iJRASET

International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VII Month of publication: July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36882

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Cyber Security: Cyber Fraud on Carding: A Review

Arpit Pandey[1], Kanchan Thool[2]
[1]B.E Student, [2]Assistant Prof, School of Engineering and Technology, Vikram University, Ujjain, India

***Abstract:** This chapter provides one person case study of Mr. Dan DeFilippi who was arrested for master card fraud by the US u. s. SS in December 2004. The episode delves into the psychology of a cybercriminal and also the inside workings of master card fraud. A background context of master card fraud is presented to border the first interview. Slightly on the identification of issues and controversies with reference to carding is then given. Finally, the convicted cybercriminal turned key informant makes advice on how to reduce the growing prevalence of cybercrime. A giant finding is that master card fraud is simply too easy to enact and merchants have to conduct better staff training to catch fraudsters early. With increases in global online acquiring, international carding networks are proliferating, making it hard for enforcement agencies to be "policing" illegal transactions. Big data could have a task to play in analyzing behaviors that expose cybercrime.*

***Keyword:** cyber security; Cybercrime; cyber fraud; networks; connected; carding; credit card; debit card .*

I. INTRODUCTION

The technique of protecting internet-connected systems like computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is understood as cybersecurity. we are able to divide cybersecurity into two parts one is cyber, so the other is security. Cyber refers to the technology that has systems, networks, programs, and data. And security is worried with the protection of systems, networks, applications, and knowledge. In some cases, it's also called electronic information security or information technology security. "Cyber Security is that the body of technologies, processes, and process designed to protects networks, devices, programs, and data from attack, theft, damage, modification or illegal access."

"Cyber Security is that the set of principles and practices designed to safeguard our computing resources and online information opposing threats."

A. Types of Cyber Security

Every organization's assets are the combinations of a range of various systems. These systems have a powerful cybersecurity posture that needs coordinated efforts across all of its systems. Therefore, we will categorize cybersecurity within the following sub-domains:

1) *Network Security:* It involves implementing the hardware and software to secure a electronic network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps a corporation to guard its assets against external and internal threats.
2) *Application Security:* It associate protecting the software and devices from unwanted risks. This protection is done by constantly updating the apps to confirm they're secure from attacks. Successful security begins within the design stage, writing ASCII text file, validation, threat modeling, etc., before a program or device is deployed.
3) *Information or Data Security:* It involves implementing a robust data storage mechanism to take care of the integrity and privacy of information, both in storage and in transit.
4) *Identity management:* It deals with the procedure for determining the extent of access that every individual has within a company.
5) *Operational Security:* It associate processing and making judgments on handling and securing data assets.
6) *Mobile Security:* It involves securing the organizational and private data stored on mobile devices like cell phones, computers, tablets, and other similar devices against various malicious threats. These risks are unauthorized access, device loss or theft, malware, etc.
7) *Cloud Security:* It involves in protecting the data stored within the digital environment or cloud architectures for the organization. It uses various cloud service providers like AWS, Azure, Google, etc., to confirm security against multiple threats.

8) *Disaster Recovery and Business Continuity Planning:* It deals with the processes, monitoring, alerts, and plans to how a corporation responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the identical operating capacity as before the event.
9) *User Education:* It deals with the processes, monitoring, alerts, and plans to how a corporation responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the identical operating capacity as before the event.

II. CYBER SECURITY GOALS

Cyber Security's main objective is to make sure data protection. the protection community provides a triangle of three related principles to guard the information from cyber-attacks. This principle is termed the CIA triad. The CIA model is meant to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of those principles has been violated.

We can crack the CIA model into three parts: Confidentiality, Integrity, and Availability. it's actually a security model that helps people to consider various parts of IT security. allow us to discuss each part intimately.

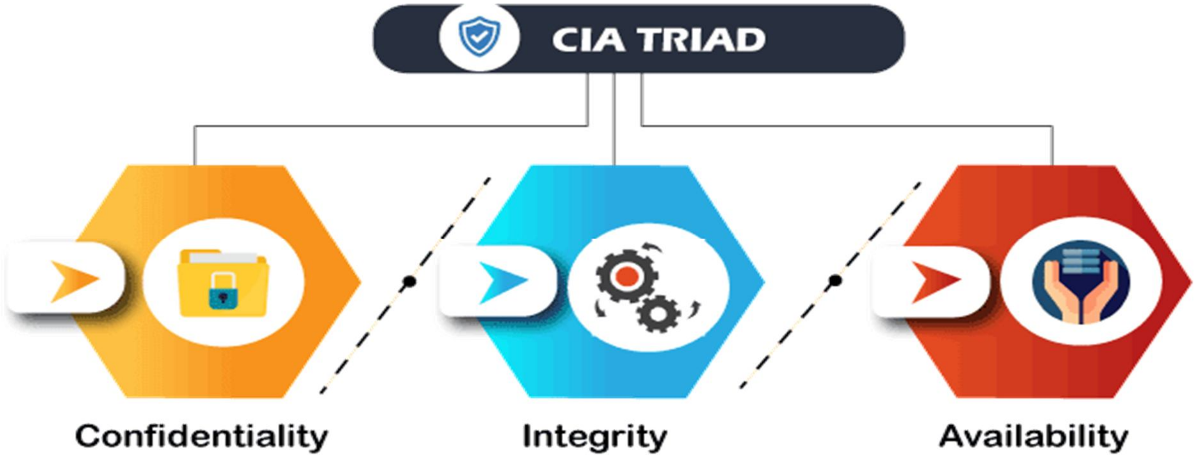

Figure 1 : common goals of cyber security

A. *Confidentiality*

Confidentiality is love privacy that avoids unauthorized access of knowledge. It involves ensuring the info is accessible by people who are allowed to use it and blocking access to others. It prevents essential information from reaching the incorrect people. Encryption is a wonderful example of ensuring confidentiality.

B. *Integrity*

This principle ensures that the info is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to shield the sensitive data from corruption or loss and speedily endure such an occasion. additionally, it indicates to form the source of data genuine.

C. *Availability*

This principle makes the knowledge to be available and useful for its authorized people always. It ensures that these accesses don't seem to be hindered by system malfunction or cyber-attacks.

III. CYBER CRIME

Crime that involves a computer and Network . While most cybercrimes are dispensed so on come up with profit for the cybercriminals, some cybercrimes are allotted against computers or devices on to wreck or disable them, Others transmit viruses, unlawful information, pictures, and other things via computers or networks. Some cybercrime attempts to infect computers with a worm, which subsequently spreads to other devices and, in some cases, whole networks

In other words, “crimes committed against people or groups of persons with the aim to maliciously damage the victim's reputation or cause physical injury” Hacking is a type of cybercrime. In simple words

A. Type of Cyber Crime

1) *Hacking:* Hacking is defined as an unauthorised access into a computer system and/or network.

Figure 2 : Hacking

2) *Child Pornography:* The internet is used for sexual abuse of children
3) *Carding:* Carding is a kind of fraud in which a criminal takes credit card details, checks them for validity, and then uses them to purchase prepaid gift cards. The prepaid cards may be sold or used to purchase other products that may then be resold for cash by the fraudster.
4) *Cyber Stalking:* This phrase refers to stalking through the use of the internet, email, or other electronic communications devices
5) *Denial of Service:* This is a technology-driven cyber incursion in which an influencer floods the bandwidth or blocks the user's email with spam, denying the user access to the internet and the services it provides.

B. Dissemination of Malicious software (Malware)

Malware is software that is meant to carry out an undesired unlawful conduct through a computer network.

1) *Virus:* A worm could be a program which may harm our device and files and infect them for no further use. When a virulent disease program is executed, it replicates itself by modifying other computer programs and instead enters its own coding. This code infects a file or program and if it spreads massively, it's going to ultimately end in crashing of the device.
2) *Trojans:* Trojan is another from of malware, Trojans do things other than what is expected by the user.
3) *Hoax:* A hoax is an e-mail that alerts the recipient about a system that is causing computer damage.
4) *Spyware:* Spyware infiltrates a computer and, as the term suggests, monitors a user's actions without their permission.
5) *Phishing:* Phishing is a sort of social engineering assault that is frequently used to obtain sensitive information from users, such as login passwords and credit card details. When a hacker appears as a trustworthy entity and persuades a victim to open an email, instant chat, or text message, this is known as phishing.

IV. CARDING

A. How Does Carding Work?

The criminals — also referred to as carders — use different methods to induce master card numbers. This introduce phishing attacks and buying stolen payment card numbers for carding from the dark web once carders have that information, they test the cardboard numbers to work out if they're active and haven't been reported stolen. They often do that by making multiple small transactions at e-commerce sites, sometimes with the assistance of automation Carders cover their tracks by using the stolen master card numbers to get prepaid cards, usually store gift cards. The gift cards are then accustomed purchase goods like laptops and TV sets which will be resold later for cash.

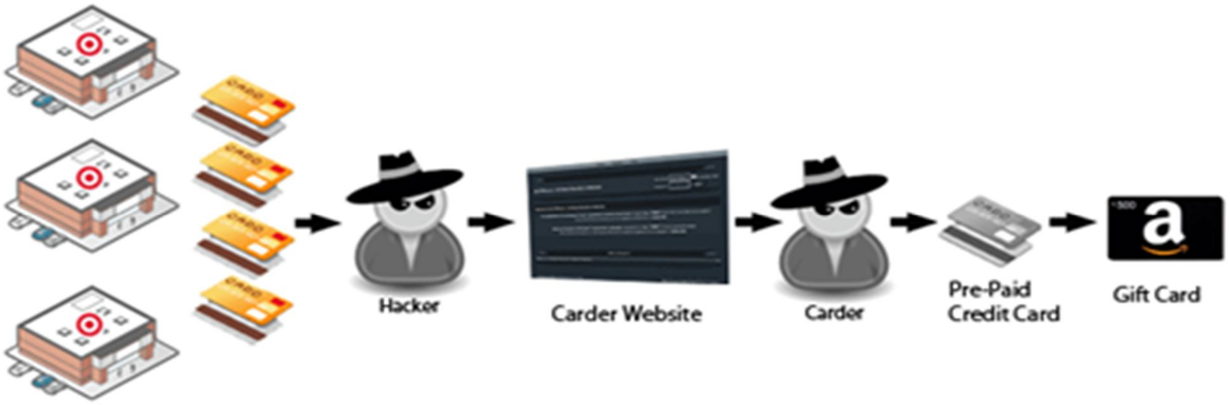

Figure 3 : example of carding

V. PREVENTION OF CARDING FRAUD

No one wants to be a victim of master card fraud, but cardholders are typically only on the hook for up to $50 in unauthorized charges, due to the Fair Credit Billing Act. But by the time the cardboard is canceled, the fraudster has often made several purchases — hurting the retailer within the process "Card-not-present" fraud, also called remote fraud, which encompasses debit cards, credit cards, and other varieties of payment cards, increased 29% within the us between 2015 to 2016. And in 2018, this kind of fraud cost $27.85 billion in worldwide losses, in line with The Nilson Report. In a shot to assist shut out carders, online merchants have implemented security measures that may help protect consumers and sellers. Here are several of them.

1) *Multifactor Authentication (MFA):* Beyond inputting a username and password, this technique adds additional stages to the login procedure. for example, the merchant might send you a text message with a code that you simply type in before using your card. Carders would want to steal your master card number and your phone to interrupt into your account, which is unlikely.
2) *CAPTCHA:* A CAPTCHA could be a kind of challenge-response test that helps an internet merchant verify you are a human shopper. for example, you may must read and sort out a block of distorted text. Carders who use automated bots to test a large number of cards will be required to manually log in, making CAPTCHA-enabled websites less tempting targets.
3) *Address Verification System:* Merchants use this fraud-prevention measure on card-not-present transactions, like online purchases and phone orders. The cardholder will provide their credit card's billing address at checkout, and therefore the AVS compares the address you enter with the one within the card issuer's system to verify it matches. The transaction are going to be declined if the patron fails this test.
4) *Card Verification Value (CVV):* Cardholders may need to enter their card's CVV at checkout. this can be a three- or four-digit code usually listed on the rear of the cardboard. this is often imagined to prove the net shopper has possession of the physical card, not just a card number they've purchased on the dark web.
5) *Velocity Checks:* during this context, velocity is that the number or speed at which transactions are made during a given time. Merchants use this metric to spot irregular patterns within the checkout process which may indicate fraud. for instance, it's unusual for somebody to form several purchases within seconds or minutes of every other. If a merchant suspects a robot is trying a stolen card number, the transaction might be declined

Figure 4 : credit card

6) *Authorization/Capture:* Using this method, a merchant verifies that your card may be charged but holds off on collecting the funds from the cardboard issuer. Gas stations, as an example, typically authorize atony low amount and wait some days before charging the remainder to the cardboard. If there are signs of fraud during the transaction review, the merchant won't request funds from the cardboard issuer. Instead, they'll issue a refund to the cardholder.
7) *Payer Authentication Systems:* Have you ever received a call or text from your card issuer to test on a transaction you've made? which will happen when the merchant uses a payer authentication system, like 3-D Secure or Verified by Visa. These systems verify your identity at checkout by transferring data between the web merchant and your master card provider. Using settings in their payment software programmes, the provider can compare your transaction to data such as your purchasing history and device security characteristics. These allow retailers to automatically accept, reject, or flag orders supported preset criteria For instance, merchants may create rules that flag high-dollar orders placed by new customers, or orders during which the customer doesn't provide a CVV. they'll also set a max number of transactions per customer per day. These measures can help stop thieves from using stolen master card numbers

VI. CONCLUSION

A. Digital Signatures

A digital signature is a technique by which it is possible to secure electronic information in such a way that the originator of the information , as well as the integrity of the information , can be verified

B. Encryption

One of the most powerful and important methods for security in computer systems is to encrypt sensitive records and in storage

C. Security Audit

A security audit is a systematic evaluation of the security of a company information system by measuring how well it conforms to a set of established criteria

D. Cyber Forensics

Cyber forensics is a very important ingredient in the investigation of cyber crime. Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of computer system, computer networks, computer media and computer peripherals that allow investigators to solve a crime.

REFERENCES

[1] DeFilippi, D., & Michael, K. (2017). Credit Card Fraud: Behind the Scenes. 20.
[2] Hardeveld, G. J., & Webber, W. (2016, may 22). Discovering credit card fraud methods in online tutorials. OnSt '16, 1-5.
[3] Meijerink, T. J. (2013, 02 01). CARDING;crime prevention analysis. 1-49.
[4] Thomas Freyhult, M. B. (2014, APRIL 3). GRID INOVATION. Retrieved from TD WORLD: https://www.tdworld.com/grid-innovations/article/20964127/uhvdc
[5] Wifistudy (Composer). (2019). cyber crime. [a. avasthi, Performer, & unacademy, Conductor] alwar, rajastan, india.
[6] WILSON, S. (n.d.). Calling for a Uniform Approach to Card Fraud Offline and On. Journal of Internet Banking and Commerce, 1-5.
[7] Yip, M., & Webber, C. (2013, jan 13). Trust among Cybercriminals? Carding Forums, Uncertainty and. 3, 516-540.
[8] https://www.katinamichael.com/research/tag/carding
[9] https://thebusinessprofessor.com/what-is-a-cyber-crime/
[10] https://www.scribd.com/document/22465470/Hacking-in-Simple-Terms-Means-an-Illegal- Intrusion-Into-A
[11] https://www.lifelock.com/learn-identity-theft-resources-what-is-carding.html
[12] https://www.imperva.com/learn/application-security/phishing-attack-scam/