Universidade Politécnica

A Politécnica

Instituto Superior de Gestão, Ciências e Tecnologias

Licenciatura em Engenharia Informática e de Telecomunicações

Análise de Riscos de Segurança de Informação de *Internet Banking* em Sistemas Bancários Moçambicanos: Perspectiva dos Clientes

NEIDY MÁRIO CANDA

MAPUTO

2021

Universidade Politécnica

A Politécnica

Instituto Superior de Gestão, Ciências e Tecnologias

Licenciatura em Engenharia Informática e de Telecomunicações

Análise de Riscos de Segurança de Informação de *Internet Banking* em Sistemas Bancários Moçambicanos: Perspectiva dos Clientes

NEIDY MÁRIO CANDA

SUPERVISOR: MSc. GRAÇANE MUHATE

Monografia apresentada a Escola Superior de Gestão e Tecnologias – Universidade Politécnica, como parte dos requisitos para obtenção do grau de Licenciatura em Engenharia Informática e de Telecomunicações.

MAPUTO

2021

FOLHA DE APROVAÇÃO

Aos _____ de _____ de _____ a presente Monografia foi apresentada, numa defesa pública, na qual se lavrou uma Acta onde consta que a autora foi aprovada com classificação de _____ valores, feita pelos seguintes Membros de Júri:

Presidente: _____

Surpervisor: _____

Arguente: _____

PARECER DO SUPERVISOR

Tendo sido realizadas as secções de supervisão com a estudante Neidy Mário Canda, no trabalho com o tema: Análise de Riscos de Segurança de Informação de Internet Banking em Sistemas Bancários Moçambicanos: Perspetiva dos Clientes. Constatou-se, desta forma que o trabalho encontra-se em um nível correspondente as normas definidas na Universidade Politécnica no que diz respeito a trabalhos de monografia científica.

Durante as secções de supervisão a aluna mostrou-se bastante proactiva e com um nível de profissionalismo e integridade na elaboração das diversas tarefas indicadas por mim como supervisor, de forma que sua performance pode ser considerada excelente. Em relação ao desenvolvimento das atividades propostas pelo orientador e cumprimento do plano de trabalho deve-se ressaltar que a aluna mostrou-se bastante motivada com a pesquisa.

Sendo assim afirmo que o trabalho reúne os requisitos para a submissão a comissão científica para candidatura a defesa para obtenção do grau de Licenciatura.

Maputo, Junho de 2021

_____

(MSc. Graçane Xavier Muhate)

DECLARAÇÃO DE HONRA

Eu, Neidy Mário Canda, nascida a 4 de Fevereiro de 2000, no Hospital de Chamanculo, filha de Mário Armando e Gracinda Zacarias Vilanculos, discente da Universidade Politécnica, do curso de Engenharia Informática e de Telecomunicações, declaro por minha honra que este trabalho nunca foi apresentado, parcial ou integralmente em nenhuma instituição de ensino para obtenção de qualquer grau académico e que constitui o resultado da minha investigação pessoal e orientações do meu supervisor, estando indicadas no texto e nas referências bibliográficas as fontes utilizadas.

Maputo, Junho de 2021

_____

(Neidy Mário Canda)

AGRADECIMENTOS

Em primeiro lugar, agradeço à Deus, pelo dom da vida e por ter-me acompanhado durante os 4 anos da minha formação e em particular durante todo o processo da realização deste trabalho.

Aos meus pais, Mário Armando e Gracinda Vilanculos, e ao meu irmão Mário Armando Júnior, vai o meu muito obrigado pelas palavras de incentivo, pelo apoio e compreensão durante toda minha vida e principalmente durante o meu percurso académico.

Agradeço ao meu tutor, o professor Graçane Muhate, pela atenção e disponibilidade que sempre manifestou na orientação deste trabalho.

As minhas colegas e amigas Marlen Cumbane e Neila Mabombo pelas longas horas de sessões de estudo e pelos conselhos.

A Universidade Politécnica e ao corpo docente que tornou a minha formação possível.

Agradeço a minha família e a todos aqueles que contribuíram para que este trabalho se tornasse uma realidade, directa ou indirectamente.

EPÍGRAFE

“A ciência de hoje é a tecnologia de amanhã.”

(Edward Teller)

RESUMO

A introdução do canal digital *internet banking* trouxe inúmeras vantagens às instituições bancárias e aos seus clientes. Para os clientes, veio a comodidade de realizar as suas operações bancárias sem a necessidade de deslocar-se ao seu balcão mais próximo ou a uma ATM, podendo fazê-las em suas casas ou postos de trabalho. Para os bancos veio a redução do custo operacional pois agora contam com um único portal que oferece diversos serviços aos clientes. Mesmo com grandes vantagens, o canal está sujeito a riscos de ataques cibernéticos. Contudo, ao longo do tempo, os responsáveis por cometer este tipos de ataques, os *hackers*, verificaram que ao invés de gastar longas horas em tentar invadir sistemas de grandes instituições bancárias é muito mais fácil focar-se onde há menos resistência, aplicando técnicas de engenharia social (*phishing* e *pharming*) aos clientes destas instituições. O presente trabalho foca-se em propor medidas de protecção às instituições bancárias que operam em Moçambique, de forma que as mesmas possam amenizar os riscos de ocorrência de ataques desta natureza. O tipo de pesquisa adoptada é exploratório, tendo como instrumentos um questionário *online*, com perguntas de sim/não simples e clara, consulta bibliográfica. O questionário foi enviado a 75 utentes de internet banking de instituições bancárias que operam em Moçambique com o objetivo de verificar quais as práticas de segurança que o mesmo adopta ao usar internet banking e qual a percepção dos mesmos no que concerne às ameaças de segurança de internet banking, mas apenas 50 responderam. Diante dos resultados obtidos foi possível constatar que os utentes estão ainda mais propensos a serem vítimas de ataques de engenharia social pois os mesmos não têm conhecimento dos mesmos e porque os mesmos não seguem algumas práticas de segurança que devem ser cumpridas de forma a ter um ambiente de internet banking seguro. As medidas de protecção propostas neste trabalho foram traçadas conforme as disparidades encontradas entre as expectativas das instituições bancárias que operam em Moçambique e a resposta comportamental de seus clientes, quando se trata do *internet banking.*

Palavras – Chave: *Internet Banking*, Engenharia Social, *Phishing*, *Pharming*, Medidas de Protecção

ABSTRACT

The introduction of the digital channel Internet Banking has brought numerous advantages to banking institutions and their customers. For costumers, came the convenience of carrying out their banking operations without the need to go to their nearest bank or an ATM, they can do it at their homes or work. For banks, came the reduction in operational cost, as they now have a single portal that offers different services to customers. Even with great advantages, this channel is prone to risks of cyber-attacks. However, over time, those responsible for committing these types of attacks, the hackers, have found that instead of spending long hours trying to break into systems of large banking institutions, it is much easier to focus where there is less resistance, applying social engineering techniques (phishing and pharming) to the clients of the banking institutions. This paper focuses on proposing protection measures to banking institutions operating in Mozambique, so that they can mitigate the risks of attacks of this nature. The type of research adopted is exploratory, using as instruments an online questionnaire, with simple and clear yes / no questions, bibliographic consultation. The questionnaire was sent to 75 internet banking users from banking institutions operating in Mozambique with the aim of verifying which security practices they adopt when using internet banking and their awareness of internet security threats. banking, but only 50 responded. In the results obtained, it was possible to verify that users are even more likely to be victims of social engineering attacks because they are unaware of them and because they do not follow certain safety practices that must be complied in order to have a secure internet banking environment. The protection measures proposed in this paper were designed according to disparities found between the expectations of banking institutions operating in Mozambique and the behavioral response of their customers, when it comes to internet banking.

Keywords: *Internet Banking, Social Engineering, Phishing, Pharming, Protection Measures.*

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

LISTA DE SIGLAS E ABREVIATURAS

ATM	Automated Teller Machine
BCI	Banco Comercial e de Investimentos
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP/HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
IA	Inteligência Artificial
OTP	One Time Password
PIN	Personal Identification Number
POS	Point of Sale
SMS	Short Message Service
SSL/TLS	Service Sockets Layer/Transport Layer Security
URL	Uniform Resource Locator

CAPÍTULO I: INTRODUÇÃO

As tecnologias de informação e comunicação têm passado por uma rápida evolução ao longo dos anos, tendo assim transformado a forma como as interacções sociais e empresariais são conduzidas. O advento do *E-business*, (Negócio Electrónico do *inglês Electronic Business*, que é definido como o uso da internet para conectar organizações e potenciar os processos de negócios das mesmas[1]) acompanhado de inovações de tecnologias de informação e comunicação e da globalização, tem constantemente impulsionado organizações a redefinir suas operações de negócio em termos de reengenharia e reestruturação de modelos de negócio. Várias organizações investiram nesta área de forma a apostar em novas soluções tecnológicas, que ofereçam vantagens para os seus negócios.

O sector bancário possui características próprias que o apontam como um dos que mais utiliza tecnologias de informação como um recurso inovador para alcançar velocidade, eficiência, redução de custos, atendimento ao cliente e vantagem competitiva (JOSHUA; KOSHY, 2011, p. 2). Esta transição das operações de negócios pelos bancos criou um novo modo de operação denominado *E-Banking*. *Internet Banking*, também conhecido como banco electrónico (*E-Banking*), Banco Online e Banco Virtual, é amplamente promovido como uma solução bancária conveniente (ALGHAZO et al., 2017, p. 2). É uma infra-estrutura de tecnologia de informação que as instituições bancárias usam actualmente além de outros canais também conhecidos como *Mobile Banking*.

Reis (2018, p. 11), citando Tjøstheim e Moen (2005), caracteriza *Intenet Banking* como um processo inovador por proporcionar aos utentes, a possibilidade de controlo de suas contas bancárias, sem necessidade de ir à algum posto de atendimento. Este serviço envolve clientes particulares e corporativos (empresas) e inclui transferências bancárias, pagamentos, empréstimos corporativos e domésticos entre outros (MIA et. al, 2007, p. 37 citando UNCTAD, 2002). Desta forma, os utentes podem visitar ambientes virtuais dos bancos via web, o que possibilita aos mesmos mais fácil e rápido acesso as suas informações bancárias, bem como agilidade e comodidade nas transacções financeiras.

[1] (ROMÃO, 2010, p. 19)

Em Moçambique maior parte dos bancos, migrou rapidamente para esta tecnologia/serviço a fim de reduzir custos e melhorar a experiência do cliente, e nos dias de hoje com a pandemia do Covid-19, a tendência é de procurar meios que evitem a saída dos utentes para fazer tarefas simples como pagamentos ou depósitos para desta forma, evitar aglomerações.

Dado que, novas ameaças surgem continuamente, os bancos precisam adoptar medidas para proteger os seus utentes e a si próprio. Actualmente, os *hackers* dedicam-se em explorar as vulnerabilidade de pessoas, por meio de técnicas de engenharia social (*phishing* & *pharming)* do que gastar tempo e dinheiro em invadir sistemas. Este trabalho foca-se em propor medidas de protecção de forma a eliminar o risco de ocorrência de ataques usando estas técnicas.

O trabalho foi dividido em 6 capítulos:

O primeiro de carácter introdutório, onde é apresentado a definição do problema, a motivação e justificativa do trabalho, os objectivos, as questões de pesquisa, e por fim as hipóteses.

No segundo capítulo é feita uma abordagem literária sobre o *internet banking*, as vantagens e riscos que esta inovação tecnológica trouxe ao sector bancário.

No terceiro capítulo, é feita a descrição dos principais métodos e técnicas empregues na pesquisa de forma a alcançar os objectivos da mesma.

No quarto capítulo é feita a apresentação dos resultados obtidos com o questionário.

No quinto capítulo é feita uma comparação dos resultados obtidos no questionário com o que o banco espera do cliente, de acordo com as informações providas pelos mesmos em seus *websites*.

Por fim, no sexto capítulo são apresentadas as principais conclusões, limitações e recomendações da pesquisa em questão.

1.1. Descrição do Problema

Com a introdução do canal digital *internet banking*, tornou-se necessária a implementação de recursos que garantissem um ambiente seguro, de forma que os clientes pudessem efectuar as suas operações bancárias. Alguns dos recursos adoptados pelos bancos que operam em Moçambique incluem o protocolo SSL/TLS (*Secure Sockets Layer* & *Transport Layer Security*), que garante a protecção de informações sensíveis como senhas ou números de cartões de crédito, quando enviadas para o site do banco; *Firewalls*, que impedem o acesso não autorizado e interrompe o tráfego de fontes não seguras da internet; Código de autorização para operações transaccionais; Tempo limite automático, permite que o sistema desconecte da janela de transacção caso não haja nenhuma actividade dentro de 15 minutos, e entre outros recursos. Mas, porque a manutenção de um ambiente de *internet banking* seguro não depende só dos bancos, algumas instituições bancárias alertam sobre o papel do cliente na protecção de seus dados, listando um conjunto de medidas que devem ser cumpridas pelos seus clientes, alertando-os principalmente sobre pessoas que se fazem passar por entidades bancárias para obter os seus dados e *spywares* que podem ser instalados no computador do usuário sem a sua autorização, com a intenção de gravar as teclas pressionadas no teclado ao fazer login no *internet banking*, isto se os mesmos não fizerem o uso de *anti-spywares*.

Porém, mesmo com estes critérios, a política de segurança dos sistemas bancários, é comprometida pelos seus clientes, isto porque os mesmos, muitas vezes falham em seguir as práticas de segurança listadas nos *websites* de alguns bancos que fornecem *internet banking*. Estas falhas podem resultar em sérios riscos de segurança como o roubo de credencias bancárias para fins ilícitos. Só em 2014, foi noticiado a apreensão de cerca de 14 milhões de meticais através de crimes cibernéticos cometidos por grupos que clonavam cartões e exigiam informações das contas bancárias das vítimas, fazendo-se passar por funcionários de instituições bancárias (DIÁRIO DE NOTÍCIAS, 2018).

Sendo assim, a questão que aqui se coloca é: como é que as instituições bancárias que operam em Moçambique podem amenizar os riscos de segurança em ambiente de *Internet Banking*, que ocorrem por negligência ou falta de conhecimento por parte de seus clientes.

1.2.Motivação e Justificativa

A difusão do Internet Banking mudou significativamente a interação dos utentes com o sistema bancário, mas com todo esse crescimento vêm os riscos, pois bem se sabe que o sector financeiro é listado entre os 3 maiores alvos dos ataques cibernéticos (Verizon, 2016). Alguns dos riscos associados aos usuários do Internet Banking são os próprios usuários; o seu comportamento quando se trata do e-banking, por exemplo a compartilha de credenciais de login por parte do utente com outras pessoas consciente ou inconscientemente. Isto pode levar ao comprometimento da conta do utente e pode levar a violações de segurança. Sendo assim, a motivação por detrás da escolha desde tema, deve-se ao facto de haver cada vez mais necessidade de estudos que possam ajudar a aperfeiçoar os mecanismos de forma a garantir a segurança das informações, tanto dos utentes do Internet Banking, tanto da Instituição Bancária que o fornece.

1.3.Objectivos

Geral

O objectivo deste estudo é propor um conjunto de medidas que visam colocar mais responsabilidade em instituições bancárias que operam em Moçambique, de forma a mitigar os riscos de segurança que ocorrem devido a falta de conhecimento ou por negligência de seus clientes.

Específicos

- Analisar quais as práticas de segurança que os utentes de *internet banking* adoptam, perante o uso de serviços do *internet banking* e a percepção dos mesmos no que concerne às ameaças de segurança do *internet banking*;
- Avaliar o nível de informação provido pelas instituições bancárias que operam em Moçambique em seus *websites*, sobre os riscos de segurança e as práticas de segurança que os clientes devem seguir ao usar *internet banking*;
- Identificar as lacunas que existem entre as expectativas das instituições bancárias que operam em Moçambique e a resposta comportamental de seus clientes, quando se trata do *internet banking*;

- Explicar quais as medidas que as instituições bancárias que operam em Moçambique podem adoptar, de forma a eliminar as lacunas que existem entre as suas expectativas e a resposta comportamental de seus clientes, quando se trata do *internet banking*.

1.4. Questões de Pesquisa

Para alcançar o objectivo deste estudo, são formuladas as seguintes questões:

- Os clientes de serviços de *internet banking* estão cientes das ameaças que abrangem *internet banking*?
- Que medidas de protecção, o cliente adopta quando faz o uso de *internet banking*?
- Quais as informações que as instituições bancárias que operam em Moçambique disponibilizam aos seus clientes em seus *websites* acerca dos riscos de segurança e práticas de segurança que os clientes devem seguir ao usar *internet banking*?
- Quais as lacunas que foram identificadas entre as expectativas das instituições bancárias que operam em Moçambique e a resposta comportamental de seus clientes, quando se trata do *internet banking*?
- Que abordagem deve ser adoptada pelas instituições bancárias que operam em Moçambique, de forma a suprir os riscos de segurança do internet *banking* que ocorrem devido a falta de conhecimento ou por negligência de seus clientes?

1.5.Hipóteses

H0: As medidas de protecção propostas não poderão ajudar as instituições bancárias que operam em Moçambique a mitigar os riscos de segurança cibernética do *internet banking* causadas pela falta de conhecimento ou negligência de seus clientes.

H1: As medidas de protecção propostas poderão ajudar as instituições bancárias que operam em Moçambique a mitigar os riscos de segurança cibernética do *internet banking* causadas pela falta de conhecimento ou negligência de seus clientes.

CAPÍTULO II: FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são discutidos conceitos que permitem explicar melhor o problema, sendo o primeiro a inovação tecnológica, de forma a enfatizar como a introdução de novas tecnologias de informação e comunicação mudaram a forma como as instituições bancárias entregam serviços aos seus clientes, os riscos de segurança que esta inovação trouxe, e quais os mecanismos de prevenção que os bancos adoptam para mitigar estes riscos.

2.1.Inovação Tecnológica

Rodrigues, et al. (2016, p. 2) afirmam que o factor chave para o sucesso de uma organização é entregar aos seus consumidores, produtos e serviços com maior valor agregado possível (performance/preço), atendendo assim as suas necessidades em menor tempo e melhor que a concorrência. Sendo assim inovações tecnológicas podem ser entendidas como a introdução no mercado de produtos, serviços, processos novos ou significativamente melhorados.

Em um contexto de globalização e competição em que as organizações estão inseridas, a utilização inadequada dos recursos tecnológicos ou a sua não utilização, podem representar uma ameaça à sobrevivência das empresas. Diante deste facto, observa-se que as empresas que não se adequarem ao mercado, buscando inovação e tecnologia, tornar-se-ão obsoletas e sem condições de serem competitivas (Rodrigues et al. 2016, p. 3 citando Davis et al. 2001).

Com o surgimento e popularização da internet, para além do rápido desenvolvimento das tecnologias de informação, criou-se um ambiente favorável para ocorrência de mudanças radicais em instituições bancárias (TIVANE, 2015, p. 18). A indústria bancária que opera hoje no mercado moçambicano é totalmente diferente de algumas décadas atrás. Hoje, já existem plataformas que permitem realizar diversas operações, desde consulta de saldo, transferências etc. sem que o cliente dirija-se a uma agência bancária.

Tivane (2015, p. 2) advoga que o processo de inovação tecnológica em instituições bancárias, é directamente influenciado pelo desenvolvimento e pela introdução de tecnologias de informação e comunicação, dando assim origem as novas formas de disponibilizar produtos e serviços bancários, através de diversas infra-estruturas da banca electrónica.

Na banca moçambicana, estão disponíveis várias infra-estrutuuras da banca electrónica como ATM (*Automated Teller Machine*), *Internet Banking*, POS (*Point of Sale*), *Mobile Banking*, entre outros. Sendo que o foco deste estudo é o *internet banking*, tem-se abaixo uma explicação detalhada sobre o mesmo.

2.2.Internet Banking

Al-Weshah (2013, p. 3) citando Hertzum et al. (2004), define *internet banking* como "banco baseado na web". Em outras palavras, o *internet banking* refere-se às operações bancárias que são feitas pela *World Wide Web*, ou seja, implementação de serviços bancários na internet. Estes serviços incluem transferências bancárias, pagamentos, cobranças entre outros.

Internet banking, permite que o utilizador faça a gestão da sua conta bancária e execute transacções financeiras na internet, ao invés de recorrer ao caixa no balcão ou ao telefone para realizar as operações (TIVANE, 2015, p. 25).

No entendimento de Tivane (2015, p. 25), para que um banco ofereça *internet banking*, necessita de um servidor (que pode ser próprio ou de terceiros), um endereço electrónico que indica a localização do website no servidor, links e protocolos de segurança.

Internet Banking, é um serviço fornecido pelas instituições bancárias através de um navegador *web* que pode ser acessado usando um computador, *smartphones* ou *tablets*. Para tal, o cliente deve possuir um código de utilizador, um código de acesso e um código de autorização para poder realizar as operações bancárias (TIVANE, 2015, p. 41). As operações disponibilizadas pelas instituições bancárias que operam em Moçambique, atráves do internet banking incluem:

- Consultas de saldo, movimentos de conta, extractos de conta;
- Transferências intra e interbancárias;
- Compra de recargas (Mcel, Vodacom, Movitel, Credelec);
- Pagamento de serviços (Água, Luz, Propinas, Pacotes de TV – DStv, GOtv, Startimes, TV Cabo, ZAP);
- Alteração de credencias.

Para poder realizar operações de consulta, o cliente deve possuir um código do utilizador, e um código de acesso e para realizar operações como transferências, compras ou pagamentos, o cliente deve fornecer um código adicional, o código de autorização. O código de autorização é uma OTP (*One Time Password*) que é enviada para o telemóvel do cliente para cada operação bancária que o cliente efectuar (TIVANE, 2015, p. 42). Alguns bancos disponibilizam um *Token*, que é um dispositivo electrónico responsável por gerar OTPs para cada operação que o cliente faz.

2.3.Segurança de Informação

A informação constitui uma peça fundamental não só no sector financeiro, na descoberta e introdução de novas tecnologias. Esta compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano, ou seja, trata-se de tudo aquilo que permite aquisição de conhecimento (CARMO, 2013, p. 9).

A Segurança da Informação é definida como um conjunto de medidas que se constituem basicamente de controlos e políticas de segurança, tendo como objectivo a protecção das informações dos clientes e da empresa (ativos/bens), controlando o risco de revelação ou alteração por pessoas não autorizadas.

Para Carmo (2013, p. 10):

> A segurança da informação consiste em garantir que a informação existente em qualquer formato esteja protegida contra o acesso por pessoas não autorizadas (confidencialidade), esteja sempre disponível quando necessária (disponibilidade), confiável (integridade) e autêntica (autenticidade).

Sendo assim, a segurança de informação baseia-se em três aspectos, que visam assegurar a confidencialidade, integridade e disponibilidade. A internet agregou a esta tríade os conceitos de privacidade, não-repúdio e autenticidade (ADACHI, 2004, p. 18 citando CAMP, 2000).

A confidencialidade defende a prevenção contra o uso não autorizado da informação e busca evitar a quebra de sigilo de dados; a integridade busca evitar a alteração ou modificação de informações a usuários não autorizadas e a disponibilidade refere-se a manter a informação disponível para os usuários, quando estes necessitam da mesma.

A segurança de informação gira em torno destes três princípios sendo imperioso que instituições bancárias ou qualquer outra organização que trabalha com informações sensíveis, adopte mecanismos de segurança que satisfaçam esta tríade, e assim, preservar os dados de seus clientes e até mesmo de seus funcionários.

2.4.Riscos de Segurança Informação associados ao *Internet Banking*

Um dos marcos do avanço tecnológico foi o surgimento da *internet*, o que ocasionou em transformações drásticas, mas favoráveis no modo como as organizações operam. O ponto vulnerável desta evolução, é que a partir do momento em que as organizações se integram em redes de computadores e a sociedade se comunica por meio da *Web* e de *e-mails*, elas expõem as suas fragilidades de segurança das informações e do patrimônio vivendo em um ambiente de risco (ADACHI, 2004, p. 15 citando GARFINKEL; SPAFFORD, 1997).

Foi descrito no ponto anterior que a segurança de informação visa assegurar a confidencialidade, integridade e a disponibilidade. Mas os mecanismos de segurança usados para cumprir com estes princípios não tem-se mostrado suficiente, pois, há cada vez mais indivíduos que procuram forcar-se em manipular a confiança de outra pessoa a fim de obter acesso à suas informações privadas (SILVEIRA et al., 2017, p. 2). Esta técnica é chamada de Engenharia Social. Abaixo é feita uma descrição detalhada sobre o assunto.

2.4.1.Engenharia Social

A segurança do *internet banking* pode ser comprometida pelos próprios usuários, isto porque os mesmos não possuem conhecimento acerca dos golpes que acontecem na rede acabam por disponibilizar informações privadas e relevantes, para golpistas, conhecidos como engenheiros sociais.

Para Costa (2018, p. 36) citando Hadnagy (2016):

> A engenharia social pode ser definida a partir do significado de dois termos: engenharia e social. Entende-se "engenharia" como uma ciência que visa aplicar conhecimentos técnicos às questões cotidianas; e "social" inclui a capacidade de relacionamento dos indivíduos dentro de um grupo.

Sendo assim, a pessoa que executa a técnica de engenharia social, o engenheiro social aproveita-se das informações que já possui, aplica seus conhecimentos técnicos na qual, com antecedência, prevê como as pessoas irão se comportar diante de tal situação, fazendo então, com que chegue ao seu objetivo final: obter dados para o seu privilégio (COSTA, 2018, p. 35).

A Engenharia Social é um conjunto de técnicas e habilidades utilizadas para induzir as pessoas a revelarem dados confidenciais, que se tornam informações úteis para o fraudador (COSTA, 2018, p. 35 citando WHITMAN; MATTORD, 2012). Este tipo de ataque representa um maior risco para as instituições bancárias, pois trabalha com o comportamento das pessoas, utentes dos serviços de *internet banking*. Com a popularização do acesso à internet, os chamados engenheiros sociais procuram explorar desejos de ganhar prémios e a curiosidade dos usuários, para dissimular acções de ataque (POUCHAIN, 2007, p. 101).

De acordo com Lord (2020), ataques de engenharia social normalmente envolvem alguma forma de manipulação psicológica, enganando utilizadores para entregar dados confidenciais ou sensíveis. O mesmo autor advoga que apenas cerca de 3% dos *malwares* são lançados com o objetivo de explorar uma falha técnica, os outros 97% estão tentando enganar um usuário através de algum tipo de esquema, que leva a uma exposição indevida de informações pessoais.

As camadas de segurança implementadas no ambiente de *internet banking* das instituições bancárias proporcionam um nível confortável de exposição ao risco de invasão, levando aos atacantes a investirem no elo mais fraco do sistema, os usuários.

Geralmente, a engenharia social envolve e-mails ou outra comunicação que invoca a urgência, o medo ou emoções semelhantes nos usuários, levando-os a revelar prontamente informações sensíveis, clicar num *link* malicioso ou abrir um ficheiro malicioso. Porque a engenharia social envolve um elemento humano, prevenir estes ataques pode ser complicado para as empresas (LORD, 2020).

De acordo com Lau (2006, p. 44), são muitos os factores ou técnicas de persuasão ou manipulação usados pelos engenheiros sociais em ambientes de *internet banking*, sendo o que mais se destaca o factor autoridade. Este é usado em casos onde as vítimas recebem *e-mails* em nome de instituições muito bem conhecidas, sejam elas públicas ou privadas. O conteúdo destes emails apresenta um assunto pendente entre a vítima e a instituição, e a partir deste a vítima sente-se coagida a resolver o assunto pendente levando a clicar em um *link* malicioso presente no *e-mail* por exemplo. Os outros factores incluem a oferta de um produto muito procurado e de uma quantia que não convém com a posição financeira da vítima, obrigando os interessados a ceder na aquisição do mesmo sem desconfiar da proveniência do tal produto.

Existem várias técnicas que são usadas pelos engenheiros sociais, mas neste estudo serão abordadas somente duas.

2.4.1.1.Técnicas usadas pelos Engenheiros Sociais

Existem diversos meios e técnicas realizadas sobre clientes bancários, usuários de *internet banking*, e estes baseiam-se em ataques como *phishing* e *pharming*.

Na primeira, o "*phisher*" envia e-mails com conteúdo fraudulento às vítimas sem a solicitação ou consentimento das mesmas fazendo-se passar pelas instituições bancárias aderidas pelas vítimas. No segundo, a vítima é redirecionada a uma página web ilegítima, similar à páginas web de instituições bancárias aderidas pelas vítimas.

De forma a ter uma melhor compreensão dos termos citados, tem-se abaixo uma descrição detalhada destas técnicas.

2.4.1.1.1.Phishing

Phishing é uma forma de ataque de engenharia social que envolve a obtenção de informações pessoais como senhas de acesso bancário, por meio de *e-mails* que aparentam ser de origem de bancos (Factor autoridade, visto acima), mas que provém de golpistas.

Esta técnica envolve o envio de *e-mails* que geralmente indicam que a vítima deve fornecer atenção imediata, convidando-os a acessar a páginas *web* fraudulentas. O termo *phishing* é um homófono para *fishing* – no sentido de que a vítima é o peixe que mordeu a isca. A chave para o *phishing* é atrair usuários para visitar um *website* falso, que pode ser efectivamente alcançado por meio de um *e-mail* falso.

No mundo em que se vive hoje, em que tudo é divulgado em redes sociais, a segurança das credenciais pessoais é colocada em risco. Vayansky e Kumar (2018, p. 15) consideram *phishing* como uma das formas mais antigas e fáceis de roubar informação de pessoas e é usado para obter uma ampla gama de detalhes pessoais. Explorando o conhecimento limitado das pessoas, os *phishers* enganam os usuários *online* para que divulguem informações sensíveis (ALEROUD; ZHOU, 2017, p. 161).

Segundo Lau (2006, p. 62), classificam-se como phishing, *e-mails* que apresentam as seguintes características:

- Conteúdo da mensagem contém uma marca comercial forjada;
- Contém endereços de *e-mail* e *links* forjados;
- Busca representar uma instituição de comércio electrónico ou financeiro;
- O golpe busca atingir a vítima, colectando informações digitados em formulários existentes no *email* ou uma página *web*, resultante do *link* forjado no *email*.

Figura 1: Exemplo de *e-mail phishing*

Fonte: Webpage1 (2021)

Figura 2: Exemplo de *e-mail phishing*

Fonte: Webpage1 (2021)

Figura 3: Exemplo de *e-mail phishing*

Fonte: Webpage1 (2021)

Em alguns *e-mails phishing*, os golpistas pedem as vítimas que abram um anexo em formatos ".exe, .pdf, .doc, .js "etc. indicando no texto do *e-mail* algo como "Por favor, confirme os detalhes da sua conta", ou "Confirme as suas informações de pagamento".

Alguns podem até pedir que as vítimas façam *downloads* de aplicativos, alegando ser uma nova actualização do banco, como mostra a figura abaixo.

Figura 4: Exemplo de phishing

Fonte: Webpage2 (2021)

Ao abrir qualquer um destes anexos ou baixar aplicações como na figura acima, o cliente coloca a sua máquina (*laptop, smartphone* ou *tablet*) em um ambiente vulnerável, pois os anexos podem conter programas maliciosos que registam as actividades da máquina infectada e enviam para máquina do golpista, mais conhecidos como *spywares*.

De acordo com Elisan (2013, p. 34) *spyware* é um software que colecta informações sem o conhecimento da vítima. O mesmo ainda advoga que, mesmo que o uso de um *spyware* claramente viole a privacidade da vítima, ele pode ser usado, por exemplo, por um pai que deseja para monitorar a atividade de uma criança enquanto esta faz o uso de um computador.

Porém, estes são mais usados para colectar dados sensíveis como PINs, números de conta, números de cartões de crédito etc.

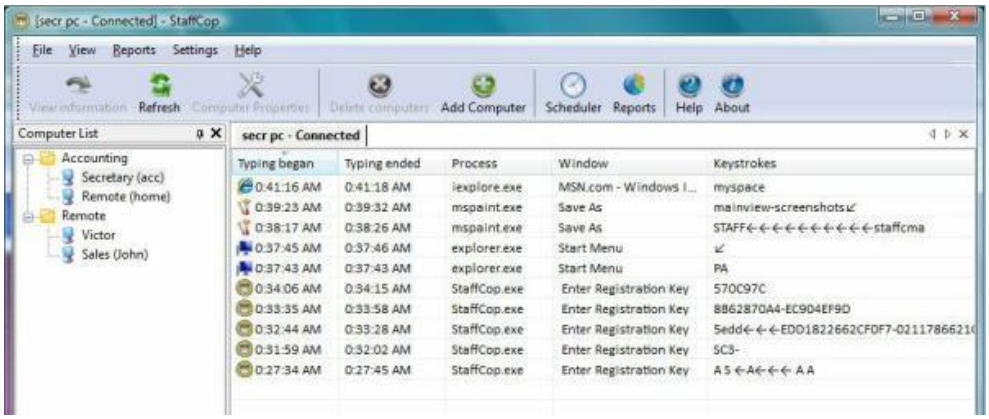
Segundo Pounchain (2007, p. 89), os *spywares* podem ser classificados nos seguintes tipos de ataques, directamente relacionados ao ambiente *internet banking*:

Keyloggers: Programas que capturam dados digitados pelo usuário, durante a execução de transações bancárias e de seguida enviam a lista de informações para o endereço do golpista. Actualmente, maior parte das instituições bancárias moçambicanas implementaram a tecnologia de teclado virtual, como forma de impedir este ataque.

Mouseloggers: Estes foram criados como forma de contornar os teclados virtuais, ou seja, a cada clique do *mouse*, o programa captura a imagem sob o cursor, sendo assim, os golpistas conseguem determinar a sequência de imagens para cada clique que usuário efectua.

Screenloggers: Estes também agem por meio de captura de telas, vigiando e monitorando as acções do cliente, quando este acessa a página *web* do banco. Porém, é independente de teclados e cliques do *mouse*.

Figura 5: Exemplo de relatório de um *keylogger*



Fonte: Webpage3 (2021)

Em um ataque *phishing* mais elaborado, o "*phisher*" cria um *website* muito semelhante ao legítimo, usando os mesmos logotipos, imagens, estruturas, etc. No entanto, se a vítima examinar atentamente o URL (Uniform Resource Locator) exibido na barra do navegador *web*, nota que o URL (especialmente o nome de domínio) não é o usual (GASTELLIER-PREVOST et al., 2011, p. 1).

De acordo com Dunham (2008, p. 125), a primeira coisa que o *phisher* faz ao criar um ataque phishing é criar uma cópia do *website* legítimo que ele tem como alvo. Geralmente estes usam um aplicativo de recuperação de conteúdo capaz de realizar uma cópia completa do website em apenas alguns minutos. O *wget* é um exemplo de aplicativos desta natureza, ou seja, ele efectua a recuperação de conteúdo e arquivos livre usando HTTP, HTTPS, e FTP. É suportado em sistemas operativos como o UNIX, Windows, Mac OS X, etc. Supondo que o atacante queira imitar o site www.meubanco.com por exemplo, tudo o que ele tem de fazer é executar wget www.meubanco.com e uma cópia completa do http://meubanco.com é baixada instantaneamente.

Em alguns casos, os atacantes são mais descuidados, fazem apenas a captura do ecrã do *website* legítimo, e o resultado é que algumas partes do website não têm funcionalidade. O exemplo abaixo mostra uma página *web* do BCI (Banco Comercial e de Investimentos) em que o rodapé contém um carrossel sem funcionalidade. Em sua página oficial, as imagens mudam em intervalos de tempo, o que não é possível verificar. Estes são pequenos detalhes muitos importantes e é necessário que o cliente tenha especial atenção.

Figura 6: Exemplo de *phishing*

Fonte: Webpage1 (2021)

Outras ameaças emergentes no ambiente móvel, variantes do *phishing* são o *smishing* e o *vishing*. O *smishing* que deriva da expressão SMS (Short Message Service) *phishing* é uma técnica de phishing em que o atacante tenta obter informações da vítima por meio de uma SMS e no *vishing*, que deriva da combinação de *voice* e *phishing* o atacante tenta fazer com que a vítima partilhe informações por meio de uma chamada de voz. Estes têm-se tornado muito comum em Moçambique. Visto que em muitas instituições bancárias as notificações de transacções são enviadas por SMS, os golpistas aproveitam-se disso para confundir os clientes. Os usuários do serviço M-Pesa por exemplo, por vezes recebem chamadas ou SMSs pedindo-os que devolvam uma quantia de dinheiro enviada por engano.

2.4.1.1.2.Pharming

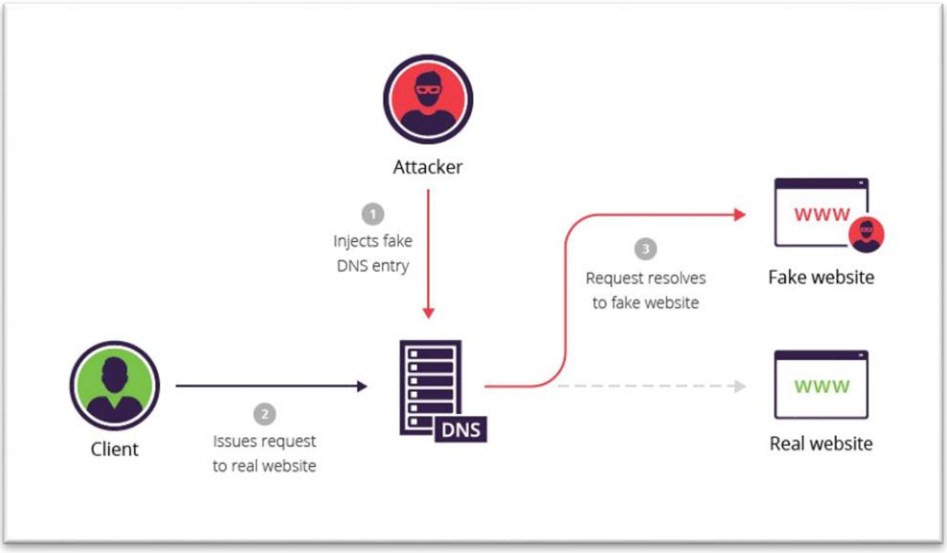
Pharming é uma técnica mais sofisticada e mais difícil de detectar, pois este redirecciona a vítima a páginas *web* falsas sem que a mesma aceda *links* contidos em *e-mails* como foi visto no *phishing*, ou seja, ao invés de depender totalmente dos usuários acederem a um *link* em *e-mails* falsos, o "*pharmer*" redirecciona as vítimas mesmo se digitarem o endereço correcto de seu banco.

O ataque mais comum e considerado mais perigoso é o DNS (*Domain Name System*) *poisoning*.

A tarefa do DNS é de traduzir nomes de domínio em endereços IP (*Internet Protocol*), que representam a localização real do *site*, permitindo assim que o navegador de *internet* conecte-se ao servidor no qual o site está hospedado. Esta técnica foi introduzida com o intuito de relacionar os nomes de domínio com o endereço IP. Para os humanos, seria muito complicado lembrar o endereço IP de um site a cada vez que pretende acessá-lo e os computadores não sabem interpretar nomes com o código alfabético, no entanto, o sistema DNS compreende e processa ambos. Quando um cliente digita, por exemplo www.qualquerbanco.com em seu navegador, os servidores DNS o traduzem para um endereço IP como 192.168.0.25 por exemplo, que fornece instruções de roteamento. Depois do servidor DNS fornecer informações do endereço, a solicitação de conexão do usuário é encaminhada para www.qualquerbanco.com. Os servidores DNS locais podem ser "envenenados" para enviar os clientes a um site diferente do solicitado. Este envenenamento pode ocorrer como resultado de configuração incorrecta, vulnerabilidades de rede ou um *malware* instalado no servidor.

Abaixo consta um exemplo de como funciona um ataque *pharming.*

Figura 7: Funcionamento de um ataque DNS *Poisoning*



Fonte: CISAR, PINTER (2019, p. 136)

De uma forma geral, o DNS *poisoning* envolve explorar vulnerabilidades em um servidor DNS e "envenenar" as entradas da tabela do servidor DNS com informações falsas. Estas informações podem ser um endereço IP falso na entrada da tabela – sendo assim, quando o cliente o URL correcto no motor de busca, este é direccionado para um endereço IP incorrecto Uma das razões pelas quais este tipo de *pharming* é considerado perigoso é porque este pode se espalhar para vários servidores DNS.

2.5.Mecanismos de Segurança Adoptados pelos Bancos

De forma a garantir a privacidade, confidencialidade e integridade das informações que são trocadas, divulgadas, compartilhadas, armazenadas ou usadas nos sistemas bancários, os bancos implementaram mecanismos de autenticação, criptografia e auditoria que servem de barreiras contra ataques à rede dos mesmos. Estes mecanismos incluem:

- **SMS *Token*:** Um código é enviado para o telemóvel do cliente sempre que efectuar uma transacção. Tem o objectivo de garantir que a operação está a ser executada pelo titular da conta. O código é uma OTP, ou seja, só pode ser usado naquela operação.
- ***Smart Card* & Leitor de Cartões:** O *smart card* é um elemento de autorização de transações. O leitor de cartões é um dispositivo onde é inserido o *smart card* de forma a gerar uma OTP. Quando inserido o *smart card*, o leitor de cartões pede um PIN e só depois de validar fornece uma OTP ao cliente, que é válida para uma só operação.
- **Teclado Virtual:** Tecnologia desenvolvida com o intuito de impedir que programas maliciosos capturem informações digitadas no dispositivo do cliente (*keyloggers*).
- ***Automatic Timeout*:** O tempo limite permite que o sistema desconecte o cliente da janela de transacção se não houver actividade em um intervalo de 15 minutos, o que reduz o risco de acesso fraudulento se o cliente deixar o computador sem supervisão.
- **Certificado Digital:** Os certificados digitais são usados para autenticar os usuários e o próprio sistema bancário.

- **Notificação por SMS:** Método usado para notificar os usuários sempre que houver qualquer login / tentativa de login perfil de *internet banking*.
- **Negação de Acesso Temporária:** Depois de três tentativas de *login* consecutivas, o acesso à internet *banking* será temporariamente negado. Só depois de repor a palavra-passe por meio de uma linha segura do banco, o acesso será habilitado. Esta medida evita que utilizadores fraudulentos tentem palavras-passe falsas.

CAPÍTULO III: METODOLOGIA DE PESQUISA

Neste capítulo, é apresentado como a pesquisa foi desenvolvida, descrevendo os métodos empregues para o alcance dos objectivos estabelecidos. É descrito, qual a população e amostra da pesquisa e quais as técnicas usadas para colectar dados e como estes foram analisados e interpretados.

3.1.Tipo de Pesquisa e Desenho de Investigação

Quando elaboradas, as pesquisas têm sempre uma finalidade específica. Estas são aplicadas de acordo com o objectivo ou por meio do conhecimento que o pesquisador quer produzir. Gil (2008, p. 27) classifica as pesquisas em três grupos: as pesquisas exploratórias, descritivas e explicativas. O tipo de pesquisa ou estudo que foi adoptado nesta pesquisa é Exploratório. Segundo Gil (2008, p. 27), as pesquisas deste tipo têm como objetivo principal proporcionar uma visão geral, acerca de determinado facto. O mesmo autor advoga que este tipo de pesquisa constitui a primeira fase de uma investigação mais ampla, sendo assim, o produto final passa a ser um problema mais esclarecido, passível de investigação mediante procedimentos mais sistematizados.

Um desenho de investigação ou pesquisa pode ser definido como os métodos e técnicas escolhidas pelo pesquisador, que ao combiná-los permite que o problema apresentado na pesquisa seja tratado de forma eficiente. Para o trabalho de campo, o desenho de investigação adoptado foi por meio de técnicas quantitativas, usando inquéritos por questionário, aos utentes de serviços de *internet banking*. Para Gerhardt e Silveira (2009, p. 33) as técnicas quantitativas, geralmente são aplicadas quando as amostras são de grande porte e consideradas representativas da população, e desta forma, os resultados são apresentados como se constituíssem um retrato real de toda população alvo da pesquisa. As mesmas autoras, defendem que técnicas quantitativas recorrem à linguagem matemática para descrever as de um fenômeno, as relações entre variáveis e entre outros.

3.2.População e Amostra

Segundo Moreira (2016, p. 36), população é qualquer conjunto de elementos (pessoas ou objectos) que tenham, entre si, uma característica comum e por sua vez, uma amostra é uma parcela da população, com dimensões menores, sem perda das características essenciais. A amostragem refere-se a técnica para obter uma amostra de uma população. A população do presente estudo são todos os utentes de instituições bancárias que operam no mercado Moçambicano que usam os serviços de *internet banking*. Estes foram seleccionados por meio de uma amostragem não probabilística, por conveniência. Segundo Tivane (2015, p. 9), em amostragens não probabilísticas as amostras são escolhidas por critérios subjectivos de acordo com a experiência do pesquisador e ou objectivos do estudo. Neste caso não é conhecida a probabilidade de escolha de um determinado elemento da população. O mesmo autor ainda advoga que em amostragens não probabilísticas por conveniência as amostras são escolhidas de acordo com a conveniência do pesquisador, podendo ser constituída por indivíduos que estejam ao alcance do pesquisador e dispostas a colaborar no estudo.

3.3.Técnicas de Recolha de Dados

As técnicas de recolha de dados permitem orientar ao pesquisador na obtenção de dados que lhe possibilita responder as questões da pesquisa (TIVANE, 2015, p. 10).

Nesta pesquisa, serão usadas as seguintes técnicas: inquérito por questionário, consulta de websites das instituições bancárias que fornecem *internet banking* (15 instituições), consulta bibliográfica.

Questionário

O questionário, também chamado de *survey* é um dos procedimentos mais usados para recolha de dados. Esta é uma técnica de custo razoável, apresenta as mesmas questões para todas as pessoas, garante o anonimato e pode conter questões para atender finalidades específicas de uma pesquisa. Gil (2008, p. 121), define questionário como a técnica de investigação composta por um conjunto de questões que são submetidas a pessoas com o propósito de obter informações sobre conhecimentos, crenças, sentimentos, valores, interesses, expectativas, aspirações, temores, comportamento presente ou passado etc.

Para a pesquisa em questão, foi elaborado um questionário, de forma a colectar dados sobre:

- Quais as atitudes ou práticas de segurança que o usuário adopta, ao usar *internet banking*;
- A percepção dos utentes, no que concerne às ameaças de segurança do *internet banking*.

O questionário está no formato electrónico, e foi elaborado na ferramenta gratuita oferecida pelo *Google*, o *Google Forms*. Este foi enviado via email, e foi também partilhado o link do mesmo na plataforma *Whatsapp* (https://forms.gle/T1qrSZ3mFejwMNNi9). O questionário foi desenhado com perguntas de sim/não simples e claras, de forma a não deixar margem de dúvidas nos inquiridos (Anexo 2).

Internet

As consultas nas páginas *web* dos bancos, foram feitas com o intuito identificar quais os bancos que fornecem serviços de internet banking e avaliar o nível de informação provido pelos mesmos, sobre os riscos de segurança e práticas de segurança que o usuário deve adoptar quando faz o uso de *internet banking*.

Consulta Bibliográfica

As consultas bibliográficas, incluem pesquisas sobre o tema em estudo para além da metodologia de investigação científica.

Para Gil (2008, p. 50), a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho desta natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográfica.

3.4.Análise e Interpretação de Dados

Após a recolha dos dados, a fase que se segue é a de análise e interpretação. Para Teixeira (2003, p. 191) citando Gil (1998) a análise tem como objetivo organizar e resumir os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação. Já a interpretação tem como objetivo a procura do sentido mais amplo das respostas, o que é feito mediante sua ligação a outros conhecimentos anteriormente obtidos.

Teixeira (2003, p. 193) advoga que, para que seja feita uma análise de dados é necessário que primeiro se defina a unidade de análise, que por sua vez, se constitui na forma pela qual os dados são organizados. Em contrapartida, a definição da unidade de análise requer a decisão sobre o que se deseja investigar, o que pode ser uma organização, um grupo, diferentes grupos em uma comunidade ou determinados indivíduos.

Os dados desta pesquisa foram analisados e interpretados no período compreendido entre maio e junho de 2021. Sendo que o questionário foi enviado pela primeira vez em meados de abril e as respostas foram recebidas no final do mesmo mês.

Sendo que para a colecta de dados usou-se uma abordagem quantitativa, por meio de um inquérito por questionário, as informações colectadas foram tabuladas e agrupadas de acordo com os resultados de diferentes variáveis, de forma a oferecer uma imagem clara dos dados e auxiliar no processo de identificação de padrões. A plataforma *Google Forms* ajudou muito, pois nela já consta a percentagem das respostas, sendo assim não foi necessário fazer a contagem das respostas manualmente.

CAPÍTULO IV: APRESENTAÇÃO DOS RESULTADOS

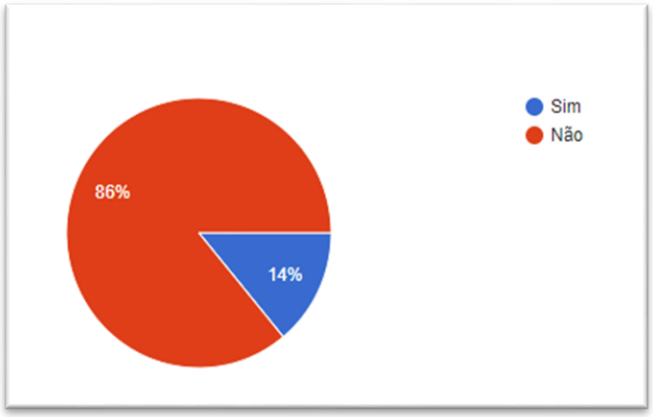
Neste capítulo são apresentados os resultados do questionário aplicado a 50 utentes de *internet bankung*.

4.1.Análise das Respostas dos Clientes de *Internet Banking*

Após a recolha de dados por meio do questionário, tem-se a base para analisar as atitudes ou práticas de segurança que os utentes de *internet banking* adoptam, perante o uso de serviços do internet *banking* e a percepção dos mesmos no que concerne às ameaças de segurança do *internet banking*. Sendo assim, serão aqui apresentados os dados obtidos com a aplicação do questionário. A amostra conta com 50 (cinquenta) respostas no total.

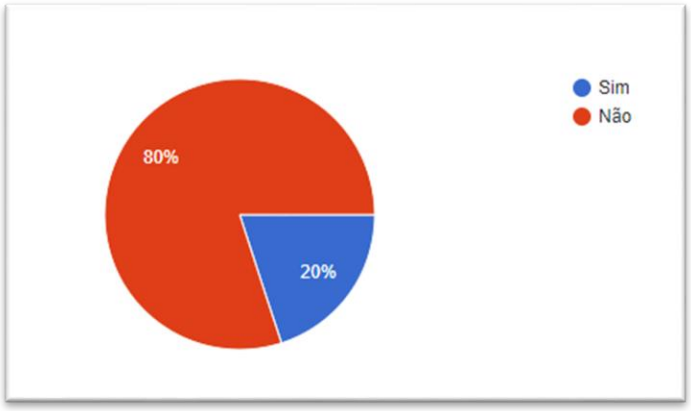
Os primeiros 3 gráficos abaixo, estão relacionados com o conhecimento de ataques de engenharia social, o *phishing* e *pharming* respectivamente, no qual foi questionado se o utente já ouviu falar dos mesmos.

Gráfico 1: Conhecimento de Ataque de Engenharia Social



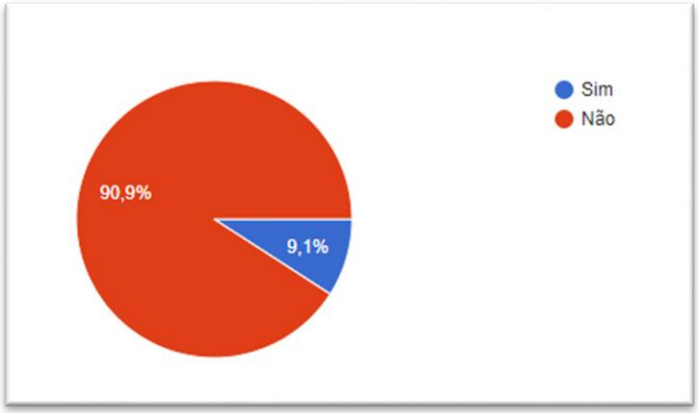
Fonte: Dados da pesquisa (2021)

Gráfico 2: Conhecimento de Ataque *Phishing*



Fonte: Dados da pesquisa (2021)

Gráfico 3: Conhecimento de Ataque *Pharming*

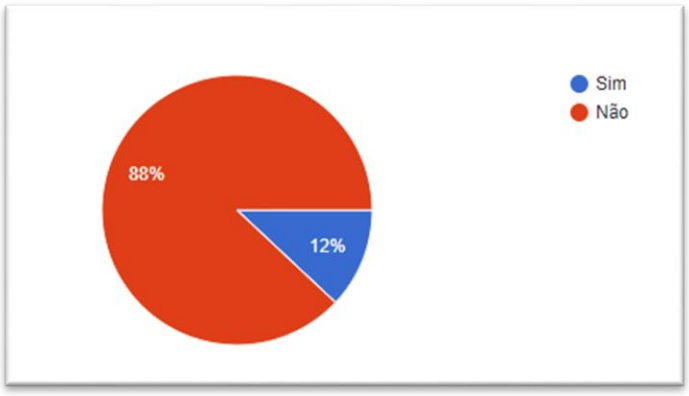


Fonte: Dados da pesquisa (2021)

Por meio dos gráficos, é possível verificar que 86% não tem conhecimento de um ataque de engenharia social, 80% e 90,9% nunca ouviu falar dos ataques *phishing* e *pharming* respectivamente. O que já constitui um risco, pois é impossível que o usuário proteja-se de algo que não sabe. Hoje em dia, em que as pessoas colocam tudo sobre suas vidas nas redes sociais, o trabalho dos engenheiros sociais tornou-se mais fácil, pois estes podem rastrear os interesses, curiosidades das pessoas e assim traçar uma oferta "apelativa" usando instituições bancárias como "*interface*", levando a vítima a acreditar que é algo legítimo e aceitar a oferta.

O gráfico 4 diz respeito alteração de palavras-passes, onde foi questionado se o respondente tem o hábito de alterar as mesmas.

Gráfico 4: Alteração de palavras-passe

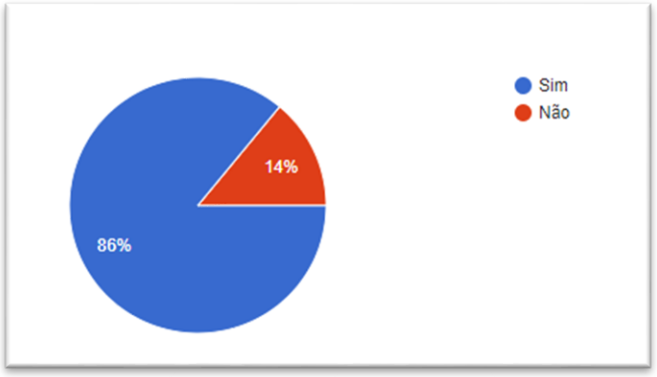


Fonte: Dados da pesquisa (2021)

Foi constatado que 88% dos respondentes não altera as suas palavras – chaves. A ideia por detrás de mudança de senhas é limitar o acesso da sua conta bancária por exemplo, caso ela seja roubada por alguém. Caso alguém tenha realmente roubado a senha e o utente não tenha percebido o mesmo, o invasor pode ter acesso à conta por um tempo limitado.

O gráfico 5 diz respeito ao uso da mesma palavra-passe para outros fins, no qual foi perguntado se o respondente usa palavras-passe únicas.

Gráfico 5: Uso da mesma palavra-passe para outros fins

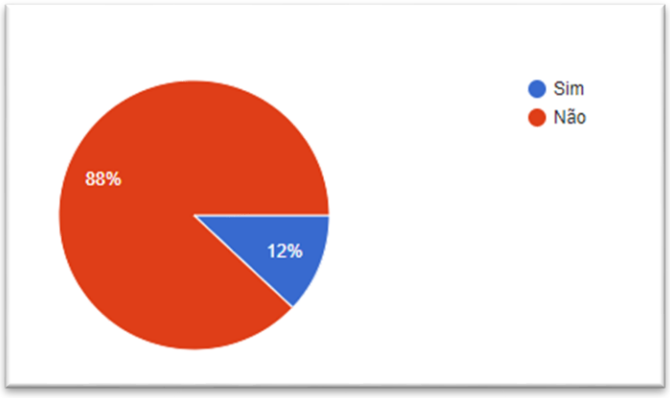


Fonte: Dados da pesquisa (2021)

É possível verificar que, 86% usa a mesma palavra – passe para outros fins. Utilizar mesmas *passwords* pode parecer melhor em termos de memorização, mas por outro lado, é vantajoso para pessoas mal intencionadas, afinal basta descobrir qual a senha para ter acesso aos dados dos utentes, usando técnicas de engenharia social aqui mencionadas.

O gráfico 6 diz respeito a verificação do extracto bancário, no qual foi questionado se o respondente tem o hábito de verificar o extracto.

Gráfico 6: Verificação de Extracto Bancário

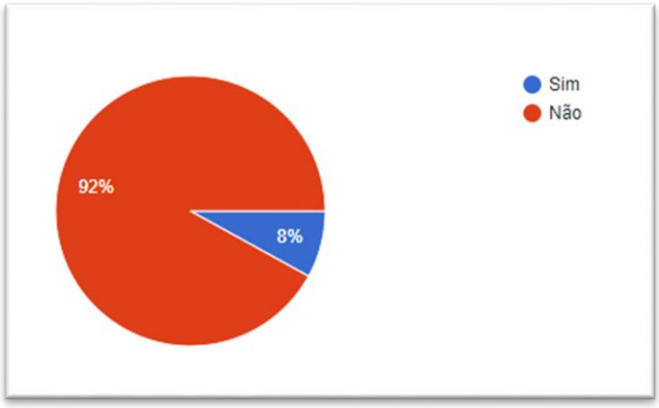


Fonte: Dados da pesquisa (2021)

É possível constatar que apenas 12% tem o costume de verificar o seu extracto bancário, e 88% não tem. É muito importante conferir o extracto bancário pois este constitui um veículo fornecido pelas instituições bancárias para o controle dos clientes, ou seja, com este documento os clientes podem verificar todas as transacções feitas em ordem cronológica.

O gráfico 7 diz respeito a leitura das condições de adesão do serviço de *internet banking*.

Gráfico 7: Leitura das condições de adesão do serviço de *internet banking*



Fonte: Dados da pesquisa (2021)

Foi constatado que apenas 8% leu as condições gerais do contracto ao adquirir o serviço. Ao aderir os serviços de *internet banking* o cliente é dado pelo banco, um documento onde constam as responsabilidades de ambas partes, que deve ser lido pelos clientes de forma a entender quais as condições de adesão do serviço.

CAPÍTULO V: DISCUSSÃO DOS RESULTADOS

Neste capítulo é feita uma comparação dos resultados obtidos no questionário com o que o banco espera do cliente, de acordo com as informações providas pelos mesmos em seus *websites*. Por fim, são propostas medidas traçadas conforme as expectativas das instituições bancárias que operam em Moçambique e a resposta comportamental de seus clientes, quando se trata do *internet banking*, que podem atenuar os riscos de fuga de informação por meio de técnicas de engenharia social.

5.1.Informações de Segurança providas pelos Bancos aos Clientes

Foi anteriormente constatado que, embora o *internet banking* forneça várias vantagens e oportunidades, este também é acompanhado de riscos de segurança. Com isto em mente, as instituições bancárias tomam medidas extensas para proteger as informações transmitidas e processadas em transacções bancárias *online*, isto inclui por exemplo, garantir que os dados confidenciais enviados pela *internet* não possam ser acessados ou modificados por terceiros não autorizados. Porém, os bancos não têm influência nenhuma sobre as máquinas usadas pelos seus clientes, estando estes expostos a riscos fora do controlo dos bancos. Daí que, para garantir que as medidas de segurança não sejam prejudicadas por manipulação, é fundamental que os clientes também cumpram algumas medidas de forma a proteger a máquina que usam para *internet banking*, e estas incluem:

1. **Usar um antivírus e mantê-lo actualizado:** Os antivírus são programas de computadores que têm como finalidade proteger a máquina do usuário contra vírus, *spywares*, *trojans*, ataques *phishing*, *pharming* ou seja, estes programas detectam ameaças e as eliminam de seus dispositivos, evitando assim a instalação de programas maliciosos e a contaminação de outros dispositivos conectados à rede.

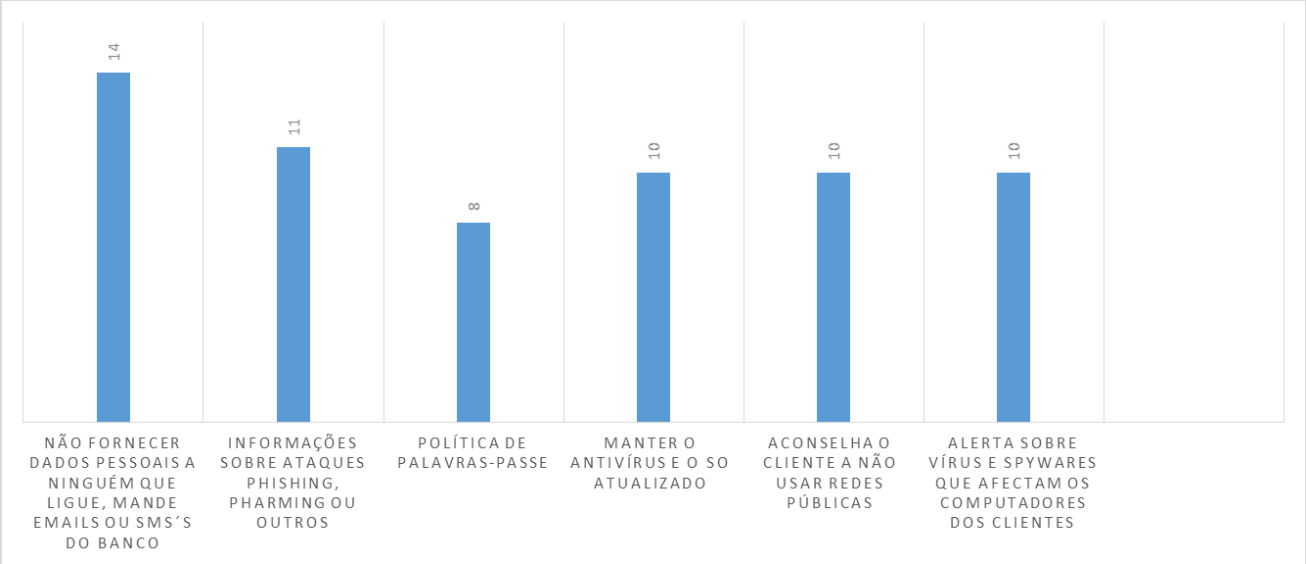
Figura 8: Exemplo de actuação de um antivírus contra ataque *phishing*

Fonte: A autora (2021)

2. **Manter o sistema operativo actualizado:** Versões recentes do sistema operativo podem eliminar falhas existentes em versões anteriores que tornavam as máquinas vulneráveis à ataques.
3. **Não efectuar *downloads*** de programas em páginas não oficiais, estes podem conter códigos maliciosos escondidos.
4. **Escolher uma *password* segura:** *Passwords* complexas que incluem uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais dificultam a descoberta das mesmas e o acesso não autorizado. E não usar as mesmas *passwords* que as de redes socias para *internet banking*.
5. **Mudar *passwords* a cada seis meses**
6. **Bloquear s*martphones, laptops*** ou qualquer dispositivo que use para *internet banking* usando padrões ou *passwords* fortes. Alguns smartphones têm a opção de identificação biométrica (impressão digital ou reconhecimento facial) como forma de bloqueio de acesso.
7. **Ler o acordo/contracto de *internet banking:*** Este contém informações sobre o papel do cliente na protecção de *passwords*, PINs etc.

Dos 19 bancos que operam em Moçambique, 15 fornecem o serviço de *internet banking*. O gráfico abaixo foi gerado com base nas informações que os mesmos fornecem aos seus clientes em seus *websites*, acerca dos riscos de segurança em ambiente de *internet banking* e as medidas de protecção que os clientes devem adoptar.

Figura 9: Nível de Informação provido pelos Bancos no que concerne a Segurança



Fonte: A autora (2021)

Foi possível concluir que, boa parte dos bancos fornece sim as informações essências sobre os riscos de segurança e as medidas de protecção que os seus clientes devem adoptar. Somente em uma pequena porção dos *websites* dos bancos a informação é escassa, ou muito difícil de encontrar. O que pelo menos 46% deve melhorar em seus *websites* é apresentar informações concretas, de forma resumida sobre os riscos de segurança em internet banking, que deve preencher todas as informações do gráfico. Foi verificado que em apenas *websites* de 3 bancos possuem todas as informações citadas acima. Foi possível verificar também que em um banco em particular não existe nenhuma informação sobre segurança em *internet banking*, inclusive o programa *Kaspersky Internet Security* emitiu um alerta de possível tentativa de *phishing*, o que é muito preocupante pois significa que o *website* não apresenta

recursos de segurança que devem ser implementados de forma a evitar fuga de informação, como o protocolo SSL/TLS, certificado digital, entre outros.

Excluindo estes detalhes, é possível afirmar que sim, os bancos informam aos seus clientes de *internet banking* sobre os perigos e as ameaças de segurança e como estes devem proteger-se.

Sendo assim, a responsabilidade de manter uma experiência de ambiente de *internet banking* seguro, recai também nos usuários. Com base nos resultados obtidos no questionário foram constatadas as seguintes disparidades entre o que o banco espera do cliente, e o que o cliente realmente faz:

Tabela 1: Comparação entre as expectativas do banco e as respostas do cliente

Expectativa do Banco	**Resposta do Cliente**
O banco espera que o cliente mude as suas passwords de 3 a 3 meses.	Apenas 12% tem este hábito.
O banco aconselha a nunca usar palavras - passe única (Por exemplo, a palavra – passe que usa para bloquear *smartphone* ou *laptop*, ou para redes sociais – instagram, twitter, facebook - é a mesma de login para *internet banking*).	86% usam palavras – passes únicas.
O banco aconselha a verificar o extracto bancário frequentemente.	Apenas 12% tem este costume.
Conhecimento sobre os ataques de engenharia social (*phishing* & *pharming*).	Apenas 20% e 9,1% respectivamente, têm conhecimento sobre estes ataques.
Ler as condições gerais do contracto de *internet banking.*	8% leu as condições gerais do contracto ao adquirir o serviço.

Fonte: A autora (2021)

5.2.Proposta de Medidas de Protecção que Eliminam as Disparidades Encontradas entre as Expectivas do Banco e as Respostas dos Clientes

Os modelos de segurança de sistemas de *internet banking* actualmente adoptados pelas instituições bancárias são baseados na identificação e autenticação dos usuários de i*nternet banking*, onde maior parte das fraquezas do sistema de internet banking são encontrados, pois já foi visto nos capítulos anteriores que os criminosos procuram manipular a confiança de usuários de *internet banking* a fim de obter acesso à suas informações privadas por meio de técnicas de engenharia social. Isto não só compromete o usuário mas também a instituição bancária, pois esta permite a execução de transacções fraudulentas. Este facto indica que um ambiente *internet banking* seguro deve mitigar o risco de fugas de informações relacionadas com o usuário (SHEIKH; RAJMOHAN, 2015, p.21).

Desta forma, são apresentas as seguintes medidas de protecção, de forma a mitigar os riscos de fuga de informações do usuário por meio de técnicas de engenharia social, traçadas com base nas disparidades encontradas do que o banco espera do cliente, e o que o cliente realmente faz:

i. Forçar o Usuário a alterar Palavras-Passe

Como foi possível constatar com o questionário, 88% dos utentes de *internet banking* não tem o costume de alterar as suas *passwords*. Os bancos poderiam adoptar uma política em que são dados 3 meses de validade das palavras – passes e se passados estes 3 meses, e o cliente não efectuarr a alteração da senha, o seu acesso será interdito até que o faça. É um processo que parece complicado mas necessário. Alterar palavras – passe é considerada boa prática para um ambiente internet banking seguro e os usuários devem estar conscientes do mesmo.

ii. Não Repetir Palavras-Passe anteriores

Este é um requisito muito importante, junto com o de alterar palavras-passe regularmente e não usar a mesmas *passwords* para redes sociais no internet banking. Se os engenheiros sociais descobrem qual a *password* que usa para redes sociais, sendo esta usada para outras plataformas, isto pode levar ao comprometimento da conta.

Os bancos não devem permitir que o cliente repita pelo menos duas passwords anteriores. Para facilitar o trabalho do cliente em pensar em passwords fortes regularmente, existem programas de antivirus acompanhados de um pacote de gestão de passwords, que têm a função de gerar passwords fortes.

iii. Adoptar Modelos de Inteligência Artificial (*Machine Learning*) e *Big Data* para Identificação de Actividades Suspeitas

O *Big Data* é um termo usado para referir-se a grandes conjuntos de dados. Os bancos lidam diariamente com grandes quantidades de dados, gerados a partir de inúmeras transacções de seus clientes. Inteligência Aritificial (IA) é um campo de ciências de computação que se propõe a desenvolver máquinas que tenham a habilidade de pensar e agir como seres humanos. Machine Learning é um subcampo da IA, que permite a autoaprendizagem a partir dos dados e, em seguida, aplica esse aprendizado sem a necessidade de intervenção humana. Ao combinar estas 3 tecnologias, os bancos podem usá-las para identificação de usuários e padrões suspeitos. Esta tecnologia (combinação das 3 citadas acima) pode fazer julgamentos sobre o comportamento do usuário, por exemplo, transferência de uma quantidade anormal de dinheiro para um destino fora de um padrão mensal do usuário. Ainda pode ser usado para detectar todas as transações eletrônicas, incluindo transações com cartão de crédito e será capaz de detectar se o usuário fez uma compra fora do seu padrão, alertará e em situações críticas desativará o cartão de crédito ou conta de banco eletrônico até que a identidade do cliente seja verificada. A inteligência artificial ou *machine learning* deve ser capaz de prever essa anomalia e tomar as medidas adequadas.

iv. Conscientizar mais o usuário sobre segurança

Educar o cliente, é o ponto-chave para garantir uma experiência segura no *internet banking*. O banco pode fornecer alertas de segurança em suas páginas *web* assim que o usuário iniciar sessão com sucesso, de forma a familiarizar os mesmos sobre as ameaças que constituem um risco para *internet banking*. Organizar programas de treinamento para seus clientes, não necessariamente um programa em que o cliente deve estar presente fisicamente; existem agora vários cursos que podem ser feitos em menos de uma hora sobre security awareness e todos são grátis, e estes podem ser recomendados aos clientes pelos bancos. Adoptar uma política de *newsletter* ou sms *tips* onde são enviados dicas sobre *security awareness.*

CAPÍTULO VI: CONCLUSÕES, LIMITAÇÕES E RECOMENDAÇÕES

Neste capítulo, são abordadas as principais conclusões, limitações e recomendações da pesquisa em questão. A pesquisa teve como principal foco, propor medidas de protecção contra ataques ao *internet banking*, que ocorrem devido a falta de conhecimento ou por assim dizer, negligência dos mesmos.

6.1.Conclusão

O serviço de internet banking é oferecido pelas instituições bancárias de forma a proporcionar melhor comodidade aos seus clientes. Para o ano de 2020, com a eclosão da pandemia de Covid-19, o internet banking foi uma mais-valia para os clientes pois este permitiu que os mesmos efectuassem as suas operações bancárias sem deslocar-se de suas residências ou postos de trabalho, sendo este um factor muito importante no que concerne a redução da propagação do vírus, visto que os clientes bancários não precisam aglomerar-se para realizar operações simples como transferências ou pagamentos.

O presente trabalho teve como objectivo, propor um conjunto de medidas que visam colocar mais responsabilidade em instituições bancárias que operam em Moçambique, de forma a mitigar os riscos de segurança que ocorrem devido a falta de conhecimento ou por negligência de seus clientes. Estas medidas foram traçadas com base nas disparidades encontradas entre o que o banco espera do seu cliente e o que o cliente realmente faz. Para tal, aplicou-se um questionário a uma amostra de 50 clientes de internet banking de instituições bancárias que operam em Moçambique de forma a perceber dos mesmos quais as atitudes ou práticas de segurança que os utentes de *internet banking* adoptam, perante o uso de serviços do *internet banking* e a percepção dos mesmos no que concerne às ameaças de segurança do *internet banking.*

Para além de proporcionar benefícios aos seus clientes, o *internet banking* também traz grandes vantagens aos bancos sendo a mais importante a redução do custo operacional, pois o banco incorpora vários de seus serviços em seu portal *online*, ou seja, em suas páginas *web*. Ao longo da pesquisa foi constatado que os *hackers* de hoje em dia, ao invés de optarem por fazer um ataque elaborado em instituições financeiras que por sinal têm sistemas de segurança de melhor desempenho, estes optam pelo elo mais fraco, os clientes destas

instituições. Desta forma os *hackers* gastam menos recursos, mandando somente uma mensagem electrónica as suas vítima e aguardam que as mesmas cedam e enviem as informações que eles precisam.

Como foi discutido anteriormente, os actuais modelos de segurança adoptados pelos bancos são fortemente focados na identificação e autenticação do usuário, onde a maioria das fraquezas do *internet banking* são encontrados. Este facto indica que um ambiente de *internet banking* deve atenuar os riscos de fuga de informação relacionados com os usuários, como o *phishing ou pharming*. As medidas de protecção aqui propostas têm por objectivo colocar mais responsabilidade em instituições bancárias que operam em Moçambique de forma a garantir que as políticas de tecnologias de informação são cumpridas pelos clientes para que desta forma os bancos possam fortificar os modelos de segurança. Por exemplo, ao invés dos bancos informarem aos seus clientes que estes devem mudar de palavras – passe a cada três meses, estes devem forçar os seus clientes a mudar de palavras – passe, dando um prazo de expiração de 3 meses para que os clientes sejam forçados a mudar as suas senhas.

Algumas das tecnologias aqui propostas são existentes, como os algoritmos de inteligência artificial projectados para aprender padrões comportamentais dos clientes e detectar anomalias no mesmo. Grandes companhias como Netflix, usam algoritmos de inteligência artificial e aprendizagem de máquina para apreender os gostos e interesses de seus subscritores e assim poder recomendar séries ou filmes aos mesmos. Isto só para dizer que existem algoritmos capazes de aprender com o comportamento de pessoas, estes só precisam ser integrados e adaptados para o que se pretende alcançar nos bancos, que é detectar anomalias no comportamento dos clientes.

Sendo assim, os bancos deveriam levar mais responsabilidade em garantir um ambiente de internet banking mais seguro para os seus clientes. Mesmo não tendo sido possível avaliar o nível de aceitação das medidas aqui propostas por parte dos bancos como é abordado nas limitações, de forma a confirmar as hipóteses levantadas, os resultados obtidos do questionário, demonstram a necessidade da adopção de técnicas ou medidas desta natureza, de forma a amenizar os riscos de segurança descritos no trabalho.

6.2.Limitações

Como todo trabalho de pesquisa, o trabalho teve algumas limitações que comprometeram o cronograma do mesmo, sendo elas:

- A indisponibilidade dos utentes seleccionados em fornecer as respostas do questionário rapidamente. Foi necessário enviar o questionário várias vezes de forma a obter no mínimo 50 respostas.
- A indisponibilidade dos bancos em fornecer respostas no que concerne a aceitação por parte dos mesmos, das medidas de segurança propostas aqui no trabalho. Foram procuradas um total de 4 bancos, sendo que 2 recusaram, devido a pandemia de covid-19. Os 2 restantes, aceitaram a credencial da faculdade e prometeram respostas mas até então não se pronunciaram.

6.3.Recomendações

Para trabalhos futuros, recomenda-se aos pesquisadores interessados no tema Segurança de Informação em *Internet Banking*, que proponham modelos que abranjam as medidas aqui citadas para que possam ser implementados. Outro ponto relevante é a questão dos teclados virtuais. Estes foram projectados para impedir que programas maliciosos como *keyloggers* capturem dados digitados pelos usuários e enviem para máquina do *hacker*. Mas actualmente existem outros programas maliciosos para contornar os teclados virtuais, que podem capturar dados digitados por meio do *mouse* e até mesmo capturar dados sem que haja acção do usuário (do teclado ou mouse). Em trabalhos futuros, os pesquisadores podem incluir no modelo uma tecnologia que contorne estes três programas maliciosos.

REFERÊNCIAS BIBLIOGRÁFICAS

[1]. ADACHI, T. Gestão de Segurança em *Internet Banking*: Estudo de Casos Brasileiros. Dissertação (Mestrado em Administração de Empresas). FGV - Fundação Getúlio Vargas, São Paulo, p. 121. 2004.

[2]. AL-WESHAH, G. (2013). *The role of internet banking in continuous improvement areas: Quantitative evidence from Jordanian banks. Int. J. of Business Performance Management*. p. 181 - 196.

[3]. ALEROUD, A. & ZHOU, L. (2017). *Phishing Environments, Techniques, and Countermeasures: A Survey.* Computers & Security, p. 160-196.

[4]. ALGHAZO, J.; KAZIMI, Z. & LATIF, G. (2017). *Cyber security analysis of internet banking in emerging countries: User and bank perspectives.* p. 1-6.

[5]. BARBOSA, E. F. (2008). Intrumentos de Colecta de Dados em Pesquisas Educacionais. p. 1-5.

[6]. CARMO, J. S. d. A Segurança da Informação na Rede Bancária no Município de Rolim de Moura / RO. Trabalho de Conclusão de Curso (Bacharel em Administração). Universidade Federal de Rondônia. p. 41. 2013.

[7]. CARVALHO, R. d. O. Segurança de Informação nas Organizações.Trabalho de Conclusão de Curso (Bacharel em Administração). Centro Universitário de Brasília. Brasília, p. 41. 2009.

[8]. CISAR, P. & PINTER R. (2019). *Some Ethical Hacking Possibilities in Kali Linux Envvironment. Journal of Applied Technical and Educational Science (jATES),* Sérvia, v. 9, n. 4, p. 129-149.

[9]. COSTA, J. E. Engenharia Social e Segurança da Informação no Ambiente Corporativo: Um Estudo de Caso em uma Cooperativa de Crédito Localizada no Sul de Santa Catarina. Trabalho de Conclusão do Curso (Bacharel em Tecnologias da Informação e Comunicação). Universidade Federal de Santa Catarina. Araranguá, p. 73. 2018.

[10]. DUNHAM, K. *Mobile Malware Attacks and Defense.* 1ª ed. Burlington: Syngress Publishing, Inc., 2008.

[11]. ELISAN, C. C. *Malware, Rootkits & Botnets: A Beginner's Guide*: McGraw-Hill, 2013.

[12]. GASRELLIER-PREVOST, S.; GRANADILLO, G. & LAURENT, M. (2011). *A Dual Approach to Detect Pharming Attacks at the Client-Side. 4th IFIP International Conference on New Tecnologies, Mobility and Security. Paris*, p. 1-5.

[13]. GERHARDT, T. E.; SILVEIRA, D. T. Métodos de Pesquisa. 1ª ed. Porto Alegre: UFRGS Editora, 2009.

[14]. GIL, A. Métodos e Técnicas de Pesquisa Social. 6ª ed. São Paulo: Editora ATLAS, S.A., 2008.

[15]. JOSHUA, A. J. & KOSHY M. P. (2011) *Usage Patterns of Electronic Banking Services by Urban Educated Customers: Glimpses from India. Journal of Internet Banking and Commerce* (JIBC)**,** Reino Unido, v. 16, n. 1.

[16]. LAU, M. Análise das Fraudes Aplicadas sobre o Ambiente *Internet Banking*. Dissertação (Mestrado em Engenharia de Sistemas Electrónicos). Universidade de São Paulo. São Paulo, p. 130. 2006.

[17]. LORD, N. *Social Engineering Attacks: Common Techniques & How to Prevent an Attack, Digital Guardian*. Dec 2020. Disponível em: <Social Engineering Attacks: Common Techniques & How to Prevent an Attack | Digital Guardian> Consultado em: 19-02-2021.

[18]. MOREIRA, A. S. Características Pessoais e Decisórias dos Gerentes de Banco e Uso de Sistemas de Apoio à Decisão. Trabalho de Conclusão de Curso (Bacharel em Gestão de Informação). Universidade Federal do Paraná. Curitiba, p.79. 2016.

[19]. MIA, A. H.; RAHMAN, M. A. & UDDIN, M. (2007) *E-Banking: Evolution, Status and Prospects. The Cost & Management,* Bangladesh, v. 35, n. 1, p. 36-48.

[20]. POLÍCIA moçambicana desmantela duas quadrilhas suspeitas de praticar crimes cibernéticos. Diário de Notícias, Lisboa, 19 de Jul. de 2018. Disponível em <https://www.dn.pt/lusa/policia-mocambicana-desmantela-duas-quadrilhassuspeitas-de-praticar-crimes-ciberneticos-9614446.html> Consultado em: 21-02-2021.

[21]. POUCHAIN, A. d. M. Gestão de Riscos Aplicada ao Ambiente *Internet Banking* das Instituições Financeiras do Brasil. Dissertação (Mestrado em Engenharia Eléctrica). Universidade de Brasília. Brasília, p. 150. 2007.

[22]. REIS, A. P. d., Análise de vulnerabilidades de segurança em sistemas de Internet Banking utilizando ferramentas de código aberto. Trabalho de conclusão de curso (Bacharel em Sistemas de Informação). Universidade Federal de Uberlândia. Uberlândia, p. 46. 2018.

[23]. RODRIGUES, E. R.; BÓ, M. D.; GANZER, P. P.; NODARI, C. H.; OLEA, P. M.; DORION, E. C. H.; SILVA, O. T. & d' AVILA, A. A. F. (2016). Inovação Tecnológica em Produtos e Processos: Estudo de Caso em Empresas de Automação Industrial. Revista Mundi Engenharia Tecnologia e Gestão. p. 9-20.

[24]. ROMÃO, F. A. C. e-Business: Estratégias e Modelos. Dissertação (Mestrado em Estatística e Gestão de Informação). Universidade Nova de Lisboa. Lisboa, p. 88. 2010.

[25]. SILVEIRA, L. A.; REALAN, M. & AMARAL E. Engenharia Social: Uma análise sobre o ataque de *Phishing.*

[26]. SHEIKH, A. B. & RAJMOHAN, P. (2015) *Internet Banking, Security Models and Weakness. International Journal of Research in Management & Business Studies* (IJRMBS), India, v. 2, n. 4, p. 17-22.

[27]. TEIXEIRA, E. B. (2003). A Análise de Dados na Pesquisa Científica. importância e desafios em estudos organizacionais. Desenvolvimento em Questão, Rio Grande do Norte: Editora Unijuí, p. 177-201.

[28]. TIVANE, F. J. Gestão de Risco Operacional. Estudo do Caso de Infra-estruturas da Banca Electrónica em Moçambique. Dissertação (Mestrado em Sistemas de Informação). Universidade Eduardo Mondlane. Maputo, p. 94. 2015.

[29]. VAYANSKY, I. & KUMAR, S. (2018). *Phishing – challenges and solutions. Computer Fraud & Security*. p. 15-20.

[30]. Verizon. (2016). Data Breach Investigations Report. Nova York. p. 85.

[31]. Webpage1, 2021. Fraudes Recentes de Internet Banking. Disponível em: https://www.bci.co.mz/seguranca/#fraudes-recentes. Consultado em: 25-03-2021.

[32]. Webpage2, 2021. Alerta: Fraudes por SMS. Disponível em: https://ind.millenniumbcb.pt/pt/Particulares/seguranca/Documents/Aviso2020124/sms-fraudulentos.html. Consultado em: 25-03-2021.

[33]. Webpage3, 2021. *Keyloggers*. Disponível em: https://www.tecmundo.com.br/amp/spyware/1016-o-que-e-keylogger-.htm. Consultado em: 23-04-2021.

GLOSSÁRIO

De forma a harmonizar os conceitos usados no trabalho, a autora apresenta abaixo algumas definições que julga necessárias para melhor compreensão do documento.

Termo	**Definição**
Hacker	Especialista em penetrar sistemas da segurança ou descodificar programas e códigos da informação.
Link	Um link (abreviação hyperlink, hiperligação em português) é um objecto HTML que permite pular para um novo local ao clicar ou tocar nele.
One Time Password	Refere-se a uma cadeia de caracteres numéricos ou alfanuméricos geradas automaticamente que autentica o usuário para uma única transação ou sessão de login.
Password	Refere-se a uma sequência de caracteres que permite o acesso a um sistema ou serviço de computador.
Phisher	Pessoa que se faz passar por uma entidade autoritária, por email ou outras formas de comunicação, de forma a extrair credenciais de login ou informações de conta das vítimas.
Pharmer	Pessoa ou entidade que tenta tirar proveito de pequenos erros ortográficos em nomes de domínio para induzir os usuários a visitar inadvertidamente o website do mesmo.
Website	Refere-se a uma colecção de páginas web interligadas e acessíveis ao público que compartilham um único nome de domínio.

ANEXOS

Anexo 1 - Ética de Investigação

Caro (a) participante, você está sendo convidado (a) para participar da pesquisa "Análise de Riscos de Segurança de Informação do *Internet Banking* em Sistemas Bancários Moçambicanos: Perspectiva dos Clientes", como Trabalho de Final de Curso para obtenção da Licenciatura em Engenharia Informática e de Telecomunicações.

Sua participação é voluntária e anónima. Mesmo não tendo benefícios directos ao participar, estará a contribuir para a compreensão do fenômeno estudado e para a produção de conhecimento científico.

Ao participar, estará de acordo com a declaração: Declaro que entendi os objectivos e benefícios da minha participação na pesquisa e consinto em participar no estudo.

Encontre abaixo o formulário.

Agradeço desde já, pela atenção dispensada.

Este questionário foi adaptado do artigo de Alghazo et al. (2017), com o título *Cyber security analysis of internet banking in emerging countries: User and bank perspectives*.

Anexo 2 - Questionário para Recolha de Dados (Utentes de *Internet Banking*)

1. Usa Anti-Virus?
   ( ) Sim ( ) Não ( ) Não conheço o termo
2. Tem o *Firewall* activado?
   ( ) Sim ( ) Não ( ) Não conheço o termo
3. Usa algum *Anti – Spyware*?
   ( ) Sim ( ) Não ( ) Não conheço o termo
4. Mantém o seu Sistema Operativo actualizado?
   ( ) Sim ( ) Não
5. Usa rede pública (*Wi-Fi* em *internet* cafés, parques, ginásios etc.) para *Internet Banking*?
   ( ) Sim ( ) Não
6. Faz o *Sign Out* depois de terminar todas actividades do *Internet Banking*?
   ( ) Sim ( ) Não
7. Tem palavras – passe para bloquear o seu *Laptop* ou *Smartphone*?
   ( ) Sim ( ) Não
8. Usa palavras – passe únicas?
   ( ) Sim ( ) Não
9. Tem o hábito de alterar palavras – passe?
   ( ) Sim ( ) Não
   9.1. Se respondeu sim na questão anterior, por favor indique com que frequência (Por exemplo: Altero a cada 3 meses)
   _____
10. Tem o hábito de verificar o seu extrato bancário?
    ( ) Sim ( ) Não
    10.1. Se respondeu sim na questão anterior, por favor indique com que frequência (Por exemplo: verifico mensalmente)
    _____
11. Já ouviu falar de ataque *Phishing*?
    ( ) Sim ( ) Não

12. Já ouviu falar de ataque *Pharming*?

    ( ) Sim ( ) Não

13. Já ouviu falar de ataque de Engenharia Social?

    ( ) Sim ( ) Não

14. Ao aderir aos serviços de *internet banking*, leu as condições gerais do contracto de adesão do mesmo?

    ( ) Sim ( ) Não