FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES

Iago Piccoli Leite

Engenharia Social: Não seja mais uma Vítima

Porto Alegre
2019

Iago Piccoli Leite

Engenharia Social: Não seja mais uma vítima

Trabalho de conclusão de curso de graduação apresentado a Faculdade de Tecnologia Alcides Maya – AMTEC Curso Tecnológico em Redes de Computadores como requisito parcial para a obtenção do título de Tecnólogo de Redes de Computadores.

Orientador (a): Fagner Coin Pereira

Porto Alegre

2019

Dedicatória

Com muita garra e suor é chegado o momento que se almeja ao longo dos anos da carreira estudantil, a conclusão de um curso superior. Colegas, professores e amigos foram formados nestes anos, muitas ideias nasceram e foram abandonadas nessa trajetória, algumas simplesmente apareceram do nada e acabaram tomando proporções que não se era esperada. A dedicação deste trabalho é para aqueles que mesmo vendo o passar dos anos nunca desistiram de me apoiar, ao meu filho que foi minha inspiração e minha força para erguer a cabeça todos os dias sem medo de tentar ser melhor, a minha mãe que esteve sempre junto mesmo estando distante, a minha avó que mesmo sem entender muitas vezes o que eu estava fazendo estava ali torcendo, a madrinha pelos puxões de orelha e apoio em vários momentos críticos, ao meu padrinho que me auxiliou a chegar até aqui, mesmo observando de longe se mostrava preocupado, a minha prima irmã pelos momentos juntos de lazer e descontração, a minha companheira /suporte, por toda sua compreensão, pelo apoio e incentivo, por muitas vezes ser meu porto de paz.

Resumo

A engenharia social está presente cada vez mais no dia-a-dia de todos os usuários, todos os dias surgem golpes de *Phishing* usando uma nova estratégia, independente da mídia social, sempre aparece algum impostor oferecendo algum serviço, produto ou até mesmo “amigos fictícios” em troca de algum tipo de informação. A conscientização do usuário se faz importante para discernir quando existe a possibilidade de um golpe destes citados acima, atentar-se para a exposição massiva de dados em redes sociais é importante para proteção do usuário e seus dados, assim evitando que algum “atacante” utilize tais informações para fraudar algum tipo de golpe. Existem muitas pessoas que necessitam de um esclarecimento quanto a formas de se precaver quanto a golpes na internet, este projeto traz como objetivo mostrar graficamente esta exposição e auxiliar os usuários que indiretamente ajudaram a montar esta estatística.

Palavras chave: Engenharia social, *Phishing*, redes sociais.

Abstract

Social engineering is increasingly present in the daily lives of all users, every day Phishing scams appear using a new strategy, regardless of social media, always appears an impostor offering some service, product or even “friends fictitious” in exchange for some kind of information. User awareness is important to discern when there is the possibility of a scam from the above, paying attention to the massive exposure of data on social networks is important for the protection of the user and their data, thus preventing any “attacker” from using it such information to defraud some kind of scam. There are many people who need clarification as to how to be aware of scams on the Internet, this project aims to graphically show this exposure and assist users who indirectly helped to assemble this statistic.

Keywords: Social engineering, Phishing, social networks.

Sumário

Índice de imagens

1 - Introdução

Engenharia social é a prática de roubar informação de alguém com base na interação social. Pode ser aplicada a diversas áreas de vivência de um ser humano, podendo ser utilizada em uma simples conversa em um círculo de amizades tanto quanto a um ataque indireto por correio eletrônico. A principal vulnerabilidade é a falta de conhecimento da vítima sobre um determinado assunto ou desconhecimento de procedimentos de alguns fatos que o cercam no dia-a-dia.

Ao longo da evolução das comunicações através de redes sociais temos diversos exemplos: A criação do correio eletrônico (e-mail) em 1971 segundo a editora Abril: (Super Abril, 2011), Twitter desenvolvido em março de 2006, por Evan Williams (Olhar Digital, 2012), o Okut foi criado em janeiro de 2004 por Büyükkökten engenheiro turco do Google, o Facebook foi criado em 4 de fevereiro de 2004 por Mark Zuckerberg (Globo 1, 2014) e WhatsApp criado em 2009 por Jan Koum (Globo 2, 2014).

Segundo o Canaltech, as tentativas de captura de dados do usuário para fins maliciosos têm acompanhado esta evolução, como por exemplo o vírus MORIS e mais recentemente técnicas de *Phishing*. O Termo *Phishing* foi criado em meados de 1996 por cybers criminosos que praticavam roubo de contas da AOL (*America Online*) (UOL, 2014).

No caso do *Phishing*, o fraudador utiliza e-mail, aplicativos e sites que são projetados especificamente para roubar dados pessoais. O criminoso se faz passar por uma pessoa ou empresa confiável enviando uma mensagem para conseguir atrair suas vítimas.

Dessa maneira, ao enviar uma mensagem, o fraudador apenas aguarda até que o destinatário receba e abra a mensagem. Em muitos casos, isso já basta para que a vítima caia no golpe, já em outros é preciso que a vítima clique em um determinado *link* para que o criminoso tenha acesso às informações que deseja.

Este trabalho visa verificar a porcentagem atual de usuários que ainda são afetados por golpes de engenharia social através de *Phishing*, mesmo tendo um vasto material disponível para o público se informar sobre este tipo de ataque.

Nesta pesquisa será mostrada uma estatística de usuários que possivelmente são “fisgados” nestes tipos de ataques, analisando 10 perguntas criadas na plataforma *Google Forms*. A pesquisa será analisada com gráficos indicativos das perguntas, estas perguntas contemplam em sua maioria a análise comportamental das pessoas mediante o a navegação da internet.

Para coleta e análise dos dados será aplicado um questionário elaborado na plataforma *Google Forms*, este questionário deverá passar pelo corpo de segurança de uma empresa na qual aceitou que seus colaboradores participassem de tal pesquisa acadêmica.

O *link* da pesquisa será divulgado através de e-mail, serão enviados 3 e-mails no período de um mês e meio lembrando para quem não respondeu a pesquisa, que o faça, pois trata-se de dados importantes de análise. A pesquisa ficará disponível online até dia 05/12/2019 e será enviada para 100 colaboradores onde se espera que 80% das pessoas respondam.

Após a coleta dos resultados, serão gerados gráficos que indicarão diversas fragilidades na navegação e comportamento das pessoas, o formulário não terá coleta de dados pessoais para não expor quem responder a pesquisa.

A pesquisa será focada nos ataques do tipo *Phishing*, onde uma breve análise comportamental das questões que mostrará pontos fracos a serem reforçados com possíveis treinamentos e palestras.

Na próxima sessão de revisão bibliográfica trataremos de três aspectos do trabalho: o meio, o destino e o local. O meio de ataque é representado por Técnicas de *Phishing* – principais técnicas e exemplos de ataques; o destino final diretamente relacionado ao usuário e a engenharia social – detalhamento aprofundado para as causas e efeitos sobre o tema; e por fim o local onde isso ocorre são as Mídias Sociais – onde ocorrem os ataques.

No capítulo de metodologia será explicada a forma na qual o processo da análise do problema será desenvolvido, na sessão soluções propostas teremos uma explicação da de como a metodologia escolhida será aplicada, assim como no capítulo de coleta e análise de dados será demonstrado o resultado obtido com a aplicação descrita no capítulo anterior.

Na sessão conclusão será mostrado a análise final do trabalho com a apresentação do conteúdo elaborado para resolução do problema, assim como

considerações a respeito do que foi desenvolvido e por último o capítulo bibliografia, onde será colocado todas as fontes de pesquisa deste trabalho.

1.1 Delimitação do trabalho

Este trabalho delimita-se ao estudo do comportamento e das instruções de segurança cibernética que os usuários possuem frente às ameaças e técnicas de *Phishing* presentes na utilização da internet durante sua rotina de trabalho, juntamente com uma análise voltada para os costumes pessoais de cada colaborador.

Propor possíveis soluções e formas de conscientizar tantos os usuários que já possuem certo conhecimento na área de segurança digital quanto os usuários não possuem quaisquer instruções de segurança, após a análise de dados coletados com a pesquisa.

1.2 Problema

Uma publicação criada com criatividade e um bom jogo de palavras é postada em uma rede social, sem nenhum alvo específico, apenas aguardando que alguém leia e se interesse, e de forma gratuita ceda um determinado dado pessoal. Esta é a forma mais simples de se descrever um ataque de *Phishing*.

Com a grande exposição de dados pessoais online, há a possibilidade de que qualquer um analise os perfis de usuários que acessam principalmente as redes sociais, pessoas mal intencionadas buscam alvos fáceis que desavisados acabam caindo em golpes diversos.

Estes golpes são elaborados com temas da cultura popular, como filmes que estão em alta na mídia, personagens infantis carismáticos como, por exemplo: personagens como Os Vingadores, a turma da Mônica, dente outros. Neste meio é comum a oferta de pacotes de viagens, entre outros brindes atraentes a fim de chamar a atenção do usuário.

Sabendo de tais informações, foi dado o início a uma análise dos usuários de uma determinada empresa, focando no comportamento e conhecimento sobre

segurança básica ao navegar na internet e as ações que os usuários utilizam para evitar possíveis ameaças como *Phishing*.

2 - Objetivos

2.1 - Objetivo Geral

Este trabalho tem como objetivo geral:

- Alertar os usuários sobre a fragilidade de seus dados e dos malefícios de um click mal pensado.

2.2 - Objetivos Específicos

Os objetivos específicos se resumem em:

- Analisar graficamente o conhecimento dos usuários sobre precaução contra possíveis ataques de *Phishing*.

- Comparar a porcentagem das respostas a fim de verificar o déficit de informação.

- Alertar os colaboradores de uma empresa sobre o risco que correm ao clicar em um link duvidoso.

3 - Revisão Bibliográfica

Engenharia social consiste em estudar o comportamento do ser humano e empregá-lo de forma a fim de se obter informações. Um exemplo de método para engenharia social é o uso de arquitetura de jogos mentais com finalidade de buscar uma informação específica do usuário. Um aspecto alarmante disso, é que engenheiros sociais podem estudar suas vítimas para atacar de um modo mais incisivo como no *spear phishing* (CAMURÇA, 2019).

“O famoso *hacker* Kevin Mitnick ajudou a tornar popular nos anos 1990 a expressão “engenharia social”. A ideia é simples e já existe há muito tempo: enganar alguém para que ela faça ou divulgue alguma informação sensível sem se dar conta disso. Especialistas dizem que os *hackers* continuam a roubar senhas, instalar *malware* em busca de algum lucro empregando uma combinação de táticas novas e antigas.” (BANRISUL, 2019)

De acordo com o site da Kaspersky, em 2018 os Brasileiros foram as maiores vítimas de golpes do tipo *Phishing* no mundo. Este estudo revela que no ano de 2018 aproximadamente 23% dos internautas do país sofreram ataques, e em 2017 esta margem foi de 30%. (KASPERSKY, 2018)

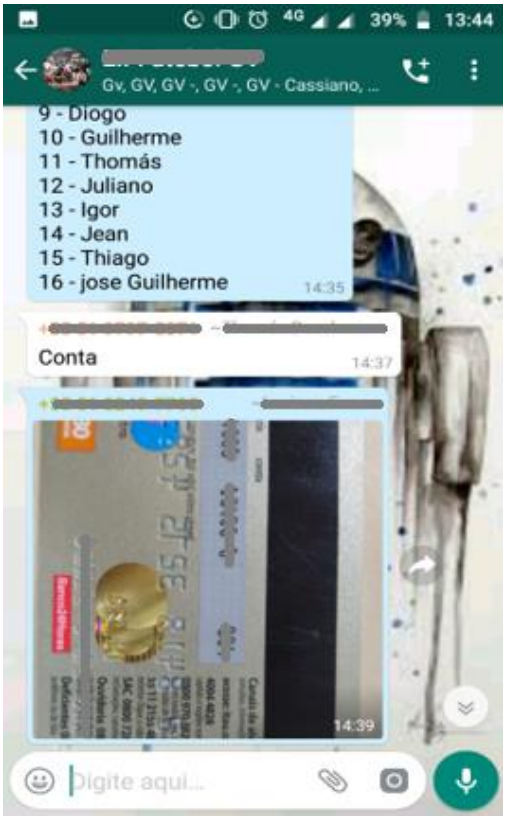
O estudo apresentado indica que quanto maior conscientização sobre a utilização de um antivírus e sobre a exposição desnecessária dos dados pessoais de um indivíduo, menores serão as chances de sucesso de um engenheiro social.

É sabido pelo estudo americano "*Overwork in America*" que pessoas são suscetíveis a erros, grande parte dos erros ou falhas devido a atribuições demasiadas de tarefas (GALINSKY, 2001). Uma sutil distração entre trabalho e lazer, os pensamentos sem foco na tarefa que está se exercendo no momento é o que basta para não ser reservado em suas particularidades para se tornar um alvo fácil.

Um exemplo é caso de exposição demasiada que ocorreu num grupo de WhatsApp no qual faço parte, neste caso o usuário com pressa e precisando fornecer os dados de sua conta, acaba mandando a foto do seu cartão, no caso em questão este estava tentando passar dados de agência e conta para depósito em sua conta, o que exemplifica o fato da engenharia social contar com a

ingenuidade das pessoas, este caso ocorreu em 09/05/2019, conforme pode-se verificar na figura 1.

Figura 1: Cartão exposto no WhatsApp



Fonte: Elaborado pelo autor

Em suma, a engenharia social está muito presente no cotidiano das pessoas, sendo assim, muitas vezes é difícil de identificar. Por mais incrível que pareça, conversas tanto formais como informais são bons estudos para engenharia social pois atacantes podem obter informações tais como nome completo, data de nascimento, telefone, endereço, em alguns casos até dados como RG, CPF.

As pessoas não dão a devida importância para a segurança de seus dados básicos, porém estes dados podem levar a informações mais pessoais, não percebendo assim, que estão sendo atacadas/roubadas. A exposição excessiva em redes sociais pode gerar presas fáceis, como crianças por exemplo.

Podemos ver o caso interessante do falso vidente, apresentado em uma matéria do fantástico uma pessoa se fez passar por guru em uma tenda em um shopping, porém este falso guru contava com diversos especialistas de segurança

da informação que iam mapeando o perfil dos clientes em redes sociais e o golpe ia sendo aplicado (GLOBO, 2012).

Neste caso, o guru possuía um ponto de escuta na orelha onde recebia as informações dos profissionais, aplicando assim um golpe nas pessoas. No final do atendimento era explicado para o cliente que a tenda do guru se tratava de uma matéria para abordar o assunto e tentar fazer as pessoas se conscientizarem quanto a exposição de suas informações pessoais.

O caso dos cartões de créditos personalizados no Tweeter, um usuário publicou fotos convincentes de cartões de crédito personalizados, cobrando um valor para personalizá-lo, onde o cliente teria que passar os dados do seu cartão, nome impresso, data de validade e CVV. Segundo CAMURÇA, 2019 tiveram duas pessoas caindo no golpe em questão de minutos, e de 27 a 30 de maio de 2019 a publicação alcançou mais de 27 mil curtidas e 11 mil *retweets* conforme se pode verificar nas firas 2, 3 e 4;

Figura 2: *Phishing* no Tweeter 1

Fonte: (CAMURÇA, 2019)

Figura 3: *Phishing* no Tweeter 2

Fonte: Elaborado pelo autor

Figura 4: *Phishing* no Tweeter 3

Fonte: Editada pelo autor

Pode-se questionar se podemos chamar de engenharia social do bem, a técnica utilizada por psicólogos para resolver problemas de seus pacientes, pois muitas vezes estes profissionais têm que descobrir a informação específica ou um conjunto seleto de informações para a cura de um possível trauma, ou auxiliar no desenvolvimento de seus pacientes.

Figura 5: Psicólogo

Fonte: (BlogSaúde, 2018)

Engenharia social inclui diversos métodos perigosos tais como: *Tailgating, Quaid Pro Quo, Pretexting, Baiting, Phishing, Spear Phishing* são bons exemplos de artimanhas utilizadas, para que seja possível a compreensão de como funciona os ataques anteriormente citados, abaixo segue uma breve descrição de como cada um destes funciona:

Figura 6: *Social Engineering-Tailgating*

Fonte: (JUSTISECSECURITY, 2018)

O método *Tailgating* é uma técnica muito antiga, e é usada inclusive em edifícios residenciais. Este método consiste em seguir um dos funcionários de perto até que ele chegue a uma área de acesso controlado eletronicamente. Quando o profissional abre a porta, o criminoso pede para segurar para ele, porque “está atrasado”, em alguns casos o criminoso utiliza algum objeto para

simplesmente impedir que a entrada se feche, sem alarmar sua presença (JUSTISECSECURITY, 2018).

Esse é um dos exemplos de como a simples desatenção aliada ao carisma de uma pessoa mal-intencionada pode dar até acesso físico aos servidores da empresa. De lá, o *hacker* provavelmente terá muito tempo e pouco monitoramento para comprometer os dados como quiser.

Figura 7: *Quid Pro Quo*

Fonte: (NSWorld, 2018)

O método *Quaid Pro Quo* é uma expressão latina significa “tomar uma coisa por outra” e é a origem da nossa palavra quiproquó. Segundo o dicionário Collins (COLLINS, 2019), este método consiste em criar uma confusão na cabeça do usuário. Nesse caso, o criminoso liga para vários números dentro da empresa oferecendo determinado serviço, dizendo que é do suporte de TI e ligou para resolver o problema da pessoa, por exemplo.

Em algum momento, isso será algo que um dos funcionários está esperando de verdade e ele vai acreditar naquele contato. É no processo de “ajudar” o profissional que o *hacker* consegue dados de credenciais que vão permitir que ele tenha acesso ao sistema no futuro.

Figura 8: *Pretexting*

Fonte: (MAILFENCE, 2018)

O método *Pretexting* nome dado a este ataque origina-se da palavra “pretexto”, que é exatamente o que o atacante cria para obter as informações importantes do usuário.

Esta técnica consiste em o hacker poder utilizar vários métodos para convencer o usuário a dar informações sigilosas sobre ele ou a empresa. Podendo ser uma pesquisa falsa ou um perfil falso de rede social que crie uma relação de amizade e utilize essa proximidade para extrair algum dado útil para a invasão (MAILFENCE, 2018).

Figura 9: Baiting

Fonte: (MAILFENCER, 2019)

O método *Baiting* é uma tática que já foi mais comum no passado, quando as mídias físicas de armazenamento eram bastante utilizadas. Mas esse tópico ainda precisa de uma atenção da TI da empresa. (MAILFENCER, 2019)

Neste método conta-se com a curiosidade do usuário oferecendo um brinde como um *pendrive* ou um DVD de um filme popular, até mesmo um CD de música, em um lugar de muita circulação no escritório. Caso algum funcionário curioso morda a isca e tente descobrir o que tem dentro daquela mídia, acaba instalando um malware sem perceber.

Imagem nº 10 – *Phishing*

Fonte: (Avast, 2019)

O método *Phishing* é o tipo mais comum de engenharia social utilizado hoje por criminosos no mundo todo, principalmente por ser barato e escalável para milhares, milhões de contas. Este termo pode ser traduzido como “pescaria”, onde basicamente utiliza a estratégia do envio de e-mails falsos. Neste método o *hacker* cria uma mensagem bem convincente que pode ser de uma loja, instituição financeira ou até do governo. (AVAST, 2019)

Em geral, o texto alerta para algum problema financeiro (que chama mais atenção das pessoas) e termina sugerindo uma solução que envolve o *download* de um anexo. Nesse arquivo, está o *malware* (código malicioso, comumente apresentado em forma de um, programa) que será instalado naquele computador.

Muitas vezes o usuário pensa que o problema foi resolvido ou que não concluiu com sucesso os passos e acaba esquecendo do programa, que fica ativo em uma máquina com credencial liberada para o banco de dados da companhia.

Figura 11: Pharming Phishing

Fonte: (AVAST, 2019)

O *pharming* possui duas formas. A primeira forma os hackers usam algum método para instalar vírus ou outros tipos de *malware* no computador do usuário, este vírus instalado redireciona o usuário que quer acessar um site legítimo para um site falso com a mesma aparência do site desejado, muitas vezes trata-se de bancos, lojas, sites ranqueados com muitos acessos. A outra maneira que o pharming se apresenta é como um redirecionador de links, o criminoso infecta um servidor de resolução de nomes e redireciona os usuários que tentarem acessar um site legítimo para o falso.

Figura 12: *Spear Phishing*

Fonte: (DEEP, 2019)

O método *Spear Phishing* consiste é similar ao *Phishing* comum, anteriormente citado, mas potencialmente mais perigoso por ser focado em uma empresa ou instituição. Neste método, o criminoso elabora seu e-mail a partir de assuntos e fontes que são comuns ao negócio (o banco que ele usa ou um grande fornecedor), às vezes focado em um departamento específico para garantir que pelo menos um de seus profissionais seja enganado. (DEEP, 2019)

Em suma, os seis métodos descritos acima exemplificam o perigo oferecido dessa prática. Um dos motivos para essa periculosidade é a ingenuidade dos usuários. Esses métodos utilizam técnicas quase imperceptíveis para apropriar-se de informações pessoais de uma pessoa. Isso porque muitas vezes utiliza o usuário contra ele mesmo, visto que em grande parte é utilizada por profissionais ou neófitos para o roubo ou apropriação de informações que podem causar algum prejuízo pessoal.

Um caso referente a criptomoedas foi o caso Ethereum Classic ocorrido em 2017, onde várias pessoas perderam milhares de dólares em criptomoedas depois que o site da Ethereum Classic foi hackeado (PAYÃO, 2019), os hackers personificaram o proprietário da Classic Ether Wallet com o uso da engenharia social, assim tiveram acesso ao registro de domínio do site, e redirecionaram este domínio para um servidor próprio. Com isso os *hackers* roubaram as criptomoedas Ethereum das vítimas após incluírem um código no site que permitia a visualização de chaves privadas que são usadas para transações.

Casos de *Phishing* ocorrem quase que diariamente nas redes sociais, o caso mais recente, foi o citado anteriormente “cartões de crédito personalizados em 27/05/2019”, todavia existem diversas situações em que o *Phishing* pode ser

aplicado, em minha visão as situações mais propícias tendem a mexer com financeiro das pessoas e com a vontade de se destacar para outros indivíduos, promoções de itens de qualquer natureza que possa despertar o interesse nas pessoas pelo simples fato de ser algo em comum entre diversos indivíduos e que apresente um custo atrativo, ou o fato de algum trabalho gratuito que alguém, esteja fazendo.

Pode-se precaver os ataques de engenharia social de diversas formas, com a utilização de um bom antivírus, com a aplicação de um *firewall* e se tratando de falha humana, os usuários podem tomar as seguintes precauções:

- Prestar atenção nos links que se pretende clicar.

- Suspeitar e-mails com origens estranhas ou até mesmo as origens conhecidas como bancos.

- Cuidar ao receber anexos nos e-mails, sempre verificando a extensão do arquivo recebido.

- Analisar a informação na qual se pretende expor em redes sociais

- Atentar-se a exposição demasiada de informações ao conversar com pessoas desconhecidas.

4 - Metodologia

Para este estudo foi executada uma pesquisa qualitativa utilizando 10 perguntas sobre a utilização da internet no dia-a-dia das pessoas.

A pesquisa de natureza básica busca tratar estes dados que serviram levantar estatísticas de falhas de uso e atenção quanto a possíveis golpes na internet.

Foi utilizado o procedimento Survey, onde o participante não é identificado, pois está sendo analisado o comportamento geral dos colaboradores de uma empresa.

Esta pesquisa foi enviada para 100 usuários, 81 pessoas completaram o questionário**.**

5 - Solução proposta

Foi criada uma pesquisa utilizando 10 questões envolvendo a utilização da internet e demais costumes de alguns usuários frente a um computado em seu dia-a-dia. As questões apresentadas foram desenvolvidas com o âmbito de verificar a criticidade das exposições que cada indivíduo oferece a falhas na segurança de um acesso, seja pela falta de atenção ou informação dos males que um simples "*click*" pode causar. A composição das questões se deu da seguinte forma:

1-Você sabia que páginas *HTTPS* são mais seguras que *HTTP*? Sites de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados. Você costuma verificar se a pagina utiliza conexão segura antes de cadastrar seus dados?

2-Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao site verdadeiro.

3-Golpistas costumam usar técnicas para ofuscar o *link* real para o *Phishing*. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso. Você verifica o *link* apresentado na mensagem recebida?

4-Quando você deseja acessar um determinado site que conhece o endereço, você digita o endereço conhecido no navegador *Web*, ou você acessa pela pesquisa do Google?

5-Você costuma abrir e-mails ou acessar *links* enviados por pessoas conhecidas?

6- Você considera importante a utilização de antivírus dentro de seu ambiente de trabalho?

7- Você tem o costume de experimentar novos jogos em seu celular, seja por curiosidade, testar o jogo ou porque tem gráficos atraentes?

8- Você costuma salvar arquivos pessoais na sua área de trabalho?

9- Em um de seus grupos de WhatsApp, caso algum conhecido indique ou convide você para um grupo de rede social, você costuma clicar no *link* para fazer parte?

10 - Você costuma clicar em propagandas ou anúncios em redes sociais ?

A análise destas questões pode sugerir a necessidade de uma maior conscientização de como utilizar as redes sociais/internet, evitando que o usuário venha a ser uma possível vítima de truques que utilizam principalmente o *Phishing*.

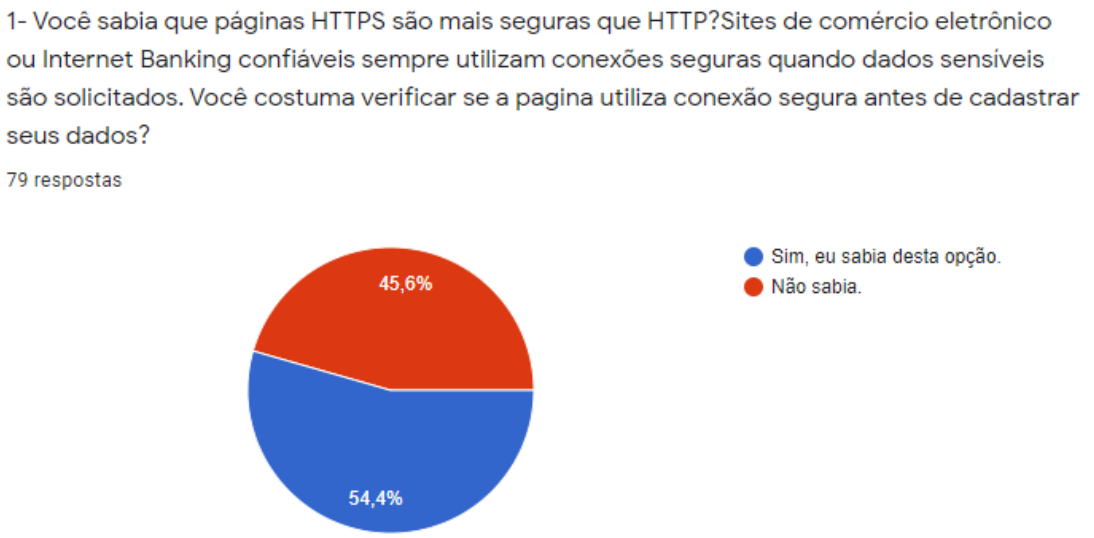
A pesquisa foi criada em 03 setembro de 2019 e foi aplicada em 13 de novembro, a distância das datas de criação e aplicação são atribuídas ao processo que o questionário foi submetido por ser aplicado dentro de uma empresa particular. A pesquisa foi encerrada em 21 de novembro de 2019 para coleta de informações e composição dos gráficos, após a composição do material, encontra-se novamente disponível no link: <https://docs.google.com/forms/d/e/1FAIpQLSc4Hq1rzUV8Bppr0--5fuB13JFoUKGvxgvyVd5aYa5iKk2wsg/viewform?usp=sf_link>

5.1 - Coleta e análise dos resultados

Os gráficos abaixo demonstram o resultado de 81 respostas de 100 questionários disponibilizados.

Na questão um podemos notar que 54,4% das pessoas tinha uma orientação básica de visualizar a barra e endereços do navegador identificando se o site acessado utiliza recursos seguros ou não.

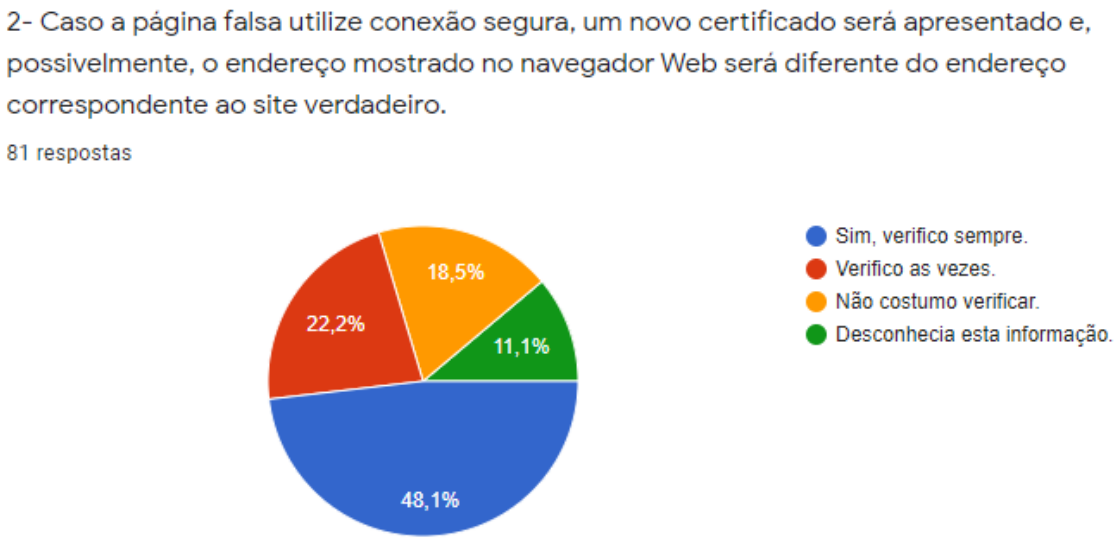
Figura 13: Gráfico pergunta 1



Fonte: Elaborado pelo autor

A questão dois requer que os usuários tenham um pouco mais de conhecimento, podemos ver que 11,1% das pessoas que completaram a pesquisa, não conheciam tal informação, 22,2% responderam que verificam as vezes, e 18,5% não costumam verificar, estes 3 índices somam 51,8% das repostas, que indica a falta de prática ou conhecimento dos usuários em fazer uma checagem mais meticulosa ao acessar conexões possivelmente seguras.

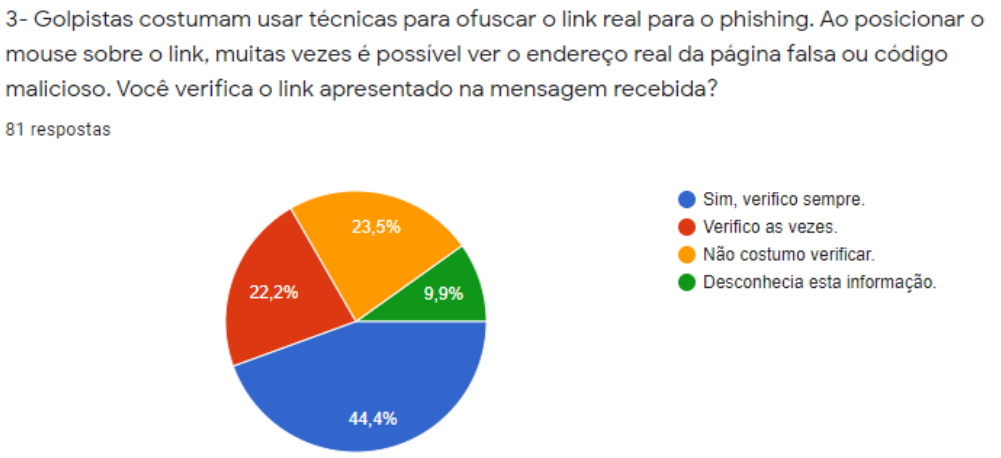
Figura 14: Gráfico pergunta 2



Fonte: Elaborado pelo autor

A Prática da verificação de link como aborda a questão três, é uma instrução que auxilia a evitar muitos golpes e armadilhas na internet. A pesquisa indica que 55,6% não costumam verificar ou verificam as vezes e ou desconhecem a informação, a falta de uma prática simples muitas vezes pode levar a um potencial golpe, o usuário deve buscar analisar com mais atenção onde clica.

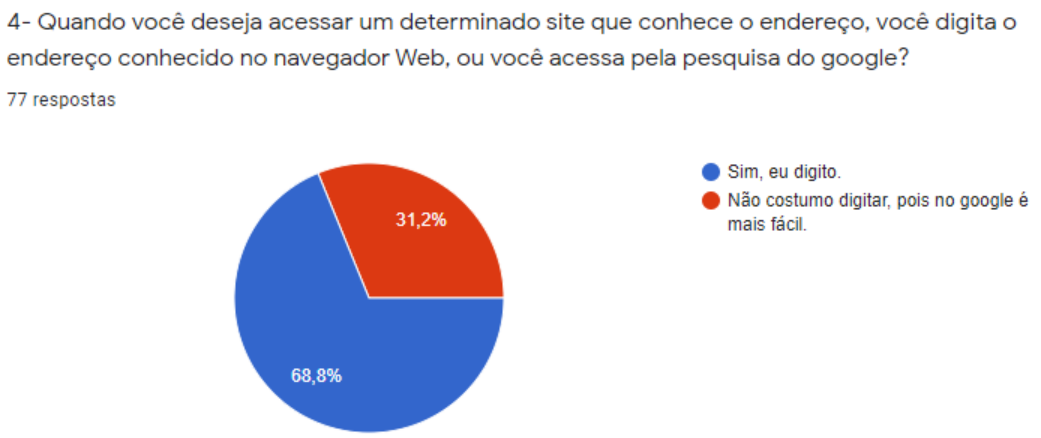
Figura 15: Gráfico pergunta 3



Fonte: Elaborado pelo autor

Na pergunta quatro, o usuário que possui o costume de digitar no Google o site que quer acessar, está sujeito a ser redirecionado a páginas falsas, o indicado neste caso é que ao digitar o site na pesquisa do Google, verifique a URL que o mesmo está apontando.

Figura 16: Gráfico pergunta 4



Fonte: Elaborado pelo autor

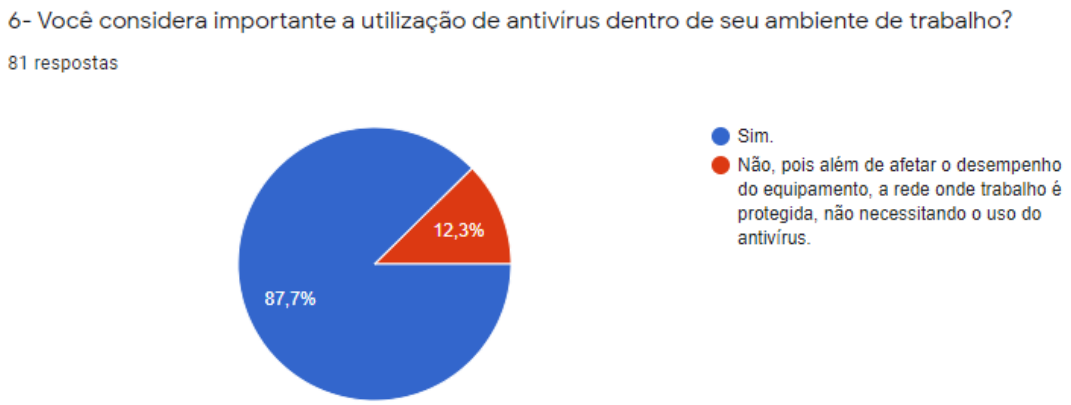
A questão cinco aborda uma ação muito corriqueira para grande parte dos usuários, neste caso a conscientização de checagem de links via e-mail é de 67,9%, mesmo que o remetente seja uma pessoa conhecida.

Figura 17: Gráfico pergunta 5

Fonte: Elaborado pelo autor

A questão seis trata-se do conhecimento de níveis de proteção que se tem dentro do ambiente de trabalho, podemos ver que 12,3% das pessoas não se importam com a utilização de antivírus no meio empresarial, todavia é válido lembrar que em meios residenciais a grande parte da população busca uma proteção por mais simples ou gratuita que esta possa ser.

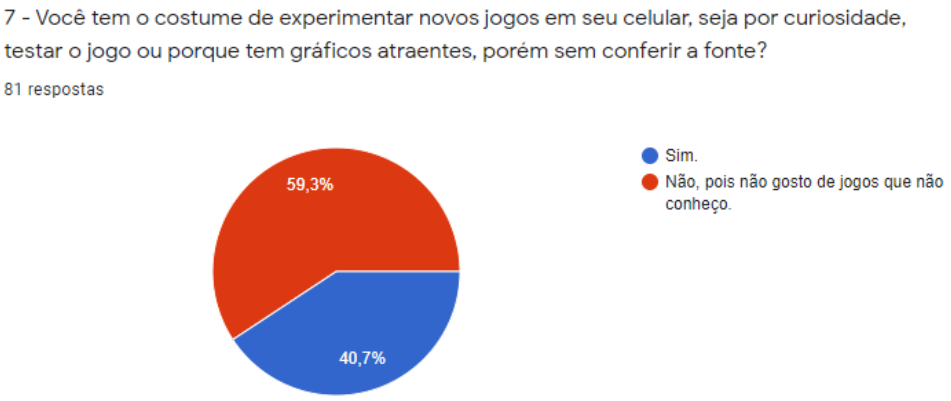
Figura 18: Gráfico pergunta 6



Fonte: Elaborado pelo autor

A questão sete foi elaborada com o intuito de analisar o uso de celulares, como podemos ver 40,7% das pessoas responderam que tem o costume de instalar jogos sem conferir a fonte, quando um possível jogo não é encontrado em uma loja virtual, mesmo que disponibilizado de forma gratuita, este deve apresentar uma origem, quando não se confere a fonte de desenvolvimento ou a fonte de origem do jogo desenvolvido o mesmo pode trazer malefícios ao equipamento do usuário.

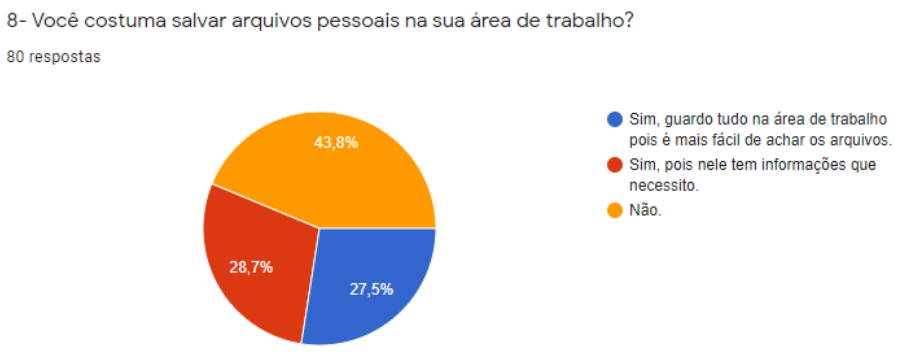
Figura 19: Gráfico pergunta 7



Fonte: Elaborado pelo autor

A questão oito traz à tona o habito de salvar arquivos pessoas na área de trabalho, este hábito pode acabar afetando no desempenho do equipamento além de expor certa fragilidade dos dados pessoais se armazenados em local de fácil acesso, arquivos pessoais podem conter vírus e quando colocado em um ambiente de trabalho pode causar alguns problemas para a empresa caso esta esteja desequipada de um bom antivírus.

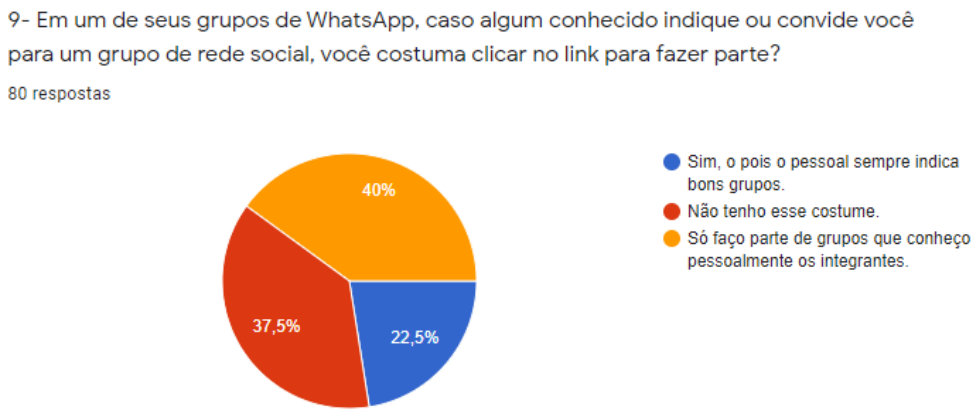
Figura 20: Gráfico pergunta 8



Fonte: Elaborado pelo autor

A questão nove trás uma reflexão sobre confiança, pois nem todas pessoas de um grupo de redes sociais estão dispostos a auxiliar, muitos bandidos abusam de certa “confiança” que um determinado grupo passa para aplicar seus golpes.

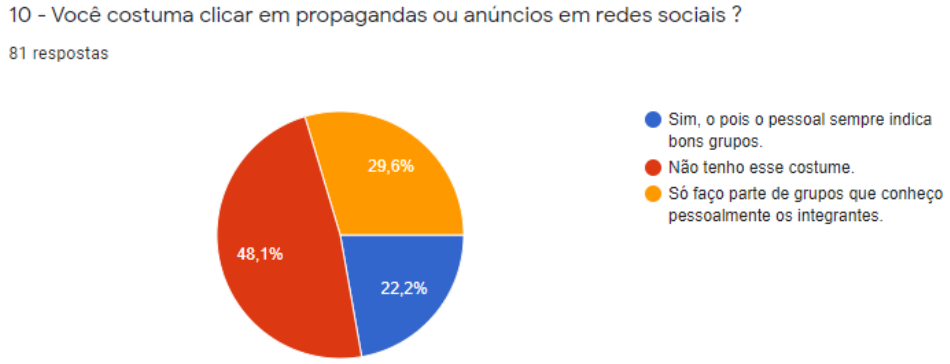
Figura 21: Gráfico pergunta 9



Fonte: Elaborado pelo autor

O Gráfico da questão dez traz a questão dos anúncios em redes sociais, um dos principais focos de armadilhas de Phishing, nota-se que 48% das pessoas não costumam clicar em anúncios de redes sociais, 22,2% clicam por indicação de grupos e 29,6% só compra ao fazer parte do grupo no qual possui pessoas conhecidas pessoalmente, a menor porcentagem neste gráfico refere-se a um mal costume, no qual os usuários tendem a verificar anúncios em que um grupo indica. Deve-se tomar cuidado caso não conheça ninguém do grupo em questão, pois pode ser um grupo de golpistas ou com sorte apenas um grupo de boas indicações.

Figura 22: Gráfico pergunta 10



Fonte: Elaborado pelo autor

6 - Conclusão

É notória a falta de instruções básicas do usuário comum, este déficit de informação em uma empresa pode trazer grandes prejuízos, quando analisado que a porcentagem mínima negativa que a pesquisa alcançou foi de 9,9% na questão três, esta abordava a prática simples de checar se o *link* parece condizer com o que está sendo acessado apenas passando o mouse em cima deste.

Sabendo que esta porcentagem corresponde às pessoas que não obtinham tal informação, esta porcentagem reflete a pior situação, que indica a real falta de informação, em contra partida, obteve-se o resultado de mínimo positivo de 40% na questão nove que se refere ao clicar em *links* de grupos do WhatsApp sem ter noção da confiabilidade do link.

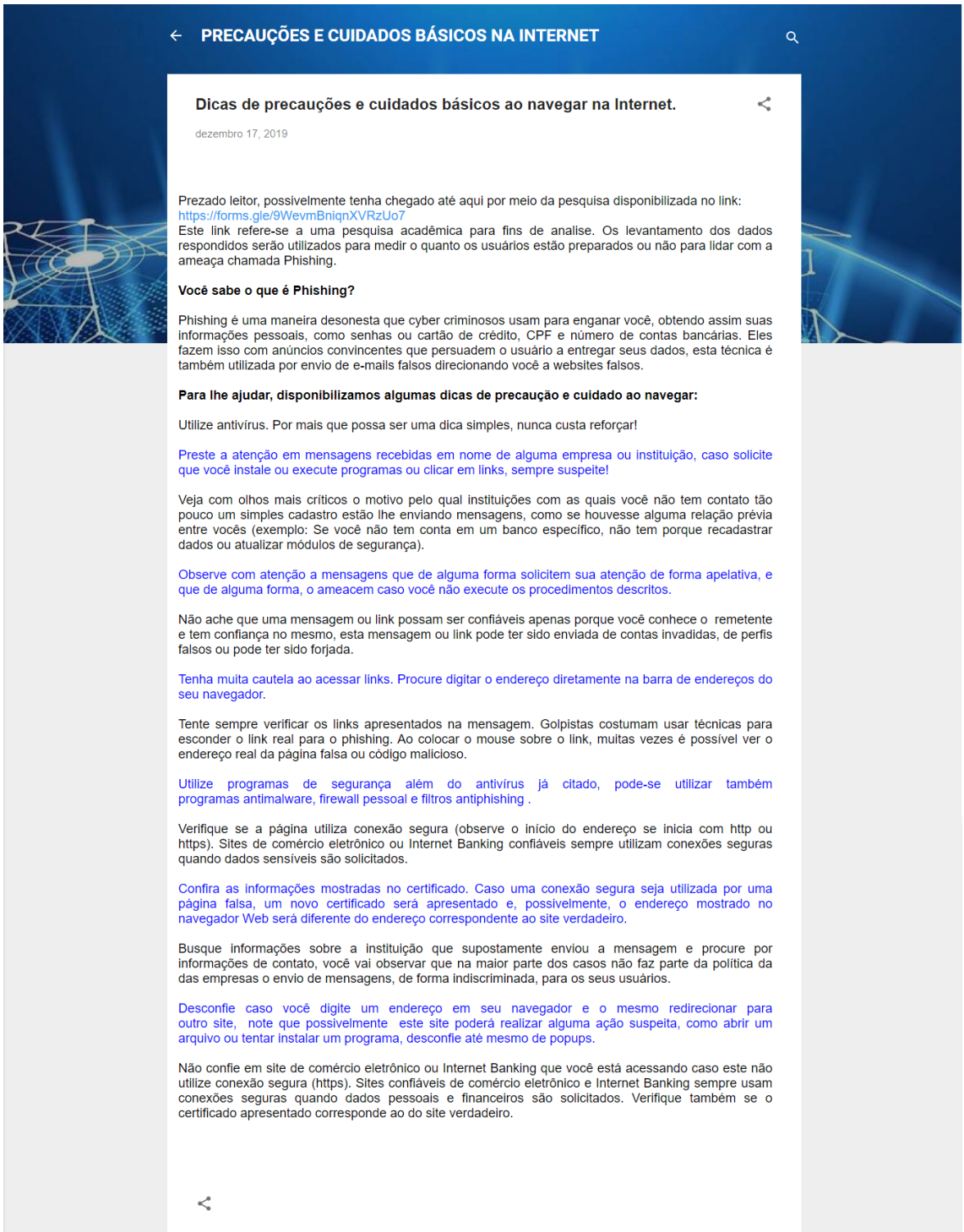
Nota-se que a porcentagem de 59,9% das pessoas que responderam o questionário é de pessoas que possuem um mínimo conhecimento em questão a segurança, no caso de uma empresa esse número é um forte indicativo de que se deve reforçar as instruções simples de segurança para os colaboradores, seja com cartilhas, palestras, e-mails instrutivos, anúncios em portais informativos, dentre outras formas de divulgação.

Pondera-se que a pesquisa indica que a maior parte das pessoas tem um cuidado maior quando o assunto abordado é e-mail, como se pede comparar entre as questões cinco que refere ao click em e-mails ou links enviados por conhecidos, com a questão nove que se trata de indicação de grupos no WhatsApp por conhecidos, as pessoas desconfiam mais independente do remetente quando recebem um e-mail ou link, do que em uma rede social, o que indica também que o foco de atenção também deve ser voltado para redes sociais além do grande foco que sempre foi os e-mails empresariais.

Ao investir na elaboração de um treinamento instrutivo, ou uma palestra a respeito de *Cyber Security* em uma empresa, em contrapartida é possível obter uma grande economia no futuro, quando se tem funcionários conscientizados e que buscam utilizar das melhores práticas indicadas para navegação e utilização da internet, a segurança desta empresa consequentemente aumenta, tornando-a um alvo mais difícil de ser persuadido pelas artimanhas da engenharia social.

Para alertar os usuários foi criado um blog disponível no endereço https://precaucoesecuidadosnainternet.blogspot.com/ com dicas de precauções e cuidados básicos como se pode ver na figura 23.

Figura 23: Blog



Fonte: Elaborado pelo autor

7 – Bibliografia

DÂMASO, Lívia. A História do ORKUT. **Techtudo**, 2014. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/07/historia-do-orkut.html>. Acesso em: 19/09/ 2019.

JULY, Luís. Quem enviou o primeiro e-mail da história? **Super Abril**, 2011. Disponível em: <https://super.abril.com.br/mundo-estranho/quem-enviou-o-primeiro-e-mail-da-historia/>. Acesso em: 05/05/2019.

G1. Facebook completa 10 anos; veja a evolução da rede social. **Tecnologia e Games**, 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/02/facebook-completa-10-anos-veja-evolucao-da-rede-social.html>. Acesso em: 17/04/2019.

GOMES, Helton. Criado em 2009, WhatsApp cresceu mais rápido que Facebook em 4 anos. **Globo1**, 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/02/criado-em-2009-whatsapp-cresceu-mais-rapido-que-facebook-em-4-anos.html>. Acesso em: 17/04/2019.

CANALTECH. O que é phishing?. **Redação**, Disponível em <https://canaltech.com.br/seguranca/O-que-e-Phishing/>. Acesso em: 19/04/2019.

RODRIGUES, Renato. Brasileiros são maiores vítimas de golpes phishing no mundo. **Kaspersky**, 2018. Disponível em: <https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/>. Acesso em: 25/06/2019.

BANRISUL. Cuidados com a Engenharia Social. **Banrisul**. Disponível em: <http://www.banrisul.com.br/bob/download/Banrisul_cuidados_com_a_engenharia_social.pdf >. Acesso em: 17/06/2019.

COBUILD, Advanced English Dictionary. Copyright © HarperCollins Publishers. **Collins Dicionary**, Definição de 'quid pro quo'. Disponível em: <https://www.collinsdictionary.com/pt/dictionary/english/quid-pro-quo>. Acesso em: 25/06/2019.

GLOBO, Play. Conheça o vidente. **FANTASTICO**,2012. Disponível em: <https://globoplay.globo.com/v/2201081/>. Acessado em: 05 de Julho de 2019.

PAYÃO, Felipe. Ataque rouba cerca de US$ 500 mil Ethereum Classic; devs negam. **Tecnomundo**, 2019. Disponível em: <https://www.tecmundo.com.br/seguranca/137691-ataque-rouba-cerca-us-500-mil-ethereum-classic-devs-negam.htm> Acessado em: 04/09/2019.

FOLHA, Uol. Profissional sobrecarregado é mais suscetível a erros e doenças. **Online**, 2005. Disponível em:

<https://www1.folha.uol.com.br/folha/equilibrio/noticias/ult263u3900.shtml>. Acessado em: 20/06/2019.
CURIOSIDADES, UOL. O que é phishing. **UOL**,2014.Disponível em:<https://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-e-phishing.html#rmcl>. Acessado em: 29/09/2019

Trustaira. The Art of Hacking Humans is Social Engineering. **Trustaira Staff**, 2018. Disponível em: <https://trustaira.com/art-hacking-humans-social-engineering/>. Acessado em: 02/10/2019

MATSUNAGA, Igor. Os Principais Golpes de Engenharia Social. **nsworld**, 2018. Disponível em: <https://nsworld.com.br/os-principais-golpes-de-engenharia-social/> Acesado em: 15/10/2019

AVAST. c-phishing. **Avast.** Disponivel em: <https://www.avast.com/pt-br/c-phishing>. Acessado em: 20/06/2019

SOUZA, Valter. o que é pretexting. **Mailfence** , 2018. Disponível em: <https://blog.mailfence.com/pt/o-que-e-pretexting>. Acessado em:25/06/2019

SOUZA, Valter. engenharia social o que é baiting. **Mailfence** , 2018. Disponivel em: <https://blog.mailfence.com/pt/engenharia-social-o-que-e-baiting/>. Acessado em: 25/7/2019

SWINHOS, Dan. Spear phishing: por que ataques direcionados desafiam equipes de segurança. **Computerworld**, 2019. Disponível em:<https://computerworld.com.br/2019/01/22/spear-phishing-por-que-ataques-direcionados-desafiam-equipes-de-seguranca/> .Acessado em: 30/10/2019

TOSTES, Thiago. DIA DO PSICÓLOGO: MARCELA LEAL FALA DA SUA ROTINA NO NEMS/RJ. **BlogSaúde**, 2018. Disponivel em: <http://www.blog.saude.gov.br/index.php/entenda-o-sus/53492-dia-do-psicologo-marcela-leal-fala-da-sua-rotina-no-nems-rj>. Acessado em: 08/05/2019

DEEP, Akash. How To Prevent Spear Phishing Attacks. **Hackernoon**, 2019. Disponivel em: <https://hackernoon.com/how-to-prevent-spear-phishing-attacks-df35b11133b7>. Acessado em: 27/07/2019

STAFF. Art hacking humans social engineering. **Trustaira**, 2018.Disponível em: <https://trustaira.com/art-hacking-humans-social-engineering/> Acessado em: 29/07/2019

STERN, Aauron. Cuidado com as redes sociais: Facebook é o maior portal de phishing. **Kaspersky** 2014 .Disponível em: <https://www.kaspersky.com.br/blog/cuidado-com-as-redes-sociais-facebook-e-o-maior-portal-de-phising/3301/>. Acessado em: 25/09/2019

NOTICIAS, Pesquisa - phishing sites falsos facebook. **33GIGA**, 2018. Disponivel em: <https://33giga.com.br/pesquisa-phishing-sites-falsos-facebook/>. Acessado em: 20/09/2019.

KAULUAN, Bernardo. Uma breve história do Tweeter no brasil. **Olhar Digital** 2012. Disponível em:<https://olhardigital.com.br/noticia/uma-breve-historia-do-twitter-no-brasil/31118>. Acessado em 25/09/2019

AVAST. c-pharming. **Avast.** Disponivel em: < https://www.avast.com/pt-br/c-pharming>. Acessado em: 17/12/2019

GALINSKY, Ellen. FEELING OVERWORKED: WHEN WORK BECOMES TOO MUCH. **FamiliesAndWork,** 2001. Disponível em: <https://familiesandwork.org/downloads/feelingoverworkedsumm.pdf>. Acessado em: 25/09/2019

CAMURÇA, Francisco. Usuários compartilham no Twitter dados de cartão de crédito em troca de customização. **WELIFESECURITY**, 2019. Disponível em: < https://www.welivesecurity.com/br/2019/05/30/usuarios-compartilham-no-twitter-dados-de-cartao-de-credito-em-troca-de-customizacao/> Acessado em: 12/12/2019