WI-FI PÚBLICO RISCOS E SOLUÇÕES*

Jâmison de Mendonça Martins (UEMG Carangola)
Lucas Borcard Cancela (UEMG Carangola)
Luciano Dias de Souza(UEMG Carangola)
Maxwel dos Reis Silva (UEMG Carangola)

RESUMO

Observa-se o crescimento considerável de usuários conectados através das redes públicas. Acompanhando o aumento de usuários se conectando através de redes públicas sem fio, estão as ameaças relativas a ataques cibernéticos, invasões e roubo de informações, ocasionando problemas para os usuários que se sentem desprotegidos e vulneráveis a estes ataques. Portanto, como identificar se está navegando através de uma conexão segura? Diante deste contexto, o presente estudo apresenta uma análise sobre questões importantes relacionadas à circunspeção ao utilizar as redes Wi-Fi para se conectar à Internet. Além de apresentar os riscos e vulnerabilidades, este trabalho também visa demonstrar soluções preventivas e corretivas a fim de sanar tais adversidades, apontando sugestões sobre o que fazer para minorar a insegurança na rede. A metodologia utilizada trata-se de pesquisas qualitativas, que tiveram por base estudos bibliográficos e páginas na web.

PALAVRAS-CHAVE: Wi-Fi público. Redes de computadores. Segurança. Ameaças.

INTRODUÇÃO

As redes de computadores têm uma história peculiar. Criada com finalidade de proporcionar comunicação entre usuários e o compartilhamento de arquivos entre os mesmos, melhorando assim o fluxo de informações e a comunicação entre seus utilizadores, consta também que as redes foram desenvolvidas com fins de minimizar limites impostos por distanciamentos geográficos entre as pessoas.

Inicialmente limitada a conexões locais, nos dias de hoje existem inúmeras possibilidades para se conectar na rede e, dentre estas possibilidades, estão as redes cabeadas (que utilizam links de comunicação físicos como o cabo par trançado ou fibra óptica) e as redes sem fio (redes Wi-Fi), que serão estudadas neste trabalho.

Conforme ENGST & FLSIESHMAN (2005), a grande vantagem em instalar uma rede sem fio é a mobilidade. Há alguns anos, um cenário onde se permitia que as pessoas pudessem desfrutar da conectividade de uma rede sem a necessidade de fios era um tanto quanto futurista. Hoje a realidade mudou.

O usuário que deseja se conectar em uma rede necessita de tomar algumas precauções para se asseverar de que está conectado a uma rede segura e não em uma rede que servirá de porta de entrada de ataques cibernéticos por pessoas mal intencionadas. O fato é que não existe uma maneira de conectar que seja 100% segura. Até mesmo uma rede com equipamentos caros e que esteja bem configurada, está vulnerável a problemas relacionados a invasões e ataques.

Não existe um consenso referente ao início da utilização das redes wireless. Segundo Adam Engst e Glenn Fleish Man (2005), o uso das redes sem fio começou através de um projeto que interligou universidades no Havaí no ano de 1971. Porém, com a ideia de compartilhar dados entre computadores, elas começaram a se popularizar na computação pessoal em meados do ano de 1980.

Impulsionada pelo desenvolvimento das telecomunicações aliadas com a imprescindibilidade das pessoas se manterem informadas e conectadas, as redes Wi-Fi se tornaram extremamente populares nos últimos anos.

Segundo a SYMANTEC (2006), a utilização das redes sem fio está se multiplicando cada vez mais à medida que a qualidade das mesmas vai melhorando e os preços dos equipamentos vão se tornando mais acessíveis.

1 WI-FI

De acordo com o site institucional da Wi-Fi Alliance o termo "Wi-Fi" foi criado em 2000 pela Wi-Fi Alliance, rede mundial de empresas que estabelece tecnologias e softwares Wi-Fi inovadores. Além disto, certifica produtos que cumprem os padrões de qualidade, desempenho, segurança e capacidade.

> In 1999, several visionary companies came together to form a global non-profit association with the goal of driving the best user experience, regardless of brand, using a new wireless networking technology. In 2000, the group adopted the term "Wi-Fi®" as the proper name for its technical work and announced its official name: Wi-Fi Alliance. Since our start, every year an increasing number of member companies works within Wi-Fi Alliance to improve the interoperability, ubiquity, and value of Wi-Fi. (https://goo.gl/QfmGXt).

A tecnologia IEEE 802.11, que possibilita a conexão de dispositivos sem fio, é o que vem sendo chamado informalmente de "Wi-Fi".

1.1 Pontos de wi-fi público

Os pontos públicos de acesso à internet estão cada vez mais fáceis de se encontrar. Muitos estabelecimentos comerciais disponibilizam suas redes Wi-Fi para atrair clientes, praças públicas em alguns municípios e até mesmo em transporte público é possível conectar-se à internet por meio de rede Wi-Fi.

Uma das grandes vantagens é o pequeno custo, quando cobrado pelos proprietários das redes, ou até mesmo custo zero por este serviço adicional. Outra atração é a velocidade e acesso sem franquia de downloads, uma grande oferta em relação aos planos de rede móvel disponíveis pelas operadoras de telefonia móvel.

Os acessos às redes públicas são realizados por meio de autenticação sem senha, ou com senha fornecida pelo proprietário da rede aos interessados.

2 FALTA DE SEGURANÇA AO USAR WI-FI PÚBLICO

Segundo ASSOLINI; IKEDA et al (https://goo.gl/Pnai9X, 2013), não é seguro acessar à internet em redes Wi-Fi públicas. A falta de segurança se dá pela possibilidade de captura dos dados trafegados nessas redes.

> Não é seguro, segundo Fábio Assolini, analista sênior de malware da Kaspersky, empresa especializada em segurança. É preciso tomar várias precauções básicas ao usar essas redes. "Qualquer dado trafegado nesse Wi-Fi público pode ser capturado por alguém mal-intencionado naquele mesmo local", alerta. (https://goo.gl/HGDF6Y, 2013).

Thiago Hyppolito, engenheiro de produtos da McAfee no Brasil, complementa que a intrusos desfrutam das falhas de segurança proporcionados pelos roteadores, que partilham a internet por ondas de rádio (IEEE 802.11).

Hyppolito; TAGIAROLI (https://goo.gl/QgdSZK, 2015) também diz que não é necessário muito conhecimento de computação para a interceptação de dados pois há tutoriais na internet explicando o procedimento.

O monitoramento da rede e a coleta de dados como senhas de banco e login de e-mail e outros semelhantes.

2.1 Amizade inconfiável na rede

Segundo JORDÃO (https://goo.gl/HGDF6Y, 2013) uma rede doméstica normalmente possui firewall e senha de autenticação a rede para proteger seu(s) computador(es) à tentativa de acesso externo aos dados da rede.

Ele afirma também que uma rede Wi-Fi pública há dezenas ou até mesmo centenas de conexões simultâneas. O firewall dos roteadores entende que todos os dispositivos conectados sejam "amigos" e com isto, não impede a conexão entre os dispositivos, permitindo invasão com possibilidades de captura, exclusão ou alteração de dados do dispositivo infiltrado.

2.2 Você pode estar conectado à rede errada

Algo que poucos suspeitam é a criação de uma rede falsa. Esta é uma das técnicas usadas para interceptação de dados. Wi-Fi públicos com nomes de estabelecimentos comercias são os mais comuns para tal técnica.

JORDÃO (https://goo.gl/HGDF6Y, 2013) alerta que nestes casos, a configuração da rede falsa pode desviar o tráfego de dados para uma coleta.

3 ACESSO À INTERNET EM WI-FI PÚBLICO COM SEGURANÇA

Visto que as redes Wi-Fi públicas não proporcionam devida segurança para a conexão à internet e identificado cada falha de segurança, foram desenvolvidas algumas soluções.

Alguns cuidados são necessários para realizar uma conexão a fim de minorar a insegurança na rede.

3.1 Acesso com cautela

Realizando conexão em redes públicas sem proteção, atividades de riscos devem ser evitadas para maior segurança.

Com isto, o melhor a fazer é realmente aguardar para acessar uma rede doméstica, por exemplo, que possui risco inferior a rede pública, ou utilizar outros métodos mais satisfatório no quesito privacidade dos dados trafegados na rede.

3.2 Rede móvel

Se preciso realizar navegação que haja a necessidade de efetuar login ou até mesmo operações bancárias, o recomendado é a utilização das tecnologias 3G ou a 4G. A última ainda não se encontra disponível em todo o território nacional.

3.3 Verificar autenticidade da rede

Falsa autenticidade da rede é a armadilha despercebida por muitos usuários das redes.

Estabelecimentos comerciais tendem a utilizar senhas para permitirem o acesso de seus clientes e a disponibilizam ao efetuarem compras ou simplesmente no balcão principal.

4.4 VPN

Uma Rede Particular Virtual (Virtual Private Network – VPN) é uma forma viável de conexão direta de dois computadores ao usar Wi-Fi público como um tunelamento,

Na VPN, os dados são criptografados e encapsulados para serem enviados. Informações extras, como endereço IP, são anexadas aos dados a serem enviados ao computador de destino.

O computador destinatário recebe o pacote de dados, desencapsulados, por meio de um “túnel” que o liga ao computador remetente, que é identificado por suas informações anexadas ao pacote de dados. Concluindo a transmissão com a descriptografia e armazenamento dos dados.

CONCLUSÃO

O presente artigo teve por objetivo analisar os riscos e soluções das redes Wi-Fi públicas, apresentando as vulnerabilidades e os principais métodos de conexão com maior confiabilidade.

As redes Wi-Fi públicas oferecem riscos quando realiza-se conexão à internet sem as devidas medidas de proteção, assim como qualquer ambiente lógico não possui total segurança.

É importante que os usuários, ao se conectarem em redes desconhecidas, tenham certos cuidados quanto às ameaças eminentes.

REFERÊNCIAS

ENGST, Adam; FLEISHMAN, Glenn. **Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh.** 2ª ed.: São Paulo. Ed.: Pearson Makron Books. 2005.

IKEDA, Ana. **Wi-Fi público: saiba como tirar proveito da internet sem fio gratuito. 2013.** Disponível em: <https://goo.gl/Pnai9X>. Acesso em 10 mar. 2017.

JORDÃO, Fabio. **Quais os riscos de usar um WiFi público?. 2013.** Disponível em: <https://goo.gl/HGDF6Y>. Acesso em 9 mar 2017.

SYMANTEC. **Implementando Uma LAN Sem Fio Segura. 2006.** Disponível em: <http://www.symantec.com/region/br/enterprisesecurity/content/framework/BR_3074.html>. Acesso em 12 mar. 2017.

TAGIAROLI, Guilherme. **Usar rede Wi-Fi aberta oferece riscos aos usuários. 2015.** <https://goo.gl/QgdSZK>. Acesso em 10 mar. 2017.

WI-FI ALLIANCE. **Who We Are.** Disponível em: <https://goo.gl/QfmGXt>. Acesso em 9 mar. 2017.