GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 5 May (2024)

COMPUTER CRIME PSYCHOLOGY: MOTIVATIONS AND DRIVING FACTORS

Qurbonova Aziza Davlat qizi
Sharof Rashidov nomidagi Samarqand davlat
universiteti psixologiya kafedrasi magistranti

ABSTRACT

This article provides information on what motivates individuals to engage in illegal online activities to effectively combat computer crime and the psychological factors, psychological profiles and motivations that incite them. In addition, the modification of cybercrime types and the psychological portrait of a computer criminal have been interrupted separately.

Keywords: Cybercrime, psychological profile, psychological portrait, hacker.

INTRODUCTION

Increasingly, in the digital world, computer crime in other words, cybercrime has become a common and constantly evolving threat. Understanding the psychology of cybercriminals is vital not only to prevention, but also to law enforcement efforts. Examining the factors that motivate criminals to commit cybercrime helps them gain valuable insights into the world of criminal activity.

The rapid development of the Internet has opened up a wide range of opportunities, but it has also brought in a new type of criminals - cybercrime criminals. These individuals or groups use digital tools and technology to commit crimes ranging from hacking and personal data theft to anti-payment attacks and online fraud. To effectively combat cybercrime, it is necessary to understand what drives these individuals to engage in illegal online activities and the psychological factors that fuel them. One example of these situations is:

Lack of empathy: A great feature of some cybercriminals is their apparent lack of empathy. They may not be able to fully understand the true consequences of their actions.

Narcissism and ego: Some cybercrims are controlled by narcissism and ego. They pride themselves on their hacking capabilities and seek recognition and validation in a hacking society.

Risk Avoidance: Cybercrime offers anonymity and a degree of victimization, which can reduce perceived risks to many offenders. This factor tempts some to engage in illegal activities.

Addiction behaviors: Engaging in cyberstalking can lead to addiction. Excitements of successfully disrupting the system or obtaining sensitive data may create a compulsory craving for more cybercrime activities.

To truly understand the world of cybercriminals, we must also investigate their motivations. Common factors that motivate people to cybercrime:

Financial Gain: One of the most common motivations behind cybercrime is financial gain. Cybercriminals may try to steal valuable information, steal personal data, or launch ransomware attacks in order to exact money from victims.

Revenge and ideological beliefs: Some cybercriminals are motivated by a sense of revenge or a loyalty to certain ideological beliefs. They can target individuals, organizations or governments they perceive as hostile or hostile.

Seeking out excitement: As mentioned above, the adrenaline rush associated with successful use can be extremely addictive. For some people, incredible excitement of security systems becomes the main motivation.

Curiosity and hassle: Curiosity is a powerful motivation for some cybercrims. They are driven by the problem of simply accessing systems and networks to test their skills and push the boundaries.

In addition, various scientists have modified computer crime or cybercrime differently. Based on the works of D. L. Shinder (USA), T. L. Tropina, the following modifications of types of cybercrime have been developed:

a) violent or other potentially dangerous cybercrime that violates a person's physical safety, life and health;

b) crimes that violate the confidentiality of information - illegal access to computers or computer systems without damaging information;

c) destructive cybercrimes that harm data, undermine their integrity and the safety of computer systems;

d) crimes that violate property, property rights, as well as the right to own information and copyright through theft;

e) crimes that violate public morality;

f) offensive crimes of public safety;

g) other cybercrimes committed through computer networks and encroaching on various objects protected by law (traditional crimes, whose occurrence helps the computer implement them or creates new opportunities).

Speaking of a psychological portrait of a computer criminal, a criminal often leaves his mouth on a computer as a child. For it, a computer system is a mystery that must be studied and used efficiently. Analysis of local and foreign practices and a study of literary sources show that the ages of computer offenders vary in very wide margins, that is, between the ages of 15 and 45 on average. According to research, 33% of those who committed crimes at the time of the crime were under the age of 20, 13 were over the age of 40, and 54% were young people between the ages of 20 and 40. So computer criminals, in other words, hackers are not always young children, as previously believed.

Males make up more than 80% of the hackers, while it should be noted that percentage of women's participation is growing rapidly, mainly due to the professional orientation of certain specialties and positions filled by women secretary, accountant, economist women. However, the amount of damage from crimes committed by men is four times greater than that committed by women.

Interestingly, 77% of computer criminals had an average level of intellectual development, 21 were above average and only 2% were below the average level, 20% of criminals had secondary, 20% had secondary education, 60% had higher education.

The individual characteristics of a computer offender are an active life position, originality (non-standard) thinking and behavior, caution, caution. They focus on understanding, predicting and managing processes, which become the basis of their skills and skills. Given the psychophysical characteristics, such a criminal, as a rule, is a bright, thoughtful and creative person, a professional, valuable employee in his field. Outwardly, the behavior of computer criminals rarely differs from the social norms established in society. Moreover, practice shows that most of them are not convicted.

Research allowed computer criminals to be divided into groups.

The first group includes individuals who are distinguished by a stable combination of professionalism in the field of computer technology and programming with their own fanaticism and zukkolik elements.The second group includes people with a new type of mental illness - information diseases, computer fear (with which information medicine is involved).

The third and most dangerous group includes professional computer criminals.

In conclusion, the psychology of computer criminals is complex and versatile. Understanding the causes of computer crimes helps individuals and businesses better protect themselves from cyber threats. By taking preventive measures and investing in cybersecurity, businesses can reduce the risk of becoming victims of cybercrime and protect their confidential information and financial information.

REFERENCES

1. Ushatikov A.I., Kovalev O.G., Korneeva G.K.
2. APPLIED CRIMINAL PSYCHOLOGY Textbook.
3. Ryazan, 2012. C 210-215.
4. Vasiliev Vladislav Leonidovich "Legal Psychology" M.,2009 p 292-294
5. Sobolnikov V.V. "Criminal Psychology" M.,2009 p 197-2001

Used Sites:

https://www.wallix.com\
https://www.researchgate.net