IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

# Hacking on Crime with Workable Solution: A Survey

**Sugandhi Aakash[1], Sumit Chaudhary[2]**

Student, Computer engineering, IIST, Ahmedabad, India [1]

HOD, Computer engineering, IIST, Ahmedabad, India [2]

**Abstract:** A scattered group of people often called “hackers" have been characterized as unethical, irresponsible, and a serious danger to society for actions related to penetrating into computer systems and websites. In the current day, the world has witnessed an unmatched index of Cyber-crimes whether they involve various attacks like Trojan attacks, salami attacks, e-mail bombing, DOS attacks, information theft, or the most common offence of hacking. Over the last decade, the frequency of cyber-crime has been increased despite a large number of technological measures implemented by corporate organizations and individuals. This paper endeavors to construct a picture of hackers, their concerns, and the discourse in which hacking takes place. This paper depicts the significance of hackers and gives suggestion that hackers are learners and explorers who want to help rather than causing damage, and who often have very high standards of conduct.

**Keywords:** Hacking, Phishing, Computer crime, Computer Security, cyber fraud, Prevention of cyber-crime.

## 1. INTRODUCTION

“A 15-year-old boy sits behind a phosphorescent black monitor, typing frenziedly. The green text rindle across his screen like a waterfall. His neurasthenia escalates perilously as he sends precipitate proclamation to the farfetched computer. Unanticipatedly, he lets out a swaggering laugh and proceeds to steal money.”

These devices are used as a target by attacking the computer conclude viruses, as a backsword to commit crimes or as an accessory to store actionable information. Cyber Crimes also affect business every year, losing billions of money and mischievous the company's approval leading to loss of future business as well. Now a days, cyber systems replenish adjustability leading to its felonious use.

Reprehensible using computers will not stop their crimes to the precinct of the world which have thus far enjoyed the harvest of network technology. Criminals will also swindle singleton and standardization of developing camaraderie and transpire equalitarianism. These societies are particularly assailable because their institutions are in their incunabulum, thus beneficence criminals a greater juncture to victimize individuals and organizations. In augmentation, these governments, organizations, and individuals in developing societies do not have the wherewithal and technology to protect themselves.

In the present day world, India has corroborator and huge increase in Cybercrimes whether they affect to Trojan attacks, salami attacks, e-mail bombing, Clickjacking Attacks, Waterhole attacks, DOS attacks, Eavesdropping (Passive Attacks), Phishing,Bait and switch,information theft, or the most common offence of hacking the data or system to commit crime.

## 2. LITERATURE REVIEW COMPARISON

In “Cyber Crime–A Threat to Persons, Property, Government and societies.” Author proposed that the rapid augmentation of computer technology and the amalgamation of computer and communication technology have made indicative changes to human propaganda activities. Firstly, the systematic and yielding power of information concoct has made computer the most important tool for data processing. As a result, more and more data are processed and stored in computer systems. The out vie nature of the Internet has made it one of the major channels for human communication.

In “Password security: An empirical investigation into e-commerce passwords and their crack times.” Author proposed that Strong passwords are essential to the security of any e-commerce site as well as to individual users. Without them, hackers can break in a network and stop cavallies working that assist end user and keep companies operating. For most e-commerce sites, end user have the incumbency of creating their own passwords and often do so without conveyance from the web site or system chairperson. One fact is well known about password procreation ―consumers do not create long or labyrinthine passwords because they cannot remember them.

In “International computer crimes.” Author proposed that since the nature of network electronic components creates opportunities for criminals to remotely swindle anyone on the planet, a reverberation to computer crime needs to be cosmopolitan in nature. Consequently, this Article describes the nature of computer crimes and addresses issues and problems which will pursuance the international

DOI10.17148/IJARCCE.2017.6373

territory. The Background. It make vivid how network technology has created a new type of criminal and criminal big idea that uses unique techniques to flimflam individuals and organizations.

In “Security Research on WEP of WLAN.” Author proposed that Reconnaissance is the first thing hackers have to do before attacking the WLAN. Hackers drive around in a car equipped with wireless gears looking for unsecured WLAN to break in. They have to prepare some equipment to finish this work. For example: Laptop or PDA, 802.11b wireless card, antenna, GPS receiver and vehicle.

In “Denial-of-service attacks rip the Internet.” Author proposed that Denial-of-service attacks have been around for years. The attacks have used several techniques to crash, hang up, or overwhelm servers with malformed packets or large volumes of traffic. However, said Northcutt, it is the highly distributed aspect of February’s attacks that made them so different and frightening.

In “Wi-Foo: the secrets of wireless hacking.” Author proposed that the definitive guide to penetrating and defending wireless networks. Straight from the field, this is the definitive guide to hacking wireless networks. Authored by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack -- or protect -- any wireless network. The authors introduce the 'battlefield,' exposing today's 'wide open' 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools: crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless 'citadels" including cryptography-based techniques, authentication, wireless VPNs, intrusion detection, and more.

## 3. HOW TOPREVENT HACKING?

**Update your devices and software on time**
As soon as an update becomes available for anything from the Facebook app on your phone to your computer's entire operating system, you should apply it if possible.

**Don't give out your password**
This is an obvious piece of advice, but one that bears revisiting: with the exception of some school services, you shouldn't ever have to provide a site administrator with your password for them to access your account.

**Change your passwords often**
In addition to keeping your password a secret, you should change the passwords on your various accounts and devices at least once every six months.

**Download programs only from reputable sites**
This methodology goes for sites you visit on an unsecured connection as well. If there isn't a padlock icon to the left of the URL address, it's best to avoid the site (and downloading anything from it) entirely if possible.

**Use secured wireless networks**
Generally speaking, secured networks require you to enter a password before you can connect to them. In some locations (such as airports or coffee shops), you can request the password after purchasing an item.

**Make sure you're on an official website when entering passwords**
Phishing scams--instances in which a malicious page pretends to be a login page for a social media or bank account--are one of the easiest ways for you to get hacked. One way to spot phishing scams is to look at the site's URL: if it closely resembles (but doesn't exactly match) a reputable site's URL (e.g., "Faecbook" instead of "Facebook"), it's a fake site.

**Log out of accounts when you're done with them**
Simply closing the browser window isn't always enough, so make sure you click (or tap) on your account name and select **Log Out** (or **Sign Out** in some cases) to manually sign out of your account and remove your login credentials from the site.

**Log out of accounts when you're done with them**
Simply closing the browser window isn't always enough, so make sure you click (or tap) on your account name and select **Log Out** (or **Sign Out** in some cases) to manually sign out of your account and remove your login credentials from the site.

**Install antivirus software on your computer**
Antivirus software recognizes and removes potentially harmful files and programs as soon as you download them. AVG and McAfee are both competent cross-platform (Mac and PC) antivirus programs.

## 4. CONCLUSION

This paper applause for security mechanism to stop crime occur on internet or cyber-crime. There is various types of crimes that depends on various technologies. Now a day the situation is like “the more technology and security, the more crimes”. A hacker can break any security mechanism with various and latest technical tools to hack anything easily. To avoid cyber-crime we should make more secure software to protect people and also provide information through webinar and seminars to be careful and one should not take hacking in a wrong way or negative way

## 5. FUTURE SCOPE

One can build such software or technology that provides more security to avoid hacking and people can use internet securely. We should provide knowledge regarding hacking to students to take hacking in positive way.

DOI10.17148/IJARCCE.2017.6373

## REFERENCES

[1] Kharat, Shital Prakash. "Cyber Crime–A Threat to Persons, Property, Government and Societies." (2017).
[2] Cazier, Joseph A., and B. Dawn Medlin. "Password security: An empirical investigation into e-commerce passwords and their crack times." Information Systems Security 15.6 (2006): 45-55.
[3] Zakaras, Matthew R. "International computer crimes." Revue international de droit pénal 72.3 (2001): 813-829.
[4] Ye, Peisong, and Guangxue Yue. "Security Research on WEP of WLAN." Proceedings of the Second International Symposium on Networking and Network Security (ISNNS'10) Jinggangshan, PR China. 2010.
[5] Icove, David, Karl Seger, and William VonStorch. Computer crime: a crimefighter's handbook. California: O'Reilly & Associates, 1995.
[6] Casey, Eoghan. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.
[7] Carter, David L. "Computer crime categories: how techno-criminals operate." FBI law enforcement bulletin 64.7 (1995): 21.
[8] [8] Garber, Lee. "Denial-of-service attacks rip the Internet." IEEE Computer 33.4 (2000): 12-17.
[9] Warren, Matthew, and William Hutchinson. "Cyber attacks against supply chain management systems: a short note." International Journal of Physical Distribution & Logistics Management 30.7/8 (2000): 710-716.
[10] Barber, Richard. "Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated." Computer Fraud & Security 2001.3 (2001): 9-12.
[11] Vladimirov, Andrew, Konstantin V. Gravrilenko, and Andrei A. Mikhailovskiy. Wi-Foo: the secrets of wireless hacking. Pearson Education, 2004.

## BIOGRAPHIES

**Sugandhi Aakash** is pursuing BE in Computer Engineering from IIST, rajpur, kadi, Gujarat, India. He is currently doing her 8th semester project in .Net language. Her interest of area is networking in WSN.

**Sumit Chaudhary** is working as Head of Department in CSE at Indrashil Institute of Science & Technology, Cadila Group, Rajpur, Ahmedabad (Gujarat). He is pursuing Ph.D. from Uttaranchal University, Dehradun (Uttarakhand). He worked with various institutes like Uttaranchal Institute of Technology (UIT), Dehradun, Shri Ram Group of colleges, Muzaffarnagar (U.P.), IIMT Institute of Engineering & Technology, Meerut (U.P.), INDIA including all that he has more than 7 year experience in teaching. He obtained his M-Tech (Computer Science & Engineering) with Hons from Shobhit University and B-Tech (Computer Science & Engineering) from SCRIET, Meerut (U.P.). During this short period of time, he has been supervised several dissertation of M.Tech students. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes Cloud Computing, Wireless Sensor Network (WSN), Network Security, Neural Network, Artificial Intelligence and MANET (Mobile Ad-Hoc network)..

DOI10.17148/IJARCCE.2017.6373