SEGURANÇA DA INFORMAÇÃO E OS DESAFIOS DA NOSSA SOCIEDADE PERANTE AS NOVAS TECNOLOGIAS

WILLIAM ROGER DA SILVA ALVES[1]
Marcio Freitas[2]

1. INTRODUÇÃO

O trabalho tem como objetivo principal a Segurança das informações na internet e os desafios que nossa sociedade apresenta diante das Novas Tecnologias.

Cada vez mais a sociedade se mostra dependente da tecnologia e do mundo virtual, basicamente tudo está conectado às redes, é inegável que a tecnologia nos trás oportunidades e facilidades, abrindo possibilidades positivas para otimização de serviços, e comodidades aos usuários, más também abre portas para perigos ao compartilhar e acessar dados sem a devida certeza de que está realmente protegido.

Estamos cada vez mais conectados ao mundo virtual, atividades que antes eram necessárias à presença física hoje podemos resolver na palma das nossas mãos, como por exemplo, atividades bancárias, hoje em dia podem ser realizadas de qualquer lugar, ou qualquer hora, basta ter um dispositivo móvel conectado à rede, ou um computador.

Mas aquilo que se mostra como uma facilidade para o usuário, também abre possibilidades para novos tipos de perigos e ameaças, além de roubos de senhas, o usuário pode ter sua vida espionada pelos cibercriminosos, outro fato importante está relacionado ao furto de identidade e onde as relações sociais podem ser mascaradas através de uma tela de computador ou Smartphones, expondo um ser humano que não corresponde ao que é na vida real.

O objetivo deste artigo é refletir sobre o uso da internet no nosso dia a dia, e em como podemos manter nossos dados a salvo, em como não cair em golpes de pessoas

[1]Aluno Curso Técnico Alcides Maya
[2]Prof. Espec. Alcides Maya. marcio_freitas@alcidesmaya.edu.br

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

mal intencionadas, principalmente alertar os usuários em como proteger suas senhas e seus dados.

1.1 Segurança da informação e os desafios da nossa sociedade perante as Novas tecnologias.

A internet está presente no dia a dia da maior parte da população Brasileira, a tecnologia vem avançando de uma forma extremamente rápida nos últimos anos, e com isso acaba trazendo facilidades e comodidades para dentro do nosso cotidiano.

Hoje em dia é difícil imaginar algo que não esteja conectado a rede, a internet nos trás muitas facilidades desde: Os smartfones aparelho inseparável de cada usuário, notebooks, Smart TVs, Relógios inteligentes.

É inegável que toda essa tecnologia trouxe benefícios para nossas vidas, mas para que essas práticas sejam seguras é importante estar sempre atento à privacidade e segurança dos dados que estão trafegando na rede.

1.2 Problema

Com o surgimento de novas tecnologias um número crescente de usuários estão sendo enganados por armadilhas virtuais com o intuito de roubar informações e dados pessoais.

É importante estar sempre atento à links maliciosos que podem chegar através de mensagens por SMS, Spams, é importante tomar cuidado com sites fraudulentos, que se passam por sites oficiais de instituições financeiras.

Como podemos manter em segurança nossos dados pessoais na internet?

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

1.3 Justificativa

Justifica-se a realização de trabalho acadêmico, mediante a questionamentos do pesquisador sobre como podemos proteger nossos dados e informações pessoais em quaisquer interatividades no meio virtual.

Pois se seguirmos algumas dicas, até mesmo as mais simples de proteção de dados, conseguimos evitar transtornos virtuais que possam ser prejudiciais financeiramente e psicologicamente.

1.4 Objetivo Geral

O foco principal deste trabalho acadêmico é orientar o usuário em como não ter os seus dados roubados, ou criptografados por crackers na internet.

E auxiliar e não fornecer seus dados pessoais através de links via mensagens SMS, não fornecer nenhuma informação sobre, senhas, números de documentos ou cartões de créditos.

1.5 Específico

Identificar mecanismos de segurança para auxiliar usuários a não serem vitimas de crimes virtuais, através de pesquisas bibliográficas.

Definir a forma correta para proteção de senhas e dados dos usuários, para que não ocorra perda ou furto de dados, e invasão de privacidade, através de pesquisas bibliográficas.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

1.6 Metodologia

O método de pesquisa será através de uma revisão da literatura acadêmica, observando os principais livros, artigos e sites.

REFERENCIAL TEÓRICO

O referencial teórico tem por objetivo referenciar os temas tratados no presente artigo. A fim de conceituar as principais ideias de que, os desafios da nossa sociedade diante as novas tecnologias e como podemos manter nossos dados e informações em segurança, diante de ataques maliciosos e não éticos, de pessoais mal intencionadas na internet.

1.5 Mecanismos de Segurança

Para compreender e entender como a internet nos trouxe todas essas facilidades e comodidades nos dias atuais, como ocorreu e como aconteceu todo esse avanço tecnológico, precisamos entender como e onde surgiu a internet.

A internet como conhecemos teve início nas décadas de 1960, 1970, e 1980, como um projeto acadêmico e militar, na época da Guerra Fria, o departamento de defesa Americano criou uma rede de computadores em locais estratégicos com o objetivo de descentralizar as informações em caso de ataques, onde o governo Americano poderia se tornar vulnerável.

ARPA (advanced Research Projects Agency) uma das subdivisões do departamento Americano, criou a ARPANET.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

Com a alta conectividade faz com que as pessoas fiquem mais vulneráveis a ataques, logo para se proteger é necessário que haja certa preocupação quanto à segurança dos nossos dados e das informações na internet.

De acordo com (Tomé Sérgio, Faculdades Est Programa de Pós-Graduação Em Teologia, 2017) “O aumento da utilização de internet decorrente de valores mais acessíveis disponibilizados pelas operadoras do serviço de telefonia, houve um aumento significativo também de procedimentos não éticos por parte daqueles que querem lesar de alguma forma os usuários de computadores.”

Mas como realmente o usuário deve se proteger contra ataques maliciosos e não éticos por parte de pessoas mal intencionadas na internet?

De acordo com o centro de estudos, respostas e tratamento de incidentes de Segurança no Brasil (Cert.br, 2021)

> “ Com o objetivo de disseminar boas práticas de segurança e ampliar o nível de proteção dos usuários dos serviços de tecnologia da informação da ANAC, a Superintendência de Tecnologia da Informação (STI) reuniu nesta página dicas e recomendações de boas práticas voltadas à segurança da informação.
>
> O assunto foi dividido em dez tópicos e a página será atualizada semanalmente, sempre às quartas-feiras, com novas recomendações para promover a utilização mais consciente e segura de dispositivos digitais com acesso à Internet. A cada semana será apresentada uma nova cartilha com dicas práticas para o dia a dia sobre assuntos como senhas, privacidade, uso de redes sociais, entre outros.”

Os usuários precisam estar atentos à códigos maliciosos vírus ou malwares que são programas que pode entrar e infectar seu computador através de links ou anexo que são enviados por e-mail ou páginas via website, o usuário que tem seu host ou smartphone infectado pode contribuir para disseminação de spam e pode estar vulnerável a golpes.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

A privacidade nas redes sociais, quanto menos informações forem divulgadas nas redes sociais, se torna mais difícil do usuário ter seus dados furtados por pessoas maliciosas, é importante salientar que nesse caso podemos nos referir que “menos é mais”. Menos informações nas redes sociais é mais segurança para o usuário

É importante sempre manter o computador com o antivírus atualizado, de acordo com (Pereira Fernandes, cadernos bad 1, 2005)

> “Os antivírus são uma ferramenta essencial e a sua utilização é uma boa prática fundamental. A sua utilização e actualização regular é crucial, mais ainda quando se está ligado ao exterior, nomeadamente à Internet, seja para utilização do correio electrónico, para partilha de ficheiros, pesquisa de informação, para downloads ou qualquer outro motivo. O risco está sempre presente. Afinal de contas, todos os dias surgem novos vírus, aos quais há ainda a acrescentar os worms, os trojan horses, entre outros. Assim, a utilização dos antivírus tem que ser regular, sendo comum serem os próprios, sistemas que efetuam as atualizações e testes regulares.”

Ou no caso dos smartphones sempre ter instalado a última atualização de softwares, para corrigir possíveis erros ou falhas no sistema, que podem causar alguma brecha de Segurança.

Não abra links suspeitos ou duvidosos, os links podem ser enviados de diversas formas, ou plataformas, é importante ter uma atenção redobrada quando o assunto se trata de links, alguns links podem levar o usuário a sites falsos, outros podem infectar o aparelho apenas com um simples toque.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

Verifique sempre o domínio em sites, e e-mail, normalmente um site falso tem o mesmo layout do site original, muitos usuários acabam sendo enganados por conta disso, é importante reparar que o site de uma instituição oficial sempre terá no início do URL o protocolo Https (Hypertext transfer Protocol Secure) que indica que o site é seguro, porém o que seria esse Https?

HTTPS (Hypertext transfer Protocol Secure) é uma garantia em um bom nível e alto nível de confidencialidade entre o navegador (Browser) e o Servidor Web.

De acordo com (Bertagnolli Castro de Sílvia, Instituto Federal De educação, ciência e Tecnologia, 2014) “O protocolo HTTPS utiliza um mecanismo de criptografia mista, criando um canal criptográfico entre Navegador (Browser) e Servidor”)

2.2. Proteção De Senhas

De acordo com a empresa (kaspersky, 2019)

> “O uso de malware para coletar as senhas dos internautas cresceu significativamente em 2019. De acordo com os dados da Kaspersky, o número de usuários que sofreram ataques envolvendo roubo de senhas atingiu um pico de 940 mil pessoas – aumento de 60% em comparação com o primeiro semestre de 2018, quando este número ficou abaixo de 600 mil. O roubo de senhas (Password Stealing Ware – PSW) é uma arma importante no kit dos cibercriminosos para sabotar a privacidade dos internautas.”

Quais os cuidados que realmente devemos ter com nossas senhas? (Password), Certifique-se que não esteja sendo espionado ou observado por pessoas maliciosas enquanto digita sua senha, logins, ou nome de usuário, nunca forneça sua senha a terceiros (apenas em caso de pessoas em que você con Certifique-se de sair sites que necessitem de login, isso evita que suas informações sejam mantidas pelo (Browser), elabore senhas forte com 9 caracteres ou mais, onde envolvam números e letras maiúsculas e minúsculas, nunca utilize senhas fáceis de serem fia) mesmo assim o recomendado é não fornecer em hipótese alguma sua senha.

descobertas, como data nascimento, procure sempre ter uma senha diferente para cada site, cartão, ou aplicativos.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

Ao usar perguntas para identificação de recuperação de senhas evite usar palavras de fácil adivinhação, fuja do óbvio.

Conforme (“O centro de estudos, respostas e tratamento de incidentes de Segurança no Brasil, Cartilha de Segurança, Cert.br, 2021”)

“Uma senha bem elaborada é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada, se ela puder ser facilmente descoberta por um atacante.”

2 ANÁLISE E DIAGNÓSTICO

Após a análise do referencial teórico podemos afirmar que a internet além de ser uma ferramenta fundamental no nosso dia a dia, e que nos trás muitas comodidades, e facilidades, também é um lugar extremamente hostil e perigoso, onde precisamos estar sempre atentos, a segurança dos nossos dados.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

4. CONCLUSÃO

Concluímos que para manter a segurança das nossas informações e dados, é preciso sempre estar vigilante quando o assunto se trata de internet, é preciso estar atento a cada detalhe, desde a mensagem recebida pelo e-mail, quanto às mensagens que são recebidas via SMS, e também vários outros métodos que podem vir, a ocasionar em um furto de identidade, roubo de informações e dados dos usuários.

Cuidado com as máquinas (Host) ou Smartphones é fundamental, procurar sempre manter os dispositivos eletrônicos atualizados, antivírus, e softwares, e nunca divulgar os dados para terceiros ou sites desconhecidos, é importante que haja uma boa prática por parte do usuário quando o assunto se trata de segurança da informação.

5º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396, Centro Histórico de Porto Alegre – Rio Grande do Sul – maio – 2021.

5 REFERENCIAL

Cartilha de Segurança da Informação (< https://manuaisti.anac.gov.br/seguranca/cartilha//>) Acesso em 15/02/2021. Segurança da Informação (< https://blog.diferencialti.com.br/seguranca-da-informacao-praticas-para-usuarios//> 2019) Acesso em 15/02/2021. Segurança da Informação digital (Pereira Fernandes, cadernos Bad 1, 2005). Acesso em 15/02/2021. O uso da internet e Novas Tecnologias Numa Sociedade Conectada: Possibilidade Desafios, Perigos á luz da Ética, (Tomé Sérgio, 2017). Acesso em 08/02/2021. Número de Vitimas de Ladrões de Senhas cresce 60%, (https://www.kaspersky.com.br/blog/vitimas-ladroes-senhas-cresce-60/12114/) Acesso em 10/02/2021.

Desenvolvimento de Software II Introdução ao Desenvolvimento Web com HTML, CSS, Javascript e PHP (Bertagnolli Castro de Silvia, Instituto Federal De educação, ciência e Tecnologia, 2014).