OS PERIGOS DE REDES WIFI ABERTAS

Alex Rafael Oneda[1], Guilherme Schweitzer[2], Layne Laís de Castilho Firmino[3], Fabiano de Oliveira Wonzoski[4]

1. Discente do Curso de Ciência da Computação, UNOESC, Videira, SC
2. Discente do Curso de Ciência da Computação, UNOESC, Videira, SC
3. Discente do Curso de Ciência da Computação, UNOESC, Videira, SC
4. Docente do Curso de Ciência da Computação, UNOESC, Videira, SC

Autor correspondente: Alex Rafael Oneda, a.oneda@unoesc.edu.br

Área: Ciências Exatas e Tecnológicas

Introdução: O acesso gratuito à internet por meio de redes WiFi abertas frequentemente disponibilizadas em locais públicos como shoppings, restaurantes, praças e aeroportos tem se tornado cada vez mais comum. Apesar de proporcionar praticidade e conectividade, essas redes apresentam sérios riscos à segurança da informação. Sua principal fragilidade esta na ausência de criptografia e da facilidade de acesso por pessoas mal-intencionados, o que deixa seus usuários expostos a ataques cibernéticos. Genaro analisou ambientes públicos e destacou que, mesmo em redes WiFi abertas, é possível identificar nós, capturar pacotes e varrer portas, evidenciando que ambientes públicos podem ser ainda menos seguros que ambientes corporativos. **Objetivo:** Análise dos perigos de utilizar redes WiFi abertas. **Método:** Este estudo se foi realizado através de uma pesquisa de forma qualitativa, com foco exploratório e descritivo, baseada em uma análise de bibliografias e documentos. **Resultados:** Existe uma semelhança nos documentos, a falta de criptografia é a principal vulnerabilidade das redes WiFi abertas. Assim como, a ausência de um método de autenticação seguro, o que facilita ataques como o Man-in-The-Middle. Também foi mencionado a criação de redes falsas, conhecidas como honeypots, usadas para capturar informações dos usuários. Vários estudos ainda reforçam que os usuários muitas vezes não estão conscientes dos riscos e acabam acessando contas bancárias, links e pastas de e-mails ou redes sociais em conexões inseguras, sem usar ferramentas de proteção como autenticação em duas etapas ou conexões HTTPS. **Conclusão:** As redes Wi-Fi públicas, embora sejam práticas e bastante acessíveis, trazem vários riscos que podem comprometer a segurança das informações dos usuários. Por não utilizarem criptografia ou por não terem uma autenticação adequada. Os principais perigos que identificamos incluem os ataques do tipo Man-in-The-Middle. Outro risco comum são os ataques Evil Twin, onde um invasor cria uma rede falsa para capturar senhas e informações pessoais dos usuários. Além disso, há também o risco de vazamentos de dados, especialmente quando as pessoas acessam serviços sensíveis sem tomar os devidos cuidados, colocando suas informações em risco. A recomendação mais importante é evitar, sempre que possível, usar redes públicas para atividades que envolvam dados pessoais ou financeiros. Quando o uso dessas redes for inevitável, é essencial tomar medidas de proteção, como usar uma VPN, desativar recursos de compartilhamento automático, adotar autenticação de múltiplos fatores e criar senhas específicas, diferentes das contas principais.

Palavras-chave: Uso da Internet; Análise de Vulnerabilidade; Internet; Redes de Comunicação de Computadores; Segurança Computacional.

Agradecimentos: Os autores Alex R. Oneda e Guilherme Schweitzer agradecem ao programa Universidade Gratuita, do Governo do Estado de Santa Catarina, pela concessão de bolsas para o custeio integral das mensalidades do curso de Ciências da Computação da Universidade do Oeste de Santa Catarina (UNOESC), campus de Videira – SC. A autora Layne Laís de Castilho Firmino agradece ao Programa Universidade para Todos (PROUNI), do Governo Federal, pela concessão de bolsa destinada ao custeio integral das mensalidades do curso de Ciências da Computação da Universidade do Oeste de Santa Catarina (UNOESC), campus de Videira – SC.