Inside the mind of a hacker: Psychological profiles of cybercriminals

11 February 2020, by Kevin Manne

Credit: CC0 Public Domain

Whether cracking digital security for good or ill, hackers tend to be people who are manipulative, deceitful, exploitative, cynical and insensitive, according to research from the University at Buffalo School of Management.

Recently presented at the Hawaii International Conference on System Sciences, the study analyzed the psychological profiles of college students in computer science and management to see which personality traits led to three different kinds of computer hacking: white hat, gray hat and black hat.

White hats are the ethical hackers, who help organizations detect and fix their security vulnerabilities. Gray hats are the "hacktivists," who hack for ideological reasons, such as attacking a political adversary, a company policy or even a nation-state. And black hat hackers, sometimes called crackers, are motivated by personal gain to breach computer systems—or may just be in it for the thrill of the attack, revenge or notoriety.

"Gray hatters oppose authority, black hatters are thrill-seeking and white hatters—the good guys—tend to be narcissists," says Lawrence Sanders, Ph.D., professor of management science and systems in the UB School of Management. "So even though white hats may be devious and psychopathic, we need them to address nefarious hacking activity."

The researchers surveyed 439 college sophomores and juniors to determine their personality traits, and developed a set of scales to determine the three hat categories, as well as a scale to measure each person's perception of the probability of being caught for violating privacy laws.

"Engaging in criminal activity involves a choice where there are consequences and opportunities, and individuals perceive them differently," says Joana Gaia, Ph.D., clinical assistant professor of management science and systems in the UB School of Management. "But, they can be deterred if there is a likelihood of punishment—and the punishment is severe."

The results of the study suggest that security compliance will continue to be a problem, but there are several ways businesses and organizations can reduce the impact or prevent security breaches.

"Firms can use monitoring technology and multifactor authentication to prevent unauthorized access to physical and digital spaces," says Gaia. "Organizations could use personality traits to evaluate employees as security threats, but that should be approached cautiously for practical, ethical and privacy reasons."

Provided by University at Buffalo

APA citation: Inside the mind of a hacker: Psychological profiles of cybercriminals (2020, February 11) retrieved 27 January 2021 from https://techxplore.com/news/2020-02-mind-hacker-psychological-profiles-cybercriminals.html