INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II
CURSO ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FRANCISCO RANNYSON COSTA SILVA

ANÁLISE PRÁTICA E MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NA ERA DIGITAL

PEDRO II
2022

FRANCISCO RANNYSON COSTA SILVA

ANÁLISE PRÁTICA E MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NA ERA DIGITAL

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Profº. Esp. Cleber da Silva Araujo.

PEDRO II

2022

ANÁLISE PRÁTICA E MITIGAÇÃO DOS RISCOS DA ENGENHARIA SOCIAL NA ERA DIGITAL

Francisco Rannyson Costa Silva Autor [1]
Cleber da Silva Araujo [2]

RESUMO

Este artigo descreve uma análise prática e conceitual de forma simples sobre a Engenharia Social abordando dados desde a coleta de informações de um alvo até o uso de ferramentas de testes de invasão. O trabalho desenvolve conceitos e práticas simples e alerta usuários e empresas quanto aos perigos expostos na internet, e ajuda na proteção da segurança de dados. No período da pandemia, houve um aumento expressivo de golpes realizados na internet, e parte deles envolve Engenharia Social, neste contexto, o tema mostra-se altamente relevante a fim de se conhecer as principais técnicas utilizadas por invasores e como se proteger. Nesta perspectiva o foco do trabalho é mostrar um ataque de phishing real e na prática a fim de alertar os danos e perigos que podem ser provocados.

Palavras chaves: Engenharia social, segurança da informação,phishing,hacker, dados**.**

ABSTRACT

This paper describes a simple conceptual and practical analysis of Social Engineering, from collecting information from a target to the use of intrusion testing tools. The paper develops simple concepts and practices and alerts users and companies to the dangers exposed on the internet, and helps in the protection of data security. In the pandemic period, there was a significant increase in scams carried out on the internet, and part of them involve Social Engineering. In this context, the theme is highly relevant in order to know the main techniques used by attackers and how to protect yourself. In this perspective, the focus of this work is to show a real and practical phishing attack in order to warn of the damage and dangers that can be caused..

Keywords: social engineering, information security, phishing, hacker, data.

1 INTRODUÇÃO

No mundo contemporâneo é inegável que a tecnologia chegou a tudo e a todos. Antes mesmo da pandemia acontecer as pessoas já eram dependentes dos meios digitais, e com o agravamento dessa situação veio a necessidade das pessoas permanecerem conectadas, e com isso, esse número aumentou consideravelmente. Segundo o Jornal Folha de Brasília (2022), após os decretos de isolamentos, boa parte das pessoas, das mais diferentes faixas etárias, passaram a trabalhar em home office e muitos deles não tiveram o menor preparo bem como orientação mínima de se proteger na internet e, com isso, muitos destes usuários expõem

[1] Instituto Federal do Piauí Campus Pedro II. rammysom@hotmail.com
[2] Instituto Federal do Piauí Campus Pedro II. cleber.araujo@ifpi.edu.br

dados sensíveis que podem cair nas mãos de pessoas maliciosas causando prejuízos irreparáveis.

O conceito de Segurança da Informação é necessário para qualquer indivíduo que utilize as redes sociais ou qualquer outro meio conectado à internet Fontes (2017). Se temos todo cuidado ao sair de casa, em estar em uma fila no caixa eletrônico, por quê não teríamos os mesmos cuidados ao navegar na grande rede? O objetivo da Segurança é exatamente impedir, identificar e responder a acessos não autorizados a ativos organizacionais, com intuito de manter confidencialidade, integridade e disponibilidade das informações sensíveis (Devmedia, 2022).

Com a globalização das redes sociais houve um crescimento na quantidade de ataques e golpes na internet (CERT.br, 2022). Diante disso, um termo muito antigo e que voltou após esse processo é a Engenharia Social que consiste em um método que tem como objetivo usar técnicas e ferramentas para persuadir indivíduos ou até mesmo empresas para ter vantagens sobre elas (MITNICK; SIMON, 2003). Em outras palavras estes "engenheiros sociais" aproveitam estas informações coletadas de forma pública para fazerem seus ataques focados no contexto da sua vítima. A falta de informação faz com que aumente a cada dia o número de vítimas desses cibercriminosos. E-mails, por exemplo, estão, muitas vezes, sendo "bombardeados" por pessoas de má índole, que têm por objetivo acessar dados desprotegidos, a fim de tomar algum proveito, na maioria financeiro.

Com a crescente popularização das redes sociais tornou-se mais fácil a coleta de informações de forma muito rápida e perspicaz na estruturação de crimes, afinal, as pessoas expõem muito sobre dados e tornam esse processo para os cibercriminosos mais simples. Com isso, a partir dessas informações coletadas, entra a perspicácia, aplicabilidade, criatividade e o conhecimento do criminoso que irá colocar em prática o cibercrime no qual se aplica a engenharia social.

Neste contexto, este artigo apresenta de forma prática as principais técnicas de Engenharia Social conceituando, assim, as melhores práticas de prevenção evitando danos irreparáveis aos usuários e/ou empresas.

1.1 OBJETIVOS

Nesta seção são explanados os objetivos geral e específicos deste trabalho.

1.1.1 Objetivo geral

Apresentar conceitos sobre engenharia social, descrevendo os perigos e os modos como são feitas as coletas de dados de alvos na internet e ferramentas práticas utilizadas por hackers que auxiliam na eficácia dos ataques digitais. A partir disso, objetiva-se criar mecanismos de defesa contra essas técnicas.

1.1.2 Objetivos específicos

- Detalhar processos e procedimentos de um ataque de engenharia social;
- Apresentar os conceitos e princípios da Segurança da Informação;
- Listar um fluxo lógico de como coletar dados que estão públicos na rede a partir da visão do atacante;
- Entender como as pessoas tratam e conhecem os conceitos de Segurança da Informação e seus comportamentos na internet.

1.2 JUSTIFICATIVA

O Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil (CERT.br), que presta serviços voltados para a segurança da informação e criado em 1997, divulga dados sobre incidentes por ano desde 1999. Segundo dados levantados por esta instituição houve aumento significativo nos últimos dois anos (2020-2021) em incidentes ligados à segurança da informação. Em 2019 foram reportados 875.327 incidentes, período no qual iniciou-se o isolamento provocado pela pandemia da Covid-19. E no ano seguinte houve uma redução destes incidentes que passaram a ser de 665.079 ataques, sendo 3,21 % deste valor foram feitos por cavalos de tróia, 85,15% phishings financeiros e 11,64% outros tipos de fraudes de dados entre janeiro e dezembro de 2020. Com esses números podemos concluir a importância e atualidade da pesquisa e discussão sobre a temática. Com base nos números levantados, este trabalho justifica-se pela necessidade de alertar sobre os riscos da Engenharia Social na atualidade, e como os cibercriminosos estão se valendo disso para conseguir acessar dados e recursos indevidamente tanto de pessoas como de empresas.

1.3 TRABALHOS RELACIONADOS

Nesta seção serão detalhados os trabalhos relacionados ao tema proposto neste artigo.

1.3.1 Engenharia Social: um perigo oculto em simples técnicas

GERALDO no artigo Engenharia Social: um perigo oculto em simples técnicas, o autor descreve conceitos e faz um questionário para validar alguns dados. No artigo em questão o autor sugere que, sejam criadas rotinas de conscientização sobre o tema abordado, que seja uma ação regular e objetivando a participação de membros da empresa que possam identificar ataques maliciosos que venham a prejudicar a empresa e consequentemente evitar cair nesse tipo de ataque (DA S. GERALDO, 2019).

O artigo teve como foco de suas atividades uma revisão bibliográfica, no documento o autor tentou abordar questões relacionadas ao comportamento do usuário de forma ampla. Parecido com o que o nosso trabalho se propõe, porém, mesclar conceitos e prática de Engenharia Social.

1.3.2 O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa

ARAMUNI por outro lado, o trabalho intitulado “O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa” aborda os impactos causados pelo fator humano nas organizações trazendo alguns conceitos sobre o tema. Segundo o autor a sociedade com passar dos anos se torna cada vez mais dependente da tecnologia e consequentemente da informação contida nela, e a engenharia social está em uma ascensão tornando assim, uma das maiores ameaças aos sistemas de informação (ARAMUNI, 2020).

O trabalho abordou tema com foco na conscientização mas, partindo da visão da vítima. O interessante sobre este trabalho é a abordagem feita pelo autor com pesquisas e entrevistas com pessoas envolvidas na problemática do tema. Diferente deste artigo que visa mostrar como funciona as técnicas praticadas por hackers de forma prática. E mostrar também o lado de quem está atacando e mostrar esse processo.

1.3.3 Os Impactos da Disseminação das Fakes News na Sociedade

Santos (2022) aborda e fomenta uma discussão sobre os impactos dos roubos de identidades nas redes sociais e destaca os efeitos causados pela manipulação de massas utilizando fakes news, ele descreve ainda como são os impactos causados na vida das vítimas.

1.4 REFERENCIAL TEÓRICO

Nesta seção serão apresentados os principais termos e tecnologias que serão utilizadas para alcançar os objetivos propostos por este artigo.

1.4.1 Segurança da Informação

Segundo Fontes (2017) a informação é um bem importantíssimo para as pessoas e empresas,visto que vivemos em um mundo interconectados, com isso, devemos ter uma certa cautela com o ambiente em que compartilhamos tudo e, principalmente, com os nossos equipamentos de compartilhamento de informações. O autor reafirma que a informação tem um valor imensurável para organizações, sejam elas públicas ou privadas, e devem ser consideradas por elas como um bem ativo e da sequência, afirmando que uma organização sem informação não tem capacidade alguma de gerir seus negócios. A segurança da informação segue 5 princípios principais sendo elas de acordo com Fontes (2017): Confidencialidade, Disponibilidade, Autenticidade, Integridade e Irretratabilidade.

- A confiabilidade é o princípio em que o sistema deve ser confiável e assegurar que os dados estejam íntegros.
- A disponibilidade é o princípio em que esse sistema deve estar disponível 99.99% do tempo de forma protegida e que dê acesso a quem de fato tem permissão .
- A autenticidade é o princípio que garante que a pessoa que está acessando diz ser ela mesma, e se essa informação for verdadeira esse princípio concede o acesso.
- A integridade da informação é o princípio que garante que as informações armazenadas não sejam alteradas ou comprometidas por pessoas desautorizadas.
- O não repúdio ou irretratabilidade é o princípio que garante que é autoria de algo ou alguém logo, ela está atrelada a algum tipo de informação de assinatura.

1.4.2 Engenharia Social

A Engenharia Social pode ser considerada como a arte de enganar ou manipular pessoas, por meio de técnicas e ferramentas com o objetivo de conseguir dados,informações e quaisquer vantagens sobre determinada pessoa ou empresa. Ou seja, a Engenharia Social tenta induzir usuários que não tenham familiaridade com a tecnologia a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados. Dias (2021) diz que usa-se técnicas manipuladoras e controladoras fictícias em caráter de urgência que tem por objetivo usufruir da ingenuidade da vítima que será lesada.

1.4.3 Tipos de Engenharia Social

Engenheiros sociais dispõem de várias estratégias para fazerem seus ataques. Mas, há dois tipos de ataques que são populares e simples de fazer que são o phishing e o Bait (ClearSale, 2022). Porém, essa técnica não se abstém somente a estes ataques, existem diversos outros, como por exemplo, *pretexting*,quid pro quo, Spear-Phishing e Presencial.

- Pretexting - Criar um cenário fantasioso para induzir a vítima a fornecer seus dados sensíveis.
- Quid pro quo - Fazer com que a vítima acredite em algo inverídico se passando por algo verídico e assim, o atacante cria um solução para aquela situação e assim conseguir instalar software malicioso na máquina do alvo.

- Spear Phishing - São feitos através de e-mail “verdadeiros” e o conteúdo direciona a vítima a um site falso para que seja feita a coleta dos seus dados.
- Presencial - Assim como o atacante pode-se utilizar de ferramentas online também é possível fazer um ataque presencialmente utilizando técnicas de manipulação e persuasão é um pouco mais complexo de se fazer mas, alguns ataques hackers são feitos presencialmente depende muito de como o atacante planejou o ataque.

Com o phishing o cibercriminoso tem por objetivo “pescar” seus dados sensíveis utilizando e-mails, redes sociais e engenharia social que forja comunicações com o alvo, que possivelmente, através do início dessa comunicação o alvo venha a acreditar que está diante de algo legítimo e acaba fornecendo as credenciais como senhas, dados sensíveis e informações de cartão de crédito. Esse trabalho será baseado na técnica Phishing e sobre os seus impactos no século XXI.

1.4.4 Segurança da informação e o fator humano

O fator humano na sua grande maioria é a maior porta de acesso aos dados tanto da própria vítima como para empresas. Fonseca (2017) cita que engenheiros sociais exploram vulnerabilidades humanas como a curiosidade, ingenuidade, medo, confiança e todas essas características emocionais. Pelo uso de técnicas de manipulação e persuasão e a fragilidade do fator humano estão diretamente ligados ao aumento de casos desse tipo de ataque.

1.4.5 Google Hacking

O Google Hacking é uma prática para encontrar arquivos e/ou falhas a partir do Google, usando ele como uma espécie de scanner, inserindo comandos e possibilitando manipular todas e quaisquer buscas avançadas por strings chamadas popularmente pela comunidade de tecnologia de “dorks” ou “operadores de pesquisa”. Com ele, é possível realizar buscas específicas, como por exemplo: “intex fulano intex cpf filetype: pdf”, dessa forma ele buscaria pesquisas sobre um nome específico, cpf e com extensão .pdf. Com ele é possível descobrir informações como: Locais de trabalho, salário, viagens feitas e custeadas em casos de servidores e bolsistas, nome completo, cidade/estado, data de nascimento, e-mail, nomeação em cargos públicos, resultados de concursos, entre outras.

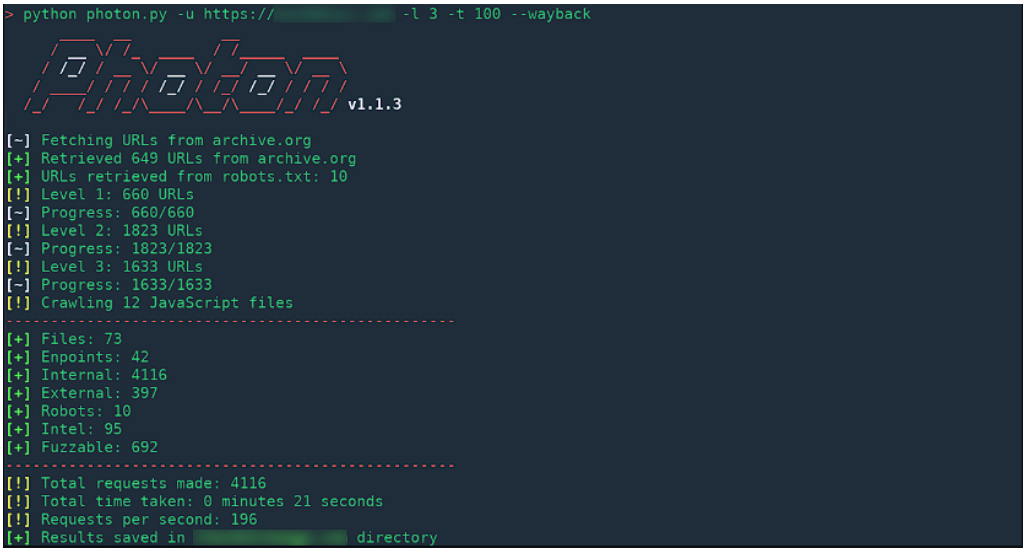
1.4.6 Ferramentas

Nesta seção serão apresentados as ferramentas que serão utilizadas para alcançar os objetivos propostos por este artigo.

1.4.6.1 Photon

Photon é um software criado na linguagem de programação python,open source ele tem como objetivo rastrear dados específicos na web como mostrado na Figura 1. Dados os parâmetros em direção a busca ela retorna todos e quaisquer dados que tenham relação com o que foi pedido para ela fazer. Gerando assim, uma lista de dados mas, caso o atacante queira filtrar algumas informações que ele julgue inútil ou irrelevante para o ataque, a ferramenta dispõe de vários tipos de filtros e tratamentos de dados com intuito de direcionar e trazer somente informações que sejam realmente úteis. (KALI TOOLS, 2022).

Figura 1 - Photon interface

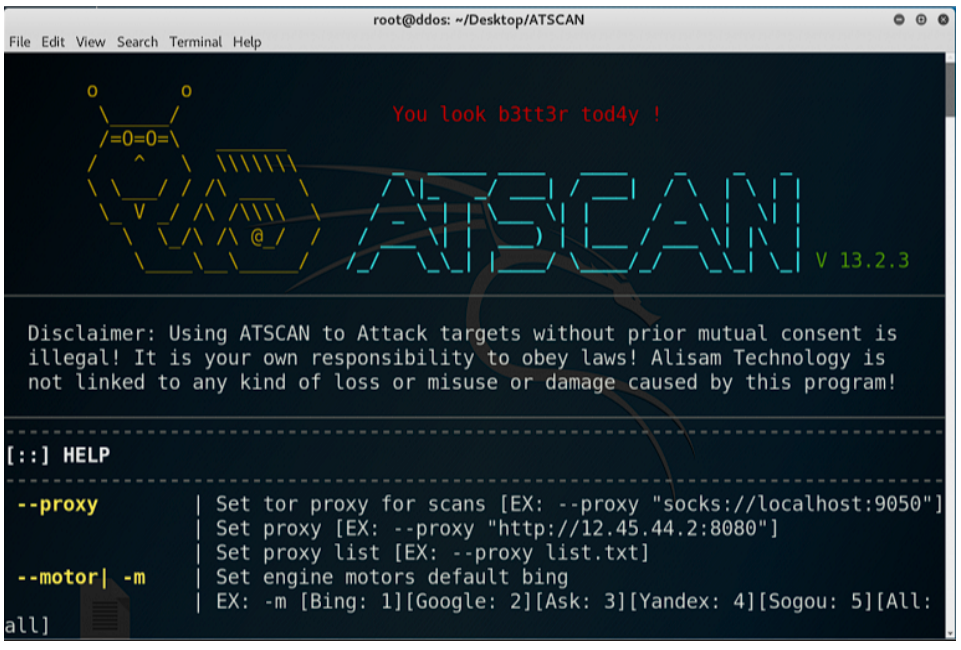


Fonte: Github.

1.4.6.2 AtScan

AtScan é uma ferramenta *open source* baseada na linguagem de programação Pearl criada com objetivo de fazer varreduras utilizando o "*Bing Ask*" e outros métodos de buscas. Este software contém vários outros tipos de ferramentas que auxiliam o seu funcionamento, ele é muito parecido com a ferramenta mostrada anteriormente na Figura 1 e em seguida mostra na Figura 2. No entanto, ela possui um diferencial que é a localização do alvo em tempo real. (ACERVOLIMA, 2022).

Figura 2 - AtScan



Fonte: Github.

O AtScan dispõe de vários tipos de filtragens e dependendo da forma que ela seja utilizada pode-se fazer ataques de *XSS,SQL,LFI e AFD*. Se o atacante precisar criptografar ou descriptografar algo, ele tem acesso a um equipamento auxiliar que usa criptografia *MD5* e de *Base64*. Sendo necessário somente um clique da vítima para que quem está atacando tenha acesso a toda estas informações. O atacante pode, inclusive, pegar ou infectar dispositivos próximos, visto que a ferramenta tem kits que fornecem auxílio de ataque em massa.

1.4.6.3 StormBreaker

O Stormbreaker é *open source* e baseado na linguagem de programação Python, ela é uma poderosa ferramenta capaz de coletar dados sensíveis do alvo como mostra a Figura 3. O Storm Break faz parte de um *tool kit hacker*. (LLUÍS *et al*., 2022). Com pouquíssimo conhecimento é possível ter acesso dos seguintes dados:

- Webcam
- Localização
- Microfone
- E dados detalhados do dispositivo que a vítima está usando.

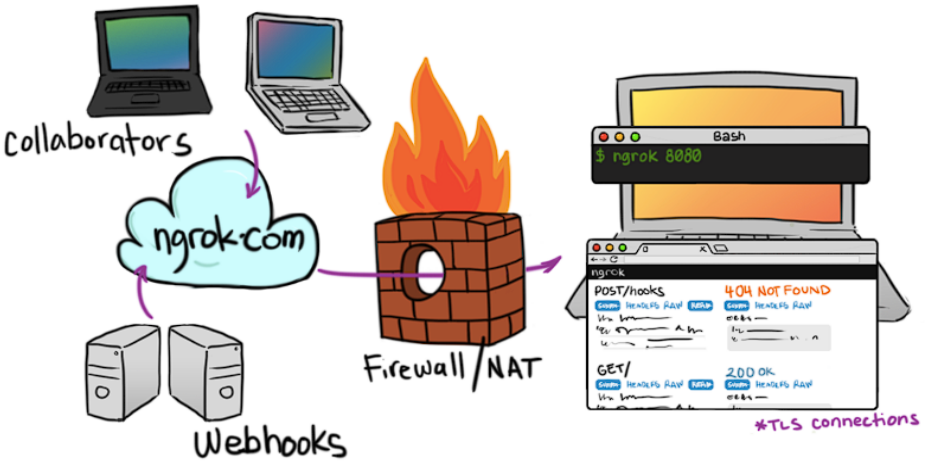
Figura 3 - StormBreaker

Fonte:Github.

1.4.6.4 Ngrok

O Ngrok é um aplicativo multiplataforma que pode criar um *URL* de túnel ou encaminhamento para que as solicitações de Internet cheguem ao computador local. Ou seja, ele é capaz de deixar uma conexão aberta entre o atacante e o alvo, fazendo com que o alvo ao menos perceba essa comunicação como descreve o fluxo da Figura 4. Com ele, é possível criar um link malicioso rodando em um servidor local e disponibilizar seu acesso para a rede externa. (Ngrok, 2022).

Figura 4 - Esquema de Funcionamento do Ngrok



Fonte: Github.

1.4.6.5 Maskphish

Criada na linguagem Bash, o maskphish auxilia na engenharia social e facilita muito a vida do atacante. Basicamente a ferramenta pega um link gerado pelo ngrok ou qualquer outra ferramenta e tenta mascarar para deixar quase que imperceptível para a vítima. (MaskPhishing, 2021). Supondo que a vítima em potencial gosta de futebol, e é um torcedor fanatico do Palmeiras, podemos modificar o *link* gerado pelo Ngrok que é algo parecido com "*https://75bc-45-561-84-105.sa.ngrok.io"* para "*https://www.camisas-oficiais-do-palmeiras-pegue-a-sua-gratuitamente*". Com o *link* camuflado é mais fácil obter sucesso com esta prática. Seu consumo de recursos da máquina é praticamente nulo, se mostrando então com uma ótima ferramenta para mascarar *links* com a logo da Figura 5.

Figura 5 - MaskPhish

Fonte: Github.

2 DESENVOLVIMENTO

Nesta seção são mostradas as etapas de desenvolvimento deste trabalho.

2.1 METODOLOGIA

Para que sejam obtidos os resultados e respostas acerca da problematização apresentada neste artigo, será feita a análise do que diz a literatura e também será mostrado o uso de todas estas coletas de forma explicativa. Além disso, serão detalhados os procedimentos de toda a pesquisa levantadas de forma simples e didaticamente compreensível para que pessoas que não tenham tanta familiaridade com o tema entendam a problemática.

O estudo deste artigo será fundamentado em ideias e hipóteses teóricas que apresentam ponderações importantes na definição e construção dos conceitos discutidos nesta análise, como por exemplo: Engenharia social, segurança da informação, ferramentas hacker, invasão de sistemas, entre outros. Para tal, tais objetos serão realizadas pesquisas para compreender os conhecimentos das pessoas em relação ao tema. Posteriormente serão estudadas fontes secundárias como trabalhos acadêmicos, artigos, livros, website,blogs e afins que foram aqui selecionados para a conclusão deste artigo. Assim sendo, o trabalho será criado a partir do método conceitual-analítico e prático, utilizando conceitos de ferramentas, softwares e ideias de outros autores, semelhantes com objetivos ao deste trabalho para a construção de uma análise científica sobre o nosso objeto de estudo.

O método de pesquisa escolhido favorece a liberdade tanto na análise conceituais e práticos dos dados coletados . Isso possibilita assumir várias posições no decorrer do percurso, não obrigando a entrega de uma resposta única e global a respeito do objeto de estudo. Portanto, podemos afirmar que a engenharia social consiste em múltiplas fases, cada uma projetada para mover o atacante um passo mais perto do objetivo final. Neste trabalho serão realizadas as seguintes etapas de forma prática:

    - 2.2.1 Pesquisa;
- 2.2.2 Coleta de dados públicos sem ferramentas;
- 2.2.3 Coleta de dados com ferramentas;
    - 2.2.3.1 Ferramentas de Coletas de Dados;
    - 2.2.3.2 Hackeando a vítima;
- 2.2.4 Mitigação.

2.2 RESULTADOS

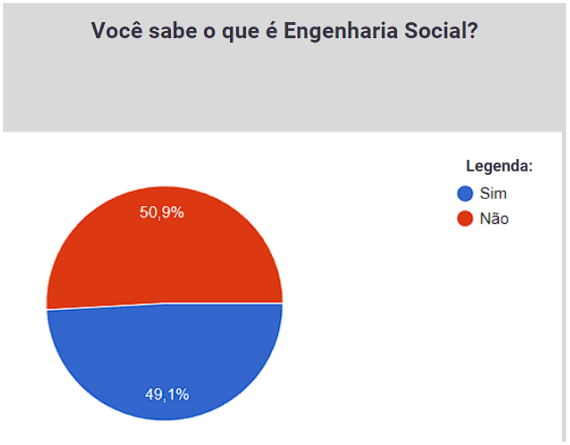
Nesta seção são apresentados os resultados das coletas e práticas deste trabalho.

2.2.1 Pesquisa Quantitativa

Para descobrir o conhecimento das pessoas e preocupação em relação à Segurança da Informação foi criado um formulário através do Google Forms contendo doze perguntas simples e objetivas (disponível para leitura no apêndice) para coletar dados que servirão como base e justificativa para nortear este trabalho. O questionário ficou aberto ao público em geral entre os dias 04 e 11 de dezembro de 2022 e foi divulgado nas mais diferentes plataformas digitais, entre elas: WhatsApp, E-mail, Instagram e Facebook. A pesquisa obteve 114 (cento e

quatorze) respostas. Entre o público pesquisado, 49,1% não sabe o que é Engenharia Social, isso é um dado alto, levando-se em consideração a quantidade de usuários ativos constantemente na internet, podendo assim tornar-se brecha para invasores. Como mostra a figura 6:

Figura 6 - Pergunta 01 do questionário



Fonte: Criação do autor

Apesar de pouco mais da metade conhecer sobre Engenharia Social, 95,6% dos participantes mostraram-se preocupados quanto à exposição na internet. Por isso, é fundamental o conhecimento sobre as principais práticas utilizadas para "roubo" de informações ou dados sensíveis, a fim de evitar possíveis novas práticas. Como mostra o gráfico da figura 7.

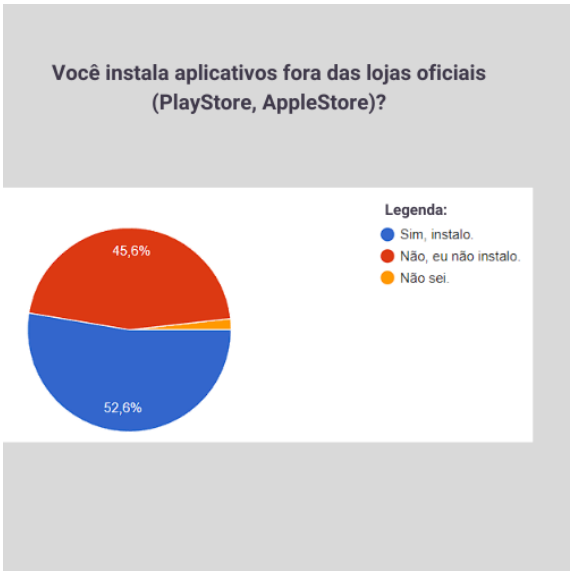
Figura 7 - Pergunta 04 do questionário

Fonte: Criação do autor

O que chamou mais atenção na pesquisa, é que apesar da grande maioria se preocupar com a Segurança, muitos deles não utilizam métodos corretos para evitar possíveis danos e exploração de vulnerabilidades por pessoas mal-intencionadas. A pergunta número 06 do questionário abordou se os participantes instalavam softwares ou aplicações fora das lojas oficiais. E 52,2% ,Como mostra a figura 8, afirmaram que sim, porém, esses dados mostram-se diferente do anterior, como as pessoas se preocupam com a Segurança, "abrindo" as portas dos seus dispositivos para softwares de terceiros? Muitos desses softwares podem se tratar de um trojan que em alguns casos podem vim com spywares, ransomware, vírus, worms, entre outros, que são programas espiões que podem monitorar atividades dos usuários, criptografar dados, enviar informações remotamente ao invasor, entre outras práticas maliciosas.

Quando indagados se trabalhavam, 62 pessoas responderam que sim, porém, 40,9% responderam desconhecer políticas de Segurança da Informação no local de trabalho, como mostra a figura 9. E outros 21,5% afirmaram não possuir medidas de segurança dos dados. O dado é ameaçador, tendo em vista que de acordo com um levantamento da Federação Brasileira de Bancos, a Febraban, os golpes de Engenharia Social cresceram mais de 165% apenas no primeiro semestre de 2021 contra empresas brasileiras, levando-se em consideração o primeiro semestre do mesmo ano. InfoMoney (2021).

Figura 8 - Pergunta 06 do questionário



Fonte: Autor.

Então, baseado em todos esses números, foi possível concluir que a falta de informação, muitas vezes podem ser "brechas" para invasores e a próxima fase pretende mostrar todo o passo-a-passo de como estamos "vulneráveis" na rede e exibir as consequências reais que essas técnicas podem trazer aos usuários.

Figura 9 - Perguntas 10 e 11 do questionário

Fonte: Criação do autor

2.2.2 Coletas de dados públicos sem ferramentas

O primeiro passo para realização do ataque foi definir o alvo, e este autorizou formalmente, que pudesse ser a "vítima" para fins acadêmicos. Com isso, a primeira fase foi fazer uma "varredura", ou seja, uma busca de informações públicas sobre o alvo utilizando o Google Hacking. Essa busca consistiu em pesquisas através de sites, redes sociais e postagens feitas pela vítima que são indexadas pelo Google. Quanto mais detalhes da busca for feita, melhor serão as possibilidades de ataque de engenharia social.

A primeira rede social explorada foi o linkedin, e para não levantar suspeitas para a vítima, foi criada uma conta "*fake*" de uma empresa fictícia, tendo em vista, que na sua versão gratuita, a rede social notifica o usuário quem o "visitou". O foco do acesso foi buscar informações de contatos do alvo. Os seguintes elementos foram adquiridos em uma simples análise:

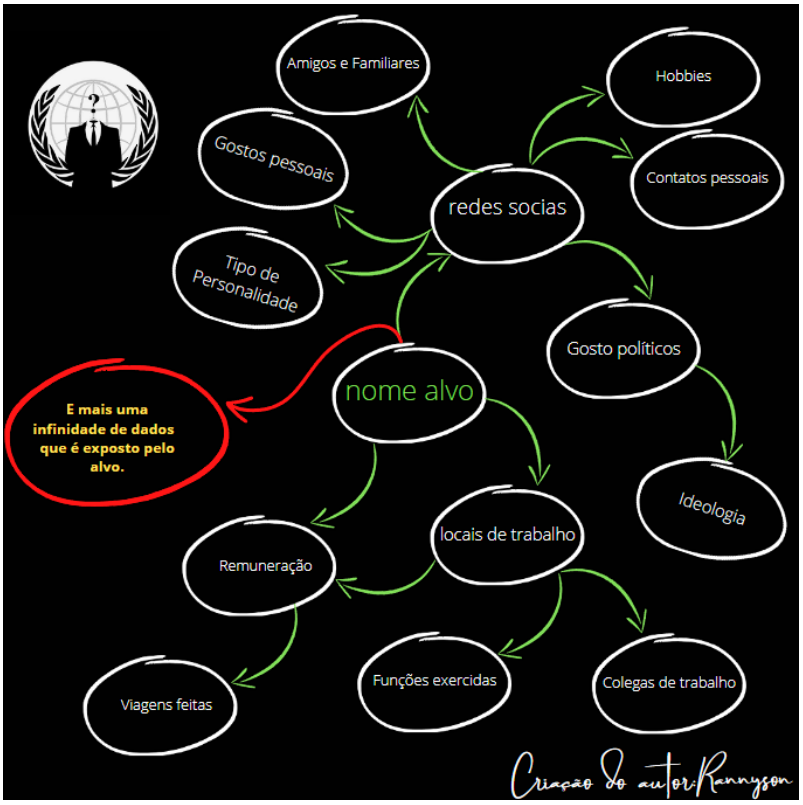
- *E-mail* Pessoal;
- Competências técnicas;
- Informações sobre outras redes sociais;
- Telefone Pessoal;
- Rede de contatos;
- Recomendações de pessoas próximas que já trabalharam com o alvo.

A partir do LinkedIn foi possível localizar outra rede social, no caso, o Twitter, e por meio desta, foi possível ter acesso a todas as suas postagens, podendo definir os seus principais gostos e hobbies. Ou seja, podemos traçar o perfil da vítima e criar a melhor estratégia, baseada em suas atividades na internet, e por meio do *e-mail* que foi descoberto, já temos a primeira porta de entrada para um possível ataque. Mas como a técnica, deve ser a mais real possível, vamos nos aprofundar um pouco mais nos dados para aumentar as chances de sucesso no ataque.

Diante disto, foi criado um mapa de características da vítima baseado nos dados coletados para que o ataque seja direcionado de acordo com estas características. A figura 10 mostra o fluxo utilizado para se obter os dados de forma genérica do alvo.

Finalizando o processo de coleta de dados públicos foi utilizado sites de buscas como o “Whois” de servidores *DNS*(*Domain Name System*) para verificar se o alvo tinha algum servidor ou algum domínio registrado em seu nome no processo padrão de coleta.

Figura 10 - Mapa dos dados coletados



Fonte: Criação do Autor

2.2.3 Coleta de dados com ferramentas

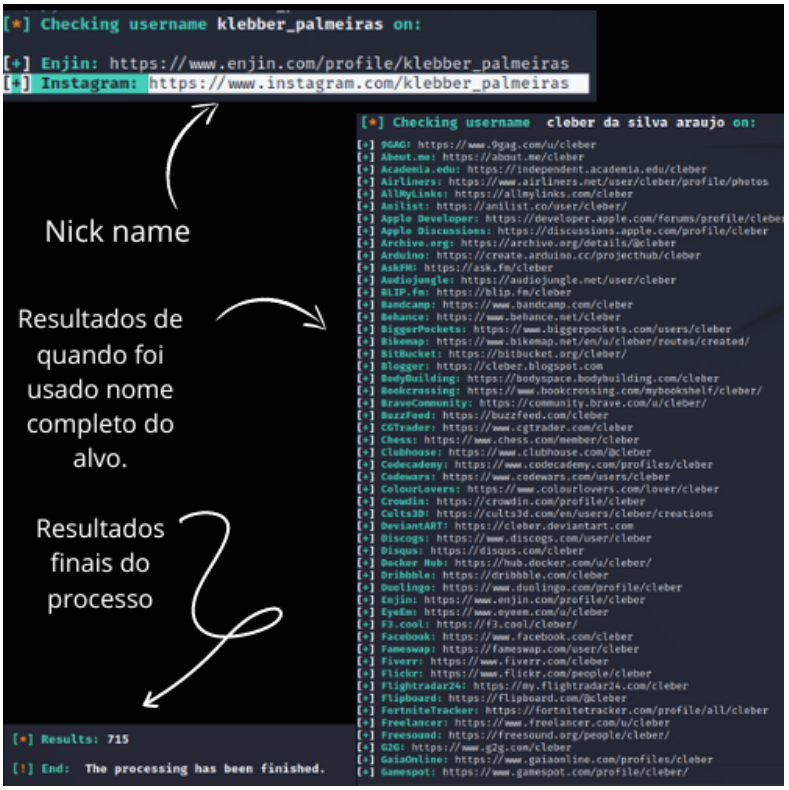
Se em apenas em simples pesquisas com o Google Hacking e em redes sociais foi possível extrair várias informações de um alvo. Considere poder utilizar ferramentas que automatizam e agilizam esse processo? Sim, essa fase do trabalho apresenta o uso de ferramentas open source para descobrir informações sensíveis das vítimas. Como este trabalho é estritamente para fins acadêmicos, serão mostrados apenas métodos simples de coletas e manipulação de dados, lembrando que essas ferramentas podem fazer muito além do que será mostrado neste trabalho. Tudo que será mostrado neste trabalho baseia-se apenas para fins acadêmicos e educacionais e segue todos os conceitos éticos e obedecendo à Legislação Brasileira. Todas e quaisquer replicação do conhecimento de forma inadequada deste trabalho sofrerá sérias consequências judiciais.

Como o intuito deste trabalho é somente mostrar os potenciais riscos da utilização de ferramentas na coleta de dados não será mostrado um passo-a-passo de fato, mas sim, a ferramenta na prática. A maioria delas possuem uma instalação simples e fácil usabilidade até para quem domina pouco sobre linguagens de programação.

2.2.3.1 Ferramentas de Coletas de Dados

A primeira ferramenta utilizada para essa prática foi o Photon . Iniciando um escaneamento simples passando como parâmetro o nome completo do alvo a ferramenta coletou 715 resultados vinculados ao nome em pouco segundos, como mostra a figura 11. Com isso, precisamos filtrar quais desses pertencem ao nosso alvo e quais pertencem apenas a pessoas com o mesmo nome.

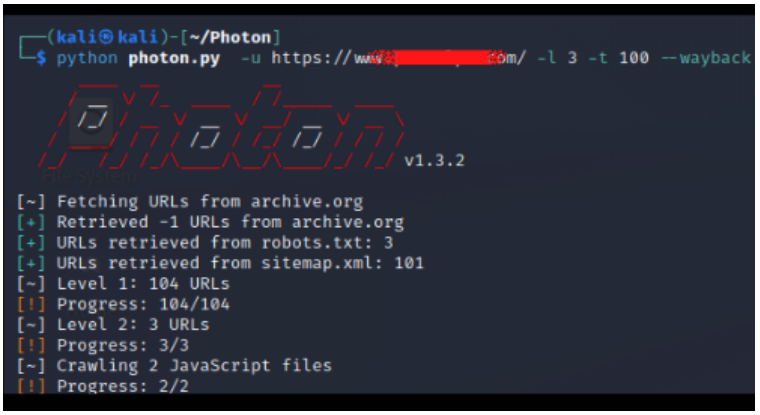
Figura 11 - Início do ataque



Fonte: Criação do autor

Entre os resultados filtrados, localizou-se que a vítima possui um site ativo sobre notícias. Sabendo disso, foi utilizado a mesma ferramenta para obter mais informações sobre o domínio do portal como por exemplo: urls conectadas, url anterior e também foi feita a verificação das 100 principais portas de comunicação do domínio do site da vítima. Como mostra a figura 12.

Figura 12 - Utilizando o Photon



Fonte: Autor.

Na sequência foi utilizado a ferramenta AtScan, com ela pode-se encontrar informações detalhadas sobre o domínio. Nesta etapa foram obtidos vários dados interessantes de acesso, desde o tamanho da rede de *links, e-mail*, endereço *IP*, localização do servidor, entre outros, como mostra a figura 13.

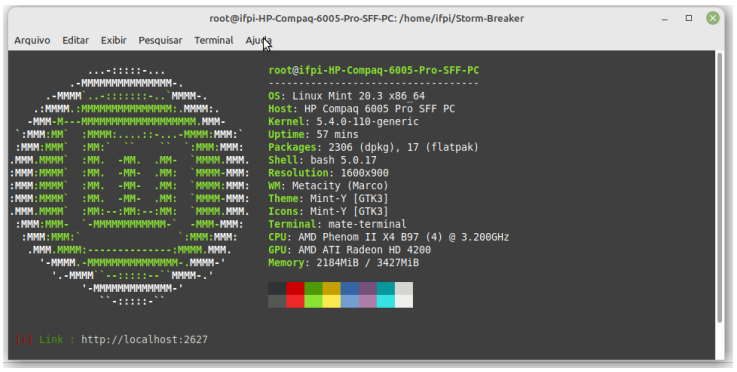
Figura 13 - Utilizando o AtScan

Fonte: Autor.

2.2.3.2 Hackeando a vítima

Após descobrir os principais *hobbies* da vítima e *e-mail*, optou-se por enviar um *link* malicioso para ela. Para isso, foi criado um *phishing* utilizando a ferramenta StormBreaker, que é capaz de invadir o microfone, câmera, localização e informações de rede e do dispositivo da vítima. (figura 14). A ferramenta gera um *link* capaz de roubar todas essas informações da vítima.

Figura 14 - Terminal ferramenta



Fonte: Autor.

O StormBreaker funciona por padrão apenas em uma rede local, para garantir uma conexão externa, como é o caso desta análise, foi feita a conexão com o Ngrok permitindo assim que o servidor local esteja acessível de qualquer parte do mundo através da internet, gerando um *link* parecido com este: *https://75bc-45-561-84-105.sa.ngrok.io*.

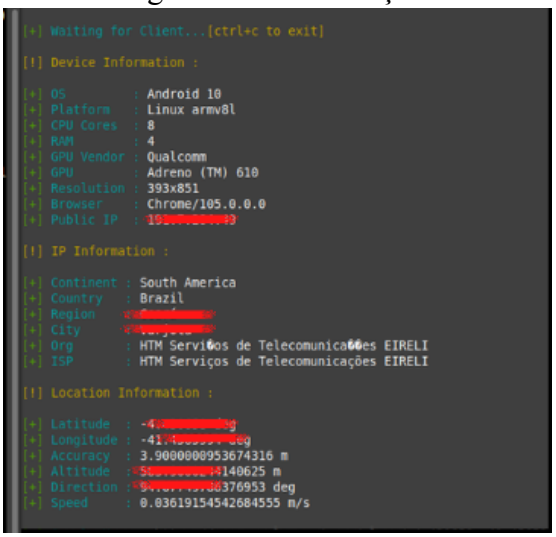
Devido a vítima ter conhecimentos sobre a área de informática, dificilmente ele entraria em um link totalmente estranho, nesse caso, entra em cena o conceito do maskphish, que auxilia na engenharia social e facilita muito a vida do atacante. Voltada pro contexto da vítima, ele ativa e desperta gatilhos emocionais criando *links* mascarados que dificultam a percepção da vítima. Por exemplo, no dia 14 de dezembro de 2022 divulgou-se uma notícia sobre um jacaré que teria sido encontrado na zona urbana de Pedro II, no Piauí, gerando muitos comentários sobre o assunto. Com a alta deste conteúdo vinculada à curiosidade do alvo, foi utilizado esse fator para aumentar as chances de sucesso para o alvo clicar. O link com seu processamento final com o maskphish ficou com o seguinte formato: "*https://www.portalp2.com-jacarep2@is.gd/TOFHsV*" e enviado para o *e-mail* coletado utilizando uma conta falsa. A figura 15 mostra o *link* sendo mascarado pelo Maskphish e a 16 mostra a aplicação na prática.

Figura 15 - Utilizando o Maskphish para aplicação de engenharia social

Fonte: Autor.

Após alguns minutos, o usuário entrou no *link* e autorizou o uso de algumas funções do celular sem ao menos perceber. Com isso foi obtido de forma simples o *IP*, coordenadas de localização, resolução da tela, sistema operacional, navegador utilizado, entre outras informações, como mostra a figura 16.

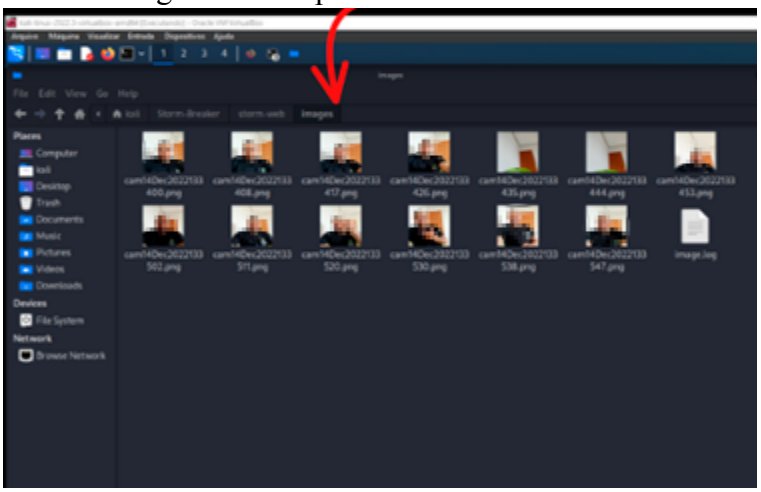
Figura 16 - Localização do alvo



Fonte: Autor.

Não parou por aí, com o mesmo *link* foi possível obter dados da câmera do dispositivo da vítima, enviando várias imagens por segundo à máquina do atacante, as fotos são registradas sem ao menos o usuário perceber, e ela continua ativa até que a vítima feche o navegador. Com essa técnica, é possível anexar um vídeo do youtube, para que o usuário permaneça olhando para a tela e ficar por vários minutos com o navegador aberto sem ao menos perceber que está sendo fotografado pelo próprio aparelho, que envia remotamente as imagens ao invasor, como mostra a figura 17. A ferramenta permite, inclusive, a captura de áudio, que não será focada neste trabalho. O dispositivo permanecerá "zumbi", enquanto o navegador estiver aberto ou dependendo das autorizações que o usuário dá para cada aplicação no dispositivo.

Figura 17 - Captura da Câmera frontal do alvo



Fonte: Autor.

E assim, o ataque utilizando técnicas de Engenharia Social foi realizado com sucesso de forma simples e detalhando todas as etapas de forma simples e direta.

2.2.4 Mitigação do ataque

Baseado nos ataques demonstrados anteriormente, uma das imitações mais óbvias basicamente é sempre se perguntar "o que se trata aquele *link*?", lógico se é algo que é focado no seu contexto, ainda sim é bom sempre se questionar sobre para onde esse link irá levá-lo. Propondo uma mitigação simples para se defender de ataques assim é utilizar "*checkouts* de *URL*" este tipo de *software* irá mostrar o caminho deste *link* até chegar no seu destino final, um bom exemplo é o site *https://www.virustotal.com/*, utilizado para analise de arquivos, domínios, *IPs* e *URLs* suspeitos para detectar *malware* e outras violações de segurança.

Além disso, é importante ler os termos de uso dos aplicativos, evitar instalação de aplicações fora das lojas oficiais e principalmente, tomar o maior cuidado possível ao autorizar aplicações terem acesso à câmera, localização e outros dados sensíveis dos dispositivos eletrônicos.

Com a visão no âmbito empresarial como foi citado por este trabalho é reforçado a criação de políticas voltadas às boas práticas de segurança da informação. Aramuni (2020) explica que as empresas não devem apenas investir em *softwares* de políticas de segurança, e sim, também, envolver toda a equipe sobre boas práticas e criação de protocolos estratégicos sobre o tema de engenharia social.

3 CONCLUSÃO

Considerando o contexto deste trabalho podemos concluir que os resultados atingiram todos os objetivos propostos e levantou questionamentos válidos de alerta tanto para indivíduos como para empresas, agregando, assim, conhecimentos relacionados a políticas de conscientização em geral.

A partir dos resultados foi possível ver o quão perigosa é a Engenharia Social na era digital, e o quão vulnerável usuários poderão estar na internet. Como abordado no trabalho, um simples *link* foi capaz de tirar fotos da vítima e enviar ao atacante. Podemos nos perguntar, e se a vítima estivesse em situação constrangedora? E o invasor resolvesse cobrar valores em dinheiro e fazer ameaças? Isso poderia gerar inúmeros outros crimes relacionados à internet.

Buscamos, então, desempenhar o papel de conscientização e sugestões para criação de boas práticas de segurança da informação, pois de pouco adianta ter os melhores *softwares* de segurança se a pessoa ou empresa não tiver o treinamento adequado para se defender de práticas maliciosas.

Como trabalhos futuros, sugerimos o uso de inteligência artificial para ataques automatizados de engenharia social e fazer a verificação de possíveis brechas de alvos utilizando *web scraping* em Python para minerar dados de forma automática na rede mundial de computadores de forma mais ampla e rápida.

REFERÊNCIAS

ACERVOLIMA. acervolima, **Advanced web Application Scanner**.Disponível em: ATSCAN - Advance Web Application Scanner no Kali Linux – Acervo Lima . Acesso em: 15,nov.2022.

ARAMUNI, João Paulo Carneiro; MAIA, Luiz Cláudio. **O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa. AtoZ: novas práticas em informação e conhecimento**, v. 7, n. 1, p. 31-37, 2020.

ARIZA, Maurício et al. **Ataques Automatizados de Engenharia Social com o uso de Bots em Redes Sociais Profissionais. In: Anais do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. SBC**, 2022. p. 153-166.

BARBOSA, Juliana Souza et al. **A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional. Research, Society and Development**, **v. 10, n. 2, p. e40510212557-e40510212557**, 2021.

CERT BR. **Centro de estudos,respostas e tratamento de incidentes de Segurança no Brasil, ano. Dados estatísticos sobre incidentes no brasil entre 1999-2020**. Disponível em:Estatísticas do CERT.br -- Incidentes . Acesso em: 14,nov.2022.

CLEARSALE. ClearSale, 2022.**Tipos de ataques de engenharia social**. Disponível em: Engenharia Social: o que é, tipos de ataque, técnicas e como se proteger (clear.sale). Acesso em: 28, nov.2022.

DIAS, Paulo Ricardo Saramago. **Prevenir um Ataque de Phishing**. 2021. Tese de Doutorado.

DA S. GERALDO, Vinicius; TAKEDA, Fábio Bento. **ENGENHARIA SOCIAL: um perigo oculto em simples técnicas. Revista Interface Tecnológica, v. 16, n. 1, p. 242-253**, 2019.

DEVMEDIA. DevMedia.**Segurança da Informação X Redes Sociais - Revista Infra Magazine 7 .Disponível em:Segurança da Informação X Redes Sociais - Revista Infra Magazine 7** (devmedia.com.br). Acesso em: 5,nov.2022.

FONSECA,Marcelo. **Engenharia Social: conscientizando o elo mais fraco da segurança da informação. 2017 Trabalho de conclusão de curso(Pós graduação em Especialização em Inteligência Em segurança pública) - Universidade do Sul de Santa Catarina, Brasília**,2017.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

INFOMONEY. InfoMoney, **Golpes de engenharia social cresceram em 2021**.Disponível em:https://www.infomoney.com.br/minhas-financas/golpes-de-engenharia-social-cresceram-saiba-o-que-sao-e-como-proteger-seu-dinheiro/ . Acesso em: 14,nov.2022.

JORNALDEBRASÍLIA. **Jornal de Brasília.Como a pandemia influenciou a tecnologia** .Disponível em:Como a pandemia influenciou o avanço da tecnologia - Jornal de Brasília (jornaldebrasilia.com.br). Acesso em: 5,nov.2022.

KALITOOLS. kalitools**,photon.** Disponível em:| de fótons Ferramentas do Kali Linux. Acesso em: 15,nov.2022.

LLUÍS, Gil; ALBERTO, Luis. **Estudio de los ataques y su defensa en la Ingeniería Social**. 2022.

MITNICK, K. D.; SIMON, W. L. M. A **arte de enganar. Ataques de hackers:Controlando o fator humano na Segurança da Informação.** Pearson Education do Brasil Ltda, 2003.

MITNICK,D.K. **A Arte de Enganar**.1.ed.São Paulo:Pearson,2004.

MASKPHISH, MaskPhising, MaskPhising: **Give A Mask To phishing URL**.Disponível em: MaskPhish : Give A Mask To Phishing URL 2020!Kalilinuxtutorials. Acesso em: 15,nov.2022.

NGROK, Ngrok,**primeiros passos no ngrok**.Disponível em: Getting Started | ngrok documentation. Acesso em: 15,nov.2022.

PLANALTO. Planalto.gov.**Lei Geral de Proteção de Dados (LGPD)**. Disponível em: L13709 (planalto.gov.br). Acesso em: 26, nov.2022.

SANTOS, Fabíola Mendes. **Fake News Nas Eleições: Uma Ameaça à Democracia**. Análise à Luz da Manipulação das Massas, Técnicas de Poder e Psicopolítica, de Byung-Chul Han. Epitaya E-books, v. 1, n. 11, p. 65-77, 2022.

APÊNDICE

Termo de Autorização para Exploração dos Dados

Eu, **Cleber da Silva Araujo**, portador do documento **056.** abaixo assinado, dou plenos direitos para que sejam realizadas "varreduras" sobre os meus dados e autorizo para que sejam utilizados no Trabalho de conclusão de curso **Análise prática e mitigação dos riscos da Engenharia Social na era digital.** Visto que, o trabalho é para fins acadêmicos e científicos, respeitando os respectivos códigos de ética.

Pelo presente também manifesto expressamente minha concordância e meu consentimento para utilização destes dados.

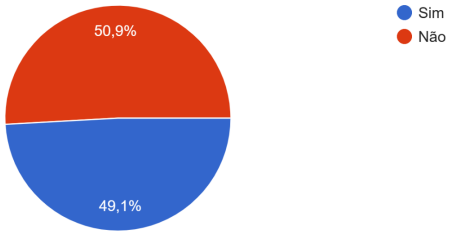
Pedro II, 01 de novembro de 2022.

Assinatura

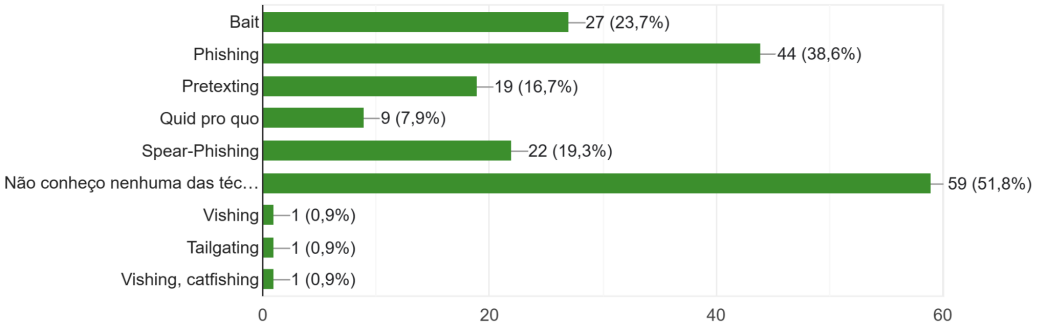
FORMULÁRIO DE PESQUISA - GOOGLE FORMULÁRIOS

formulário: perguntas e respostas do formulário

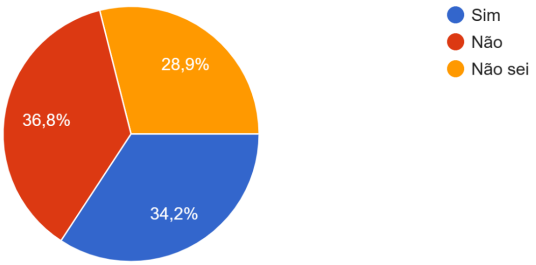
Você sabe o que é Engenharia Social?
114 respostas



Marque todas as técnicas de engenharia social que você conhece:
114 respostas

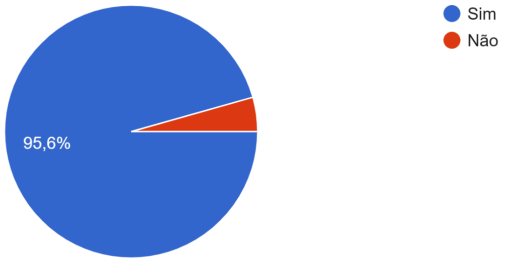


Você já sofreu ou conhece alguém que já sofreu algum tipo de ataque de Engenharia Social?
114 respostas



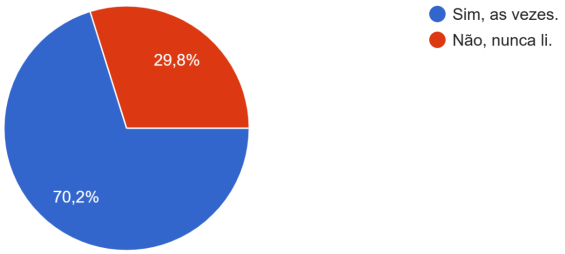
Você se preocupa como seus dados são expostos na internet?

114 respostas



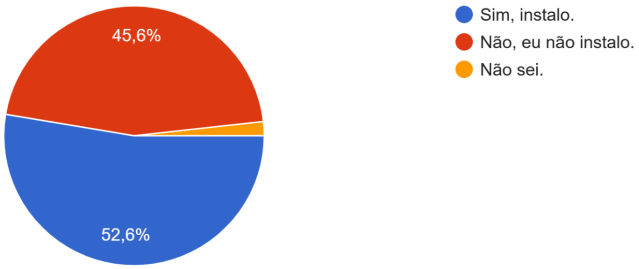
Você ler os termos de uso?

114 respostas



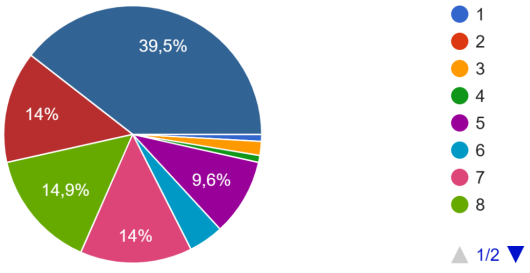
Você instala aplicativos fora das lojas oficiais (PlayStore, AppleStore)

114 respostas



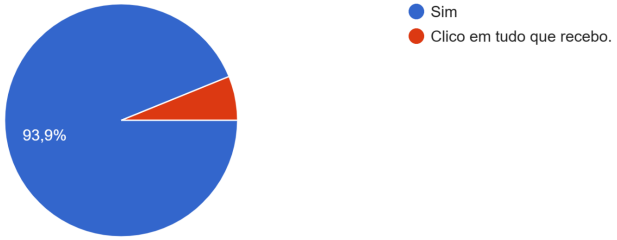
De 0 a 10 qual é o seu nível de preocupação para com seus dados?

114 respostas



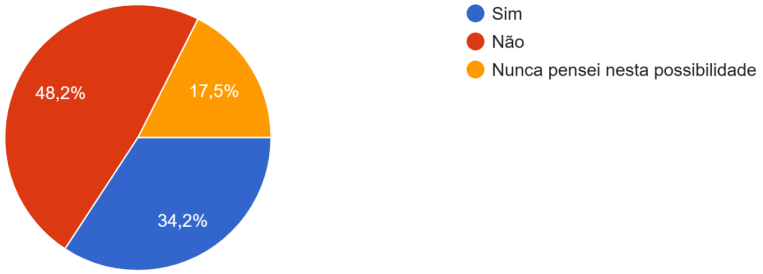
Você tem cuidados ao clicar em links?

114 respostas



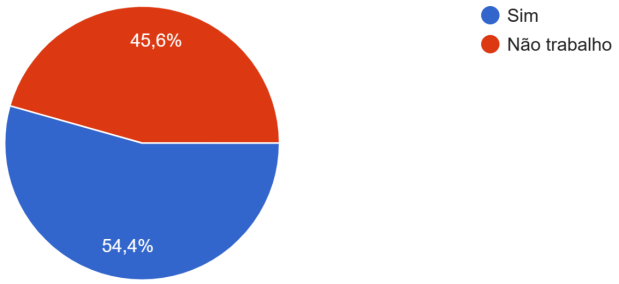
Você acha que as pessoas em volta de você têm a mesma preocupação com os dados delas, e se o fato delas serem descuidadas com seus dados p...ível abertura para terem acesso aos seus dados?

114 respostas



Você trabalha atualmente?

114 respostas



Se sim, a empresa onde você trabalha tem alguma política de segurança da informação?

93 respostas

Se não, você conhece alguma empresa que tem essa preocupação com a segurança da informação?

114 respostas