Departamento Computação
Universidade Federal Rural de Pernambuco
(UFRPE)

Lucas Edson Silva de Araújo

Vazamento de Dados: Perigos de utilização da rede de WI-FI pública e formas de proteção.

Recife, PE – Brasil
2021

Abstract: Due to the growing number of data leaked from public WI-FI users, a discussion on the subject was created. The public network is quite vulnerable to attacks, often the spreading of scams, provided by leaked data, is now visible, aggravating the problem and worsening the image, most of these attacks are caused by the user's misinformation when using such a network. This article aims to understand the dangers of using public WI-FI, showing situations and examples. Also teach the user how to protect themselves from intruders using data protection tools and through good practices. Concluding the study with knowledge and concrete ways to assist the user in protecting their data.

Resumo: Devido a crescente nos números de dados vazados de usuários de WI-FI públicas, criou-se uma discussão sobre o assunto. A rede pública é bastante vulnerável a ataques, frequentemente a divulgação de golpes, proporcionados por dados vazados veem ah tona, agravando a problemática e piorando a imagem, grande parte desses ataques são causados pela desinformação do usuário ao usar tal rede. Este artigo tem objetivo o entendimento sobre os perigos de se usar a WI-FI pública, mostrando situações e exemplos. Também ensinar o usuário a se proteger de invasores usando ferramentas para proteção de dados e por meio de boas práticas. Concluindo o estudo com conhecimento e formas concretas de auxiliar o usuário na proteção de seus dados.

1. Introdução

Sessenta por cento dos consumidores em todo o mundo sentem que suas informações pessoais estão seguras ao usar Wi-Fi público, mas 53% não conseguem diferenciar uma rede Wi-Fi pública segura ou insegura. (Norton WI-FI Risk Report,2017).

Entretanto, elas não são bem assim, a vulnerabilidade das redes de WI-FI públicas será abordada nesse artigo, bem como as maneiras de se proteger de possíveis vazamentos de dados pessoais. Já que, no Brasil, cresce o furto de dados devido aos avanços tecnológicos e desinformação da sociedade. Por meio de conhecimento passado nesse artigo objetivamos a conscientização do leitor sobre os perigos e informamos maneiras de se proteger do mesmo.

Para abordagem da proposta, este artigo será dividido em três principais seções, são elas, introdução (Seção 1), desenvolvimento (Seção 2) e conclusão (Seção 3). Além disso, alguns subtópicos dentro das mesmas, (Seção 2) terá 2.1 Referencial teórico,2.2 perigos da utilização da WI-FI pública,2.3 Como usar WI-FI pública de maneira segura,2.4 Metodologia, 2.5

Objetivos e 2.6 Problemática e Justificativa. Seguida pela (Seção 3) e finalizando o artigo com as referências usadas para a sua construção.

2. Desenvolvimento

2.1 Referencial teórico

2.1.1 WI-FI

Wi-Fi é uma tecnologia de rede sem fio que permite que computadores (laptops e desktops), dispositivos móveis (smartphones e dispositivos vestíveis) e outros equipamentos (impressoras e câmeras de vídeo) se conectem à Internet. O Wi-Fi permite que esses e muitos outros dispositivos troquem informações entre si, criando uma rede.
A conectividade com a Internet ocorre por meio de um roteador sem fio. Quando você acessa o Wi-Fi, está se conectando a um roteador sem fio que permite que os dispositivos compatíveis com Wi-Fi façam interface com a Internet.

2.1.2 VPN

VPN é uma sigla, em inglês, para “Rede Virtual Privada” e que, como o nome diz, funciona criando uma rede de comunicações entre computadores e outros dispositivos que têm acesso restrito a quem tem as credenciais necessárias. Em outras palavras, você pode compreender a VPN como uma forma de criar pontes de ligação entre diferentes dispositivos via Internet, mantendo os dados de comunicação trocados entre eles codificados e mais seguros, já que sua interceptação se torna mais difícil.

2.1.3 HTTPS e HTTP

o HTTP (*Hyper Text Transfer Protocol*) é um protocolo, ou seja, uma determinada regra que permite ao seu computador trocar informações com um servidor que abriga um site. Isso quer dizer que, uma vez conectados sob esse protocolo, as máquinas podem receber e enviar qualquer conteúdo textual – os códigos que resultam na página acessada pelo navegador.
O problema com o HTTP é que, em redes Wi-Fi ou outras conexões propícias a phishing (fraude eletrônica) e hackers, pessoas mal intencionadas podem atravessar o caminho e interceptar os dados transmitidos com relativa facilidade. Portanto, uma conexão em HTTP é insegura.
Nesse ponto entra o HTTPS (*Hyper Text Transfer Protocol Secure*), que insere uma camada de proteção na transmissão de dados entre seu computador e o

servidor. Em sites com endereço HTTPS, a comunicação é criptografada, aumentando significativamente a segurança dos dados. É como se cliente e servidor conversassem uma língua que só as duas entendessem, dificultando a interceptação das informações.
Para saber se está navegando em um site com criptografia, basta verificar a barra de endereços, na qual será possível identificar as letras HTTPS e, geralmente, um símbolo de cadeado que denota segurança. Além disso, o usuário deverá ver uma bandeira com o nome do site, já que a conexão segura também identifica páginas na Internet por meio de seu certificado.

2.1.4 “Acess Point”

o “Acess Point”, pode ser compreendido como um tipo de repetidor Wi-Fi que usa cabos e não pode ser usado como substituto ao roteador, porque apesar de ter um papel importante na transmissão de sinal, este funciona como uma ferramenta auxiliar ao roteador WI-FI.

2.2 Perigos da utilização de WI-FI pública

2.2.1 “Man in the Middle”

Como o nome indica, os ataques “*Man in the Middle*”, que traduzido seria “homem no meio”, associados a conexões a redes Wi-Fi públicas, são geralmente relacionados com a presença de um intermediário entre a vítima e o site que esta visita, podendo o cyber-criminoso acessar aos seus dados enquanto navega na web.
Tratam-se de ataques altamente eficazes, e muito difíceis de detectar, já que as informações são interceptadas no meio do caminho quando se navega entre o dispositivo do usuário e o roteador, sem que seja percebido.

2.2.2 Transações conectadas a WI-FI pública

muitos usuários realizam compras e transferências on-line ou ingressando

ao “home-banking”, conectados a uma rede Wi-Fi aberta. Independentemente dos dispositivos aos quais se conecta, o uso de uma rede pública representará sempre um risco se pretende executar qualquer ação que envolva dados privados, porque, usando o princípio de “Man in the Middle”, não sabemos se alguém está interceptando o tráfego gerado.

2.2.3 Falsos “Acess Point”

É comum encontrar **redes Wi-Fi em locais públicos sem qualquer segurança**. Se for a um café, por exemplo, é normal o nome do local ser também o nome da rede e não necessitar de senha.

Nestes casos, é importante ter em mente duas coisas: Em primeiro lugar, e embora não seja **nunca aconselhável conectar-se a redes abertas**, se o fizer, verifique o nome da rede naquele local para ter certeza se é realmente o que se vê na tela. Por outro lado, é possível (e simples) para um atacante aproveitar essas conexões para cloná-las (montando uma rede com o mesmo nome) e usá-las como isca, enquanto espera que os usuários se conectem e acessem através dos seus dispositivos e liguem os seus equipamentos à antena do atacante. Se isso acontecer, todos os pacotes de conexão que entrarem e saírem passarão pelo criminoso, que poderá ver e modificar tudo à vontade. Por exemplo, a partir da ferramenta de código aberto **FruityWiFi**, criada para realizar auditorias de redes Wireless, alguém poderia montar uma falsa rede e a partir da mesma **alterar os endereços IP dos servidores DNS** da vítima para que apontem a servidores maliciosos.

2.3 Como usar WI-FI pública de maneira segura

Não é demais dizer que contar com uma solução antivírus instalada nos seus dispositivos, sejam laptops ou smartphones, é o primeiro passo para estar seguro. Depois disso, certifique-se de ter **sempre instalada a versão mais recente da solução**, garanta assim que todas as funcionalidades estejam atualizadas e prontas para evitar o acesso de apps indesejados.

Caso decida se conectar a uma rede Wi-Fi pública, é aconselhável usar a Internet para **visitar sites que não necessitem de credenciais nem qualquer outra informação pessoal**, como portais ou jornais, e não acessar a serviços de “home-banking”, contas de e-mail, redes sociais e outros aplicativos que necessitem de usuário e senha para estabelecer a conexão.

Caso, efetivamente, você se encontre fora do alcance de uma rede de confiança e precise realmente acessar a serviços tais como “home-banking” ou e-mail, considere a utilização dos seus dados móveis, se tiver essa possibilidade. Caso se trata do dispositivo que usa para trabalhar, use uma VPN e mantenha a sua informação criptografada.

O protocolo HTTPS garante que a informação transmitida entre o computador do usuário e o site seja **encriptada na sua transmissão**. E uma vez que o tipo de ações que levamos a cabo em **dispositivos móveis e/ou tablets** são praticamente as mesmas que a partir de qualquer computador de escritório ou laptop, é importante ter o cuidado de acessar a sites que utilizem o protocolo seguro de navegação. Para evitar que a conexão seja automática e evitar possíveis riscos, lembre-se de configurar o seu dispositivo para que lhe pergunte se quer conectar-se à rede do local onde está sempre que o visite.

Uma vez que tenha a sua **solução de segurança instalada, o seu Sistema Operacional atualizado, os serviços críticos desabilitados e confirmado com o local se a sua rede é aquela que diz ser** (fundamental), estará em condições para decidir se efetivamente quer estabelecer essa conexão. Nunca é demais ter uma camada extra de proteção, como a que é adicionada com a autenticação de dois fatores. A maioria dos serviços que utilizamos no dia a dia

contam com a possibilidade de configurar o acesso ao site com uma autenticação de dois fatores. Portanto, além da senha, é pedida a confirmação de que é mesmo o usuário da conta através da solicitação de um código adicional, que poderá ser enviado para o celular, através de um SMS, um e-mail, um app ou uma chamada.

A tecnologia sem fios facilita e agiliza o nosso cotidiano, contudo, e lamentavelmente, a sua popularidade é acompanhada de riscos, aos quais devemos estar atentos para que sejamos capazes de os prevenir, aplicando as medidas de segurança adequadas, protegendo a nossa informação e garantindo que possamos aproveitar a tecnologia da forma mais segura possível.

2.4 Metodologia

Para realização desse artigo, foi utilizado conhecimento adquirido de outros artigos, listados nas referências, bem como pesquisas em alguns web sites, referenciados em suas respectivas citações, ambas com intuito de compartilhar conhecimento sobre a rede WI-FI pública, seus perigos como a facilidade de furto de dados causada pela pouca informação do usuário e como se proteger usando alguns métodos ou adquirindo disciplina no uso da rede pública, como não utilização de aplicativos bancários. Afim de obter proteção para seus usuários.

2.5 Objetivos

2.5.1 Objetivos gerais

Propor ao usuário conhecimento por meio do artigo, visando entendimento sobre os perigos de se usar a WI-FI pública, mostrando situações e exemplos. Também ensinar o usuário a se proteger de invasores usando ferramentas para proteção de dados e por meio do conhecimentos no artigo.

2.5.2 Objetivos Específicos

- Conscientizar o leitor dos perigos e formas de proteção utilizando uma rede de WI-FI pública;
- Compartilhar informação de métodos de proteção para leigos no assunto;
- Auxiliar o usuário com sugestões de boas práticas ao utilizar WI-FI públicas visando proteção dos seus dados.

2.6 Problemática e Justificativa

Infelizmente, ninguém está imune a este problema num mundo cada vez mais conectado. Ao entrar em um lugar público onde há um Wi-Fi aberto disponível, certamente você será tentado a utilizá-lo para checar suas mensagens, redes sociais, e-mails, etc. No entanto, por trás da facilidade de acesso via rede pública, você pode colocar seus dados em perigo. Utilizar conexões criptografadas é uma ótima maneira de evitar que suas informações sejam roubadas. Para o uso diário, a proteção HTTPS é suficiente, indicando que seus dados estão criptografados e seguros. Hackear uma conexão dessas é muito mais difícil, tornando a vida de invasores mais complicada. Quando você acessa um site HTTPS, o seu navegador exibe um cadeado para indicar que a conexão é segura. Por outro lado, se o certificado digital do servidor não for válido, o seu browser exibirá um aviso. Evite ignorar estes avisos, eles são importantes para que você não acesse um site potencialmente inseguro, que poderá ser a porta de entrada para invasões. Também é viável proteger seu e-mail, habilita o firewall, utiliza a autenticação em duas etapas, desativa o compartilhamento de arquivos, evitar fazer uma transação financeira em WI-FI pública, use uma VPN, limpe os cookies de seu navegador, desligue o Wi-Fi quando não estiver usando.
Cada vez mais no Brasil o roubo de dados vem sendo abordado com frequência devido seu crescimento exorbitante com os avanços tecnológicos. Uma maneira de se roubar dados, principalmente de leigos sobre computação, é atacar em WI-FI públicas. Com minha pesquisa viso passar conhecimento sobre os riscos e proporcionar medidas para se proteger desses ricos, de acordo com o "iMaster” o Brasil é o terceiro país que mais sofre com ataques cibernéticos, com o conhecimento básico de proteção esse número tende a cair.

3. Conclusão

Portanto, com pesquisas e diversos artigos de apoio sobre segurança de dados, WI-FI públicas, abordamos algumas áreas importantes como os perigos e as formas de evitar vazamento de dados ao utilizar WI-FI públicas. Partindo de um estudo quantitativo, objetivamos o entendimento da relação usuário e

WI-FI pública, suas maneiras de acesso e principalmente suas vulnerabilidades, bem como passar conhecimento acerca de métodos de se proteger, desde práticas de bom uso como evitar acessar aplicativos bancários, como divulgação de métodos de proteção como a utilização de HTTPS para encriptar seus dados.

A partir disso, entendemos também que a fragilidade do uso de WI-FI públicas é pouco compreendido pela maioria dos usuários, com as informações passadas de proteção e os alertas de perigos objetiva-se a diminuição dessa desinformação do usuário, e abre espaço para continuação da pesquisa, visando novas formas de proteção e maneiras didáticas de aprendizado. Por fim, sanar a problemática situação de vazamento de dados pela rede de WI-FI pública.

Referências

Segurança e Privacidade: Proteção e tratamento de dados nos aplicativos de redes sociais Paulo Teruo Izumi[1], Daiane Mastrangelo Tomazeti[2] Curso Superior em Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto Federal de São Paulo - Campus Hortolândia (IFSP)

A SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO E O COMPORTAMENTO DOS USUÁRIOS INFORMATION SYSTEMS SECURITY AND USERS' BEHAVIOR Alexandre Manuel Santareno Pimenta Escola Superior de Gestão e Tecnologia, Instituto Politécnico de Santarém (ESGT-IPS), Santarém, Portugal Rui Filipe Cerqueira Quaresma Escola de Ciências Sociais – Universidade de Évora, Évora , Portugal

SEGURANÇA EM REDES DE COMPUTADORES UMA VISÃO SOBRE O PROCESSO DE PENTEST Pablo Marques Menezes 1 Lanay M. Cardoso2 Fabio Gomes Rocha

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: perspectivas baseadas na tecnologia da informação (T.I.)1 Oliveira, Gabriella Domingos de* Moura, Rafaela Karoline Galdêncio de ** Araújo, Francisco de Assis Noberto Galdino de ***

Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais Ana Vaz Administradora da Empresa de Gestão Partilhada de Recursos da Administração Pública (GeRAP)

Segurança de Dados
Brasscom - Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação
Relatório de Segurança de Dados, Inteligência de Mercado

SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO INFORMATION SYSTEMS SECURITY FABIANE RODRIGUES[1] MARCELO TEIXEIRA TORRES[2] FABIANA FLORIAN[3]

SEGURANÇA DA INFORMAÇÃO EM IOT
LEONARDO MASSAMI FUKUDA, UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ MBA EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, CURITIBA 2019

A SEGURANÇA DA INFORMAÇÃO E A SUA IMPORTÂNCIA PARA A AUDITORIA DE SISTEMAS
DALVAN CUNHA 1 MARCOS ALEXANDRE FENATO

Segurança em Banco de Dados: Uma visão geral sobre segurança e suas principais deficiências Marcos Vinicius Soares Santos, Diorgenes Ferreira, Marcos Paulo Maia Rodrigues, Renato César Oliveira Moreira

FACULDADE DE TECNOLOGIA DE SÃO PAULO LEANDRO FARIAS DOS SANTOS ABREU, **A Segurança da Informação nas Redes Sociais**, São Paulo 2011