FACULDADE DE TECNOLOGIA DE SÃO BERNARDO DO CAMPO
"ADIB MOISÉS DIB"

LUIGI MÁRIO D'ORIA
MARCELO ASSIM PEREIRA

DESENVOLVIMENTO DE CARTILHA PARA OPERAÇÕES BANCÁRIAS DIGITAIS SEGURAS

São Bernardo do Campo – SP
DEZEMBRO/22

LUIGI MÁRIO D'ORIA
MARCELO ASSIM PEREIRA

DESENVOLVIMENTO DE CARTILHA PARA OPERAÇÕES BANCÁRIAS DIGITAIS SEGURAS

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Bernardo do Campo "Adib Moisés Dib", como requisito parcial para a obtenção do título de Tecnólogo em Informática para Negócios.

Orientadora: Profª Drª Samáris Ramiro Pereira

São Bernardo do Campo – SP
DEZEMBRO/22

LUIGI MÁRIO D'ORIA
MARCELO ASSIM PEREIRA

DESENVOLVIMENTO DE CARTILHA PARA OPERAÇÕES BANCÁRIAS DIGITAIS SEGURAS

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Bernardo do Campo "Adib Moisés Dib" como requisito parcial para a obtenção do título de Tecnólogo em Informática para Negócios.

Trabalho de Conclusão de Curso apresentado e aprovado em: ___/ ___/ _____.
Banca examinadora:

_____
Profª Drª Samáris Ramiro Pereira, FATEC SBC – Orientadora

_____

_____

RESUMO

Recentemente tem havido um aumento significativo nas fraudes contra os usuários do sistema bancário e foi observado que a grande maioria delas poderia ser evitada com a alteração de alguns hábitos e ações dos usuários. Este trabalho apresenta uma cartilha sobre como se prevenir dos principais golpes aplicados nos pagamentos em comércios tradicionais e digitais, terminais de autoatendimento bancário, cartões bancários e mesmo em aplicativos de mensagem instantânea. Trata-se de uma pesquisa aplicada, composta por pesquisa bibliográfica para a discussão das contribuições de autores da área e pesquisa experimental, com vistas ao desenvolvimento de uma cartilha. Espera-se que quem leia esta cartilha tenha maior acesso a formas de evitar esses golpes.

Palavras-chave: Cartilha Bancária. Golpes Financeiros via WhatsApp. Fraudes Bancárias Digitais.

ABSTRACT

Recently there has been a significant increase in fraud against users of the banking system and it was observed that the vast majority of them could be avoided by changing some habits and actions of users. This work presents a booklet on how to prevent the main scams applied to payments in traditional and digital commerce, automatic teller machine, bank cards and even instant messaging applications. This is an applied research, composed of bibliographic research to discuss the contributions of authors in the area and experimental research, with a view to developing a booklet. It is hoped that those who read this booklet will have greater access to ways to avoid these scams.

Keywords: Banking Booklet. Financial Scams via WhatsApp. Digital Banking Fraud.

Sumário

INTRODUÇÃO

Com o advento da informatização de processos na década de 1960, o setor bancário foi um dos primeiros a se informatizar. Surgem nessa mesma época os sistemas de TAA (Terminal de Autoatendimento), no qual com a utilização do cartão magnético os clientes podiam sacar dinheiro, tirar extratos de movimentação bancária, entre outras funções. Com o tempo essas funções foram sendo ampliadas.

Ainda na década de 1960 acontece a primeira fraude em TAA, por roubo de número de conta e senha, tornando a segurança da informação algo de extrema importância. Após estudos realizados pelos bancos e instituições coligadas, notou-se que o elo fraco nesses casos é o usuário final e é a ele que se destina em última instância este trabalho de graduação.

Recentemente tem havido um aumento significativo nas fraudes contra os usuários do sistema bancário e foi observado que a grande maioria delas poderá ser evitada com a alteração de alguns hábitos e ações dos usuários.

O objetivo deste trabalho é elaborar um guia que oriente os usuários bancários sobre como evitar algumas das fraudes mais comuns aplicadas contra eles nos ambientes em que elas ocorrem com mais frequência (bancário, comércio físico e virtual). Com esse guia, espera-se que todos possam ter acesso a um esclarecimento maior sobre como utilizar os meios de pagamento bancário, terminais de autoatendimento e ainda compras nas lojas online de forma mais segura, evitando ser mais uma vítima de fraudes e golpes financeiros.

Este trabalho se divide em: Capítulo 1 – Fundamentação teórica, em que se discutem autores e teorias em que se baseia o projeto; Capítulo 2 – Metodologia, com as questões relativas ao planejamento do trabalho e com as etapas previstas para sua realização; Capítulo 3 – Desenvolvimento, em que é colocado o passo a passo da

elaboração da parte prática do projeto; por último, as Considerações Finais, com as discussões decorrentes de todo o processo.

1 FUNDAMENTAÇÃO TEÓRICA

Neste Capítulo serão apresentadas discussões sobre segurança da informação, identificação biométrica, entre outros, para conter fraudes contra os usuários do sistema bancário e instituições financeiras fundamentadas por autores da área.

1.1 Segurança da informação

Para Fontes (2017) a Segurança da Informação é um dos maiores bens de uma empresa, um processo contínuo sem fim, possibilitando às grandes empresas atuarem no mercado atual. Também pode ser descrita como área do conhecimento aplicada à proteção de ativos da informação contra acessos não autorizados, alterações inadequadas e sua indisponibilidade (VANCIM, 2016).

Fontes (2017) descreve a necessidade de regras básicas para o uso dos recursos da informação chamada política de segurança. Os colaboradores devem cumprir regras e normas que dizem respeito à proteção da informação. Esses processos envolvem a área de recursos humanos, área jurídica e administração.

Segundo a Norma Brasileira (NBR) ISO/IEC 27002, da Associação Brasileira de Normas Técnicas (ABNT 2020), é necessário que as organizações disponham de uma equipe preparada no setor de Tecnologia da Informação para elaborar as políticas relacionadas à tecnologia, está disponível em língua portuguesa na ABNT NBR ISO/IEC 27002 e em língua inglesa na ISO 27002, com um padrão de normas e procedimentos desenvolvidos para garantir a segurança da informação nas organizações.

A ABNT (2020) complementa que é necessário a preservação dos princípios básicos da segurança da informação, citados como a confidencialidade, integridade e disponibilidade:

- Confidencialidade: garantir o acesso apenas quem tem direito à informação;
- Integridade: informações corretas, confiáveis estando em sincronia de tempo e espaço, ou seja, sem alterações;
- Disponibilidade: estar disponível sempre que for necessário para as pessoas autorizadas.

Rosti (2020) cita outros princípios importantes que complementam os princípios relacionados à segurança da informação. São eles:

- Autenticidade: documento correto em termos de dados e emissor;
- Legalidade: estar de acordo com a lei;
- Não-Repúdio: o emissor não pode negar que emitiu os dados e a prova da integridade da origem dos dados.

A biometria digital é a característica mais utilizada dentre as variadas formas de identificação. Ela faz uso das variações das linhas existentes nas pontas dos dedos para autenticar a identidade de um indivíduo (GOGONI, 2019).

1.2 Utilização da biometria na segurança da informação

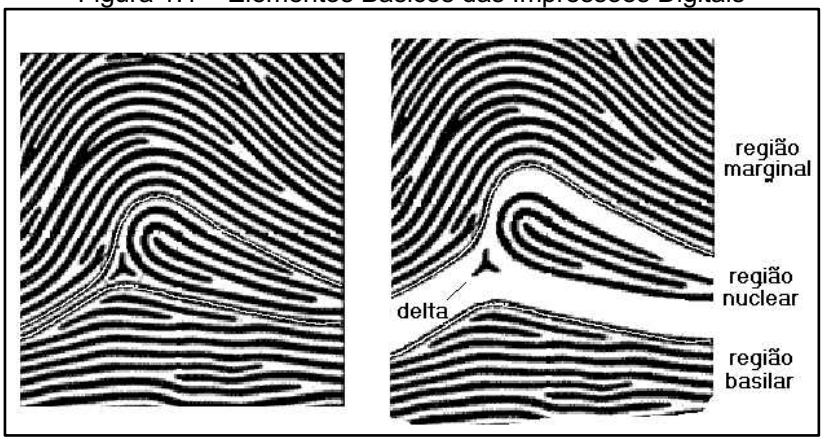
Segundo Gogoni (2019), a palavra Biometria (do latim, bio + metria) é a medição da vida, ou em termos mais gerais, o estudo estatístico de características físicas e comportamentais. Em Segurança da Informação, a biometria consiste na aplicação de métricas a atributos biológicos para fins de aferição e identificação de um indivíduo. A biometria serve para controlar o acesso físico de pessoas a certos setores e salas, identificar e localizar criminosos, e para impedir que pessoas não autorizadas acessem digitalmente dados sigilosos, protegidos por autores ou

mantenedores. Conforme descreve Gogoni (2019), existem seis tipos de biometria mais utilizados para validar a identidade de alguém, a seguir descritos.

- Impressão Digital

É o mais comum, custo mais baixo para implantação, extremamente confiável e seu uso vai desde o simples acesso a dispositivos móveis como celulares e tablets na identificação de indivíduos em investigações criminais. A Figura a seguir demonstra os elementos básicos analisados para diferenciar as digitais.

Figura 1.1 – Elementos Básicos das Impressões Digitais

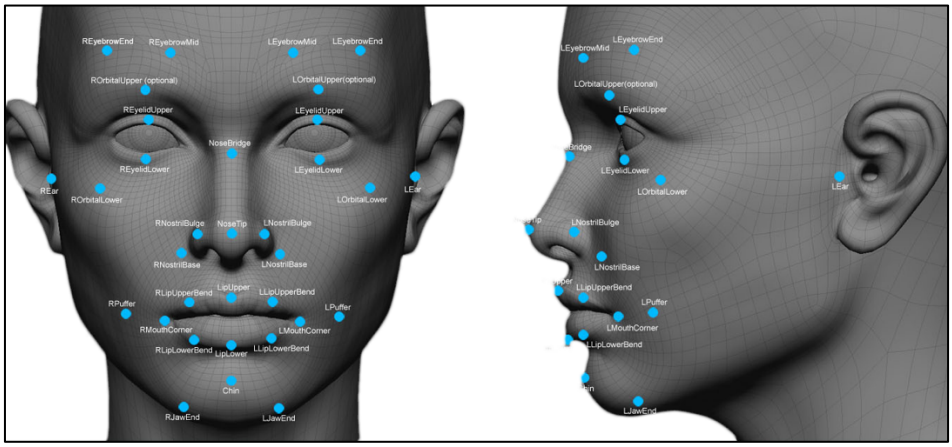


Fonte: http://www.papiloscopia.com.br/estudo_das_papilas.html, 2018

- Reconhecimento Facial

Consiste em mapear um rosto e criar uma imagem da pessoa que será utilizada para identificação. Um ponto negativo deste método é que as medidas do rosto se alteram com a idade e podem ser manipuladas com procedimentos médicos e estéticos. A Figura a seguir demonstra os pontos de análise para reconhecimento facial.

Figura 1.2 – Elementos básicos de reconhecimento facial

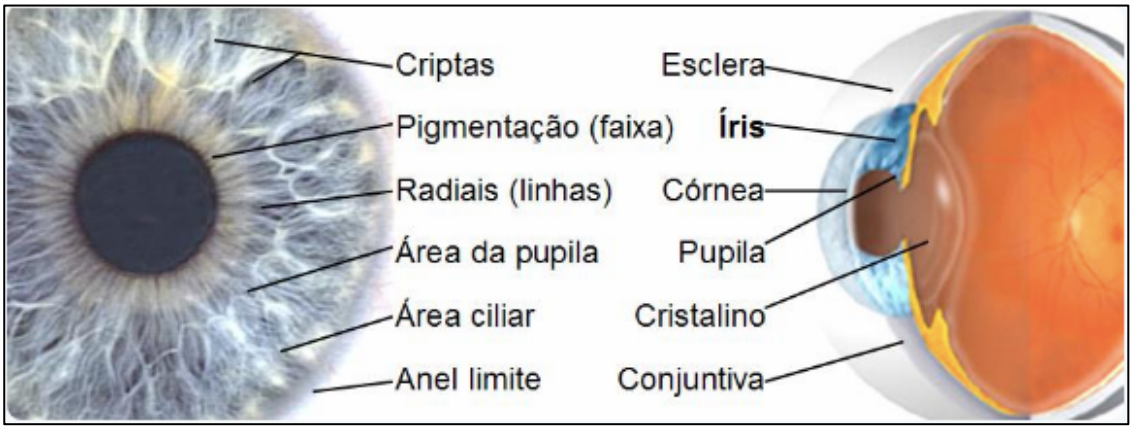


Fonte: https://www.projetodraft.com/verbete-draft-o-que-e-reconhecimento-facial/, 2018

- Reconhecimento de Íris

A biometria usando a íris é extremamente confiável, já que ela permanece a mesma ao longo de toda a vida. Entretanto a implementação desse método ainda é muito cara. A Figura 1.3 demonstra a estrutura ocular da íris.

Figura 1.3 – Estrutura ocular da íris



Fonte: https://brainly.com.br/tarefa/6656100, 2020

- Reconhecimento de Voz

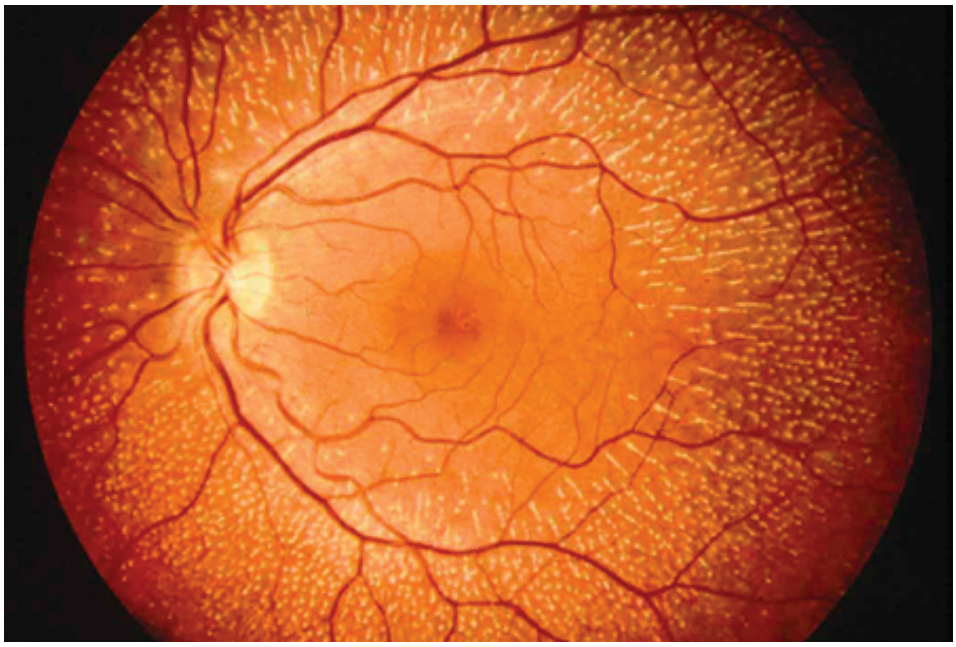
O método de reconhecimento por voz faz uma análise dos parâmetros físicos (cordas vocais, laringe etc.) e comportamentais, como sotaques, maneirismos,

entonação etc. O resultado é um perfil sonoro único que, em tese, pode ser usado como uma assinatura biométrica. Este método não é muito confiável pois qualquer ruído ambiental, problema de saúde ou até mesmo o envelhecimento podem causar distorções no padrão de reconhecimento.

- Reconhecimento de Retina

É uma das biometrias mais seguras que existe, já que a disposição dos vasos sanguíneos que irrigam a retina varia de pessoa para pessoa e não mudam. Os meios necessários para a coleta e leitura dos dados não são simples, o que dificulta a falsificação das informações. Esse método é bastante seguro, porém a forma de coletar os dados é mais invasivo e incômodo. A imagem a seguir apresenta uma retina vista internamente.

Figura 1.4 – Imagem interna da retina



Fonte: https://www.gta.ufrj.br/grad/10_1/retina/vantagensedesvantagens.html

- Reconhecimento pela Digitação

Pouco invasivo, baseia-se na análise do ritmo e cadência do usuário ao digitar. Cada pessoa possui um estilo próprio: seja a quantidade de dedos que utiliza, a velocidade com que digita ou a força que aplica às teclas. É pouco invasivo e pouco confiável, já que o estado emocional do usuário pode alterar o padrão de reconhecimento.

Outra forma de validar a identidade de alguém é a utilização da impressão da palma das mãos, muito utilizada pelas instituições bancárias no Brasil, que contêm as mesmas características das impressões digitais encontradas nas pontas dos dedos.

1.3 Sistemas bancários e segurança da informação

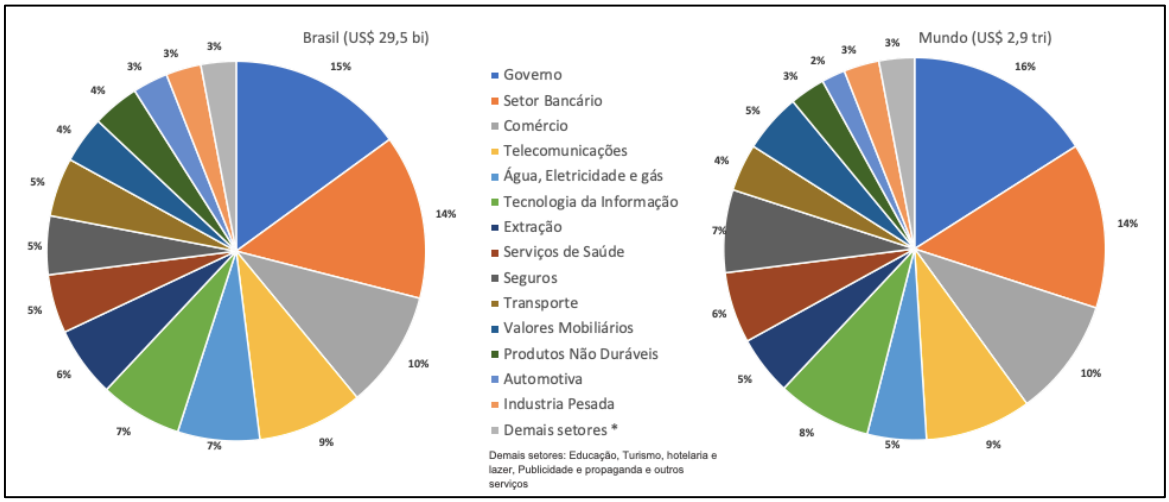
Para Loss et al. (2016), o setor bancário é considerado o ramo da economia que mais investe em tecnologia da informação, tendo parte de seus produtos e serviços dependentes de tecnologia. Diante disto, o processo de gestão bancária passa por desafios, levando as empresas a trabalharem com novas estruturas para enfrentar ambientes cada vez mais exigentes e requerendo melhores práticas de gestão corporativa.

A segurança da informação tem como objetivo a proteção dos ativos de informação, a redução de riscos de acessos não autorizados ou o uso indevido das informações e sistemas (SANTANDER, 2022).

Segundo pesquisa de 2021 da Federação Brasileira de Bancos (FEBRABAN), o setor bancário é o maior investidor em tecnologia no Brasil e no mundo.

A figura a seguir apresenta o gráfico com a composição do orçamento de tecnologia por setor em 2020 (em % do total), no Brasil e no mundo.

Figura 1.5 – Composição do orçamento de tecnologia por setor em 2020 (em % do total) no Brasil

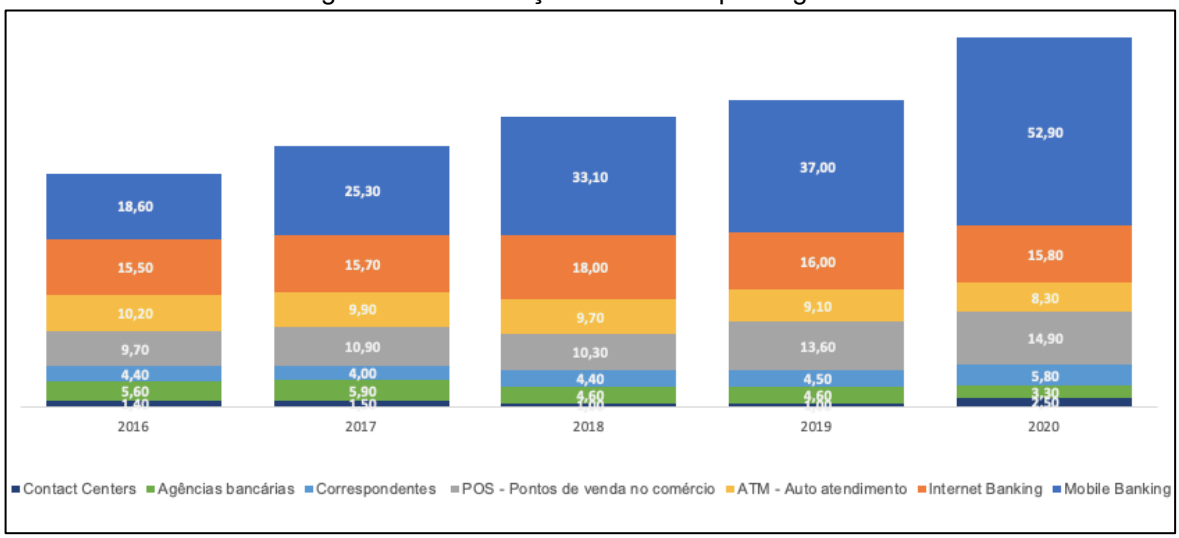


Fonte: FEBRABAN, 2021

1.3.1 Evolução da segurança bancária

O setor de finanças pessoais no Brasil está em plena transformação e a tecnologia vem-se aprimorando com destaque para o uso dos aplicativos de acesso bancário por smartphones. O volume de transações, segundo a FEBRABAN (2021), nesse segmento teve um aumento de 30% entre 2019 e 2020. A figura a seguir apresenta o gráfico com o volume de transações bancárias por segmentos:

Figura 1.6 – Transações bancárias por segmento



Fonte: FEBRABAN 2020

1.3.2 Fraudes financeiras mais comuns

Com o crescimento em transações bancárias, cresceram também os índices de fraudes contra os usuários do sistema bancário. Segundo levantamento da FEBRABAN as fraudes contra clientes cresceram 165% somente no primeiro trimestre de 2021 em relação ao mesmo período de 2020 (CÂMARA DOS DEPUTADOS, 2021).

Segundo Banco do Brasil (2022), seguem os tipos de fraude mais comuns e a forma de se prevenir delas:

- Golpes do WhatsApp

Existem dois golpes muito comuns, no primeiro os fraudadores clonam o WhatsApp e se passam por conhecidos e familiares para pedir dinheiro emprestado. Neste segundo, o fraudador consegue sua foto em alguma rede social, procuram conhecidos que tenham algum telefone de contato cadastrado e entram em contato com as vítimas mandando mensagens comunicando a troca de número por algum problema e depois pedem dinheiro emprestado como se estivessem em alguma emergência.

Para evitar ser vítima, desconfie de contas com fotos de conhecidos, mas com números diferentes. Não faça transferências ou pagamentos por solicitações feitas apenas por mensagens, principalmente se o destinatário for uma terceira pessoa. Ative no aplicativo de mensagens a opção de verificação em duas etapas e permissão para que apenas os seus contatos tenham acesso à sua foto de perfil e antes de transferir qualquer valor, ligue e conforme diretamente com o solicitante.

- Golpe do “Posso te ajudar?”

O fraudador aborda pessoas com dificuldade nos caixas eletrônicos fingindo auxiliar nas transações e troca o cartão, para realizar transações indevidas nas contas da vítima.

Recomenta-se não aceitar ajuda de estranhos nos caixas eletrônicos e no caso de dificuldades, solicite a ajuda de um funcionário devidamente identificado ou o auxílio de uma pessoa de sua confiança.

- Falso boleto bancário

Os fraudadores falsificam cobranças em boleto para fazer com que o pagamento vá para outros beneficiários em vez de quitar sua despesa.

Para evitar, verifique se o boleto está no padrão normal – procure por erros ortográficos, manchas ou borrões na impressão. Cuidado com boletos enviados por e-mail, redes sociais ou SMS.

Confira os seus dados e do beneficiário do boleto. Verifique se os primeiros dígitos o código de pagamento coincide com o código do banco que aparece como emissor do boleto. Na dúvida você pode entrar em contato com o emissor para confirmar as informações ou emitir uma segunda via do boleto.

A relação completa das fraudes mais comuns e a forma, indicada pelo Banco do Brasil (2022), de como se proteger delas, pode ser vista no Anexo A.

Os bancos Itaú (2022), Nubank (2022) e Santander (2022) apresentam em seus sites, basicamente as mesmas fraudes que são comuns entre seus usuários e os usuários do Banco do Brasil. O método mais utilizado para coletar informações é o

phishing, termo sem tradução para o português, que consiste no envio de mensagens de e-mails, SMS, ligações telefônicas e redes sociais para obter ilegalmente informações como número de documentos, senhas bancárias, números de cartões de crédito e qualquer informação que o golpista possa utilizar para conseguir vantagem financeira (PRODEST, 2022).

Mesmo sendo um banco eletrônico e sem agencias próprias, o Nubank (2022) também tem como principais mecanismos de fraude o método de phishing, prometendo vantagens maiores que as garantidas pelo banco como empréstimos e limites maiores que o cliente poderia ter e o principal meio de divulgação destas mensagens são divulgadas em redes sociais e mensagens do aplicativo de mensagens WhatsApp.

Para o Banco Itaú (2022) as melhores formas de se proteger do método phishing são:

- Nunca forneça seus dados a ninguém. Sempre se comunique com o banco por nossos canais oficiais.
- Nunca entregue seu cartão a outra pessoa. Sempre corte o chip do cartão se for descartá-lo.
- Nunca anote sua senha junto ao cartão. Sempre memorize suas senhas.
- Nunca crie senhas com dados pessoais como aniversários. Sempre use senhas difíceis de adivinhar.
- Nunca clique em links pedindo atualização de dados. Sempre atualize dados junto ao Itaú.

1.4 Ferramentas para desenvolvimento

A seguir as discussões relativas aos recursos que serão usados no desenvolvimento deste projeto de pesquisa.

Será desenvolvido um guia dividido em três partes para descrever as principais fraudes cometidas nos ambientes bancário, comércio físico e virtual. Este guia será redigido para ser uma leitura fácil e rápida no formato de dobra tripla e no seu desenvolvimento será utilizado o editor de textos Microsoft Word. E posteriormente disponibilizadas em formato PDF (Portable Document Format, que em tradução direta significa Formato Portátil de Documento), para que o arquivo possa ser divulgado e compartilhado sem que seja alterado e mantendo as características originais.

1.4.1 Editor de Textos

Segundo Pena (2021), o Microsoft Word vai muito além de um simples editor. Com o Word é possível criar, editar, modificar e personalizar os mais diversos tipos de textos. Além disso, ele conta com inúmeras ferramentas de formatação e implementação de elementos para agregar nos documentos.

Além destes fatores, o Centro Paula Souza disponibiliza gratuitamente para todos os alunos e professores o Microsoft Office 365, que contém o Word, além de outras ferramentas muito utilizadas no mercado de trabalho.

1.4.2 Arquivo no formato PDF

O formato PDF é ideal para a visualização e impressão de arquivos, visto que, uma vez neste formato, ele não pode ser alterado. Um arquivo transformado em PDF é visualizado de maneira idêntica ao seu original, propiciando assim o benefício de se manter a qualidade do projeto. Para que o arquivo em PDF seja visualizado, é preciso ter instalado na máquina ou smartphone o programa Acrobat Reader ou qualquer outro visualizador de PDF (LEOCÁDIO, 2022).

2 METODOLOGIA

Neste Capítulo são apresentadas as considerações relativas à metodologia adotada para o desenvolvimento deste Trabalho de Conclusão de Curso, projeto intitulado DESENVOLVIMENTO DE CARTILHA PARA OPERAÇÕES BANCÁRIAS DIGITAIS SEGURAS. Tais considerações englobam métodos, procedimentos, técnicas e etapas necessárias para o planejamento e consecução do trabalho.

Para o embasamento teórico deste Capítulo, foram utilizadas as contribuições de Marina de Andrade Marconi e de Eva Maria Lakatos (MARCONI E LAKATOS, 2021) e Antônio Joaquim Severino (SEVERINO, 2018). Toda a redação desta monografia baseia-se nas normas da ABNT, obtidas a partir do Manual de Normalização de Projeto de Trabalho de Graduação da Fatec SBC (DUARTE, 2021).

2.1 Classificação da pesquisa

Trata-se de uma pesquisa aplicada, com vistas ao desenvolvimento de um guia para orientar os usuários do sistema bancário sobre os golpes financeiros mais comuns a que todos estão sujeitos, com caráter explicativo, concebida a partir do método hipotético-dedutivo.

Quanto aos procedimentos técnicos (design da pesquisa), este trabalho pode ser classificado como:

– Pesquisa bibliográfica, com a discussão das contribuições de autores da área;

– Pesquisa experimental, com vistas ao desenvolvimento de um produto tecnológico.

2.2 Descrição do projeto

O intuito deste TCC é criar quatro cartilhas que possam orientar os usuários como se defender dessas fraudes. Na primeira serão descritas as fraudes que podem ocorrer quando se utilizam os terminais de autoatendimento dentro das agências bancárias, comércios ou locais públicos.

Na segunda cartilha, estão focalizadas as fraudes que podem ocorrer por aplicativos de mensagens.

Na terceira, estão descritas as fraudes que podem ocorrer ao realizar compras, tanto online quanto de forma presencial.

Na quarta cartilha estão descritos algumas dos formas utilizados para tirar informações das vítimas em métodos chamados PHISHING / SMISHING / VISHING. Que na ordem são golpes que utilizam e-mails, mensagens e ligações na tentativa de fraude.

2.3 Etapas para o desenvolvimento do projeto

As seguintes etapas englobaram aspectos teóricos e práticos:

a) Revisão da bibliografia;
b) Fichamento dos dados bibliográficos;
c) Comparação dos autores;
d) Planejamento técnico do projeto (documentação preliminar, materiais, recursos e ferramentas necessários, fases previstas do trabalho);
e) Desenvolvimento – construção do projeto, destacando as fases que o compõem, o passo a passo de sua realização;
f) Análise e discussão dos resultados;

g) Redação final do trabalho e revisão.

2.3.1 Etapas teóricas

A parte da pesquisa bibliográfica (etapas a), b) e c) anteriormente colocadas) foi a primeira atividade desenvolvida depois da delimitação do tema/problema, englobando consultas a sites especializados, manuais, livros, artigos científicos, teses e dissertações universitárias etc., além de livros relativos a metodologia científica.

Todo o material consultado foi fichado e configurou-se como a base para o Capítulo 1 desta monografia (Fundamentação Teórica).

2.3.2 Etapas práticas

As etapas práticas – itens e), f), g) acima – fazem parte do desenvolvimento do projeto (Capítulo 3) e serão concretizadas no sexto semestre do curso.

O item d) – Planejamento técnico do trabalho – refere-se à organização do projeto, fazendo parte deste Capítulo 2 (Metodologia). Esse planejamento é feito no quinto semestre e descreve o passo a passo previsto para o desenvolvimento que será realizado no sexto semestre do curso.

A seguir são apresentadas as fases metodológicas para o desenvolvimento deste TCC.

Primeira fase – Análise da literatura focalizando em segurança bancária.

Segunda fase – Levantamento das dificuldades encontradas pelos usuários dos serviços bancários.

Terceira fase – Escolha dos temas que serão abordados nas cartilhas explicativas sobre como ter mais segurança a utilização dos serviços bancários.

Quarta fase – Escolha da melhor ferramenta para diagramação e desenvolvimento das cartilhas.

Quinta fase – Desenvolvimento da primeira cartilha sobre as fraudes que podem ocorrer quando se utilizam os terminais de autoatendimento dentro das agências bancárias, comércios ou locais públicos.

Sexta fase – Desenvolvimento da segunda cartilha sobre as fraudes mais comuns que podem ocorrer por aplicativos de mensagens.

Sétima fase – Desenvolvimento da terceira cartilha, onde serão descritas as fraudes que podem ocorrer ao realizar compras tanto online como fisicamente.

As cartilhas serão desenvolvidas com os recursos do editor de apresentações Microsoft PowerPoint 365 pela sua vasta gama de recursos gráficos e facilidade de utilização.

3 DESENVOLVIMENTO

Neste capítulo será apresentada a construção do projeto intitulado “Cartilha para Operações Bancárias Digitais Seguras” e quais ferramentas foram utilizadas.

Utilizou-se a ferramenta, disponibilizada pelo Centro Paula Souza a todos os alunos e professores, Microsoft PowerPoint 365 pela grande versatilidade e facilidade de utilização na criação de elementos gráficos impressos.

As páginas estão seguindo as seguintes configurações:

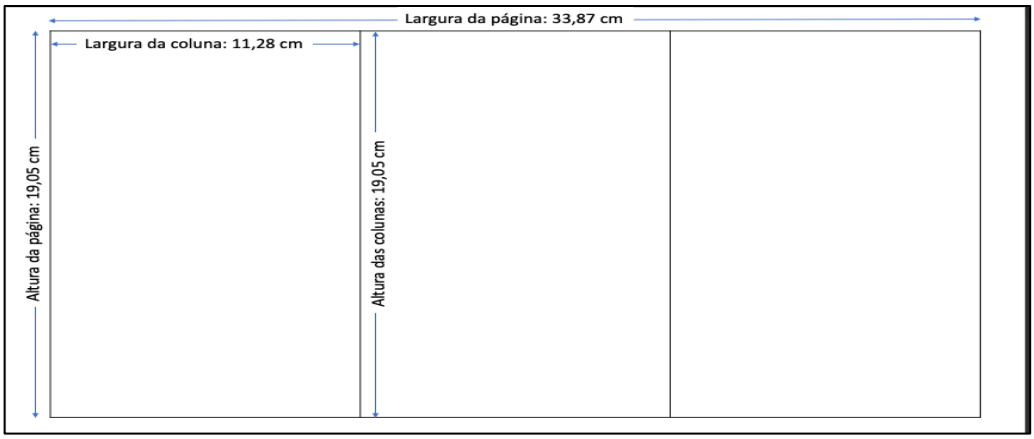
- Largura de 33,87 cm;
- Altura de 19,05 cm;
- Orientação formato paisagem.

Inseriu-se uma tabela com três colunas em cada folha para que pudéssemos fazer as dobras de cada parte da cartilha de forma que cada parte tivesse o mesmo tamanho. Cada parte da tabela tem as seguintes dimensões:

- Largura de 11,28 cm;
- Altura de 19,05 cm.

Dessa forma cada página terá as dimensões apresentadas na Figura 3.1:

Figura 3.1 – Transações bancárias por segmento



Fonte: Autoral

3.1 Legalidade e Segurança das Informações

O projeto das cartilhas atende a LGPD pois se utiliza de dados públicos, mencionados em sites e serve como instrumento para que os usuários do produto saibam como proteger seus dados.

Não existe nenhuma forma de aceite digital pois trata-se de produto físico em mídia impressa (folder em formato “carteira”), sendo assim também desnecessário aceite de termos de uso.

O produto em questão serve para aprimorar a segurança dos dados do usuário final. Maiores implicações com leis precisam ser analisadas por um profissional do meio jurídico certificadamente habilitado para tanto.

3.2 Roteiro do Desenvolvimento

1. Escolha do tema geral e suas implicações e desdobramentos;
2. Delimitação de um tema específico, no caso Transações Bancárias Seguras;
3. Levantamento bibliográfico para embasamento do produto a ser desenvolvido;
4. Levantamento de informações pertinentes ao produto a ser gerado;
5. Escolha do produto, mídia a ser utilizada e formato;
6. Desenvolvimento da Cartilha, com formatação e diagramação e testes de formato;
7. Formatação Final dos produtos a serem apresentados;

8. Término do processo escrito descritivo da criação do produto.

3.3 Resultados

Este trabalho resultou em um conjunto de cartilhas, em formato folder em dobra tipo carteira após análise e discussão entre os autores deste TCC. A princípio se pensou em fazer uma cartilha em formato livreto discorrendo sobre os golpes comumente aplicados e como se proteger, além de informações gerais de segurança para o cliente final, tais como criação de senhas numéricas mais seguras, senhas alfanuméricas mais fortes etc. Encontrou-se a dificuldade de que esse tipo de informação teria de ser transmitido de forma mais rápida e sucinta, então optou-se pelo formato do folder, sendo que se iniciou com 4 assuntos básicos que abordam a utilização dos terminais de autoatendimento, utilização de programas de mensagens instantâneas cuidados nos mercados físicos e os principais métodos utilizados para se conseguir informações por e-mail, mensagens SMS e ligações telefônicas, sendo que existe a possibilidade de se criar e expandir mais ainda, pois são muitos os golpes aplicados e o elo mais fraco nesse meio são sempre o usuário final. Todas as cartilhas podem ser lidas no Apêndice de A a E.

CONSIDERAÇÕES FINAIS

O intuito deste trabalho acadêmico é elaborar uma guia, no caso conjunto de folders, sobre os golpes mais comumente aplicados e suas formas de prevenção. Se visou esse assunto pois um dos autores do trabalho possui atuação no ramo bancário há 16 anos, tendo vivenciado todos os tipos de golpes aplicados contra os usuários do sistema bancário.

Nota-se que com a evolução das tecnologias, os golpes e fraudes também se sofisticam tornando a cada dia mais imprescindível o conhecimento de como se defender de fraudes e outros golpes digitais.

Ao se levantar os tipos de golpes cometidos, notou-se que na grande maioria dos casos o elo fraco é sempre o usuário final, motivo que levou os autores a elaborarem os guias com informações e dicas de como evitar golpes ou roubo de senhas. Nisso notou-se que a maioria dos usuários finais tendem a criar senhas chamadas como de fácil dedução, utilizando-se de datas de nascimento, sequências de números, números repetidos, ou pegam partes de números de documentos ou telefones com a desculpa de facilitar a memorização.

Outro caso de exposição a risco notado foi o empréstimo do cartão da conta para filhos ou pessoas de “confiança” realizarem transações, ato esse que constitui crime de quebra de sigilo bancário. Em casos mais extremos, notou-se o “empréstimo” da conta corrente para recebimento de valores muitas vezes tidos como ilícitos, utilizando-se da chave PIX do cliente que agiu de “boa fé” e emprestou a conta acreditando em uma conversa qualquer.

Após todos esses levantamentos e constatações in loco percebeu-se que o usuário final carecia de maiores informações sobre como os golpes são aplicados e como evitar que eles aconteçam, sendo esse o motivo que levou os autores a produzir este trabalho acadêmico e o produto desenvolvido a partir das informações que é o

conjunto de guias para auxiliar e esclarecer ao usuário final os golpes e formas de evitar.

Futuramente estas cartilhas poderão passar por mudanças e atualizações, baseadas nas tecnologias utilizadas pelos usuários para se comunicarem e pelos fraudadores na tentativa de golpes.

Uma possível atualização para as cartilhas seria a forma de distribuição, que hoje está prevista para o formato de panfleto a ser distribuído em agencias bancárias, podendo passar para formatos digitais através de redes sociais ou mesmo aplicativos de mensagem.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBRISO/IEC 27002: Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação, 2020.

BANCO DO BRASIL. Guia de Segurança – A gente faz de tudo para te alertar e te proteger. 2022. Disponível em: https://www.bb.com.br/docs/portal/disin/Guia-de-Seguranca.pdf. Acessado em: 23/02/2022.

CÂMARA DOS DEPUTADOS. FEBRABAN informa que golpes contra clientes de banco aumentaram em 2021. 2021. Disponível em: https://www.camara.leg.br/radio/programas/823732-febraban-informa-que-golpes-contra-clientes-de-bancos-aumentaram-em-2021/. Acessado em: 21/03/2022.

DUARTE, Jacy Marcondes. Manual de normalização de Trabalhos de Conclusão de Curso da Fatec São Bernardo. São Bernardo: Fatec SBC, 2021. Disponível em: http//www.fatecsbc.edu.br. Acessado em: 15/02/2022.

FEBRABAN – FEDERAÇÃO BRASILEIRA DE BANCOS. Pesquisa FEBRABAN de Tecnologia Bancária 2021, 2021. Disponível em https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-relatorio.pdf. Acessado em: 21/03/2022.

FONTES, Edson Luiz Gonçalves. Segurança da Informação. São Paulo: Editora. Saraiva Uni, 2017.

ITAÚ, Banco. Fraudes e Golpes – Conheça nossas dicas de prevenção e saiba como reportar fraudes. Disponível em: https://www.itau.com.br/seguranca/fraudes-golpes Acessado em: 13/06/2022.

LEOCÁDIO, Rodrigo. O que é PDF? Aprenda tudo sobre este formato digital. Disponível em: https://www.futuraexpress.com.br/blog/o-que-e-pdf/ Acessado em: 17/05/2022.

GOGONI, Ricardo. O que é biometria? Os seis tipos mais usados na tecnologia. 2019. Disponível em: https://tecnoblog.net/responde/o-que-e-biometria-tecnologia/. Acessado em: 20/03/2022.

LOSS, Cíntia et al. Gestão da Tecnologia Bancária: Um Estudo de Caso no BANRISUL. REVISTA SOCIAIS E HUMANAS, [S. l.], v. 29, n.1, p. 58–74, 2016. DOI: 10.5902/2317175822005. Disponível em: https://periodicos.ufsm.br/sociaisehumanas/article/view/22005. Acesso em: 8 jun. 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de Metodologia Científica. 9 ed. São Paulo: Editora Atlas, fev. 2021.

NUBANK, Banco. Aprovação imediata? Pedido da Senha Nubank? Não caia em golpes. Disponível em: https://blog.nubank.com.br/golpes-cartao-nubank/ Acessado em: 13/06/2022.

PENA, Bruna. Como usar o Microsoft Word e potencializar o uso dessa ferramenta. 2021. Disponível em: https://www.voitto.com.br/blog/artigo/microsoft-word Acessado em:17/05/2022.

PRODEST, Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo. Entenda o que é Phifhing e adote medidas para evitá-lo. Disponível em: https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo#:~:text=Ele%20consiste%20em%20tentativas%20de,e%2Dmail%20com%20conte%C3%BAdo%20duvidoso. Acessado em: 13/06/2022.

ROSTI, Andrea. A Importância da Auditoria Para a Segurança da Informação. 2020.Disponível em: https://safewayconsultoria.com/a-importancia-da-auditoria-para-a-seguranca-da-informacao/ Acessado em: 20/03/2022.

SANTANDER, Banco – Segurança da Informação e Segurança Cibernética. Disponível em: https://www.santander.com.br/institucional-santander/seguranca/seguranca-da-informacao Acessado em: 15 mar. 2022.

SEVERINO, Antônio Joaquim. Metodologia do Trabalho Científico. 24. ed. São Paulo: Editora Cortez, 2018.

VANCIM, Flávia. Gestão da Segurança da Informação. 1 ed. Rio de Janeiro, Editora SESES, 2016.

Anexo A – Tipos de Fraude mais comuns

Phishing, Smishing e Vishing	
Descrição	Prevenção
Os fraudadores, assim como na pesca, lançam uma isca, por e-mail, SMS, ligação telefônica, falso site ou falso pop-up inserido em sites desprotegidos. Utilizam-se de ofertas “imperdíveis” ou mensagens com senso de urgência e solicitam que você realize alguma ação, como abrir um link ou arquivo, fazer uma ligação ou instalar/atualizar um software específico.	Não clique em links ou e-mails com ofertas muito lucrativas, em mensagens com senso de urgência com ameaças como “seu serviço será suspenso se...” ou “sua conta foi bloqueada...”. Não abra e-mails ou clique em anexos ou links enviados por desconhecidos. Não repasse códigos de identificação enviados por SMS ou imagens de QRCode.
Falsa central de atendimento	
Fraudadores fingem ser da Central de Atendimento Bancária, simulam o número de telefone e usam de recursos tecnológicos, como gravações e menus para aumentar a sua confiança, solicitam senhas, atualizações de sistemas ou liberações de equipamentos.	Em geral os bancos não solicitam atualizações ou cadastramentos de módulos de segurança, computadores, celulares ou senhas e nem a instalação de softwares ou componentes em navegadores via telefone. Sempre acesse bancos pelos sites oficiais e só instale aplicativos fornecidos por estes sites ou nas lojas oficiais de aplicativos de celulares.
Golpes do WhatsApp	
Existem dois golpes mais comuns: 1- Fraudadores clonam o WhatsApp e se passam por conhecidos e familiares para pedir dinheiro emprestado. 2- Fraudador consegue sua foto e um número de celular de algum contato, criam um perfil falso e mandam mensagens a esse conhecido comunicando a troca de número por algum problema. Depois,	Desconfie de contas com fotos de conhecidos, mas com números diferentes. Não faça transferências ou pagamentos por solicitações feitas apenas por mensagens, principalmente se o destinatário for uma terceira pessoa. Ative no aplicativo de mensagens a opção de verificação em duas etapas e permissão para que apenas os seus contatos tenham acesso à sua foto de perfil.

pedem dinheiro emprestado como se estivessem em alguma emergência.	Antes de transferir qualquer valor, ligue e conforme diretamente com o solicitante.
Falso motoboy	
O fraudador liga para seu telefone fixo se passando por funcionário do banco e faz você acreditar que seu cartão foi clonado. Em seguida, é solicitado que você ligue imediatamente no telefone disponível no verso do cartão. A ligação é supostamente encerrada, porém, o fraudador permanece na linha telefônica. Ao ligar para a Central de Atendimento, o fraudador que permaneceu na linha simula o atendimento da Central. Solicita, então, dados, senhas e orienta que o cartão seja cortado ao meio e entregue a um motoboy que irá até a residência.	Não entregue o seu cartão a ninguém, nem mesmo se estiver quebrado. Bancos não enviam motoboy para recolhimento de cartão. Caso desconfie da ligação, desligue o telefone e retorne para a Central Bancária por outro número de telefone.
Maquininha quebrada	
Esta fraude acontece principalmente em serviços de entrega de comida por delivery. O fraudador cobra um valor maior do que seria o pagamento utilizando uma maquininha de cartão com visor quebrado ou danificado.	Prefira pagar diretamente pelos aplicativos de entrega. Suspeite de cobranças adicionais no momento da entrega. Não aceite realizar pagamentos em maquininhas com visor quebrado ou danificado. Ative o serviço de SMS para receber notificações de pagamentos.
Cadastramento de PIX	
O fraudador finge ser de instituições financeiras para solicitar um suposto cadastro a chave PIX em sites falsos.	Desconfie de links recebidos por e-mail, SMS ou WhatsApp com convites para cadastramento de suas chaves PIX. Não faça transações a pedido de terceiros para suposto teste de suas chaves. Não compartilhe códigos de verificação recebidos por e-mail ou SMS no momento do cadastro das chaves PIX.

Liberação de dispositivos	
O fraudador finge ser funcionário do banco, e por contato telefônico o WhatsApp, cria um senso de urgência sob o argumento de fraude ou de restrições/bloqueios diversos e pede para que você compareça ao caixa eletrônico. Ao chegar na agência, em frente ao terminal, o fraudador diz para você tirar fotos ou filmar a tela do caixa eletrônico, permitindo a visualização do QrCode para autorização de celular ou computador.	Desconfie sempre, bancos não ligam para pedir senhas ou atualizar computadores e celulares. Não tire fotos e nem faça vídeos das telas do caixa eletrônico.
Troca de cartões	
Esta fraude é realizada principalmente no comércio. Os fraudadores ficam de olho na sua senha enquanto você utiliza a maquininha para pagamento. Depois da transação, devolvem a você um outro cartão parecido, mas não o seu.	Não entregue o cartão ao vendedor. Insira você o cartão na maquinha e o mantenha sempre sob supervisão. Caso isso não aconteça, verifique se o cartão devolvido é realente o seu. Fique atento a olhares curiosos e verifique se está digitando a senha no campo correto.
Falso boleto bancário	
Fraudadores falsificam cobranças em boleto para fazer com que o pagamento vá para outros beneficiários em vez de quitar sua despesa.	Verifique se o boleto está no padrão normal – procure por erros ortográficos, manchas ou borrões na impressão. Cuidado com boletos enviados por e-mail, redes sociais ou SMS. Confira os seus dados e do beneficiário do boleto. Verifique se os primeiros dígitos o código de pagamento coincide com o código do banco que aparece como emissor do boleto. Na dúvida você pode entrar em contato com o emissor para confirmar as informações ou emitir uma segunda via do boleto.

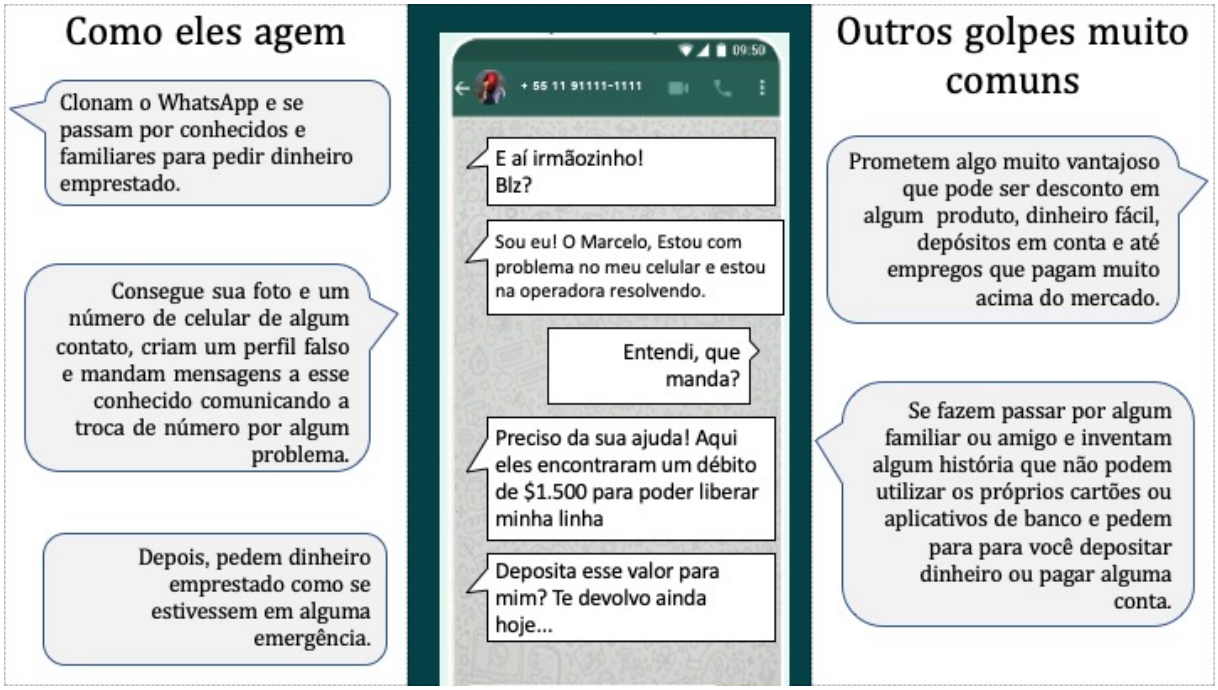
“Posso Ajudar?”	
O fraudador aborda pessoas com dificuldade nos caixas eletrônicos fingindo auxiliar nas transações e troca o cartão, para realizar transações indevidas nas contas da vítima.	Não aceite ajuda de estranhos nos caixas eletrônicos. No caso de dificuldades, solicite a ajuda de um funcionário devidamente identificado ou o auxílio de uma pessoa de sua confiança.
Depósito vazio	
O fraudador entre em contato com alguém que tenha algum anúncio vendendo um bem, tanto em sites de compras pela internet como em redes sociais. Então ele inicia uma negociação e simula o depósito do valor inserindo no caixa eletrônico um envelope vazio. Depois ele encaminha a foto do comprovante do depósito. Como a verificação bancária pode demorar algumas horas, a vítima acredita que o depósito foi realizado e entrega o bem.	Sempre aguarde a compensação do depósito para realizar a entrega do bem.
Falso empréstimo	
Os fraudadores fazem anúncios em redes sociais se passando por instituições financeiras de crédito rápido com ofertas tentadoras. Após o contato da vítima, é solicitado o pagamento de uma taxa para a liberação do empréstimo.	Instituições financeiras nunca solicitam pagamentos prévios para liberação de empréstimos. Não faça pagamentos para liberação de empréstimos. Sempre desconfie de ofertas muito atrativas.

Fonte: Banco do Brasil, 2022

APÊNDICE A – APLICATIVO DE MENSAGENS WHATSAPP

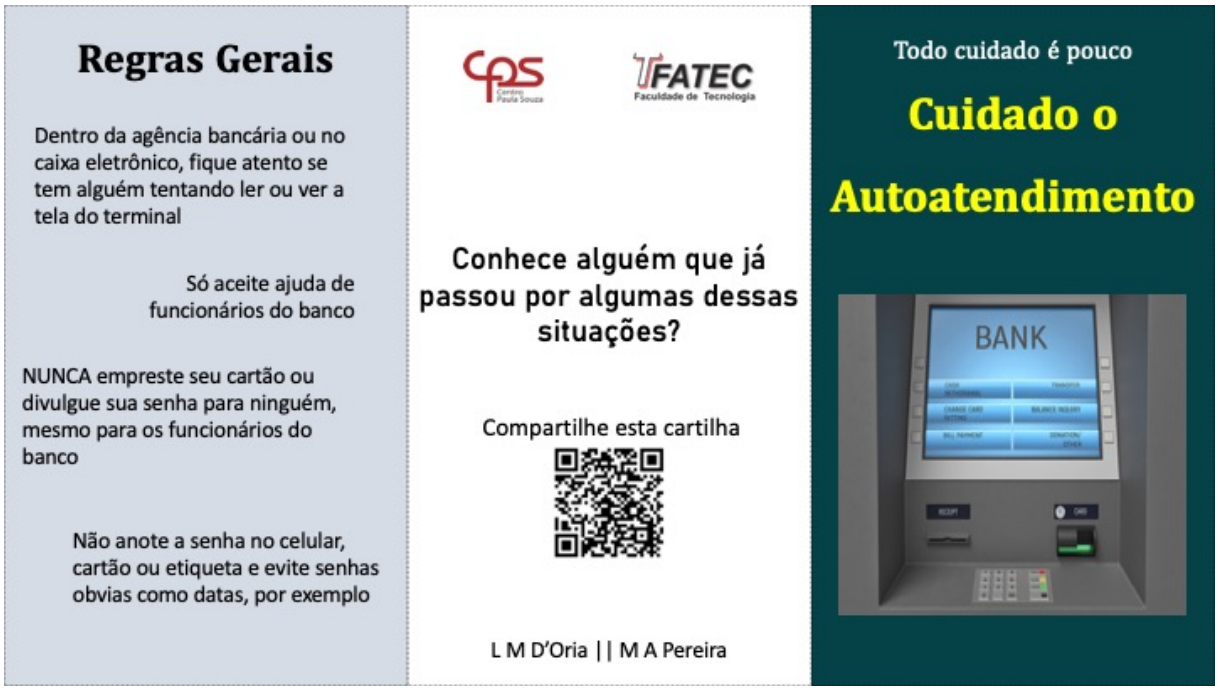
(frente)

(verso)

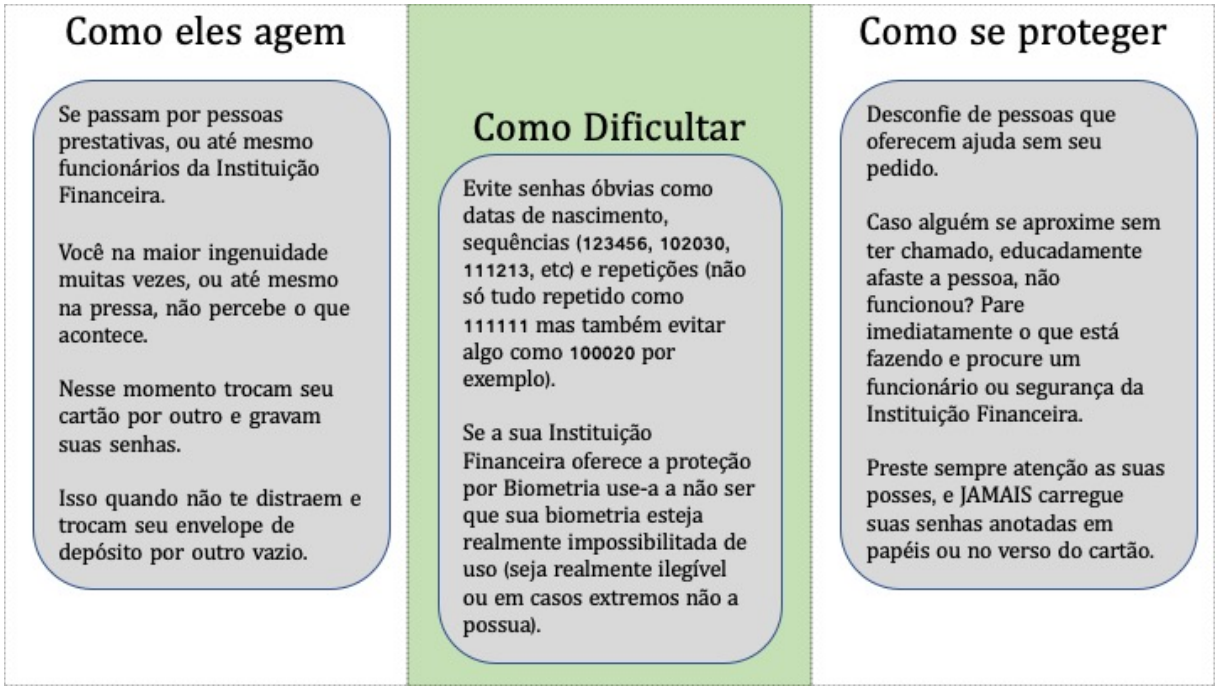


APÊNDICE B – TERMINAIS DE AUTOATENDIMENTO

(frente)



(verso)



APÊNDICE C – FRAUDES NO COMÉRCIO FÍSICO

(frente)

Falso Boleto Bancário

Fraudadores falsificam cobranças em boleto para fazer com que o pagamento vá para outros beneficiários em vez de quitar sua despesa.

Verifique se o boleto está no padrão normal - procure por erros ortográficos, manchas ou borrões na impressão. Cuidado com boletos enviados por e-mail, redes sociais ou SMS.

Conhece alguém que já passou por algumas dessas situações?

Compartilhe esta cartilha

L M D'Oria || M A Pereira

Mesmo nas lojas

Fique de olho no seu cartão

(verso)

Maquininha quebrada

Esta fraude acontece principalmente em serviços de entrega de comida por delivery. O fraudador cobra um valor maior do que seria o pagamento utilizando uma maquininha de cartão com visor quebrado ou danificado.

Prefira pagar diretamente pelos aplicativos de entrega. Suspeite de cobranças adicionais no momento da entrega. Não aceite realizar pagamentos em maquininhas com visor quebrado ou danificado. Ative o serviço de SMS para receber notificações de pagamentos.

Cadastramento de PIX

O fraudador finge ser de instituições financeiras para solicitar um suposto cadastro a chave PIX em sites falsos.

Desconfie de links recebidos por e- mail, SMS ou WhatsApp com convites para cadastramento de suas chaves PIX.
Não faça transações a pedido de terceiros para suposto teste de suas chaves.
Não compartilhe códigos de verificação recebidos por e-mail ou SMS no momento do cadastro das chaves PIX.

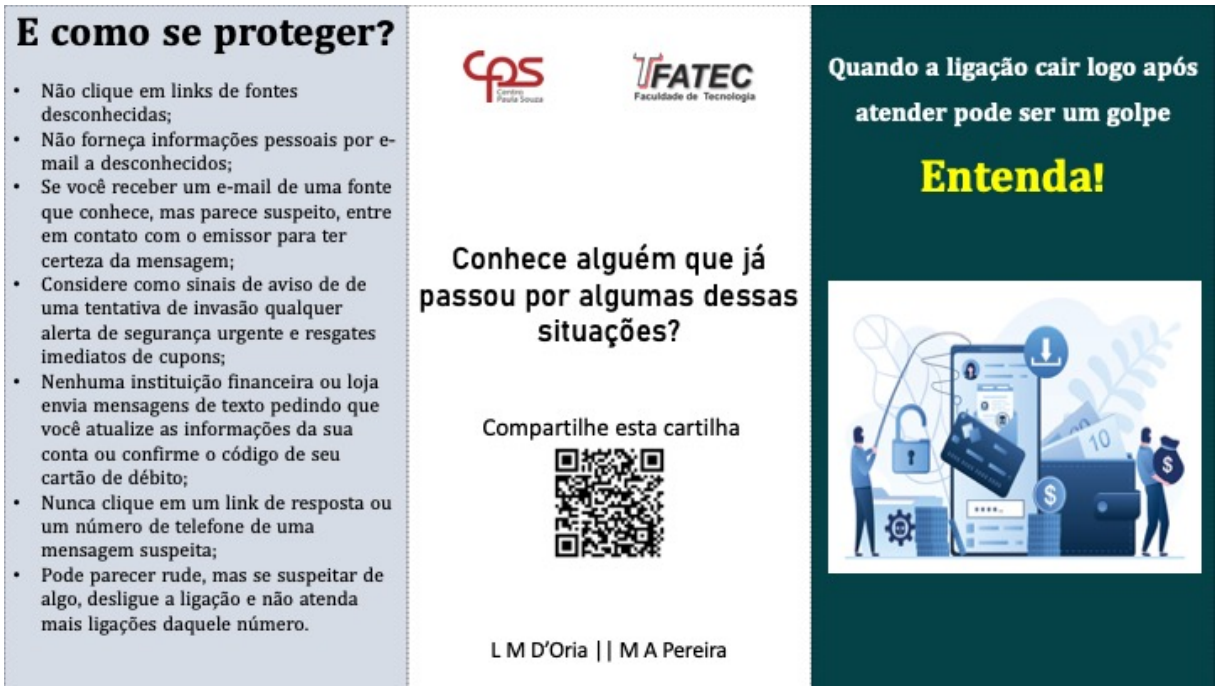
Troca de cartão

Esta fraude é realizada principalmente no comércio. Os fraudadores ficam de olho na sua senha enquanto você utiliza a maquininha para pagamento. Depois da transação, devolvem a você um outro cartão parecido, mas não o seu.

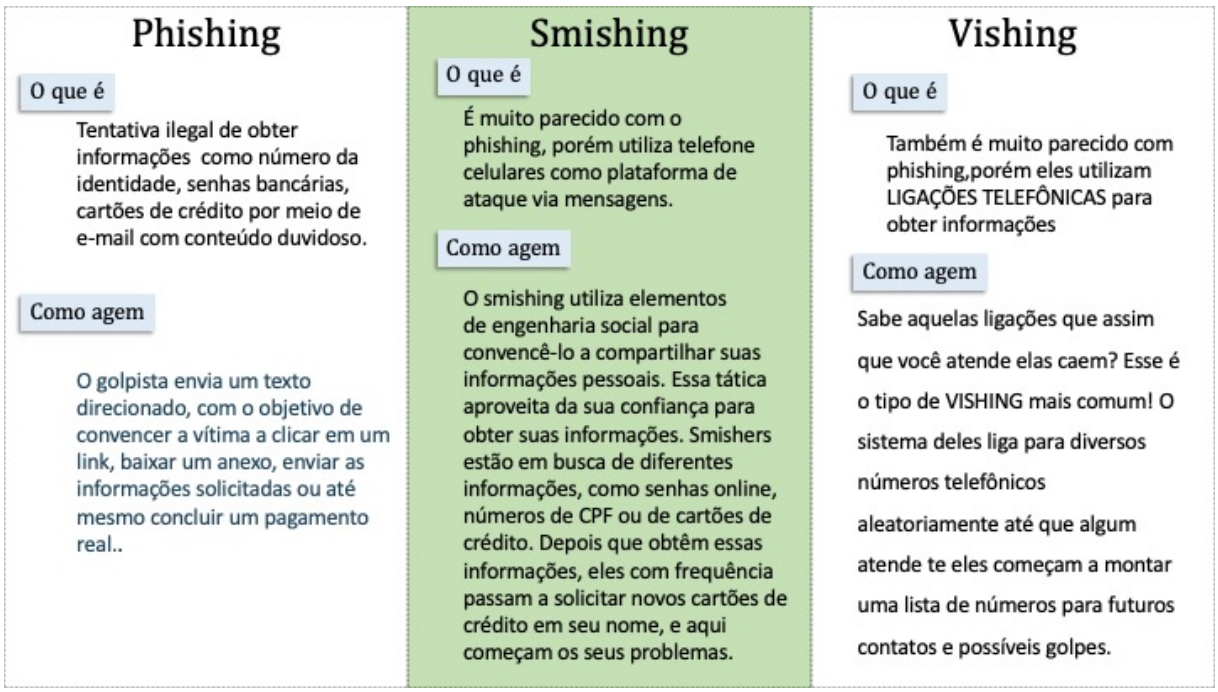
Não entregue o cartão ao vendedor. Insira você o cartão na maquinha e o mantenha sempre sob supervisão. Caso isso não aconteça, verifique se o cartão devolvido é realente o seu. Fique atento a olhares curiosos e verifique se está digitando a senha no campo correto.

APÊNDICE D – Phishing / Smishing / Vishing

(frente)

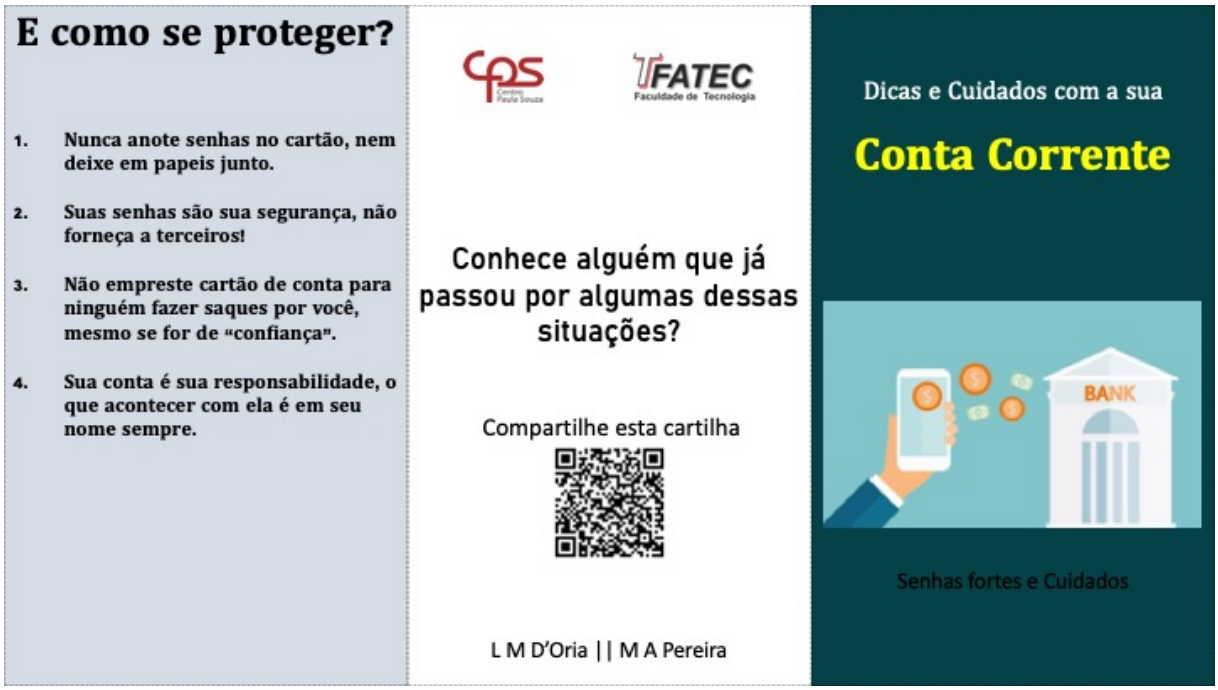


(verso)



APÊNDICE E – CUIDADOS COM A CONTA

(frente)



(verso)