Nome: Gustavo Barbato Ribeiro da Mota RA: 0030482221009

**Segurança na Web**

# Introdução

A navegação na internet se tornou parte do cotidiano de quase todas as pessoas e a sua utilização exige uma série de informações sobre o usuário, como em sites de compra, que exigem o seu endereço, nome completo, CPF, número de telefone, endereço de e-mail e, muitas vezes, dados do cartão de crédito. Com tantos dados sensíveis sendo salvos todos os dias na Web, a segurança desses dados se torna essencial para o pleno funcionamento do sistema.

# Ameaças Comuns à Segurança na Internet

Existem diferentes tipos de ataques na internet que visam desde de roubar os seus dados mais sensíveis até enganar se passando por um representante de alguma empresa ou provedor de serviços e, até mesmo, pessoas famosas. Dentre os diferentes tipos estão:

## Phishing

O Phishing é um tipo de ataque virtual que envolve o envio de e-mails enganosos com o objetivo de enganar os remetentes para que acreditem ser uma mensagem genuína, como uma mensagem do banco ou uma nota de um colega de trabalho. O Phishing é uma das técnicas mais antigas de ataques a segurança na internet, remontando aos anos 90.

## Hackeamento e Acesso Remoto

Os hackers buscam explorar vulnerabilidades nas redes com o intuito de acessar informações sensíveis e até mesmo performar tarefas e transações não autorizadas, como mover dinheiro de uma conta bancária. O protocolo que permite aos usuários controlar um computador conectado à Internet remotamente é chamado de Remote Desktop Protocol, ou RDP. Como empresas de todos os tamanhos usam amplamente o RDP, as chances de uma rede estar inadequadamente protegida são relativamente altas. Os hackers usam diferentes técnicas para explorar vulnerabilidades de RDP até que tenham total acesso a uma rede e aos seus dispositivos. Eles mesmos podem roubar dados ou vender as credenciais na dark web.

## Ameaças a Wi-Fi, Público ou Doméstico

O wi-fi público é o que apresenta o maior risco a cibersegurança do usuário, pois na maior parte dos casos apresenta segurança inadequada ou nenhum tipo de segurança aos dispositivos conectados na rede. O wi-fi doméstico apresenta um menor risco à segurança na rede, mas as empresas provedoras de serviço de internet podem vender os seus dados, mesmo que de forma anônima.

# Como Proteger os seus Dados Online

Saber das ameaças e o que elas podem causar são uma parte da resolução do problema de segurança na internet, a outra parte é saber como se proteger no espaço virtual e praticar os ensinamentos.

## Autenticação Multifatorial

É um método de autenticação que pede aos usuários pelo menos 2 métodos de autenticação, além da senha. Alguns meios comuns para a autenticação multifatorial são: e-mail com um código único para acesso, mensagem no celular com um código único, aplicativo autenticador em um dispositivo móvel ou a impressão digital. Esse método aumenta o nível de segurança, pois o invasor precisará obter diversas senhas para acessar a conta, ao invés de apenas uma.

## Firewall

O firewall funciona como uma barreira entre seu computador e outras redes, como a internet. Normalmente os sistemas operacionais mais comuns para desktop já vem com um firewall instalado, eles ajudam a bloquear tráfego indesejado e impedem que malwares infectem o seu computador.

# Conclusão

Em conclusão, a segurança na internet é um assunto sério e deve ser levada a sério por todos que navegam a web. Desde hackers até e-mails enganosos, a internet está repleta de usuários mal intencionados e se proteger dessas ameaças depende de várias etapas, como evitar wi-fi público, usar autenticação multifatorial e ter um firewall no seu dispositivo.

# Referências

<https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security~>