## O QUE É O VÍRUS NO ROTEADOR?

Esse vírus não é considerado um [malware](https://blog.intnet.com.br/saiba-o-que-e-e-como-proteger-seu-computador-contra-malware/), porém pode causar os mesmos problemas de um. Ele ataca os roteadores de uma rede — dispositivos responsáveis por gerenciar a conexão entre os aparelhos conectados.

O resultado é a confusão no DNS do dispositivo, alterando seu funcionamento. Dessa forma, em vez de navegar em sites seguros, os dispositivos são direcionados a páginas falsas e maliciosas. O objetivo dessa prática pode ser faturar com visualizações de anúncios ou, até mesmo, roubar dados pessoais.

### O QUE É DNS?

DNS é a sigla para *Domain Name System* (ou Sistema de Nomes e Domínios, em português). Essa é a configuração que realiza a conversão entre uma busca de acesso em palavras e seu significado na rede.

Para entender melhor, quando você busca por “www.google.com”, esse termo é recodificado para o IP do site, que, normalmente, é um número de 10 dígitos — nesse caso, seria 87.245.200.153. Se houver vírus, em vez de seguir o padrão normal, usa-se um padrão criado para enganar o usuário e direcioná-lo a páginas perigosas.

## COMO ESSE VÍRUS FUNCIONA?

Existem dois tipos de ataques ao roteador. O primeiro ocorre de forma remota, ou seja, não há interação entre o usuário e o roteador. Nenhum dispositivo precisa estar ligado e nenhuma pessoa tem a necessidade de realizar alguma ação. Tudo é feito a partir de um distribuidor de rede que, por meio de um software (o firmware), altera o DNS.​

Já o segundo modelo de ataque requer uma interação com o usuário: ele deve estar conectado à rede para ser infectado. Normalmente, o processo se inicia com o recebimento de um e-mail que contém um link para algum site. A mensagem pode conter diversas imagens e conteúdos que, quando clicados, acionam comandos que fazem a alteração.

Em ambos os casos, o [roteador](https://blog.intnet.com.br/como-escolher-um-roteador-wifi-confira-nossas-5-dicas/) é alterado e os problemas começam a surgir para os usuários. Vamos falar sobre isso no próximo tópico. Continue lendo para conferir!

## QUAIS OS SINTOMAS NO COMPUTADOR E DURANTE A NAVEGAÇÃO?

Uma vez que o DNS é alterado, o roteador passa a direcionar todas as navegações dos dispositivos conectados para sites controlados pelo hacker que realizou o processo. Dessa forma, não é percebido nenhum vírus ativo no computador, uma vez que ele impacta a navegação dos aparelhos.

Alguns antivírus têm recursos capazes de identificar alterações no DNS. Porém, eles funcionam melhor em sites com mais camadas de proteção, como bancos e plataformas de pagamento, não atuando em outros ambientes.

Não há uma forma ou um padrão universal de identificar esse problema, mas, ao ser redirecionado para sites maliciosos, é comum que o cadeado de segurança que fica ao lado do “https” não apareça. Portanto, essa é uma maneira de perceber o problema.

Outro sintoma que indica a presença de um vírus é a [lentidão durante a navegação](https://blog.intnet.com.br/quer-uma-internet-mais-rapida-descubra-como-com-essas-5-dicas/). Isso acontece porque os criminosos ligam você a outras vítimas — e todos compartilham a mesma rede. Em alguns casos, quando os hackers têm mais estrutura, tal quadro pode ser evitado.

## EXISTEM MANEIRAS DE SE PREVENIR OU LIVRAR DE ATAQUES?

Como falamos, existem dois tipos de ataques que resultam na presença de vírus nos roteadores de residências. Mas há formas de evitar ou identificar esse problema em ambos os casos.

Na primeira modalidade de ataque, tudo é feito de forma remota. Para solucionar a questão, é necessário atualizar o firmware do roteador. Tal prática corrige falhas de segurança que são aproveitadas pelos hackers. Porém, esse não é um processo muito simples, sendo que o mais indicado é contar com um profissional qualificado para o trabalho.

No segundo caso, em que há a interação do usuário, basta que ele fique atento a esses e-mails, não aceitando ou clicando em mensagens de desconhecidos. Ainda assim, se você clicar em um link, faça a alteração da senha do computador e de acesso à rede.

### ANTIVÍRUS E PLUG-INS DE BROWSER

Além disso, é indicado ter instalado um bom programa antivírus em todos os dispositivos utilizados. Essas soluções garantem proteção ao acessar sites de bancos e pagamentos — o que evita maiores prejuízos para o usuário, uma vez que há o risco de roubo de dados financeiros.

Outra dica é usar plug-ins de browser que administrem a execução de scripts no navegador ou trocar o IP do modem para um “não padrão”. Tais práticas, porém, são mais técnicas e demandam o auxílio de um especialista. Vale lembrar que fazer essas mudanças sem ajuda aumenta as chances de você cometer erros que [comprometam sua segurança](https://blog.intnet.com.br/10-dicas-importantes-para-navegar-na-internet-com-seguranca/).

Ficou evidente que o vírus no roteador é um problema que todos devemos considerar, não é mesmo? O problema pode ser evitado ou identificado: para tanto, basta seguir as indicações listadas acima. Lembre-se de que é importante usar um aparelho de qualidade, que não apresente tantas falhas de segurança.

Além disso, é fundamental ficar atento aos problemas causados por esse vírus, como a ausência do sinal de confiabilidade de uma página, dado por seu cadeado de segurança. Outra forma de se prevenir é avaliar a quantidade de anúncios em cada página, desconfiando quando for muito alta.