WHY DO HACKERS HACK?

To answer this question, first of all, the definition of Hacker has to be stablished.

The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music. Actually, you can find it at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them "hackers" too and some claim that the hacker nature is really independent of the particular medium the hacker works in.

In this article, we will be focusing in the software-hacker context. So, a hacker is any highly skilled computer expert that uses their technical knowledge to overcome a problem.

But why do these “computer-freaks” behave as they do? Psychologists have tried to answer this question.

In general, when people do something, they have an intentional goal. All activities are spurred by a variety of motivations. Social psychology has noted that motivations for influencing behaviors could be divided into intrinsic motivation and extrinsic motivation.

**INTRINSIC MOTIVATIONS**

A hacker who possesses integrated self (true self-esteem) may hack autonomously. That is, a hacker triggered by true self-esteem believes that he has competence, knows how to break in and out without accidental destruction to a computer system and also believes that his behaviors are based on his own ethics and are supported by others. Consequently, this intrinsic motivation may lead to hacking. Since intrinsic motivation in a hacker may not be pressured by exterior demands, threats, or rewards, hacking itself gives him happiness and enjoyment. For intrinsically motivated hackers, hacking means just having a pretty good time. They don’t see any other standard or norm. Instead, they just do it autonomously and enjoy it while exploring others’ computer system.

Post claimed that hackers were motivated by the challenge, the excitement to succeed, and a desire to learn for the pure intellectual satisfaction.

Denning reported that the thrill of illicit behaviors, excitement, and challenge is the main reason for hacking.

* FLOW

Csikszentmihalyi was one of the first psychologists to study the enjoyment dimension. He emphasized that some activities were pursued for the sake of the enjoyment derived from doing them.

He proposed a state of “flow”, in which enjoyment is maximized, characterized by intense and focused concentration; a merging of action and awareness; confidence in one’s ability; and the enjoyment of the activity itself regardless of the outcome. Flow states occur a person’s skill matches the challenge of a task. Thus hackers may be seeking flow states by selecting projects that match their skill levels with task difficulty, a choice that may not be available in their regular jobs.

Flow concept may explain why hackers keep breaking into computer systems, and why they want to explore tightly restricted computer systems such as top-secret government computer infrastructure, military networks, and nuclear plants. For instance, if a hacker endorses the cause that “information should be free from government;” if the hacker thinks how well he/she is doing; if he/she feels the confidence to break into the CIA computer systems, these situational conditions may propel the hacker to feel optimal experience (flow).   
  
In other words, after frequent illegal access to several university web sites, hackers who break into the main computer systems in a university feel that this is very easy to do might want to test their hacking techniques with computer banking systems which are a little bit more difficult to access. Once the hacker successfully attains the goal in a bank, he/she is likely to look for the most difficult computer networks such as intelligence, military, government, emergency systems, or nuclear plants.

* EXPRESSION OF DISATISFACTION

[Adam Dachis](http://kinja.com/adachis) has a very interesting perspective of hacking and why its done. He states the following:

Hacking is a means of expressing dissatisfaction, confounding the mechanism, and ultimately doing better. Is a brand of disobedience that both expresses dissatisfaction with the status quo and does something to change it.

It’s hard for a lot of people to justify disobedience because it often involves breaking rules, if not the law. There’s always at least a shred of incorrectness to disobedience, even if it’s committed for all the right reasons. Hacking gets a bad reputation for those reasons as well.

We’ve seen numerous examples of the benefits of civil disobedience over time, from Gandhi’s campaign for independence from the British Empire (e.g.: [the Salt March](http://en.wikipedia.org/wiki/Salt_march)), to the [Civil Rights Movement](http://en.wikipedia.org/wiki/Civil_rights_movement) in 1950s.

We hack because we want to do better. We hack because we want to demonstrate the desire for greater possibilities. We hack because we’re sick and tired of being caught in a net designed for other people. We hack because it’s fun. With the internet becoming the world community, hacking is our form of civil disobedience. It’s our way to passionately tear down and rebuild, confound the mechanism, and express dissatisfaction through improvement. It’s about doing better, not breaking the law.

* PRINCIPLES

Lindenberg makes the case that acting on the basis of principle is a form of intrinsic motivation. He argues that individuals may be socialized into acting appropriately and in a manner consistent with the norms of a group. Thus the goal to act consistently within the norms of a group can trigger a normative frame of action. like the case of E.H.A.P (e.g., Ethical Hackers against Pedophilia), some hackers seek out and stop the exploitation of children on the Internet.

Levy noted that a number of hacker groups wanted to maintain cyberspace as a free playground and argue that information should be free.

Shaw claimed that because they object to the control and monopolistic power from transnational corporations and governments in cyberspace, they try to sustain cyberspace as an unlimited, anti-commercial, and deregulated realm where information should be shared without any monetary compensation.

**EXTRINSIC MOTIVATIONS**

On the other hand, an extrinsically motivated hacker may consider some standards, rewards, or pressures as his or her major reason to hack, crack, or deface target web pages. That is, in order to obtain peer recognition, financial benefits in terms of stealing individual information, being the top hacker among their communities, or promoting some cultural worldviews (i.e., ideology, nationalism, and religion), they may break into others’ computer systems.

According to Rist, a prime motivational factor for hacking is “a mixture of ego and political commentary.” He pointed out that “a big chunk of a true hacker’s mind-set is ego: “I am smarter than you are, just check your web page.” Not surprisingly, hackers often brag and show loopholes in the site to webmasters thus proving that they are better technocrats than are those who manage the web site.

Parker noted that their motivations include greed, need, desensitization of the harm done to others, personification of computers and the Robin Hood syndrome (stealing from the rich is morally justified).

Taylor claimed that political acts could be one of possible motivations why engaging in hacking.

* REPUTATION, RESPECT AND ACKNOWLEDGEMENT

Like most cultures without a money-based economy, hackerdom runs on reputation. Hackers try to solve interesting problems, but how interesting they are - and whether their solutions are really good - is something that only technical peers or superiors are normally equipped to judge. Accordingly, when hackers play the hacker game, they learn to keep score primarily by what other hackers think of their skill (this is why they aren’t really a hacker until other hackers consistently call them one). This fact is obscured by the image of hacking as solitary work; and further by a cultural taboo amongst hackers that forbids admitting that ego or external validation are involved in one’s motivation in any way. Specifically, hackerdom is what anthropologists call a gift culture. Hackers gain status and reputation in it not by dominating other people, nor by being beautiful, nor by having things that other people want, but rather by giving things away. Specifically, by giving away time, creativity, and the results of their particular skill.

Reputation incentives continue to operate whether or not a craftsman is aware of them; thus, ultimately, whether or not a hacker understands his own behavior as part of the reputation game, his behavior will be shaped by that game

There are reasons common to every gift culture as to why repute amongst peers (prestige) is worth playing for:

Firstly, and most obvious, good reputation among one’s peers is a primary reward.

Secondly, prestige is a good way (and in a pure gift economy, the only way) to attract attention and cooperation from others.

Finally, the reputation-game analysis explains the oft-cited dictum that you do not become a hacker by calling yourself a hacker - you become a hacker when other hackers call you a hacker.

* TERROR MANAGEMENT

This theoretical frame stems from Ernest Becker concept: the terror of death. That is, a person’s self-esteem is driven by the denial of death. People want to escape from the anxiety that would arise from recognizing that one will die.

Therefore, to get rid of this potential terror, people tend to use “cultural worldviews that help individuals manage this terror by denying that life is a purposeless biological accident and that death is absolute annihilation for the individual

In other words, when a person is criticized by others concerning his/her cultural worldview, he or she will have more aggressive expressions against the worldview threatening others than those who do not feel any threat to their own cultural worldview. Historically, many have tried to remove the group who do not share their worldview by attempting to annihilate those who are different (i.e., massive murder of Jews by Nazi, the ethnic cleansing in Rwanda, and the crisis between Bosnians and Serbs, etc.).

Based on this rationale, we may infer that hackers can feel threatened by some others who are different in politics, religion, nation, or ethnicity. In this study, we point out hackers’ cultural worldviews espoused by nationalism, religion, ethnicity, and any kind of ideology.

As Taggart mentioned, many hackers and web defacers have participated in a series of cyber-wars on behalf of their nations, religions, or ethnicities.

Denning saw that patriotism catalyzes hacking in behalf of the hacker’s country. Hackers who have certain cultural worldviews concerning religion, ethnicity, and nationalism are enthusiastically involved in attacking web sites and computer systems of opposing sides.

**COGNITEVELY DIFFERENT?**

Psychologists have postulated that hackers perceive and experience the world differently than mainstream society and those reasons may be attributed to neurological conditions, such as Asperger's Syndrome. Nevertheless, further research must be done. For now, it only remains a hypothesis.

We can’t say specifically why a determined hacker hacked, everyone is different. Everyone has a different ideology, belief, mindset, culture, environment, political root, ethnicity, religion and economical situation. What we can say for certain, is that there are many reasons that motivate them to act the way they do and they won’t stop.

Alex Chavarria Podoliako

21020816