From Young Hackers to Crackers

Jean-Loup Richet, University of Nantes, Nantes, France

ABSTRACT

A growing number of scholars state that the Internet presents “some unique opportunities for deviant behavior” (Rogers et al., 2006). However, although some researchers have studied this issue, the factors leading teenagers to adopt a web-deviant behavior have received less attention. From this background, the present article sets out to explore the facilitators of cybercrime. The author will explain the diffusion of web-deviant behavior amongst young people through an analysis of the literature while taking into consideration the conceptual model of diffusion of innovation by Greenhalgh et al. (2004).

From Young Hackers to Crackers

Jean-Loup Richet, University of Nantes, Nantes, France

INTRODUCTION

Cyberspace has created a new dimension of social interaction. It has transcended time and space, and, as such, physical context is no longer linked with social situation. A virtual presence need not be true to the actual persona of its creator in the physical world. This simple fact has had an alarming effect on the negative cyber behaviors of today’s youth, who have used the anonymity of the web to indulge in cybercrime or hacking. It has become critical to inquire into and understand the growing criminal cyber-behavior of teenagers. This requires a detailed study of the meanings of and differences between hacking and cybercrime and the visualization and use of these terms by the youth alongside their attitudes towards both.

Further, a growing number of scholars state that the Internet presents “some unique opportunities for deviant behavior” (Rogers et al., 2006). Technology has given people the unprecedented ability to hide their identities under cover of anonymity, and they can avoid the penalty for embarrassing or illegitimate activity. Whereas few people (of any age) would be able to walk into a room full of complete strangers and share nude photos of themselves, talk about sex, or discuss illegal use of drugs, they can do it online behind the “protection” of the magically anonymous keyboard. This ability profoundly affects the online behavior of teenagers.

Nevertheless, although some researchers have studied this issue, the factors leading teenagers to adopt a web-deviant behavior have

DOI: 10.4018/jthi.2013070104
received less attention. From this background, the present article sets out to explore the facilitators of hacking and cybercrime. This paper will explain the diffusion of web-deviant behavior amongst young people through an analysis of the literature study while taking into consideration the conceptual model of diffusion of innovation by Greenhalgh et al. (2004).

CYBERCRIME VS. HACKING

Cyberspace transforms the scale and scope of offense; has its own limits, interactional forms, roles, and rules; and it has its own forms of criminal endeavor (Capeller, 2001). According to Yar (2005), the “novel socio-interactional features of the cyberspace environment (primarily the collapse of spatial-temporal barriers, many-to-many connectivity, and the anonymity and plasticity of online identity) [...] make possible new forms and patterns of illicit activity.” Anyone who is computer literate can become a cybercriminal.

There is still no clear definition of “cybercrime” (Fafinski et al., 2010). In some cases, cybercrime can encompass the use of computers to assist “traditional” offending but it can also be a crime mediated through technology (Wall, 2007) or an exclusive technological crime, such as a denial-of-service attack). Many criminal law scholars focus on the legalistic framework. For instance, Wall (2001) uses the categories of criminal law to create categories of cybercrime. Others categorize cybercrime as an offense “related to computers, related to content or against the confidentiality, integrity and availability of computer data and systems” (Council of Europe Convention on Cybercrime, 2001).

The use of the term “hacker” has changed over the years from a positive and complimentary definition — the enthusiastic computer programmer who is particularly brilliant — to a negative and pejorative one: the cybercriminal. Nowadays, “cybercriminal” is a term synonymous with “hacker.” Hacker, as a term, is commonly used by the mass media to refer to an intruder breaking into computer systems to steal or destroy data. Police describe almost any crime committed through, with, by, or against a computer as “hacking.” “For many people, the hacker is an ominous figure, a smart-aleck sociopath ready to burst out of his basement wilderness and savage other people’s lives for his own anarchical convenience” (Sterling, 1993).

This concept of “hackers” is still the subject of heated controversy. In response to the common demonization of the term hacker, The New Hacker’s Dictionary (Raymond & Steele, 1991) has coined the term “cracker.” Crackers use their computer-security-related skills to author viruses, trojans, etc., and illegally infiltrate secure systems with the intention of doing harm to the system or criminal intent and to differentiate them from the original and non-criminal hacker. This article will use the term hacker in its original positive meaning and the term cracker for those committing cybercrime.

CONCEPTUAL MODEL AND METHODOLOGY

Originally, hacking was seen as innovative behavior; even the original term “hack” was a slang word used by MIT students in the 1950s to refer to an improvement. According to Rogers (1983), an innovation is “an idea, practice, or object that is perceived as new by an individual or other unit of adoption.” Further, the central meaning of innovation relates to improvement or renewal, with novelty being a consequence of this improvement. However, eventually hacking led to many teenagers deviating from using their skills to improve or push the limits of their expertise to using those same skills for cybercrimes, such as Internet extortion and fraud. Our hypothesis is that hacking is an innovation compared to cybercrime and is different from either cyber or traditional criminal behavior. Computer hacking can lead to constructive technological developments; for example, former hackers Dennis Ritchie and Ken Thompson went on to create the UNIX
Related Content

Neighborhood Resource Center: The Library Partnership
Sol M. Hirsch (2012). *Partnerships and Collaborations in Public Library Communities: Resources and Solutions* (pp. 1-14).
[www.irma-international.org/chapter/neighborhood-resource-center/62320/](www.irma-international.org/chapter/neighborhood-resource-center/62320/)

Security Benefits of Little Data From the Socio-Technical Perspective

Using ICT to Foster Human Rights Defense Processes for Mexican Immigrants
Maria Alejandra Rocha Silva, Juan Contreras-Castillo and Ricardo Acosta-Díaz (2011). *Technology for Facilitating Humanity and Combating Social Deviations: Interdisciplinary Perspectives* (pp. 132-150).
[www.irma-international.org/chapter/using-ict-foster-human-rights/47346/](www.irma-international.org/chapter/using-ict-foster-human-rights/47346/)

Enabling Programmable Ubiquitous Computing Environments: A Middleware Perspective
[www.irma-international.org/chapter/enabling-programmable-ubiquitous-computing-environments/22412/](www.irma-international.org/chapter/enabling-programmable-ubiquitous-computing-environments/22412/)

Understanding University Students’ System Acceptance Behavior: The Roles of Personality Trait and Subjective Norms
[www.irma-international.org/article/understanding-university-students-system-acceptance-behavior/158144/](www.irma-international.org/article/understanding-university-students-system-acceptance-behavior/158144/)