International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v8i9.5440
Article Received: 28 August 2020 Revised: 05 September 2020 Accepted: 20 September 2020 Publication: 30 September 2020

Curbing Cyber Scam (Phishing, Vishing and Spoofing) through the Use of Biometrics System for Final Authentication at the Point of Withdrawal from A Bank Account

Tew, Patricia Adaku
Computer Science Department
School of Secondary Education (SC)
Federal college of Education (T), Omoku
Rivers State.

Abstract:- Fraudulent practices carried out daily on individuals and organizations using the internet and related technologies (cybercrime) are becoming alarming. It is an act that does not seem to end any time soon. So, in order reduce the statistics, there is need to seek for possible solutions to this menace.
Phishing, vhishing, pharming and spoofing has become the mainstay of hackers ('yahoo boys') on unsuspecting bank account holders and financial institutions; who have become victims and losing their fortune/ hard earned monies to cybercrimes.
In order to safeguard bank accounts and its holders from these nefarious acts, this paper is seeking to examine and recommend ways through which financial transactions have to be fully authenticated by the account holder through the use of biometrics. There by, improving customer experiences and reducing financial fraud to a large extent. Howard Berg (2019), "Biometrics can deliver a new era in digital authentication for financial institutions."

Keywords: *Cyber scam, Biometrics, Authentication, Withdrawal and Bank accounts.*

I. INTRODUCTION

Biometrics is the measurement of physical characteristics/ body measurements using identifiers (biometric identifiers). These identifiers could be finger prints, iris recognition, facial pattern, voice recognition etc. There are two types of biometrics: physiological biometrics and behavioral biometrics.

Physiology as defined by C.-I. Fan and Y.-H. Lin (2012) is the characteristics of the body and thus it varies from person to person, including fingerprint, hand geometry, face, iris and retina recognition. Physiological biometrics is the act of using the measurements of the patterns of the finger, hand geometry, face recognition technique, iris technology, retina, palm print etc. (shape of the body) as sources of identifying an individual. In other words, Physiological biometrics is a unique identifier for every human being.

Behavioral biometrics according to A. Serwadda and V. V. Phoha (2013), is the behavioral characteristics that are related to the pattern of people doing something, such as signature, typing rhythm, gait and voice, while some other schools of thought refer to behavioral biometrics as 'behaviometrics'. Summarily, it is the use of someone's behavior to determine their identity. Going far beyond technologies like voice and signatures, behavioral biometrics can focus on anything from finger movements to hand tremors and hand-eye coordination.

"Recent research has proved that behavioral biometrics have the potential to identify a smartphone owner with high accuracy," Margarita Khartanovich *(*2019) says, and it does not need more sensors, so the cost of building any device will not increase.

II. BEHAVIORAL BIOMETRICS FOR ADAPTIVE AUTHENTICATION

Biometric authentication is the process of comparing data of someone's characteristics to the person's biometric template (stored biometric data) to determine resemblance.

The introduction of online and mobile banking has given customers a convenient way to interact with their bank as and when they please.

However, with so many consumers still feeling that there are gaps in eBanking security, it's clear that banks and other institutions involved in making payments need to optimize security without compromising on convenience before these digital services can achieve their full potential, Howard Berg (2019). Some of the security threats consumers are faced with as regards e-Banking includes but not limited to phishing, spoofing, pharming and vhishing.

Phishing attack is the act of attempting to steal sensitive information, such as passwords and credit card details (knowledge factor), by masquerading as a trustworthy entity in an electronic communication (Ramzan, 2010). According to T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer (2007), Phishing attack is typically performed

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v8i9.5440
Article Received: 28 August 2020 Revised: 05 September 2020 Accepted: 20 September 2020 Publication: 30 September 2020

through email spoofing or through instant messaging (N. Leavitt, 2005) and SMS services (A. van der Merwe, R. Seker, and A. Gerber, 2005).

It often leads users to enter personal information on a fraudulent website, which makes the user look and feel the same as the legitimate one. Although several anti-phishing technologies were revealed against these malicious behaviors, it still needs training and public awareness to make it work.

Research has it that "if Behavioral biometrics is successfully deployed, it will solve problems that other forms of cyber security have faced throughout their existence."

III. PASSWORDS, USSD CODES AND PERSONAL IDENTIFICATION

NUMBERS (PINs) VERSUS BIOMETRICS

Personal Identification Numbers (PINs) are a type of password that use only numbers while Passwords could comprise of letters, numbers and special characters.

USSD Codes are special codes that can be dialed in the case of suspecting that an account is about to be hacked, which leads to the account being frozen by the central bank until the account holder shows up in the bank to restore the account.

There have been so many outlined safety rules guiding the use of a password, USSD Code or PIN. However, if someone is able to successfully guess the PIN or password that is linked to a bank account, it can be used to commit a financial crime. Also, in the case of a USSD code, what happens if there is a financial emergency and the account holder has not being able to go to the bank physically to restore his/her account? Remember: Cyber criminals can also use the act of phishing, spoofing, vhishing etc. to get these details that are linked to a bank account.

So, in a bid to avoid these scams and inconveniences related to bank accounts, Biometrics has become the best option yet, to safeguard bank accounts.

IV. METHODOLOGY

According to a publication by Andy Renshaw (2020), he said that "Biometric Authentication is the process of comparing data for the person's characteristics to that person's biometric 'template' to determine resemblance." He further outlined

the process of using a biometric authentication as thus:

• The reference model is first stored in a database.

• The data stored in the database is then compared to the person's biometric data to be authenticated. Here, it is the person's identity that is being verified. In this mode, the question is "Are you indeed, Mr. or Mrs. XY?"

• If the response is "Yes" or "Y", the person attempting to make the withdrawal from the account is further requested to verify by inputting the biometrics stored in the system for authentication.

• Once the biometrics is verified, the transaction is completed and declared successful.

No
No
Yes
Yes
Incorrect
Correct
Enter PIN (ATM/PC)
Enter BVN/ ATM card Number and CVC
Start
Is PIN >=3
tries?
Enter Activity
(
Balance, Transfer, Withdrawal
)
Withdrawal
Enter Amount
Biometric Check
/
Authentication
Complete transaction
Print receipt
Stop

V. BIOMETRICS ALGORITHM FOR BANK WITHDRAWALS

Advantages

- It is easy and convenient to use.
- It will help in curbing/reducing financial crimes.
- It increases online security.
- It will safeguard the bank accounts of individuals and organizations even when details are given out ignorantly in the case of spoofing, vishing or phishing.
- It will reduce the amount of money lost by banks/ individuals/ organizations to cybercrimes.
- All withdrawals will be made and authorized by the account holder.

Disadvantages

- There will be no third party withdrawal in the absence of the account holder.
- Account holders cannot give ATM cards or account details to another person to make withdrawals on their behalf.
- In case of an emergency/ death, the next of kin cannot make withdrawals unless the due procedures are followed.
- If banking systems are compromised, customers will be at risk of stolen biometrics.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 8 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v8i9.5440
Article Received: 28 August 2020 Revised: 05 September 2020 Accepted: 20 September 2020 Publication: 30 September 2020

VI. CONCLUSION

In conclusion, the use of biometrics for authenticating a withdrawal from a bank account is still the best option yet, to curb financial cyber crimes.

Therefore, Banks and Ecommerce platforms should incorporate the use of biometrics to ensure a seamless transition from just PINs and passwords, to a more secured online transactions for their customers.

VII. FUTURE FRAMEWORK

I would recommend that future research should be geared towards developing the flowchart in this work into an executable and customized software, using any relevant and efficient programming language for banks in Nigeria and other countries of the world.

Furthermore, mobile Apps will be developed alongside the application software to ensure a seamless progression into the use of biometrics for the final authentication of withdrawals.

Lastly, the development of a system that will ensure the integrity of stored biometrics for a top-notch customer experience and data security.

REFERENCES

1. C.-I. Fan and Y.-H. Lin, "Full privacy minutiae-based fingerprint verification for low-computation devices," *Journal of Convergence*, vol. 3, no. 2, pp. 21–24, 2012.View at: Google Scholar
2. A. Serwadda and V. V. Phoha, "Examining a large keystroke biometrics dataset for statistical-attack openings," ACM Transactions on Information and System Security (TISSEC), vol. 16, no. 2, article 8, 2013.
3. Howard Berg (2019), Senior Vice President and Managing Director, Gemalto UK. https://www.gemalto.com/financial/inspired/behavioral-biometrics
4. Z. Ramzan, "Phishing attacks and countermeasures," in Handbook of Information and Communication Security, no. 23, pp. 433–448, Springer, Berlin, Germany, 2010.
5. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007.
6. N. Leavitt, "Instant messaging: a new target for hackers," Computer, vol. 38, no. 7, pp. 20–23, 2005.
7. A. van der Merwe, R. Seker, and A. Gerber, "Phishing in the system of systems settings: mobile technology," in Proceedings of the IEEE
8. International Conference on Systems, Man and Cybernetics, vol. 1, pp. 492– 498, October 2005.
9. Margarita Khartanovich for Binary District Journal (September, 2019) an international collaborative technology community which creates unique competency-based workshops and events on new technologies.
10. Andy Renshaw (2020), 2020 fraud trends: Are you prepared for what the future holds? Friday, 17 January, 2020