needed to evaluate the security of your home, which would you hire: a burglar who claimed to be an ex-burglar or a bonded security specialist with no criminal tendencies. The fundamental problem with hiring criminal hackers is their complete lack of credibility. Criminal hackers believe in lying and cheating as a bedrock of their hobby; they misrepresent themselves to the security system and to the human beings they can trick into revealing privileged information. Their credo is tainted by the video-game fallacy: if it is possible to do something, it must be right. Morality exists for them only as a technical constraint: if you think something is wrong, make it impossible to accomplish.

So if you hire a criminal hacker to review your system security, you will make him (usually him) sign a non-disclosure agreement. Riiiiight.

Criminal hackers believe that unless you can force compliance, there is no obligation to comply with agreements and rules. I have met hackers who claim that if they *can* break into your computer system, it's *your* fault they broke in—regardless of your efforts to protect yourself. The same mentality is at the basis of every criminal act: stop me if you can. These are people with no connection to the rest of society. They live in a subculture where dishonesty is the norm, where the rest of society is seen as lame-brain jerks who don't know enough to protect ourselves. So what makes you think they will change? If you pay them to hack, why would they deal honestly with you when honesty is foreign to their view of the world? You may as well trust an unrecovered alcoholic or an active drug user. Putting confidential information within reach of the criminal hacker is like putting children within sight of a pedophile.

The next problem is that anyone who has been as anti-social as an expert criminal hacker is subject to blackmail. One of the reasons no one hires convicted felons for work requiring them to be bonded by their employer is that criminals have done bad things—and not necessarily all of it in the public record. To compromise a person with a tainted background, an enemy can dig up some dirt and threaten to reveal it. Given the moral flabbiness of criminal hackers, it's hard to imagine they'd

Fruit of the Poisoned Tree

resist pressure very well. The same problem would arise if you were to hire drug addicts and pushers to work in anti-drug operations; or if you used car thieves to stop car theft; or if you hired embezzlers to write your accounting code. It just doesn't make sense.

On a broader scale, consider the message you would be giving some thirteen year old proto-hacker. These kids, like most kids, are tremendously susceptible to peer pressure. They already find criminal hacking attractive because it's viewed as today's counter-culture—something fairly harmless (compared with, say, dealing drugs) but exciting because it's illegal. Now imagine that the older creeps can announce that they've just been hired by The Man (i.e., authority figures) to work in counter-intelligence, snooping in foreign companies' files for money (you don't imagine they'd keep it quiet, do you?). Oh man—not only is criminal hacking glittering with the allure of the forbidden now, but you can hope to earn money with it from the government!

The children and emotionally-arrested adolescents involved in criminal hacking already have a love/hate attitude towards The Man. Many of them claim that they'd like to work for security firms when (if) they grow up. This myth that criminal hacking is a reasonable basis for work in security would become even more pernicious if it were known that more hackers had in fact been solicited and used by government or corporate organizations. Using such people would reinforce the attractiveness of criminality.

Consider the outcry if the military in a democracy actively solicited murderers to be soldiers. The great challenge of military training is to temper savagery with honor; to provide a moral framework within which war is viewed as undesirable, killing as regrettable. A soldier who lies is a stain on his unit's honor. A soldier who steals is a wretch who deserves expulsion. And a soldier who breaks his word is a traitor to his country. And so how shall we deal with people whose entire way of life is to lie and to steal and to cheat?

I say they're unfit to serve.

At the most fundamental level of all, the end does not justify the means. To use criminals, to honor them, to praise them, to pay them: this would be yet another blow against morality and decency. And it would be a blow without even the excuse of necessity. We do not need criminal hackers. Information security can be strengthened using the skills of honest people—hackers, you like, not criminal hackers. We should be encouraging children who enjoy using computers to learn more, to learn deeper. We need school teachers who have more than merely a superficial knowledge of the user interface: we need teachers with a thorough grounding in computer science. We need books for children to teach operating systems fundamentals and database theory in an enjoyable, challenging way; we need recognition for the gifted—support for the oddballs who prefer trackballs to basketballs. We need donations of computer equipment and texts from companies who see that helping kids learn is a wise investment in everyone's future. Why not donate used mainframes and servers to help kids learn about operating systems and networks? Let's give brilliant kids with a knack for security summer jobs so they can use their skills to help society instead of feeling marginalized.

What we don't need is reward for dishonesty and praise for sociopathy.

In the Hacker Debate at the InfoWarCon 95, someone asked me if I recommended blackballing all hackers who engaged in illegal activity in their adolescence. I answered that no, there should not be a life-time ban on criminal hackers—as long as they show that they understand their moral and legal

Fruit of the Poisoned Tree

obligations to society and their employers or clients. If a person shows by their actions that they have matured and now repudiate their former lifestyle, by all means give them a chance. Keep them under supervision, avoid putting them in temptation's way, and be on your guard—but by all means welcome recovering hackers back to society.

Just don't solicit people *because* they are or were criminal hackers.

