# 1. Segurança na Internet

Quando você atravessa a rua deve olhar para os dois lados antes de atravessar e atravessar sempre em uma faixa de segurança, quando você vai tomar banho de piscina não deve se aventurar em locais profundos se não souber nadar. A vida toda você toma precauções de segurança para lidar com diversas situações. Na internet isso não é diferente.

Existem diversos tipos de programas que podem prejudicar seu computador, roubar dados importantes e até mesmo apagar seus arquivos. Todos estes programas – chamados de Malware – podem ser instalados em seu computador pela internet sem que você perceba.

Por isso, você deve tomar certas precauções quando estiver navegando na internet. Isso é o que aprenderemos nesta aula.

## 1.1. Como manter seu computador seguro

Em primeiro lugar, é importante saber que nem tudo são espinhos na internet. Existem diversos programas e sistemas de segurança que tentam criar verdadeiros muros em torno de seu computador para que arquivos ou programas maliciosos não entrem.

Se você fizer uso destes programas e cuidar sempre com o que está sendo instalado em seu computador – utilizando sites seguros para fazer download de arquivos, por exemplo – você provavelmente terá uma vida tranquila enquanto navega na Internet.

A primeira e talvez uma das mais importantes dicas que você deve levar em consideração é: não existe site totalmente seguro.

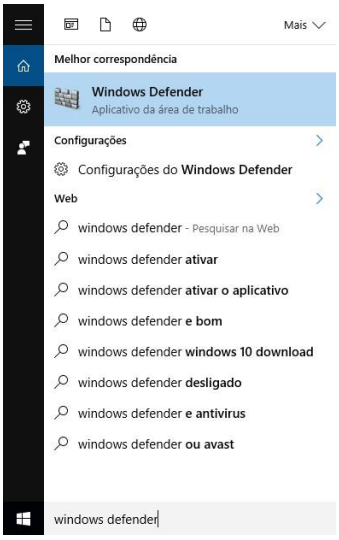
Mesmo que você esteja utilizando o Facebook, você pode clicar em um link que te envie para outra página que não tenha o mesmo esquema de segurança do Facebook.

Mesmo que você esteja em um chat com um amigo, o arquivo que ele lhe passou pode nem mesmo ter sido ele quem tenha passado – sim, existem vírus que se espalham automaticamente, enviando-se para seus contatos sem que você sequer saiba disso, fingindo ser você!

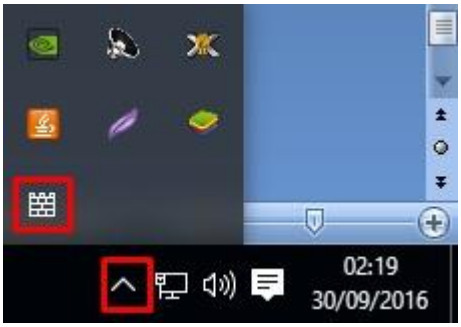
Por isso, é muito importante seguir as dicas que serão dadas abaixo:

## 1.2. Como navegar seguramente

1) Sempre mantenha seu Windows Defender ativado.
   O Windows defender é o sistema de proteção contra Malware do Windows. Você pode acessá-lo utilizando a barra de pesquisa do iniciar do Windows.

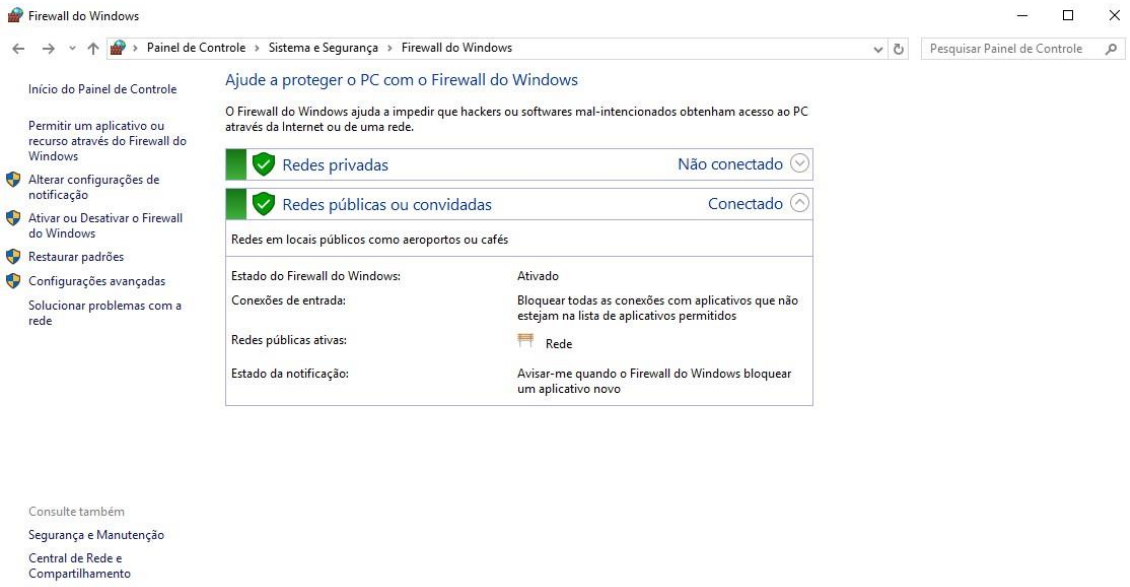



Ou visualiza-lo na barra de ferramentas do Windows, próximo a barra de notificações.




Enquanto este símbolo estiver ativo, você estará mais seguro.

2) Manter o Firewall do Windows sempre ativado.
   O Firewall do Windows é um protetor que está sempre ativo esperando uma potencial ameaça para protegê-lo.
   Para acessar o Firewall do Windows você poderá clicar com o botão direito sobre o ícone do iniciar, apontar para painel de controle, e então em Sistema e segurança, Firewall do Windows.




Mantenha este Firewall sempre ativo, ele protegerá seu computador de ameaças externas.

3) Jamais clique em links desconhecidos ou Banners muito chamativos, com propagandas grandes ou fotos indecentes.

4) Sempre que for receber um arquivo de um amigo ou conhecido, pelo facebook, whatsapp, ou quaisquer outros chats, sempre pergunte a ele se foi ele mesmo quem lhe enviou o arquivo e se é confiável.

5) Nunca abra anexos em emails de pessoas que você não conheça. Se for de alguma empresa, ou tipo de propaganda sempre envie um email de volta perguntando se é seguro e ainda assim sempre tenha cuidado. Emails estão entre os maiores distribuidores de vírus e outros malwares da internet.

## 1.3. O que são Malwares?

Malwares são, basicamente, programas maliciosos. Programas que possuem diferentes e péssimos propósitos.

Alguns são usados para causar dano, roubar informações, divulgar serviços que você não tem intenção de visualizar, etc.

Os tipos de Malwares mais conhecidos e a explicação para cada um deles são:

1) Vírus:
   Vírus é o tipo mais conhecido de Malware. E não é por menos, sua péssima reputação se deve ao fato de serem programas que se espalham automaticamente para outros arquivos e sempre tentam uma forma de se transmitirem para outros usuários, como um vírus biológico real.
   Estes são, de longe, os programas mais utilizados para causar danos e roubar informações. Por sua capacidade de se espalhar para outros computadores, são também os recordistas de prejuízos causados.

2) Trojan Horse (Cavalo de Tróia):
   Trojan, forma abreviada de seu nome, é um tipo de malware que se instala disfarçado de outros aplicativos.
   Por exemplo, digamos que você vá instalar um papel de parede animado, dentro do instalador deste papel de parede podem estar instruções para instalar algo que você, na verdade, não gostaria de instalar. Daí o nome destes arquivos, que se disfarçam de outros aplicativos para serem instalados forçadamente em seu computador.

3) Spywares:
   Spywares são programas que gravam sua navegação, como páginas visitadas, textos digitados, informações pessoais, etc.
   São os programas mais utilizados para roubo de informações sigilosas, como senhas logins, etc.
   Se você usa contas bancárias ou cartões de crédito em seu computador deve ter um cuidado dobrado com estes malwares. Hoje em dia existem alguns anti-spywares totalmente desenvolvidos para barrar estes malwares.
   O Spybot é um exemplo.

## 1.4. Exercícios de Conteúdo

Responda as questões a seguir:

1) O que são Malwares?
2) Qual a principal diferença entre vírus e spywares?
3) Para que serve o Firewall do Windows?
4) Como saber se o arquivo enviado por um amigo é seguro?
5) Quais anexos de E-mail não devemos abrir?

CLIQUE AQUI
PARA CONCLUIR