COLÉGIO JOÃO PAULO I – UNIDADE SUL
INTRODUÇÃO À METODOLOGIA CIENTÍFICA 2022
TURMA: 9º ANO B

CYBERSECURITY, A SEGURANÇA CIBERNÉTICA

Aluno: Ian Altenhofen Dos Santos
Orientador: Fabrício Dos Santos

Porto Alegre/RS
2022

SUMÁRIO

1. INTRODUÇÃO

No mundo de hoje, onde o comércio eletrônico, o ensino a distância (EAD), o uso de aplicativos e o uso da internet em geral são a realidade, a cibersegurança é necessária para manter os dados pessoais e financeiros do usuário seguros. Manter dados seguros significa conseguir identificar sites maliciosos, criar senhas complexas, utilizar antivírus e outras ferramentas para evitar golpes. A área que estuda esses métodos de proteção de dados no meio digital é chamada de segurança cibernética. Entretanto, embora um dos primeiros passos para que uma pessoa mantenha um negócio e sua vida pessoal saudáveis seja o controle de seus dados pessoais e existam meios para isso, nos últimos anos a quantidade de invasões e de ataques virtuais a grandes empresas tanto quanto a pessoas comuns tem crescido sem parar, e isso demonstra a importância da segurança no ambiente virtual. Nesse sentido, este trabalho contém casos reais de ataques e de golpes cibernéticos que ocorreram no Brasil e no mundo, assim como as camadas de segurança e de proteção necessárias para evitar esses tipos de invasão de privacidade. No ano de 2021, muitas empresas foram atacadas por hackers, o mesmo aconteceu em anos anteriores. O Tribunal de Justiça do Rio Grande do Sul (TJ-RS), por exemplo, foi atacado por hackers anônimos, que conseguiram bloquear o acesso dos funcionários às suas contas nos computadores, além de criptografar os dados e cobrar pela devolução deles([1]TJRS, 2022). Outro caso relacionado a esse tema e, possivelmente, o mais conhecido do ano de 2021, foi o ataque às lojas Renner, no qual os invasores foram capazes de sequestrar dados das transações das lojas e de impedir que a empresa continuasse vendendo produtos, causando prejuízos ([2]Tecnoblog, 2022). Esses invasores pediram aproximadamente um bilhão de reais para o resgate das informações e afirmaram que não havia interesse em vazar os dados roubados. Tendo em vista essas situações, fica claro que esse tema é de grande importância para as pessoas, para as empresas e para as escolas saberem como se proteger e se defender de possíveis ataques e de invasões hackers, assim como para saber técnicas de complexidade de senhas, além de autenticação em duas etapas. Trabalhando nessa linha, existe um outro lado da moeda, os *Ethical Hackers*. Os *Ethical Hackers* ou Hackers morais usam seu conhecimento em ataques cibernéticos para auxiliar empresas. Estas, , hoje em dia, armazenam seus dados nos seus data centers e na nuvem, ou atuam na internet, e, para tudo que se faz *on-line*, é necessário estar seguro. Nessa perspectiva, grandes

empresas, como o Santander, utilizam a ajuda de *Ethical Hackers* para encontrar falhas no seus sistemas ([3]Santander, 2022). O trabalho desses profissionais trata sobre as informações relacionadas a navegadores de internet, a criação de senhas, o submundo da internet, as camadas da segurança digital, os tipos de ataques hackers, os ataques recentes, os VPNs e as formas de se proteger em casos extremos.

Justificativa

O tema deste trabalho foi escolhido devido à importância de se proteger e de se defender não apenas de ataques e de invasões hackers, mas também de pessoas mal intencionadas que acabam por descobrir a senha de alguma conta ou de algum dispositivo e aplicam golpes nos usuários.

Objetivos

Objetivos gerais: O principal objetivo deste trabalho é conscientizar as pessoas e alertá-las sobre a importância de senhas seguras e de se proteger digitalmente. O trabalho demonstra informações sobre a infraestrutura da internet e as camadas de segurança digital.

Objetivos específicos: O trabalho contém uma explicação superficial sobre barreiras digitais, uma explicação sobre alguns dos programas mais usados por hackers e no decorrer do trabalho, algumas pesquisas sobre a composição das senhas das pessoas.

2. METODOLOGIA

Para a obtenção dos resultados do trabalho, pesquisas foram realizadas por meio de um formulário, em que se obteve resultados sobre a força das senhas de quem fez o formulário, assim se tem um resultado geral sobre o quanto as pessoas sabem sobre complexidade e sistemas de segurança. Os formulários têm como alvo indivíduos de 10-80 anos que não trabalham com TI e formandos do 4º ano à 3ª série. Além das questões sobre a complexidade de senhas e os sistemas de segurança, foram realizadas perguntas sobre o conhecimento de segurança digital que as pessoas têm, por meio do formulário. Durante as pesquisas, perguntas também foram feitas para descobrir se as pessoas usam a mecânica de autenticação em duas etapas ou outras mecânicas que podem lhes ajudar a proteger sua conta. Ademais, foi realizada uma pesquisa de campo, na internet e com profissionais da área.

3. RESULTADOS

Por meio do formulário (anexo 1), houve a obtenção das seguintes respostas:

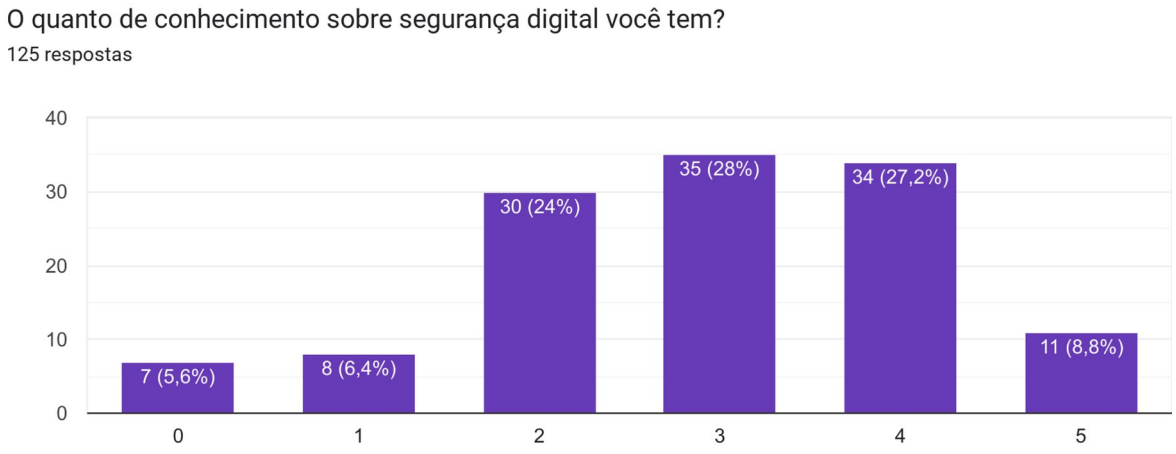


Figura 1, primeira pergunta do formulário

0= Não sei de nada sobre 1= Sei criar uma senha 2= Consigo fazer o básico

3= Estou acima da média 4= Sou bom no que faço 5= Domino totalmente o assunto

Conforme apresentado nas respostas da primeira pergunta, aproximadamente 24% dos indivíduos, o que corresponde à maioria dos que responderam ao formulário, disseram que estão na média, e apenas 8,8% das 125 pessoas entrevistadas disseram que têm um conhecimento avançado sobre o assunto. Isso se deve ao fato de que as pessoas não se interessam pelo assunto e não se preocupam em melhorar sua segurança no espaço digital.

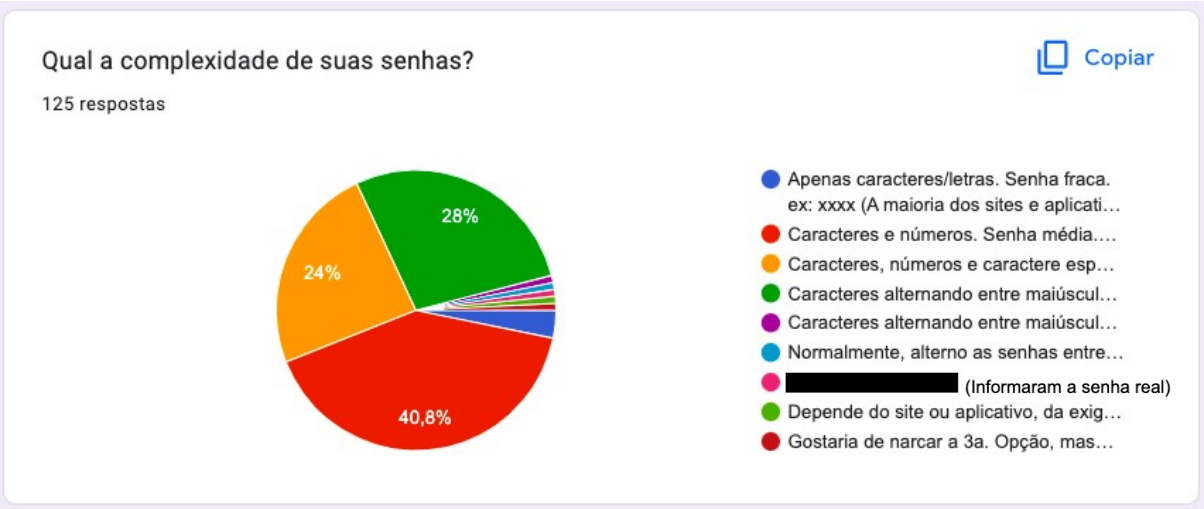


Figura 2, segunda pergunta do formulário

Segundo os resultados da segunda pergunta, a grande maioria das pessoas usa senhas médias, com apenas números e caracteres. Esse é o estilo de senha mais comum, sendo suficiente, na maioria das vezes, para impedir que sua senha seja descoberta.

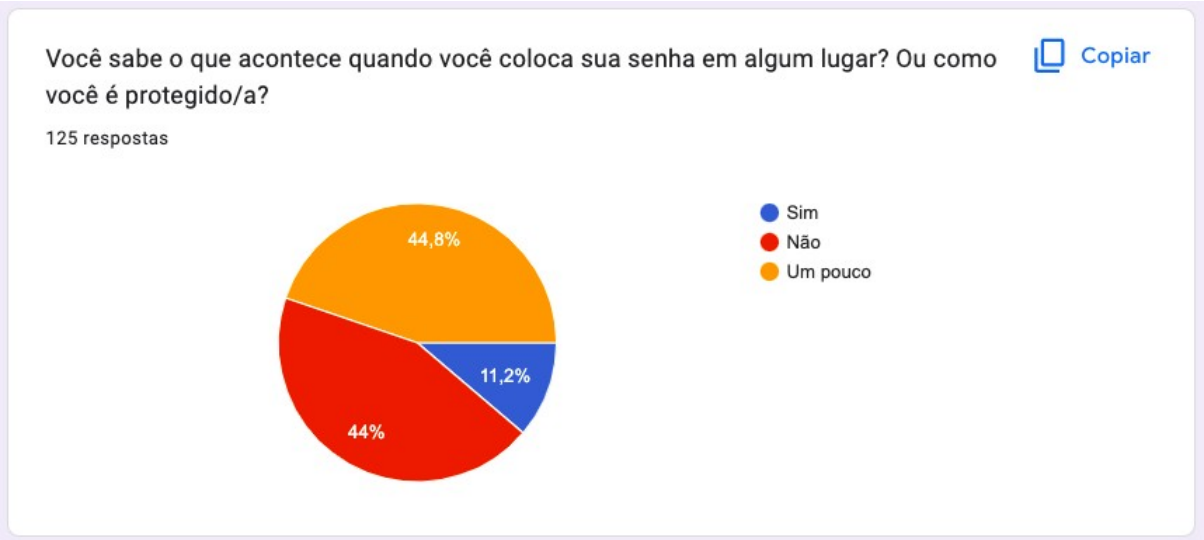


Figura 3, terceira pergunta do formulário

Os resultados da terceira pergunta indicam que as pessoas, no geral, sabem o básico. Esta pergunta tem as respostas bem equilibradas, sendo a predominante "Um pouco" o que indica que a maioria das pessoas tem o mínimo de conhecimento sobre o assunto. Isso demonstra que, atualmente, os usuários não se preocupam com a segurança do seu telefone, pois pensam que estão invulneráveis

caso ninguém tenha acesso à sua senha. As perguntas do formulário estão apresentadas no anexo 2.

Outro tópico a ser discutido são os *Ethical Hackers*, os piratas da internet que fazem o bem com seus conhecimentos de invasão cibernética. A empresa Santander conseguiu treinar um homem de 86 anos para ser um *Ethical Hacker,* a fim de provar que qualquer um pode fazer isso pelo bem ([4]Finextra, 2018).

Um assunto muito importante a ser falado é sobre os navegadores da internet, o Google, Firefox, Opera e, pensando em segurança digital, este que é o mais importante e interessante, o Tor. O Tor é o navegador mais seguro possível de acessar, sendo totalmente gratuito e fácil de usar, dependendo do seu objetivo. Ele funciona em múltiplas camadas de segurança, e essa ideia é expressa, inclusive, pelo seu logo, que traz a cebola como a representação dessas camadas. Entretanto, no mundo da cibersegurança, o Tor tem uma reputação de ser um navegador maligno usado para se acessar a *deep web*, já que ele proporciona total anonimato. Apesar disso, seu único objetivo do navegador é garantir privacidade para o usuário ([10]Torproject).

O sistema de segurança do Tor tem a capacidade de impedir que a internet consiga o endereço de IP do usuário, isto é, o “crachá” do internauta que contém dados como quem ele é, onde ela mora ou quando está online. O acesso ao IP do usuário é o jeito mais comum de identificá-lo pela internet Nesse sentido, diferente da maioria dos navegadores, que estabelecem uma conexão direta entre o dispositivo e a rede, o Tor criptografa as informações. Quando você quer se conectar a um site com o Tor, ele distribui os dados por diversos servidores pelo mundo inteiro, cada um com um pouco de informação, assim, deixando impossível de um hacker,, de site malicioso, de a polícia ou de o governo conseguir identificar e rastrear o internauta. No entanto, mesmo que o Tor seja a opção mais segura e privada para alguém que não deseja ser detectado, ele, nem nenhum outro navegador, é 100% seguro, visto que ainda é possível atravessar suas barreiras de proteção. ([5]Cybernews, 2022)

Um dos tipos de conexão segura é o VPN(*Virtual Private Network*), que não foi projetado para ser um sistema de proteção à privacidade e ao anonimato, mas sim para conectar um servidor a outro servidor remoto, por meio de um túnel seguro, onde apenas um servidor conecta a outro, sem conexões externas. Empresas geralmente usam essa ferramenta para empregar trabalhadores remotos

sem se preocupar com acessos indevidos ao seu ambiente tecnológico. Essa ferramenta evoluiu, possibilitando que uma pessoa esconda seu endereço IP ou conecte-se a um wi-fi de uma geolocalização diferente. Os VPNs também garantem uma camada adicional entre o usuário e o servidor a ser conectado. Além disso, podem ajudá-lo a conectar-se a serviços bloqueados para seu país ou região, sendo fácil alterar sua localização. ([6]Cybernews, 2022)

Para entender alguns dos mais comuns tipos de ataques hackers, é importante saber o que é um cavalo de tróia. Cavalos de Tróia são programas maliciosos que executam ações não autorizadas pelo usuário. O Backdoor é um tipo de cavalo de tróia que, enquanto entra no seu sistema, deixa o "caminho" gravado para que o invasor possa entrar posteriormente. É muito comum ver pessoas caindo diariamente nesse tipo de golpe, pois abrem links de estranhos ou o conteúdo de uma pasta ou e-mail. Outro ataque muito comum, possivelmente o mais comum atualmente, é o Phishing. Esse tipo de golpe não invade o dispositivo como o Backdoor, ele rouba dados pessoais, ou faz com que o internauta entregue essas informações. Sempre que se recebe um e-mail ou uma mensagem de um contato desconhecido, é necessário verificar se é de um contato oficial. Por exemplo: em uma mensagem do atendimento da operadora de telefonia “Oi”, caso o nome do contato não tenha o símbolo de verificado ao lado, é bem provável que seja um golpe. E-mails de supostos sites e de aplicações utilizados pelo usuário, pedem um login, muitas vezes solicitando dados pessoais. Caso seja um golpista, quando os dados estiverem no login, o criminoso pode vendê-los ou invadir a conta bancária do usuário, por exemplo. Outro ataque dos mais comuns é o DoS (*Denial of Service* ou Negação de Serviço), em que o hacker sobrecarrega o servidor com diversos pedidos e solicitações, fazendo com que fique indisponível e desligue. Este é um ataque com intenção de vandalismo e não de roubo. Outro ataque muito comum é o Decoy, disfarce em inglês. Nesse, o hacker recria um site conhecido e muito acessado e envia-o por e-mail ou por outra ferramenta para pessoas que cairiam facilmente em golpes –segundo os olhos do golpista –, o login do site capta as informações que o usuário coloca e armazena-as, depois o redireciona para o site original, assim ele nem sabe que caiu em um golpe ([12]blogunyleya).

No último trimestre, os ataques hackers no Brasil aumentaram em 46%, 14% a mais que a média global. Cada vez mais empresas estão sendo atacadas por meio de ransomware. O relatório da CheckPoint Research mostra que, globalmente,

as principais categorias de ciberataques realizados foram: Malware multiuso (23%), Cripto Mineradores (15%), o trojan Infostealer (13%), mobile malware (12%) e ransomware (8%). O Mercado Livre divulgou, na segunda-feira, dia 7, que hackers invadiram e acessaram 300 mil dados de usuários. Apesar de parte do código-fonte da empresa ter sido roubado, ela disse que, por enquanto, não encontrou nenhuma evidência de que o ataque tenha comprometido informações sensíveis dos clientes. Os responsáveis pela invasão ao ML foram os Lapsus, como reivindicam, conhecido grupo que recentemente se notabilizou por ataques cibernéticos ao Ministério da Saúde, Localiza, Nvidia e Samsung. A empresa Kapersky divulgou um relatório dizendo que os ataques a empresas pequenas e médias cresceram 143% ao longo do último ano no Brasil. Esses dados são relativos ao número de tentativas de invasão bloqueadas. Segundo a companhia, foi o Trojan-PSW (password stealing ware) que apresentou esse crescimento de mais de o dobro do ano passado para cá.

([13]olhardigital)

Na hora de criar uma senha, a maioria dos sites, jogos, contas, etc,pedem para o usuário criar uma senha com, no mínimo, oito caracteres e, no mínimo, um número. Caso se queira criar uma senha com apenas oito caracteres e somente letras minúsculas, haveria 208 bilhões de combinações, o mesmo vale para senhas com apenas letras maiúsculas. Caso se queira fazer uma senha com apenas letras maiúsculas e minúsculas, seriam 417 bilhões de combinações possíveis. Caso se queira uma senha de oito caracteres, sendo sete letras maiúsculas e minúsculas e um número, haveria 1,2 trilhões de combinações. Agora se se escolhe criar uma senha com um caractere especial, as possibilidades aumentam consideravelmente. Em um site como Pearson, uma plataforma para aprendizagem sobre tecnologia, é possível usar 4 caracteres especiais na senha. Uma senha com oito caracteres, sendo seis letras maiúsculas e minúsculas, um número e um caractere especial, há 1,5 trilhões de possibilidades. Ainda assim, existem sites que deixam usar 32 caracteres especiais diferentes. Esses números exorbitantes ainda são para senhas com 8 caracteres apenas. Mesmo com tantas combinações de senha existentes, muitos fazem senhas fáceis de lembrar, usando nomes, datas de aniversários, etc, e os hackers, na maioria das vezes, utilizam softwares de identificação de senhas, usando padrões óbvios para os humanos. Esses padrões são analisados pelas redes sociais da pessoa, o software procura por esses padrões, diminuindo a

quantidade de combinações prováveis, até encontrar a senha desejada. Esse é o método de usar informações pessoais compartilhadas e de engenharia social. Engenharia social é uma técnica usada por criminosos virtuais para induzir usuários desavisados a enviar dados pessoais e privados, infectar seus computadores com vírus ou abrir links para sites infectados. Além disso, os hackers podem tentar explorar a falta de conhecimento do usuário. ([11]Kaspersky, tecnoblog, 2022)

Quando se fala no submundo da internet, deve-se pensar em um iceberg. A pontinha do iceberg que fica para fora da água é chamada de superfície e corresponde a 4% da web. Na superfície, podemos acessar os sites comuns, que podem ser acessados por qualquer um com qualquer navegador. Os outros 96% estão na Deep Web. A Deep Web proporciona quase total anonimato e, consequentemente, liberdade de expressão ao usuário. Em um país extremamente rígido, a Deep Web é uma ótima forma de se expressar. Apesar das coisas boas, muitos aproveitam o anonimato total que ela oferece para fazer coisas ilegais, como tráfico, compartilhamento de informações secretas e vídeos de violência e de tortura. Muitas vezes, a Deep Web é confundida com a Dark Web, mas elas têm conceitos diferentes: Enquanto a Deep Web consiste em páginas inalcançáveis a partir de navegadores comuns, a Dark Web consiste em fóruns, páginas e artigos, que se escondem usando protocolos diferentes do HTTP, muitas vezes o .onion ([8]Tecnoblog, Treinaweb, 2022).

4. CONCLUSÃO

De acordo com a pesquisa, podemos concluir que esse tema tem muita importância, não apenas para uma empresa que quer proteger seus clientes e seus empregados, mas também para qualquer um que se preocupe com sua própria segurança on-line. Apesar deste trabalho estar bem aprofundado, o assunto cybersecurity é muito maior do que isso.

Para evitar de cair em golpes simples, como os mencionados anteriormente, é uma boa ideia estudar como os principais golpes cibernéticos ocorrem e como evitá-los. Os golpes mais usados normalmente consistem no usuário clicar em um link enviado pelo golpista. Para evitar isso, deve-se tomar cuidado no que se clica e se o contato é oficial. Apesar de uma senha fraca com letras maiúsculas e minúsculas de oito caracteres ter 417 bilhões de possibilidades, para um hacker, isso é facilmente diminuído para milhares de combinações baseadas apenas em dados que os hackers podem descobrir por redes sociais ou ferramentas especializadas. Por isso, uma senha muito forte é necessária, uma senha com letras, números e caracteres especiais e com mais de oito caracteres, em ordem aleatória, mas que faça sentido para o usuário. Alternar entre números letras e caracteres especiais várias vezes é uma opção como xX0xx0@X@00x@xX0. Entretanto, uma senha grande e complexa como essa seria impossível de lembrar, para resolver isso, basta anotá-la em um papel, ou mais de um, e guardar em um cofre ou um lugar físico e seguro como esse, ou podem ser utilizadas ferramentas chamadas de *password managers* ([9]Trusted Password Manager). Essas ferramentas guardam as informações que o usuário escolher de modo que seja quase impossível de acessar, usando camadas de criptografia e *firewalls*.

5. REFERÊNCIAS BIBLIOGRÁFICAS

[1]https://www.tjrs.jus.br/novo/noticia/nota-de-esclarecimento-3/, Acessado dia 16 de abril de 2022

[2]https://tecnoblog.net/noticias/2021/10/01/renner-explica-impactos-do-ataque-de-ransomware-a-pedido-do-procon-sp/, Acessado dia 14 de abril de 2022

[3]https://www.santander.com/en/press-room/dp/ethical-hacking-the-pirates-who-protect-against-cyber-attacks, Acessado dia 29 de Julho de 2022

[4]https://www.finextra.com/newsarticle/32176/santander-trains-86-year-old-to-be-an-ethical-hacker-in-minutes, Acessado dia 2 de Agosto de 2022

[5]https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/, Acessado dia 8 de Agosto de 2022

[6]https://cybernews.com/what-is-vpn/, Acessado dia 8 de Agosto de 2022

[7], Acessado dia 8 de Agosto de 2022

[8]https://www.treinaweb.com.br/blog/voce-sabe-o-que-e-e-como-funciona-a-deep-web, https://www.techtudo.com.br/noticias/2019/03/o-que-e-deep-web.ghtml, Acessado dia 8 de Agosto de 2022

[9]https://www.trustedpasswordmanager.com/what-is-a-password-manager/?https://www.trustedpasswordmanager.com&gclid=CjwKCAjwi8iXBhBeEiwAKbUofcWfFxc91bom7awHrGo7LhCKp_-QmdhokrDsDG0kcniZQk5Eg9PskRoCb10QAvD_BwE, Acessado dia 9 de Agosto de 2022

[10]https://www.torproject.org/pt-BR/, Acessado dia 9 de Agosto de 2022

[11]https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering,https://tecnoblog.net/responde/como-uma-senha-pode-ser-descoberta-por-hackers/,Acessado dia 13 de Agosto de 2022

[12]https://blog.unyleya.edu.br/bitbyte/ataques-ciberneticos/#1_Backdoor, Acessado dia 18 de Agosto de 2022

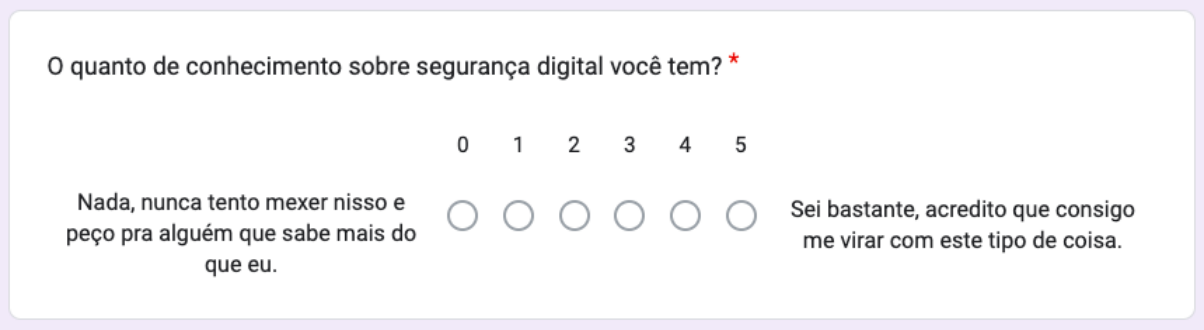
[13]https://olhardigital.com.br/2022/08/09/seguranca/ataques-ciberneticos-brasil-cresce-46/, Acessado dia 18 de Agosto de 2022

Formulário sobre segurança digital em anexo

ANEXOS

Anexo 1 - Formulário de perguntas sobre segurança digital
https://docs.google.com/forms/d/1jr9m1vkS9eBJdIci9pT-LWZjbzAltYVjkmw7fuvJRQg/edit?ts=62f1b3cc#question=1490427580&field=102954939

Anexo 2 - Perguntas do formulário



Qual a complexidade de suas senhas? *

- ◯ Apenas caracteres/letras. Senha fraca. ex: xxxx (A maioria dos sites e aplicativos proíbe que o usuário u...
- ◯ Caracteres e números. Senha média. ex: xxxx00
- ◯ Caracteres, números e caractere especial. Senha forte. ex: xxxx00@
- ◯ Caracteres alternando entre maiúsculo e minúsculo, números e caractere especial. Senha Megaforte. ex:...
- ◯ Outros...

Você sabe o que acontece quando você coloca sua senha em algum lugar? Ou como você é protegido/a? *

- ◯ Sim
- ◯ Não
- ◯ Um pouco