


# ARP Spoofing: Protegendo-se contra **interceptação de dados** sensíveis





O **ARP Spoofing** é um tipo de ataque em que um agente malicioso envia mensagens falsas de ARP (Address Resolution Protocol).



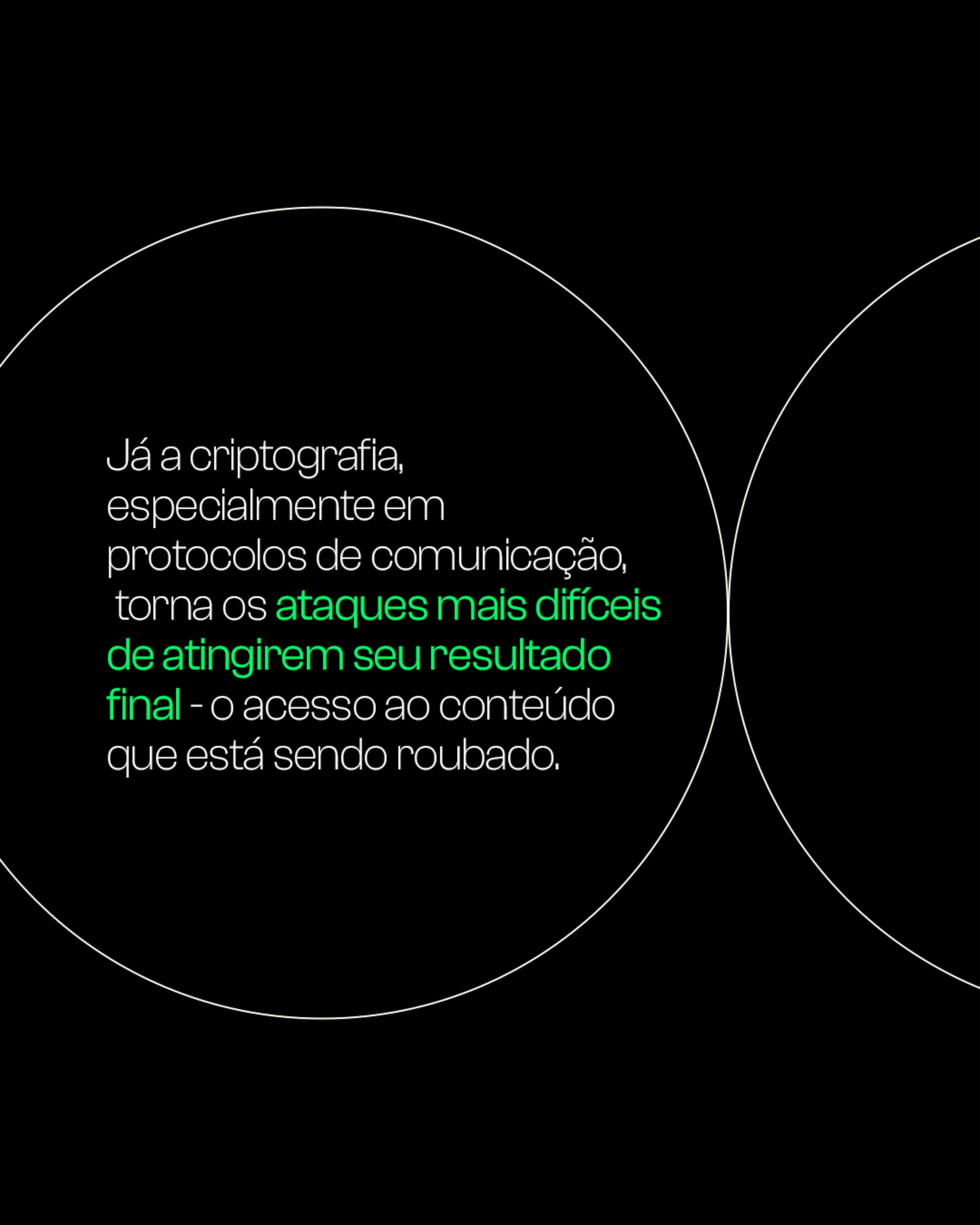
Ao enganar dispositivos para enviarem informações diretamente a eles, os **invasores ganham acesso a dados sensíveis**, como senhas e informações de cartões de crédito.

## Algumas das medidas necessárias para se proteger contra o ARP Spoofing são:

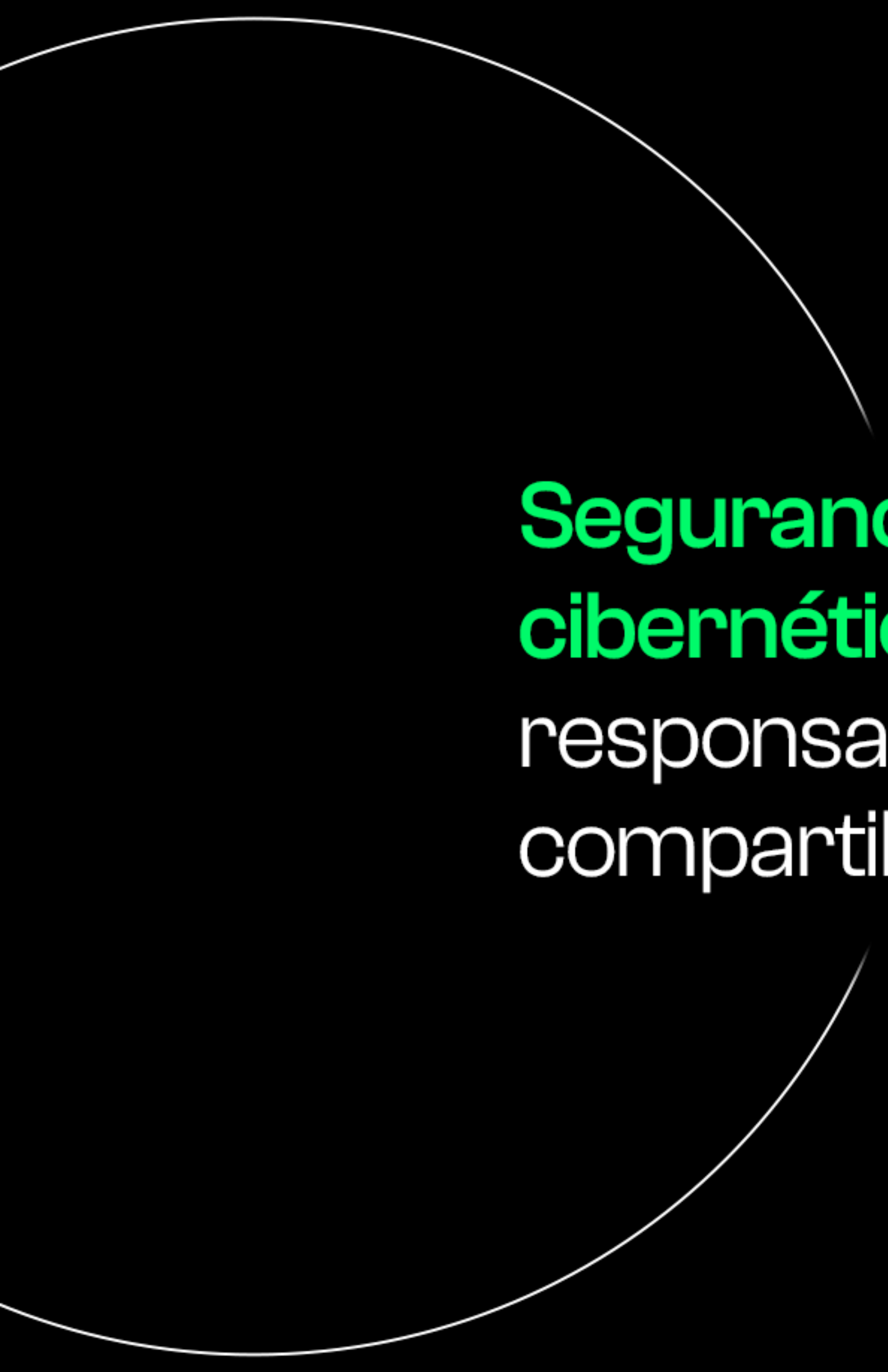
implementar controles de acesso e proteções de postura em nível de rede, utilizar firewalls que façam packet-filtering, usar software anti-ARP Spoofing e criptografar seus dados.



O uso de ferramentas de validação de solicitações ARP e firewalls de filtragem de pacotes permitem que você detecte e previna atividades suspeitas.



Já a criptografia,  
especialmente em  
protocolos de comunicação,  
torna os **ataques mais difíceis  
de atingirem seu resultado  
final** - o acesso ao conteúdo  
que está sendo roubado.



**Segurança  
cibernética** é uma  
responsabilidade  
compartilhada.

**THINK  
AHEAD,  
ACT  
NOW.**