DNS over HTTPS: Protegendo suas consultas DNS

Público-Alvo: Usuários intermediários

O DNS (Domain Name System) é uma parte fundamental da infraestrutura da Internet, responsável por traduzir nomes de domínio em endereços IP. No entanto, as consultas DNS tradicionais são enviadas em texto simples, o que pode permitir que terceiros interceptem e manipulem essas informações. Para aumentar a privacidade e segurança das consultas DNS, surgiu o DNS over HTTPS (DoH), um protocolo que criptografa as consultas DNS usando o HTTPS.

Exemplos: A seguir, apresentaremos um exemplo de configuração do DNS over HTTPS no Windows usando o navegador Firefox.

Passo 1: Abra o navegador Firefox e digite "about:config" na barra de endereço. Passo 2: Clique em "Aceitar o risco e continuar" para acessar as configurações avançadas. Passo 3: Na barra de pesquisa, digite "network.trr.mode" para encontrar a opção de configuração do DNS over HTTPS. Passo 4: Altere o valor dessa opção para "2" para habilitar o DNS over HTTPS. Passo 5: Na barra de pesquisa, digite "network.trr.uri" para encontrar a opção de configuração do servidor DNS over HTTPS. Passo 6: Insira o endereço do servidor DNS over HTTPS desejado, por exemplo, "https://dns.google/dns-query". Passo 7: Reinicie o navegador para que as alterações entrem em vigor.

Proteger suas consultas DNS é fundamental para garantir sua privacidade e segurança online. Compartilhe este artigo com seus amigos e ajude-os a configurar o DNS over HTTPS em seus navegadores para uma experiência mais segura na Internet.