COMO CONFIGURAR O DMARC PARA SUA ORGANIZAÇÃO

Antes de uma organização poder receber um Verified Mark Certificate (VMC), ela precisa atender ao DMARC (Domain-based Message Authentication, Reporting & Conformance). Este guia mostra as etapas necessárias para garantir que sua organização implemente o DMARC corretamente.

digicert®

digicert®

O QUE É O DMARC?

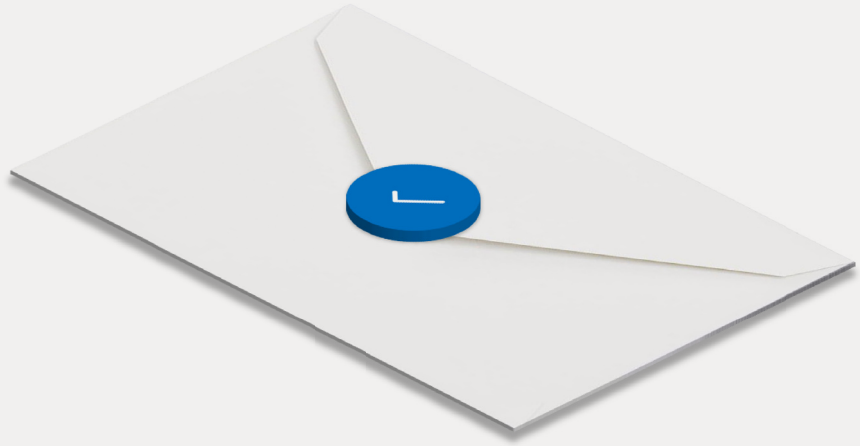
O DMARC é um protocolo de autenticação de e-mail, política e relatório que permite às organizações proteger seu domínio contra uso não autorizado, incluindo ataques de personificação e phishing.

Este é um resumo básico:

- O DMARC é um registro TXT armazenado no DNS que fornece aos destinatários de e-mail a capacidade de verificar a autenticidade dos e-mails que recebem.
- Ele foi criado para se adequar ao processo de autenticação de entrada já usado em uma organização e ajuda os destinatários do e-mail a determinar se uma mensagem está alinhada com o que o destinatário sabe sobre o remetente.
- As organizações têm três opções de políticas para tratar mensagens "não alinhadas":

- "p = none" (nenhuma aplicação de política)
- "p = quarantine"
- "p = reject"

- Para que o DMARC funcione corretamente, os protocolos Sender Policy Framework (SPF) e DomainKeysIdentified Mail (DKIM) precisam ser configurados primeiro.
- O registro DMARC de uma organização pode ser verificado por meio de ferramentas baseadas na Internet, como esta do valimail.com.



A AUTENTICAÇÃO DE E-MAIL APRIMORADA COMEÇA COM O DMARC

O objetivo do DMARC é criar um sistema de remetentes e destinatários que colaborarão mutuamente para melhorar as práticas de autenticação de e-mail dos remetentes e capacitar os destinatários a rejeitar mensagens não autenticadas.

digicert®

POR QUE O DMARC?

Ao implementar o DMARC, as organizações podem aproveitar quatro benefícios principais:

1. **Segurança**

   Proteja as pessoas de spam, fraude e phishing bloqueando o uso não autorizado de seu domínio de e-mail.

2. **Visibilidade**

   Obtenha relatórios detalhados sobre quem (e/ou o quê) na internet está enviando e-mail por meio de seu domínio.

3. **Capacidade de entrega**

   Aumente a capacidade de entrega em 5-10% e impeça que e-mails sejam sinalizados como spam.

4. **Proteção da marca**

   Defenda sua marca contra ataques direcionados a identidades.

dos clientes têm menor probabilidade de se engajar com uma marca após um ataque de phishing de alguém que se passa por essa organização.

digicert®

COMO CONFIGURAR O SPF:

1. Colete endereços IP usados para enviar e-mails de seu domínio, incluindo:
    - Servidor Web
    - Servidor de e-mail do escritório
    - Servidor de e-mail do provedor de internet
    - Qualquer servidor de e-mail de terceiros
2. Faça uma lista de seus domínios que enviam e-mail ou não.
3. Crie um registro SPF em formato .txt para cada domínio usando um programa de edição de texto (como Notepad ++, Vim, Nano etc.)

    Exemplo 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all

    Exemplo 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all

4. Publique seu SPF no DNS.

    Se você gerencia seu DNS, basta adicionar um novo registro TXT contendo o texto SPF. Se você não gerencia seu DNS, entre em contato com o administrador do servidor para adicionar o registro.

5. Após o registro ser adicionado ao DNS, verifique-o usando uma ferramenta de verificação de SPF.

O QUE É O SPF?

Não se arrisque com remetentes não autorizados.

O SPF é o padrão que lançou o conceito de autenticação de e-mail baseada em domínio. Ele impede o spoofing ao permitir que os proprietários de domínios aprovem automaticamente os endereços IP de servidores autorizados a enviar e-mails em nome do domínio. Se um servidor de e-mail com um endereço IP que não está na lista tentar enviar e-mail usando esse domínio, ele não passará na autenticação SPF.

digicert®

COMO CONFIGURAR O DKIM:

1. Escolha um seletor DKIM.

Ele deve ser uma cadeia de caracteres de texto simples e definida pelo usuário que será anexada ao nome do domínio para ajudar a identificar a chave pública DKIM (por exemplo, “standard”).

Exemplo: “standard._domain.example.com” = nome do host

2. Gere um par de chaves pública-privada para seu domínio.

- Usuários finais do Windows podem usar PUTTYGen
- Usuários finais do Linux e do Mac podem usar ssh-keygen

3. Crie e publique um novo registro TXT.

Crie um novo registro por meio do seu console de gerenciamento DNS usando a chave pública do par acima.

Exemplo: v=DKIM1; p=YourPublicKey

O QUE É O DKIM?

Impeça que os e-mails sejam violados quando em trânsito

O padrão DKIM de autenticação de e-mails usa a criptografia de chaves públicas/privadas para assinar mensagens de e-mail.

O DKIM é usado para verificar se o e-mail veio do domínio ao qual a chave DKIM está associada e se o e-mail não foi modificado quando em trânsito.

CONFIGURAÇÃO DO DMARC NO MODO DE MONITORAMENTO

1. Verifique se configurou corretamente o SPF e o DKIM

2. Crie um registro DNS

   O registro DMARC “txt” deve ter nome semelhante a “_dmarc.your_domain.com.”

   Exemplo: “v=DMARC1;p=none; rua=mailto:dmarcreports@your_domain.com”

   Se você gerenciar o DNS de seu domínio, crie um registro DMARC “p=none” (modo de monitoramento) da mesma forma que os registros SPF e DKIM.

   Se não gerenciar o DNS, peça ao seu provedor de DNS para criar o registro DMARC para você.

3. Teste seu registro DMARC com uma ferramenta de verificação DMARC
   Observação: normalmente, você precisa aguardar de 24 a 48 horas pela replicação
   Ferramenta de verificação DMARC

digicert®

O QUE É O MODO DE MONITORAMENTO DO DMARC?

Tenha visibilidade do que é enviado a partir de seu domínio

O modo de monitoramento permite que os proprietários avaliem relatórios do DMARC contendo o tráfego de e-mail para o domínio.

Esses relatórios identificam possíveis falhas de mensagens que ficariam em quarentena ou seriam rejeitadas quando o DMARC estiver totalmente em vigor. Além disso, os relatórios do DMARC mostram informações sobre todos os sistemas e serviços que enviam e-mails do domínio monitorado.

OBSERVAÇÃO: o modo de monitoramento não fornece qualquer nível de aplicação. Mensagens não aprovadas na autenticação são entregues normalmente, o que permite evitar potenciais interrupções durante a implementação do DMARC.

digicert®

TAGS COMUNS USADAS EM REGISTROS .TXT DO DMARC

NOME DA TAG	OBRIGATÓRIA?	FINALIDADE
V	OBRIGATÓRIA	VERSÃO DO PROTOCOLO
P	OBRIGATÓRIA	VERSÃO DO POLÍTICO
PCT	OPCIONAL	% DE MENSAGENS SUJEITAS A FILTRAGEM
RUA	OPCIONAL	RELATAR UTI DO RELATÓRIO AGREGADO
SP	OPCIONAL	POLÍTICA PARA SUBDOMÍNIOS DO DOMÍNIO

digicert®

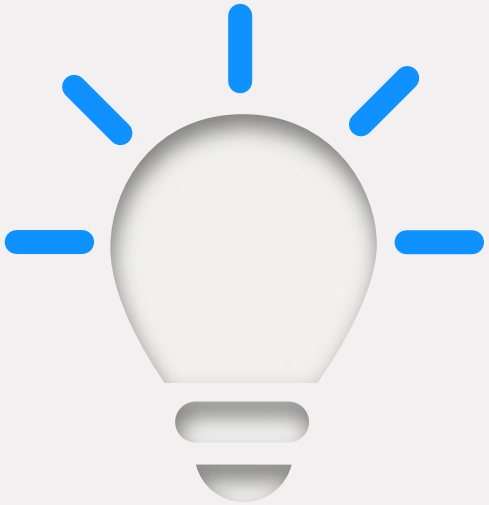
QUAIS INFORMAÇÕES O RELATÓRIO DMARC FORNECE?

O relatório mostra aos proprietários de domínio quantas mensagens fraudulentas estão usando o domínio, de onde elas vêm e se seriam detidas por uma política “quarantine” ou “reject” do DMARC.

O relatório de cada destinatário é um arquivo XML que inclui os seguintes campos:

- Uma contagem de mensagens de cada um dos endereços IP
- O que foi feito com essas mensagens segundo a política DMARC mostrada
- Resultados SPF para essas mensagens
- Resultados DKIM para essas mensagens

Embora legível, o relatório XML não é conveniente. Proprietários de domínio podem usar um processador de relatórios DMARC, como o Valimail ou outro fornecedor de serviços DMARC.



4 MANEIRAS DE USAR O RELATÓRIO DMARC

Gere uma boa linha de base antes de iniciar a aplicação

1. Identifique tráfego marcado como ilegítimo.

2. Procure e-mails legítimos que estejam sinalizados como ilegítimos pelo DMARC. Esses e-mails, dependendo da política, seriam rejeitados ou colocados em quarentena após o início da aplicação.

3. Entre em contato com possíveis proprietários de sistemas/aplicativos para esclarecer a legitimidade de e-mails que são sinalizados como ilegítimos.

4. Se necessário, atualize seu registro SPF inserindo em uma lista de permissões os endereços IP que são legítimos mas não haviam sido incluídos até então.

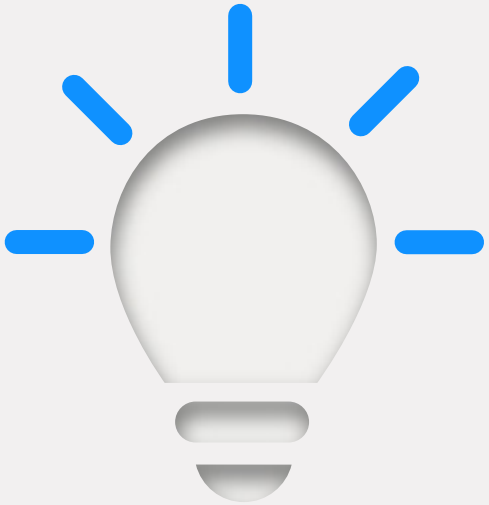
USE O RELATÓRIO DMARC PARA ARRUMAR A CASA ANTES DE ATIVAR A APLICAÇÃO DE POLÍTICAS

A análise de relatórios DMARC pode ser demorada. No entanto, se os proprietários de domínio ignorarem ou identificarem remetentes incorretamente, podem acabar bloqueando e-mails confiáveis quando a política DMARC estiver definida para aplicação ("quarantine" ou "reject"), o que pode causar ainda mais problemas que retardam seu progresso.

Aqui estão algumas tarefas internas sugeridas antes de você iniciar a aplicação de políticas do DMARC:

- Faça uma lista de todos os remetentes de e-mail identificados no relatório DMARC e todos os outros mencionados pelas partes interessadas
- Identifique os proprietários de cada serviço/remetente de e-mail
- Categorize os serviços de envio como autorizados, não autorizados ou mal-intencionados
- Identifique, com ajuda das partes interessadas, qualquer outro remetente que possa não ter aparecido no relatório DMARC
- Entre em contato com as partes interessadas para cada novo remetente identificado
- Atualize seu registro SPF com todos os endereços IP de remetentes de e-mails legítimos recém descobertos

digicert®



RECOMENDAÇÕES PARA COMUNICAÇÃO PRÉ-APLICAÇÃO

5 dicas para melhorar a adoção

- Documente uma política de implementação que você possa compartilhar com as partes interessadas
- Entre em contato com um fornecedor de suporte ao DMARC, como o Valimail, se as tarefas do DMARC sobrecarregarem você ou se precisar de ajuda.
- Comunique o resultado de relatórios DMARC assim que disponível.
- Inicie a implantação do DMARC como um projeto interno.
- Faça com que sua equipe executiva aja como o principal patrocinador do projeto.

POR QUANTO TEMPO O DMARC DEVE FICAR NO MODO DE MONITORAMENTO?

Esse tempo varia segundo a organização, com corporações necessitando de mais tempo do que organizações menores. Planeja para semanas ou meses.

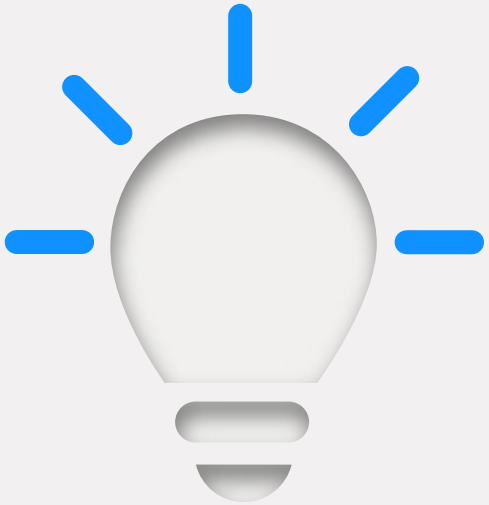
Após ter certeza de que o inventário está completo e que todos os remetentes autorizados foram mapeados e sua organização está suficientemente bem informada, você está pronto para passar para a fase de quarentena.

Quando o modo de quarentena está ativado, as mensagens não aprovadas na autenticação são colocadas em quarentena. Em geral, isso significa que as mensagens são entregues na pasta de spam do usuário.

COMO CONFIGURAR A POLÍTICA QUARANTINE DO DMARC

1. Faça login em seu servidor DNS e pesquise o registro DMARC
2. Abra o registro DMARC para o domínio especificado e atualize a política de “p=none’ para “p=quarantine”
   Exemplo: “v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@you_domain.com”
3. Adicione o sinalizador “pct” (% de mensagens sujeitas a filtragem). Sugerimos começar com 10%.
4. Aumente gradualmente a porcentagem de mensagens filtradas para “pct=100” (100%) conforme se sentir mais à vontade para isso.

   OBSERVAÇÃO: Você deve chegar a “pct=100” para atender aos padrões BIMI e VMC, mas sua política pode ser “quarantine” ou “reject”.



COMO FUNCIONA A SINALIZAÇÃO:

- Se uma política diferente de “p=none” for especificada, essa política será aplicada à porcentagem no sinalizador “pct”
- A próxima política menos restritiva será aplicada ao restante (por exemplo, para um registro DMARC onde “p=quarantine” e “pct=10,” 10% do tráfego com falha seria colocado em quarentena e os outros 90% seriam entregues normalmente)

digicert®

APÓS ALCANÇAR 100% DE FILTRAGEM, VOCÊ PODE PASSAR PARA "P=REJECT", O NÍVEL MAIS ALTO DE APLICAÇÃO.

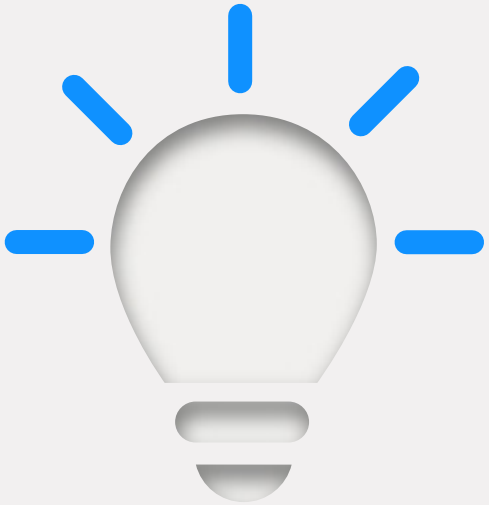
COMO CONFIGURAR A POLÍTICA REJECT DO DMARC

1. Abra seu registro DMARC usando o console DNS
2. Altere “p=quarantine” para “p=reject”
   Exemplo: “v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports @ you_domain.com
3. Salve o registro

DICA: é especialmente importante continuar o monitoramento neste estágio para garantir que e-mails legítimos não sejam rejeitados e excluídos.

Você tem mais perguntas? Envie-nos hoje mesmo para contactus@digicert.com ou visite-nos em https://www.digicert.com/pt/tls-ssl/verified-mark-certificates/

digicert®



O QUE A POLÍTICA REJECT FAZ COM OS E-MAILS?

As mensagens não aprovadas na verificação DMARC (e-mails não autorizados) serão bloqueadas/excluídas, e o destinatário do e-mail não receberá uma cópia nem será informado de sua exclusão.