

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**SEGURANÇA NA WEB**

ATIVIDADE 2

Prof.ª Denilce de Almeida Oliveira Veloso

Disciplina: Programação Web

Everton Carlos da Silva 0030481913011

Sorocaba

Fevereiro/2021

**INTRODUÇÃO**

Podemos entender como **Segurança na Internet** todas os cuidados que devemos ter para proteger as coisas que fazem parte da internet como a infraestrutura, que podem ser nossos [**computadores**](https://edu.gcfglobal.org/pt/informatica-basica/o-que-sao-os-computadores/1/) e as informações, que são as mais atacadas pelos **[cibercriminosos](https://edu.gcfglobal.org/pt/seguranca-na-internet/proteja-seu-computador-de-ameacas-na-internet/1/" \t "_blank)**. A segurança informática cria métodos, procedimentos e normas que buscam identificar e eliminar as vulnerabilidades das informações e dos equipamentos físicos, como os computadores. Este tipo de segurança conta com bases de dados, arquivos e aparelhos que fazem com que as informações importantes não caiam em mãos de pessoas erradas.

**OS PRINCIPAIS RISCOS DA INTERNET**

Algumas das coisas que os cibercriminosos tentam fazer pela Internet são:

* Roubar informações
* Corromper informações
* Atacar sistemas ou equipamentos
* Roubar identidade
* Vender dados pessoais
* Roubar dinheiro

Os criminosos cibernéticos usam várias maneiras para atacar uma vítima na rede. Eles podem por exemplo, usarem [**vírus**](https://edu.gcfglobal.org/pt/virus-e-antivirus/o-que-e-um-virus/1/) para tentar romper o sistema e alterar o funcionamento dos aparelhos eletrônicos. Outra modalidade é o **[phishing](https://edu.gcfglobal.org/pt/seguranca-na-internet/fraudes-e-spam-no-email/1/" \t "_blank)**, onde o cibercriminoso se passa por uma pessoa diferente através de e-mails, mensagens instantâneas ou redes sociais, para conseguir informações confidenciais, como [**senhas**](https://edu.gcfglobal.org/pt/seguranca-na-internet/senhas-o-primeiro-passo-para-a-seguranca/1/), números de cartões de crédito, e outros.

**COMO EVITAR?**

Se alguém lida com muitas informações e possui vários equipamentos, como no caso das empresas, é melhor solicitar ajuda de profissionais que trabalham com segurança na Internet. Por outro lado, como usuário comuns, podemos adotar várias medidas preventivas, tais como manter ativos e atualizados os [**antivírus**](https://edu.gcfglobal.org/pt/virus-e-antivirus/o-que-sao-antivirus/1/) em nossos aparelhos que acessam à Internet, evitar fazer [**transações financeiras**](https://edu.gcfglobal.org/pt/seguranca-na-internet/transacoes-financeiras-seguras-na-internet/1/) em redes abertas ou em computadores públicos e verificar os arquivos anexos das mensagens de estranhos, evitando baixá-los se não tiver certeza do seu conteúdo.

**CONCLUSÃO**

É fundamental que os gestores elaborem uma estratégia clara para garantir segurança no processo de desenvolvimento da aplicação, estruturando métodos para que sua equipe e os fornecedores possam desenvolver aplicações mais seguras, fazendo a avaliação e testes da [segurança do ambiente](http://blog.conviso.com.br/4-boas-praticas-de-code-review-para-um-ambiente-realmente-seguro/) e das aplicações projetadas pela equipe e fornecedores, além de desenvolver um projeto de Gestão de Vulnerabilidades e testes de segurança para garantir que suas aplicações estarão sob nítido controle.

**REFERENCIAS**

*https://blog.convisoappsec.com/saiba-como-aumentar-a-seguranca-de-aplicacoes-web/* - Acesso em 17/02/2021.

*https://cartilha.cert.br/seguranca/* - Acesso em 17/02/2021.

*https://edu.gcfglobal.org/pt/seguranca-na-internet/o-que-e-seguranca-na-internet/1/* - Acesso em 17/02/2021.