**Faculdade de Tecnologia de Sorocaba Tecnologia em Análise e Desenvolvimento de Sistemas**

**Programação para WEB**

**SEGURANÇA NA WEB**

**Prof.º Denilce de Almeida**

**Disciplina: Programação para WEB**

Yasmin Silva Rosa 0030482111018

**Sorocaba / Agosto**

Segurança na web

**ÍNDICE**

1. O que é segurança na web? ............................................4
2. Ameaças mais comuns ....................................................4

2.1 Phishing .....................................................................4

2.2 Malware e malvertising .............................................4

2.3 Ransomware .............................................................4

2.4 Botnets ......................................................................4

2.5 Ameaças a Wi-Fi, público ou doméstico ....................4

1. Qual a importância? .........................................................5
2. Conclusão .........................................................................6
3. Referência ........................................................................7

**INTRODUÇÃO**

Neste trabalho será apresentado a importância e exemplos de segurança da web, os mais perigosos que ocorrem consequentemente, a partir disso, a importância da segurança tem vários aspectos por ocorrer falhas na segurança em muitos softwares a quais não são visados pelo programador, assim ocorrem os vazamentos de dados, e ter mais cautela e foco na segurança ajuda a ter mais qualidade e feedback positivo de seus clientes.

1. **O QUE É SEGURANÇA NA WEB?**

segurança web se concentra em proteger sites, aplicativos baseados na internet e serviços online contra uma variedade de ataques maliciosos. Deste modo, ela serve para garantir o bom funcionamento e desempenho dos sites. As vulnerabilidades das aplicações web permitem que fatores maliciosos tenham controle não autorizado sobre o código-fonte, manipulem informações privadas ou interrompam o bom funcionamento da aplicação

1. **AMEAÇAS MAIS COMUNS**

**2.1 Phishing**

Ele consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

**2.2 Malware e malvertising**

O Malvertising é um tipo de anúncios online maliciosos que visam infectar usuários com malware ou outras coisas indesejadas.

**2.3 Ransomware**

Ransomware é um tipo de malware (software malicioso) utilizado por cibercriminosos. Se um computador ou rede for infectado com ransomware, o ransomware bloqueiao acesso ao sistema ou criptografa os dados. Os cibercriminosos exigem dinheiro de resgate de suas vítimas em troca da liberação dos dados.

**2.4 Botnets**

é uma rede de computadores infectados que podem ser controlados remotamente e forçados a enviar spam, espalhar malware ou preparar ataques de DDoS sem o consentimento dos proprietários do dispositivo.

**2.5 Ameaças a Wi-Fi, público ou doméstico**

A maior ameaça à segurança do Wi-Fi gratuito é a capacidade de um hacker posicionar-se entre você e o ponto de conexão. Então, em vez de falar diretamente com o ponto de acesso, você está enviando suas informações para o hacker, que pode retransmiti-las.

Maneiras de evitar isso é manter o antivírus e firewall ativos e atualizados, atualize seus softwares, cuidado ao fazer downloads, troque senhas de tempos em tempos, atenção aos anexos de e-mail, redes sociais e SMSs, não forneça dados pessoais, use a verificação em duas etapas.

1. **QUAL A IMPORTÂNCIA?**

É uma maneira eficaz de monitorar o ambiente virtual e investir em segurança é o caminho para conquistar a confiabilidade de seus clientes e pode ser um diferencial para a sua empresa se destacar no mercado altamente competitivo de hoje. Criminosos na internet tentam de diversas formas tornar um usuário desprotegido ou despreparado em uma vítima de ataque cibernético. Vírus no sistema, e-mails falsos e até sites muito bem construídos, com aparência idêntica ao verdadeiro são algumas das formas de conseguir um atacar usuários de internet.

1. **CONCLUSÃO**

Ao ter o conhecimento sobre a segurança na internet, vimos o que pode ocorrer caso seja vulnerável, temos a privacidade e segurança na qual nossos dados são armazenados, caso ocorra o vazamento desses dados pode haver perigos como perdas de dados da conta de banco, sendo a consequência perder todo dinheiro de sua conta, a importância da segurança é essencial para a vida no mundo da tecnologia, pois sem ela seria um caos e perdas de dados importantes e riscos inimagináveis, por isso temos que ter a qualidade e segurança de nossos softwares, para que os dados armazenados dos nossos clientes não tenham o risco de vazamentos e assim sendo algo que prejudique seus clientes e o nome da sua empresa. Ameaças à segurança na internet aumentam a cada dia. Somente no Brasil, em 2016, houve um aumento de 138% em ataques a sites principalmente de pequenas e médias empresas. Isso ocorre porque geralmente são as mais vulneráveis, uma vez que não dispõem de uma boa infraestrutura de TI e de políticas de segurança. Dessa forma, é de suma importância que o pensamento dos empresários mude e eles passem a investir em políticas de segurança que visem à proteção e recuperação de dados.

1. **REFÊRENCIA**

<https://www.eset.com/br/artigos/dicas-de-seguranca-na-internet/>

<https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo>

<https://www.kaspersky.com.br/blog/o-que-e-o-malvertising/3914/>

<https://www.kaspersky.com.br/resource-center/threats/ransomware-attacks-and-types>

<https://www.avast.com/pt-br/c-botnet>

<https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi-risks>

<https://www.linksan.com.br/qual-a-importancia-da-seguranca-na-internet-em-um-e-commerce/>

<https://www.lumiun.com/blog/o-que-e-seguranca-na-internet-e-por-que-e-importante/>

<https://blog.rebel.com.br/seguranca-para-internet-entenda-o-que-e-sua-importancia-e-como-usar/>