Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Principais tipos de ataques *Phishing* e mecanismos de segurança.

Gama-DF

2021

EDGARD MESQUITA SALVIANO
JOÃO PEDRO RIBEIRO SANTOS
MATHEUS ALMEIDA E SILVA

Principais tipos de ataques *Phishing* e mecanismos de segurança.

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas da Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof. Esp. Helder Line Oliveira

Gama-DF

2021

EDGARD MESQUITA SALVIANO
JOÃO PEDRO RIBEIRO SANTOS
MATHEUS ALMEIDA E SILVA

Principais tipos de ataques *Phishing* e mecanismos de segurança.

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama, 08 de Dezembro de 2021.

Banca Examinadora

Prof. Helder Line Oliveira
Orientador

Prof. Nome completo
Examinador

Prof. Nome Completo
Examinador

Principais tipos de ataques *Phishing* e mecanismos de segurança.

Edgard Mesquita Salviano

João Pedro Ribeiro Santos

Matheus Almeida e Silva

Resumo:

A presente pesquisa refere-se a um estudo sobre segurança da informação, com o foco em ataques do tipo *Phishing*. Com objetivos de descrever os principais riscos que ataques de *Phishing* podem trazer para as pessoas e organizações, indicar as boas práticas com o intuito de reduzir as ocorrências deste tipo de ataque, descrever alguns dos casos já registrado e apresentar dados que comprovem o aumento de ataques de *Phishing* nos últimos anos por meio de gráficos e tabelas. Quanto à metodologia, a pesquisa caracteriza-se como qualitativa, descritiva, sendo desenvolvida por meio de estudos teóricos e bibliográficos. A coleta dos dados foi realizada por meio de pesquisas fornecidas por livros de autores relevantes, sites governamentais e de informações públicas. Os resultados obtidos revelam que grande parte dos usuários ainda estão muito despreparados e vulneráveis a esse tipo de ataque.

Palavras-chave: *Phishing*. Segurança da Informação. Boas Práticas. Ataques.

Abstract:

This research refers to a study on information security, with a focus on Phishing-type attacks. In order to describe the main risks that Phishing attacks can bring to people and organizations, indicate best practices in order to reduce the occurrences of this type of attack, describe some of the cases already registered and present data that proves the increase in attacks of Phishing in recent years through graphs and tables. As for the methodology, the research is characterized as qualitative, descriptive, being developed through theoretical and bibliographic studies. Data collection was carried out through surveys provided by books by relevant authors, government and public information websites. The results obtained reveal that most users are still very unprepared and vulnerable to this type of attack.

Keywords: Phising. Information Security. Good Practices. Attacks.

1 INTRODUÇÃO

O avanço tecnológico vem crescendo nos últimos anos, por conta disso é fundamental ter uma segurança da informação sólida, porque ter eficiência nos três pilares que são a integridade, disponibilidade e confidencialidade é indispensável para o funcionamento dos negócios de uma organização. A quebra de confidencialidade ou a análise equivocada da informação pode se tornar uma grande vilã para as organizações.

Ainda assim, a segurança da informação é um tema muito amplo, pois pode se tratar de segurança física, tecnológica e conscientização organizacional, e cada uma dessas áreas tem suas ameaças específicas, tornando assim os desafios constantes. Dessa forma tornou-se muito importante uma organização focar em proteger a informação, criando normas e diretrizes que garantam a segurança da informação (MORAES, 2010) .

Portanto, o tema deste projeto consiste em analisar problemas que ocorrem com a quebra de confiabilidade por meio de ataque de *phishers* (hackers especialistas no ataque de tipo *Phishing*), o qual de acordo com PINHEIRO (2020), “ainda é o maior vetor de ataques e fraudes cibernéticas em 2020”.

1.1 Problema de pesquisa

Quais os mecanismos a serem adotados na implementação de uma política de segurança em uma organização para tornar a segurança da informação mais eficiente em casos relacionados a ataques do tipo *Phishing*?

1.2 Objetivos do trabalho

1.1.1 Objetivo geral

O objetivo geral deste trabalho é avaliar quais mecanismos a serem adotados em uma política de segurança da informação, visando a redução de ataques de *Phishing*, com o intuito de aplicação em uma instituição.

1.2.2 Objetivos específicos

1. Caracterizar as principais legislações e normas de segurança da informação.
2. Demonstrar como mecanismos de segurança podem evitar a quebra de confiabilidade.
3. Identificar os principais tipos de ataque relacionados ao *Phishing*, que afetam a quebra de confidencialidade dos dados no ciclo de vida da informação.
4. Apresentar as boas práticas de segurança contra ataques ou fraudes relacionadas ao *Phishing*.

2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem como principal objetivo evitar o vazamento e a manipulação de dados e sistemas por terceiros não autorizados, De acordo com Sêmola (2014 p.41), "podemos definir segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."

Os principais pilares da segurança da informação são a disponibilidade, integridade e confidencialidade. Esses pilares devem ser mantidos. Além de outras partes que devem ser levadas em consideração: autenticidade, responsabilidade e confiabilidade.

A disponibilidade visa que as respectivas informações dentro do sistema funcionem sem problemas. Os dados solicitados devem ser recuperados corretamente no momento desejado, o que significa que os sistemas devem ser protegidos contra falhas. De Acordo com Brown (2013, p.7) "Assegurar que o acesso e o uso das informações sejam confiáveis e realizados no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações ou de um sistema de informação."

Na integridade é necessário que os dados circulem ou sejam armazenados de maneira segura, sem que haja interferência de parte externa que possam comprometê-los, causando riscos de perda ou chance de qualquer dano à integridade dos dados. Segundo Netto e Silveira (2007), "a integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental".

Assim, na integridade, a exatidão da informação e uma fluidez do armazenamento seguro dos dados, são questões indispensáveis quando se fala de integridade na segurança da informação. De acordo com KIM e SOLOMON (2014, p.9):

> Integridade lida com a validade e a precisão de dados. Dados que não possuem integridade — isto é, que não sejam precisos ou válidos — não têm utilidade. Para algumas organizações, dados e informações são bens de propriedade intelectual. Alguns exemplos são direitos autorais, patentes, fórmulas secretas e bancos de dados de clientes. Essas informações podem ter grande valor. Alterações não autorizadas podem acabar com o valor dos dados. É por isso que integridade é um princípio de segurança de sistemas.

A confidencialidade assegura que os dados estejam acessíveis apenas para as pessoas autorizadas dentro de uma organização, garantindo que informações confidenciais não sejam roubadas por sistemas por meio de ciberataques entre outras formas. Segundo Moraes (2015, p.9) "A informação não pode ser disponibilizada a quem não tenha a devida autorização para acessá-la. A confidencialidade também é um mecanismo que garante a privacidade dos dados."

2.1 – O que é o *Phishing*

De acordo com PINHEIRO (2020), "O *Phishing* ou *phishing* scam, apesar de descrito desde a década de 1990, ainda é o *maior* vetor de ataques e fraudes cibernéticas." Ainda de acordo com PINHEIRO (2020), o Phishing:

> consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados ou acesso a elevação de privilégios. É uma técnica de engenharia social.

2.2 – Principais tipos de *Phishing*.

São exemplos de alguns tipos de *Phishing*:

2.2.1 – Scam

Tentativas onde os criminosos buscam induzir o usuário a fornecer informações pessoais, como números de contas bancárias, senhas e números de cartões de crédito por meio de abertura de links ou arquivos maliciosos.

2.2.2 – Blind Phishing

O mais comum de todos os ataques *phishing*, é caracterizado pelo grande número de e-mails enviados em teor aleatório, que contam apenas com a "sorte" dependendo se e qual usuário que irá cair na armadilha.

2.2.3 – Spear Phishing

Este tipo de ataque já é direcionado a um grupo específico. Podendo ser contra funcionários do governo, usuários ou clientes de uma empresa e até mesmo para uma pessoa em específico. O seu objetivo é de acessar o banco de dados para a obtenção de informações sigilosas, arquivos confidenciais ou financeiros.

2.2.4 – Clone Phishing

Este método clona um site original para atrair usuários. O foco desse tipo de ataque é obter dados valiosos dos usuários, os quais acreditam estarem no site original, acabam por fornecer estes dados. Os dados mais comuns acabam sendo dados de cartão de crédito. No final o usuário é redirecionado ao site original e acaba por nem perceber que caiu em uma fraude.

2.2.5 – Whaling

Este tipo de ataque tem o foco em pessoas de alto poder executivo, como por exemplo um presidente de uma corporação, e faz isso em nome da empresa para qual trabalha. Estes ataques normalmente vêm atrelados a intimidações judiciais ou notificações empresariais internas. Além de utilizar uma tática semelhante ao do *spear-phishing* visando pessoas importantes, este tipo de ataque utiliza meios como comunicados fraudulentos que fazem parecer vir de uma pessoa experiente ou muito influente na organização, adicionando assim um elemento extra de engenharia social à composição do golpe, pois normalmente os funcionários não recusam uma solicitação de alguém que eles consideram importante.

2.2.6 – Vishing

Neste tipo de ataque *Phishing* é utilizado mecanismos de voz que podem ser acompanhados de SMS (*Short Message Service*) que dizem que o cartão da vítima foi bloqueado e a mesma precisa ligar para um determinado número para solicitar a liberação. Os criminosos usam o VoIP (*Voice over Internet Protocol*) pela facilidade em esconder a identidade de quem faz a chamada.

2.2.7 – Pharming

São ataques envolvendo DNS. Os atacantes envenenam o DNS para atingir os usuários em uma larga escala, que ao tentarem acessar um determinado site digitando a URL (*Uniform Resource Locator*), são redirecionados para uma página falsa criada para o ataque.

2.2.8 – Smishing

Um tipo *Phishing* focado apenas em SMS. São mensagens que geralmente constrangem o usuário com dívidas ou que os influenciam a tomar decisões imediatas pela emoção como sorteios, prêmios ou um valor grande a se receber.

2.2.9 – Engenharia Social

Engenharia social é a arte de explorar a psicologia humana, ao invés de técnicas de hacking, para obter acesso a edifícios, sistemas ou dados. Por exemplo, em vez de tentar

encontrar uma vulnerabilidade de software, um engenheiro social pode ligar para um funcionário e se passar por uma pessoa de suporte de TI, tentando enganar o funcionário para que divulgue sua senha. Segundo Mitnick e Simon (2003, p.VII), " A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é".

A tabela 1, sintetiza e caracteriza os principais tipos de *phishing*

Tabela 1: Tipos de *Phishing*

Tipo de phishing	**Onde ocorre**	**Principais focos**
Scam	Links e arquivos maliciosos	Usuário final
Blind Phishing	Links e arquivos maliciosos com disparos feitos aleatoriamente	Usuário final
Spear Phishing	Links e arquivos maliciosos	Usuário final (funcionários públicos, clientes de empresas) Empresas e bancos
Clone Phishing	Sites clonados	Usuário final
Whaling	Links e arquivos maliciosos	Usuário de alto poder executivo
Vishing	Ligações telefônicas e SMS	Usuário final
Pharming	Link redirecionando para um site falso	Usuário final Empresas
Smishing	SMS	Usuário final
Engenharia Social	Ataques interpessoais	Usuário final

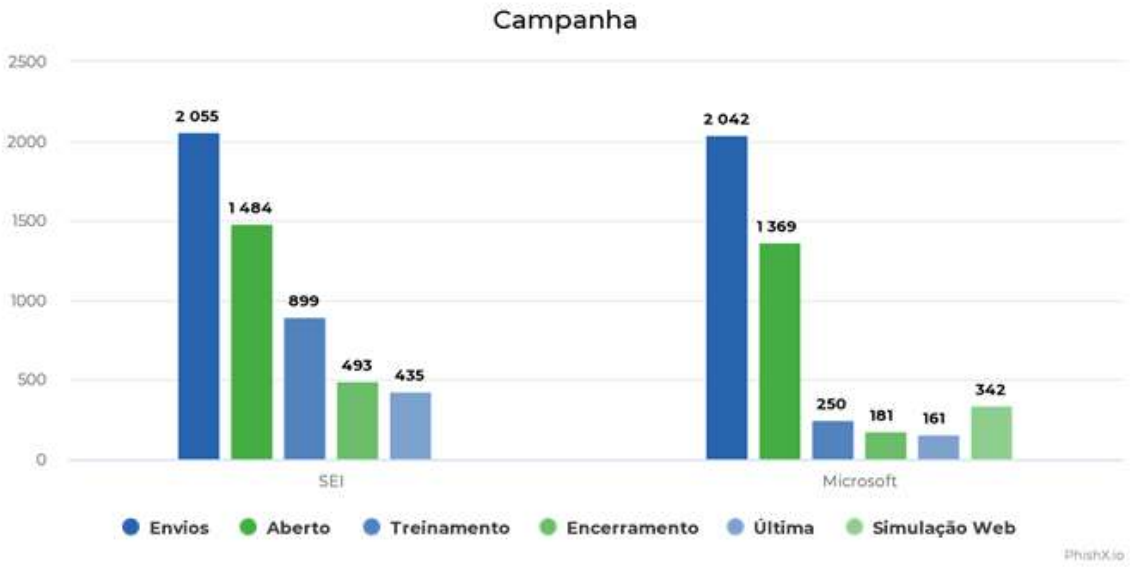
Fonte: Os autores

2.3 – Exemplo de ataque Phishing

Nos dias 15 de julho e 23 de agosto do ano de 2021 a Secretaria Geral do Ministério da Defesa, por intermédio do DETIC (Departamento de Tecnologia da Informação e Comunicação), enviou a todos os seus usuários um e-mail do tipo *Phishing* como parte da campanha de conscientização em SIC(Segurança da Informação e Comunicação), com o intuito de avaliar a sensibilidade e instruir os usuários sobre os riscos de fraude de *Phishing* e evitar que eles sofram com vazamento de dados em possíveis ataques futuros. Após o clique foi disponibilizado um treinamento para os usuários que foram pegos neste teste.

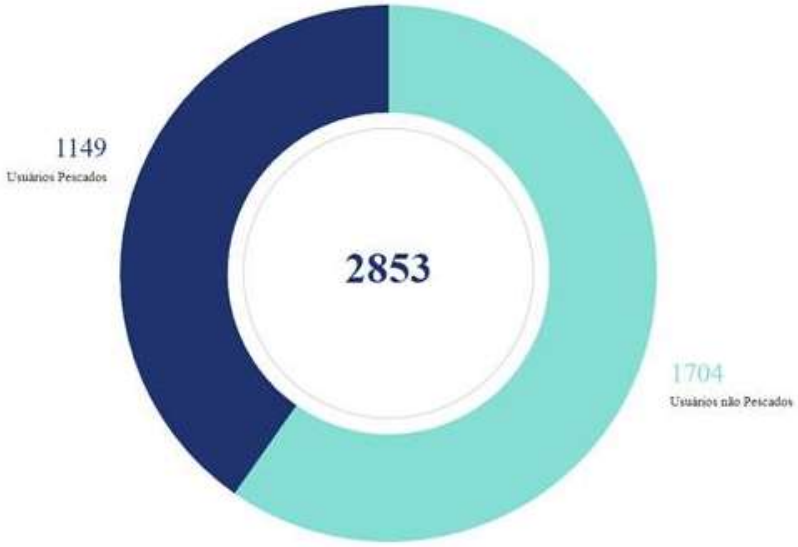
As mensagens foram enviadas em duas plataformas distintas, o Sistema Eletrônico de Informações (SEI) e a caixa de e-mail corporativa Microsoft.

Gráfico 1 – Dados da Campanha



Fonte: Secretaria Geral do Ministério da Defesa

Gráfico 2 – Usuários afetados e não afetados



Fonte: Secretaria Geral do Ministério da Defesa

Como os dados mostram no gráfico 1, ao todo foram enviadas 4097 mensagens de e-mail, onde 2853 (69,6%) dessas mensagens foram abertas. O gráfico 2 aponta que 1149 (40,3%) usuários foram "pescados" e clicaram nos links disponibilizados; 674 concluíram o treinamento disponibilizado após o clique e 596 usuários responderam a pesquisa de satisfação ao final do treinamento.

3 HISTÓRICO RECENTE

Na figura 01 podemos ver alguns dos ataques de *Phishing* entre os anos de 2011 até o ano de 2016. Um dos maiores casos já registrados sobre *Phishing* foi em 2016, quando o grupo que afirma ser afiliado do grupo Anonymous, que se autodenomina AnonSec, conseguiu invadir diversos servidores de diferentes redes da NASA, utilizando métodos de *Phishing*, a partir de apenas um computador. Conseguiu coletar mais de 270 GB de dados sigilosos. Os membros do AnonSec até a data de publicação deste artigo não foram identificados.

Figura 1 – História dos ataques de Phishing(editado)

Fonte: (https://www.elpescador.com.br/blog/wp-content/uploads/2016/05/ep-info_linha-do-tempo.jpg)

O site APWG (*Anti-Phishing Working Group*), organização que se dedica à prevenção, detecção, combate e monitoramento do *Phishing*, em seu relatório trimestral divulgou dados sobre os setores empresariais que mais receberam ataques no último ano de 2020, onde a área de comércio eletrônico foi o que mais sofreu ataques.

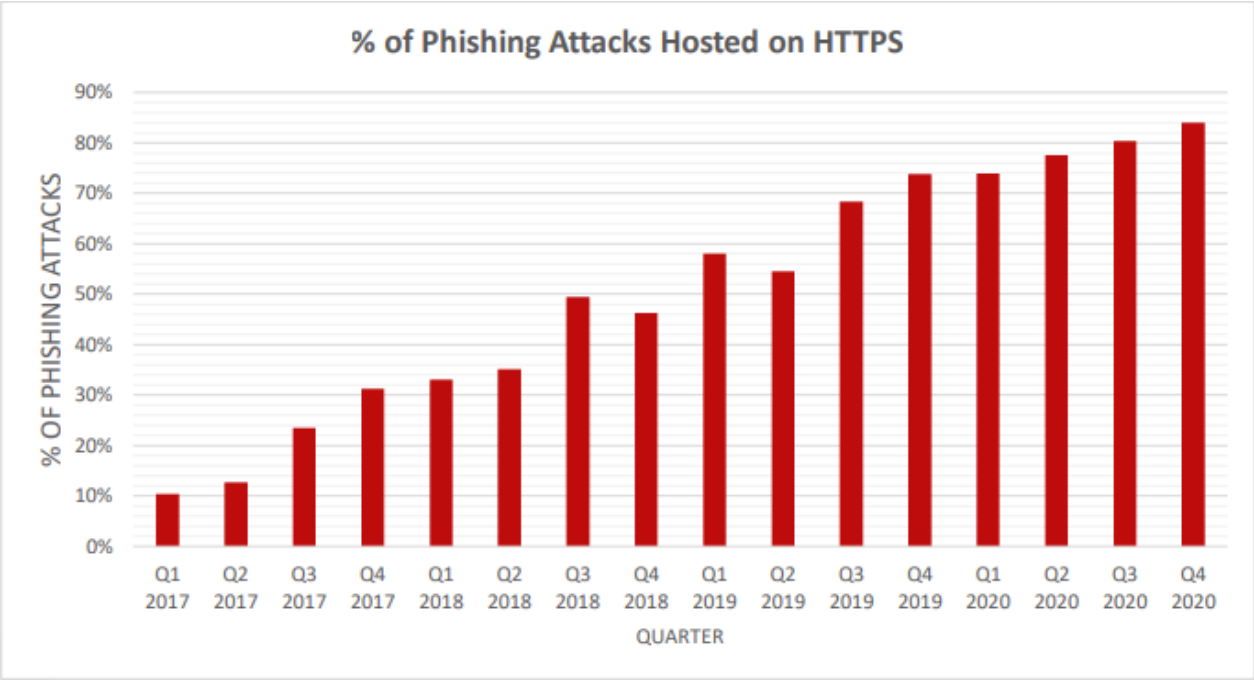
Gráfico 3 – Phishing no Brasil entre os anos de 2019 e 2020

Fonte:(https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf)

Como podemos ver no Gráfico 3, entre os anos de 2019 e 2020 o número de ataques utilizando esses métodos aumentou consideravelmente.

Ainda no mesmo site, foi publicado o gráfico 04, onde demonstra um aumento na porcentagem trimestral de ataques de sites de *Phishing* entre os anos de 2017 a 2020, sites que são hospedados com a criptografia HTTPS (*Hyper Text Transfer Protocol Secure*).

Gráfico 4 - Porcentagem de ataques de Phishing hospedados em HTTPS



Fonte:(https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf)

É possível notar que ao passar dos anos, a porcentagem de sites desenvolvidos para ataques de fraudes teve um aumento de 10% para 84% ao ano. Foi observado também que 89% dos sites de *Phishing* possuíam o certificado de domínio válido, onde os dados de um site passam por uma criptografia antes de chegar ao servidor.

4 – BOAS PRÁTICAS ADOTADAS

Além de sempre se manter informado sobre os tipos de Phishing, deve-se ficar atento também para os seguintes métodos de prevenção:

4.1.1 – Analisar os e-mails recebidos

Sempre verificar informações ao receber um e-mail, como o remetente, o assunto e links de acesso, as quais podem ser consideradas como métodos que facilitam usuários desatentos a caírem em golpes de *Phishing*. Assim, de acordo com Fontes (2001, p.81):

> Se você receber mensagens com conteúdo indevido, elimine-as de sua caixa postal. Apesar de algumas ações técnicas, em que a organização busca impedir o recebimento de mensagens indevidas, não se consegue fazer com que essa barreira funcione completamente. Nesse caso, sua ação de remover esse tipo de mensagem deve ser imediata. (FONTES, 2001, p.81).

4.1.2 – Utilizar o antivírus mais atualizado

O antivírus é o software principal para impedir que um software malicioso seja instalado em um computador, impedindo dados ao sistema. Deve-se atualizar sempre o antivírus, pois novas definições são adicionadas para conter novos golpes criados todos os dias. Para Fontes (2001, p.66) "Você deve garantir, em casa ou no trabalho, que o programa antivírus esteja ativo no seu computador e corresponda à versão mais atualizada."

4.1.3 – Verificação em duas etapas

É um processo que exige duas formas de autenticar que a pessoa que está tentando realizar o acesso é de fato quem diz ser. Normalmente é enviado um SMS ou e-mail informando um código para realizar a autenticação. De acordo com Kim e Solomon (2014), a autenticação de duas etapas fornece um nível maior de segurança se comparado com a de apenas uma etapa.

4.1.4 – Usar Firewall

O Firewall verifica o tráfego de entrada para verificar se há registros do site em listas negras, impedindo de hackers e phishers se infiltrar no computador ou na rede. Assim, "essa solução permite estabelecer o perímetro de segurança, ou seja, separar e segregar a rede interna, controlando os acessos, e aplicar a política de segurança." (MORAES, 2010, p.161).

4.1.5 – Nunca fornecer informações pessoais

Em geral, links de *Phishing* pedem informações únicas como login e senha, ou até informações financeiras. Em caso de dúvida, o primeiro passo a se fazer é ligar para a empresa ou banco perguntando se tem algum problema com sua conta ou. Para Fontes (2001, p.114):

> Também temos de ter o cuidado de não fornecer, sem necessidade, nossas informações pessoais. Se, por exemplo, ao assinar uma revista você puder participar de uma promoção para uma viagem, bastando apenas preencher um formulário, tudo bem. Essa é a regra do jogo. Mas se o questionário, que parecia simples, começar a indagar sobre características de consumo, hábitos e outros aspectos totalmente desnecessários para o propósito da promoção, fica evidente que essas informações serão utilizadas para outros fins. Você deve estar consciente se vale a pena ou não divulgar esse tipo de informação. (FONTES, 2001, p.144).

4.1.6 – Autoestudo

Como já dito anteriormente, que sempre se deve manter atualizado sobre novos tipos de *Phishing* criados todos os dias, há a opção do autoestudo, onde por conta própria é pesquisado sobre o assunto tanto online quanto em livro sobre segurança.

Para Kim e Solomon (2014), existem algumas vantagens e desvantagens em praticar o autoestudo. Nas vantagens, ainda de acordo com Kim e Solomon (2014), além

de ser uma opção mais econômica, existe a possibilidade de ter mais materiais serem flexíveis, podendo ser uma videoaula ou um livro impresso, como também há a opção de ter um horário flexível e um próprio ritmo pessoal. Entretanto, existem as desvantagens, que para Kim e Solomon (2014) seriam a procrastinação, um resultado válido para o fim dos estudos e uma seleção de recursos de qualidade e com boa informação para o material selecionado.

4.1.7 – Treinamento em segurança da informação

Em contraposto ao autoestudo existem programas educacionais continuados para adultos, que de acordo com Kim e SOLOMON (2014, p.305) "Independentemente da organização, a finalidade da educação continuada é fornecer cursos formais, sem diplomas. Em muitos casos, os alunos já têm diplomas e estão procurando atualizar suas habilidades e conhecimentos." Ainda para Kim e Solomon (2014), existem alguns cursos que atendem várias necessidades de membros da comunidade, alguns exemplos são: classes preparatórias para programas de formação, classes de enriquecimento para adultos, classes em estilo de acampamento de verão para crianças e jovens, treinamento profissional e preparação para certificação.

A tabela 2, sintetiza e caracteriza as principais boas práticas adotadas

Tabela 2: Boas práticas adotadas

Boas práticas	**Como utilizá-las**
Análise de e-mails	Sempre verificar o remetente e o conteúdo dos e-mails.
Utilização de antivírus	Manter sempre o antivírus na atualização mais recente atualizado.

Utilização da verificação em duas etapas	Com a verificação em duas etapas, a proteção a conta ou arquivos será dobrada.
Firewall	Irá manter o computador protegido contra ataques de *Phishing* com outros tipos de ataques a segurança possíveis.
Informações pessoais	Nunca compartilhar informações pessoais com desconhecidos, principalmente senha.
Autoestudo	Se manter informado sobre novos tipos de ataques para prevenção.
Treinamento em segurança da informação	Com cursos formais, para atualizar habilidades e adquirir novas informações

5 CONCLUSÃO

.

A análise do estudo apresentou que a desinformação alinhada com a falta de cuidados por meio dos usuários e das empresas, é um dos principais fatores contribuintes para o grande aumento no número de registros de ataques de *Phishing* ainda nos dias de hoje.

Acredita-se que estes números podem ser drasticamente reduzidos com a implementação de boas práticas e a conscientização dos usuários sobre este assunto, onde na maioria dos casos relacionados a *Phishing*, há uma grande falta de preparo por meio dos usuários, de maneira que os tornam mais suscetíveis a esse tipo de ataque. Outro ponto a ser tratado é em relação aos ativos de segurança, pois como foi descrito neste artigo, é um dos pontos de ataques de *Phishing* devido às vulnerabilidades nos sistemas de segurança, seja em seus firewalls, antivírus ou em falta de verificações de múltiplas etapas.

Considerando as recomendações organizadas na tabela de boas práticas adotadas, apostamos que poderia ocorrer uma diminuição no número de vítimas relacionadas a ataques *Phishing*.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 27002: Tecnologia da informação:** Técnicas de segurança - Código de prática para controles de segurança da informação. 2 ed. Rio de Janeiro: ABNT, 2013.

ALENCAR, M. **Informação, Codificação e Segurança de Redes.** Local: Editora, 2015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595155671/. Acesso em:20/05/2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro, 2002.

BROWN, Lawrie. **Segurança de Computadores - Princípios e Práticas**. Grupo GEN, 2013. 9788595155459. Disponível em: . Acesso em: 05 nov. 2021.

BRASIL. Senado Federal. Comissão parlamentar de segurança. **LGPD**. Brasília-DF: Gráfica do senado federal, 2020.

BROWN, A.B.N.B. M. **Segurança de Computadores e teste de invasão** - Tradução da 2ª edição norte-americana. Brasil: Cengage Learning Brasil, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522121366/. Acesso em:20/05/2021.

DAVID, KIM,.; G., SOLOMON,. M. **Fundamentos de Segurança de Sistemas de Informação.** Grupo GEN, 2014. 9788521635284. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788521635284/. Acesso em: 05 nov. 2021.

FERNANDES, M. **Mecanismos da Segurança:** como funcionam e qual a importância? Disponível em: https://blog.starti.com.br/mecanismos-da-seguranca/. Acesso em:30/05/2021.

FONTES, Edison. **Segurança da informação - 1ª edição**. Brasil: Editora Saraiva, 2001. 9788502122185. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 06 nov. 2021.

IT Security: What is IT Security, and why is IT Security so importante? Disponível em: https://www.hornetsecurity.com/en/knowledge-base/it-security/. Acesso em: 30/05/2021.

MCCLURE, Stuart, SCAMBRAY Joel. **Hackers expostos.** 7ª ed. Editora Makron Books, 2014.

MELANI, R. **7 Principais mecanismos de segurança da informação**. Disponível em: https://unico.io/unicocheck/blog/mecanismos-seguranca-informacao/. Acesso em:30/05/2021.

MORAES, Alexandre. Fernandes. D. **Segurança em Redes - Fundamentos**. Brasil: Editora Saraiva, 2010. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536522081/. Acesso em:20/05/2021.

ROCHA LYRA, MAURICIO. **Segurança e Auditoria em Sistema de Informação**. Ciência Moderna. 2008.

RIBEIRO, C. S. **Segurança da Informação:** O desenvolvimento de uma política de segurança da informação em conformidade com a norma ABNT ISSO/IEC 27002**.** Disponível em: https://monografias.brasilescola.uol.com.br/computacao/seguranca-da-informacao-desenvolvimento-uma-politica-seguranca-informacao.htm#indice_10/. Acesso em: 30/05/2021.

SÊMOLA, M. **Gestão da Segurança da Informação** - Uma Visão Executiva - 2 ed. São Paulo: Elsevier, 2014.

STALLINGS, William. **Criptografia e segurança de redes**. 6ª ed. Pearson Prentice Hall, 2014.