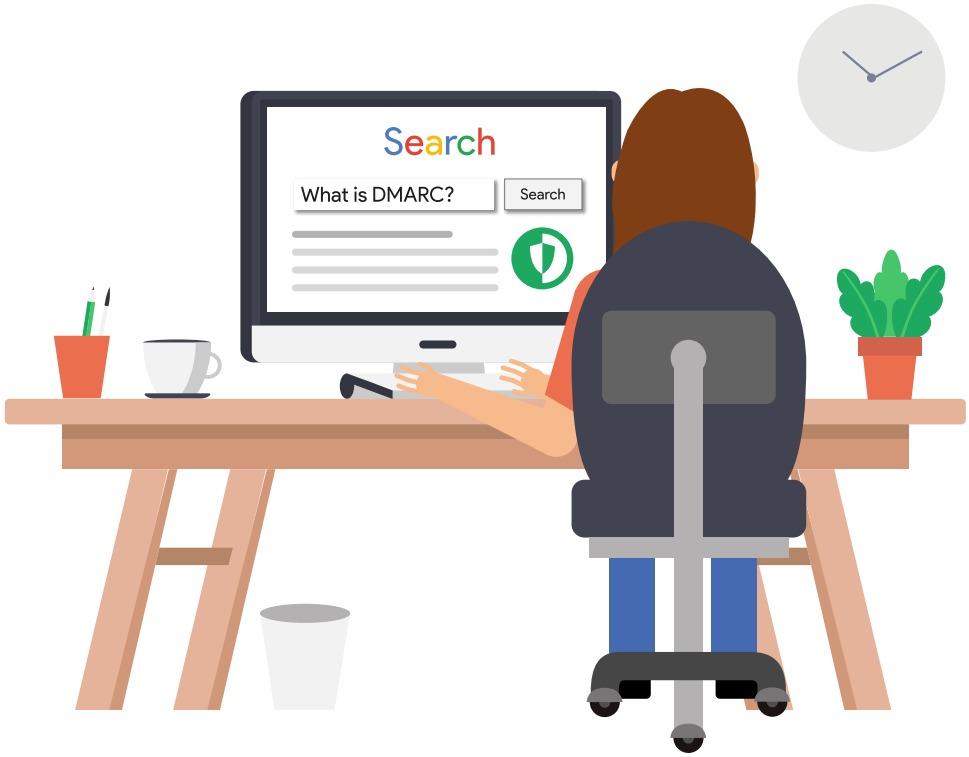
ONDMARC by RED SIFT

MANAGER ONE
gestão de mobilidade corporativa

DMARC:
O que é e por que deveria ser sua próxima prioridade?

Protocolo de autenticação de e-mail que efetivamente bloqueia ataques de phishing e aumenta a entregabilidade.



Sumário

1. Uma breve história do e-mail

1971
Primeiro e-mail enviado

1981
Lançado codificação ASCII

1982
SMTP estabelecido

1988
Microsoft e Compuserve oferecem mail via dial-up

1991
Primeiro e-mail enviado do espaço

1992
Introduzidos anexos de email

1998
Termo spam popularizado

2003
Crescimento do e-mail móvel iniciado com o Blackberry Quark

2004
Introdução do DKIM

2005
Introdução do SPF

2008
"e-mail SMTP é inerentemente inseguro" - RFC5321

2012
Nasce o DMARC

2017
269 bilhões[1] de emails enviados diariamente

2018
Adoção do DMARC sobe 51%[2]

2. E-mail: O caminho mais fácil?

De acordo com as investigações de violação da Verizon[3], o email continua sendo o vetor mais comum em ataques de phishing, tornando-se **uma das principais preocupações de segurança cibernética** para as organizações.

Spam

Mais de 50% dos emails são spam e os criminosos utilizam-se regularmente de emails spam como veículo para malwares.

Golpes de pagamento antecipado

Estes são direcionados a indivíduos vulneráveis, com golpistas tentando obter dinheiro ou detalhes bancários em troca da promessa de recompensas ou de caridade (por exemplo, os golpes 419 nigerianos[4]).

Spear phishing

Esta é uma evolução do tradicional e-mail phishing, em que os golpistas visam diretamente indivíduos ou organizações com conteúdo relevante para eles. Esses golpistas pesquisam o indivíduo ou a organização em questão - uma tarefa hoje simplificada por sites de redes profissionais como o LinkedIn - para fazer com que o e-mail pareça legítimo.

O whale phishing é uma versão do spear phishing em que um golpista envia um email phishing para um executivo sênior (o "peixe grande"). A engenharia social é essencial para golpes de phishing bem-sucedidos, com 93% das violações de dados relacionadas a incidentes de engenharia social[5].

3. A sua segurança de email protege contra uma ameaça e está vulnerável contra outras?

As tecnologias de segurança de e-mail vêm em muitas formas, mas todas as formas têm como objetivo manter o volume de e-mails de spam no mínimo e detectar conteúdo indesejado (de malware a links suspeitos) para impedir que eles cheguem à caixa de correio do usuário.

Na maioria das vezes, essas tecnologias buscam os traços mais comuns de um e-mail mal-intencionado, como um endereço IP na lista negra, ou um domínio desonesto, bloqueando-o para proteger o destinatário.

Isso se deve a uma falha imprevista na infra-estrutura de e-mail global que expõe todas as organizações.

Mas e se o e-mail vier de um domínio legítimo?

Todas as medidas de segurança de e-mail, além do DMARC, provavelmente serão virtualmente ineficazes quando um e-mail vier de um domínio legítimo.

Isso se deve a uma falha imprevista na infra-estrutura de e-mail global que expõe todas as organizações ao risco de serem violadas como resultado do SMTP (*Simple Mail Transfer Protocol*), originalmente projetado sem considerar a segurança. Isso deixou padrões de envio de e-mail hoje ainda abertos a roubo de dados e financeiros, pois um e-mail pode ser enviado facilmente com o nome de domínio de outra pessoa.

Personificação de e-mail: Seu irmão gêmeo maligno

Qualquer pessoa, mesmo com o conhecimento limitado de codificação pode aprender as etapas básicas necessárias para personificar a identidade de e-mail de alguém. Só é preciso uma rápida pesquisa no Google. O resultado é um e-mail que parece legítimo e não possui os indicadores típicos de um ataque de phishing, como um endereço de e-mail suspeito. Um servidor de e-mail aceitará esse e-mail na caixa de entrada de um usuário se as medidas de segurança adequadas não estiverem implantadas, ficando difícil para o usuário identificar que o e-mail é um ataque de phishing.

Níveis de sofisticação de ataques de phishing

1 Obviamente suspeito
hsbc@yourbank.com

2 Parece original
customercare@hsbo.com

3 Spoofing
info@hsbc.com

Olhando a ilustração acima, não é de se surpreender que muitos usuários sejam enganados por e-mail phishing. Embora não tenha havido nenhum delito cometido pelas organizações representadas nesses casos, e um criminoso não precise acessar seus sistemas para se passar por eles, a legislação considera que as organizações têm a responsabilidade objetiva de proteger seus clientes contra ataques de phishing. Como tal, as organizações que não tomaram medidas adequadas para proteger seus clientes podem ser responsabilizadas por uma violação de dados..

A personificação de e-mail viola as seguintes medidas de segurança:

Senhas fortes | Biometria | Dois fatores de autenticação | Tokens de segurança

Na última década, uma série de protocolos de segurança de e-mail foi introduzida por líderes do setor para promover autenticidade dos emails e bloquear emails phishing, bem como para aumentar a capacidade de entrega de e-mails genuínos.

Potenciais cenários de Spoofing

Um e-mail phishing geralmente contém instruções da seguinte natureza

Interno	*Externo*	*Resultado*
Por favor pague essa fatura	Seus detalhes de débito expiraram, veja detalhado	Perda financeira
Você pode enviar esse contrato?	Preciso confirmar seus dados pessoais	Perda de dados
Veja a apresentação do RH em anexo	Acesse esse link para atualizar a sua senha	Ataque cibernético

Hora de conhecer o DMARC

4. DMARC

Em 2011, vários dos principais provedores globais de email se uniram na tentativa de acabar com o phishing.

Embora já existissem dois protocolos de segurança de e-mail em vigor naquele momento, Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM), nenhum dos protocolos impedia efetivamente o phishing.

SPF

Este protocolo verifica os emails que são enviados de um endereço IP válido.

DKIM

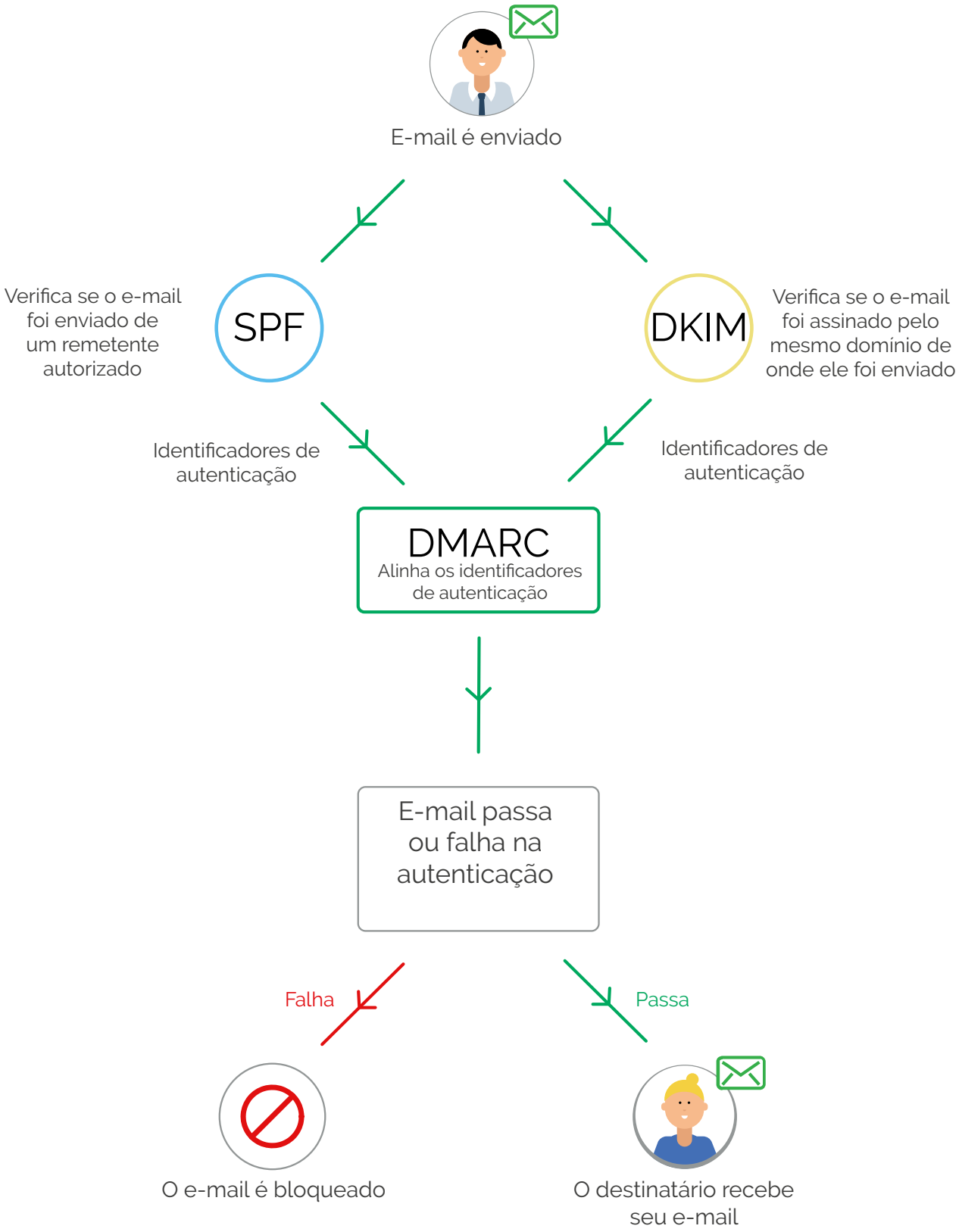
Este protocolo verifica se os e-mails recebidos foram assinados digitalmente pelo domínio do qual foram enviados ou em nome de.

Embora esses protocolos tenham sido aceitos pelos principais provedores de e-mail globais, uma camada secundária era necessária para bloquear os e-mails identificados pelos protocolos como fraudulentos ou falsificados.

DMARC

Em 2012, o **DMARC** (Domain-based Messaging, Authentication and Reporting Conformance) foi ratificado para que os proprietários de domínio pudessem retomar o controle de sua identidade de e-mail informando às caixas de entrada para rejeitar os emails falsificados. A autenticação da origem de um e-mail via DMARC também melhora muito a capacidade de entrega.

5. Como o DMARC funciona?



Ações falam mais alto que palavras: Transformando políticas de segurança em defesas reais

A entrega de e-mails é tratada pelo DMARC, escolhendo uma das três políticas a seguir, que podem ser definidas pelo proprietário do domínio:

- ***p=none*** - esta política permite que todos os emails cheguem ao destinatário, independentemente de terem sido autorizados.
- ***p=quarantine*** - quarantine - esta política determina que os e-mails com falha na validação do DMARC sejam enviados para a pasta lixo/spam do destinatário.
- ***p=reject*** - esta política determina que todos os e-mails não autorizados sejam completamente bloqueados.

Independentemente de qual política o domínio está definido, os relatórios serão enviados ao usuário para ajudar a identificar as fontes de e-mail com autenticação apropriada e aquelas sem (estas não são autorizadas).

Quais organizações já estão usando o DMARC?

Remetentes
O DMARC já foi implementado por várias grandes marcas e organizações, a maioria das quais já está em modo de proteção, incluindo:

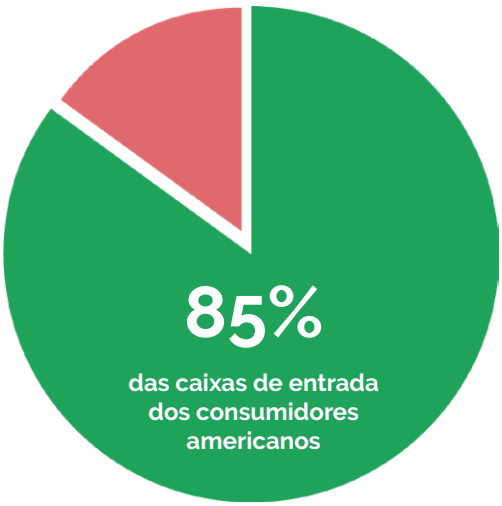
- Adobe
- Amazon
- AOL
- CNN
- Dropbox
- Facebook
- Google
- Instagram
- Microsoft
- PayPal
- Pinterest
- Pret-a-Manger
- Telefonica
- Transferwise
- Twitter
- Verizon
- Yahoo
- YouTube

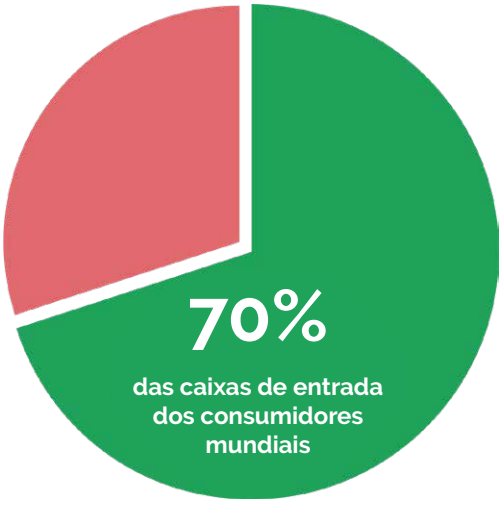
Destinatários

O DMARC foi amplamente adotado pela maioria dos receptores de e-mail (incluindo Google, Yahoo e Microsoft), o que significa que a maioria das caixas de entrada dos consumidores já está protegida. O DMARC já protege 85% das caixas de entrada dos EUA e aproximadamente 70% das caixas de entrada do consumidor em todo o mundo de e-mail phishing, desde que a organização que está sendo personificada em um e-mail phishing tenha um registro DMARC publicado.

É importante observar que uma organização que implementou o DMARC não será notificada sobre e-mails phishing que personifica essa organização se a caixa de entrada do destinatário do e-mail relevante não tiver ativado o DMARC.

- Desde **2015**, o Gartner incluiu o fornecimento do DMARC como um recurso de qualificação para posição de "líder" no Quadrante Mágico para gateways de e-mail seguros.
- Em **2016**, o governo do Reino Unido determinou o DMARC como um requisito mínimo obrigatório para uma nova estrutura de padrões para todos os domínios ".gov.uk" até março de 2019. Isso garantiu que os e-mails em trânsito fossem autenticados.
- Em **2017**, o governo dos EUA mandatou o DMARC para seus domínios do Departamento de Segurança Interna.
- **2018**, O NCSC (Parte do GCHQ) emite orientações para torná-lo uma das 5 principais prioridades para o conselho - "Organizações que implantam essas medidas adequadamente podem garantir que seus endereços de e-mail não sejam usados por criminosos".[6]





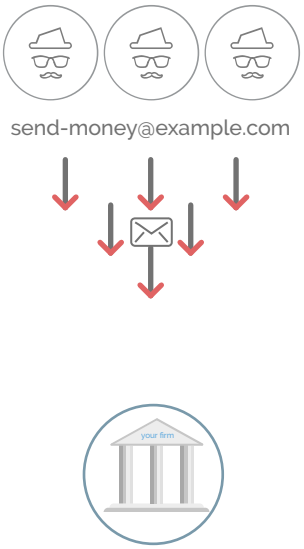
6. Como reportar a necessidade do DMARC?

Você pode verificar a configuração atual do DMARC de sua organização em ***www.ondmarc.com.br***, onde você obterá informações claras sobre o status de seu DMARC, SPF e DKIM. Ele também informará se sua caixa de entrada e DNS são compatíveis com o DMARC.

Total visibilidade do seu cenário de e-mail

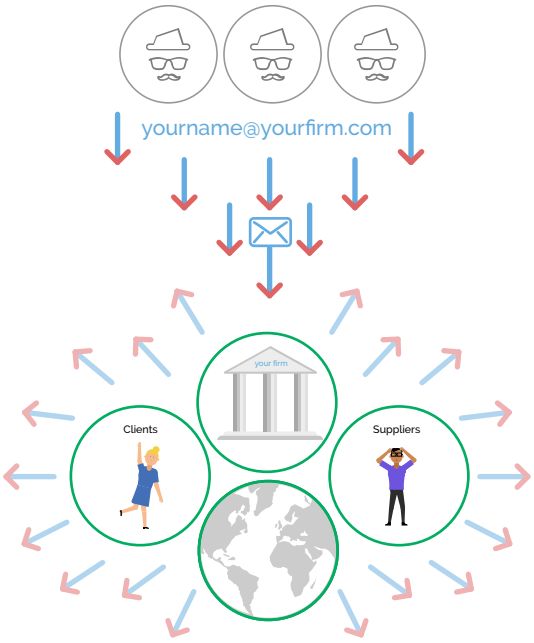
O OnDMARC fornece relatórios aos usuários que exibem a maioria dos e-mails, se não todos, provenientes do domínio de um usuário, não apenas daqueles que cruzam o limite da rede da organização. Isso contrasta com as soluções tradicionais de segurança cibernética, como o MessageLabs e o Mimecast, que apenas detectam e-mails de phishing que ultrapassam o limite da rede. Sem o DMARC, as organizações não estão obtendo um quadro completo do número e da escala de ataques contra eles.

Hackers enviam ataques de e-mail phishing para sua empresa



Várias soluções de cybersecurity filtram e-mails que entram

Hackers podem personificar seu endereço de e-mail e enviar ataques de phishing dentro e fora da sua empresa



O OnDMARC para a personificação do seu endereço de e-mail globalmente

Proteja a sua reputação

Os domínios da organização sujeitos a falsificação de emails podem sofrer danos consideráveis à reputação. Golpes de phishing podem atrair a imprensa negativa, com responsabilidade muitas vezes atribuída à organização que foi personificada.

Garantir a segurança financeira

O pagamento de faturas falsas ou o preenchimento de transferências eletrônicas que se fazem passar pelo CEO são erros comuns incorridos como resultado de falsificação de email. Na verdade, o custo financeiro aumentou consistentemente de acordo com a Pesquisa de Violações de Cibersegurança de 2018 do Governo do Reino Unido[7].

Cumprimento da LGPD e GDPR

Na Europa, o Regulamento Geral de Proteção de Dados (GDPR) entrou em vigor em maio de 2018, exigindo que você tenha Contratos de Processamento de Dados (DPAs) com todos os provedores de serviços em nuvem que manipulam dados de usuários da UE em seu nome. Com o DMARC, se um provedor de serviços de nuvem enviar e-mails em nome do seu domínio, o DMARC os revelará para você.
No Brasil a Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em agosto de 2020, da mesma forma regulamenta o tratamento dos dados pessoais dos usuários.

dos ataques cibernéticos começam com um e-mail phishing

Levando em consideração que os ataques de phishing representam a porta de entrada de mais de 90% dos ataques cibernéticos, uma empresa que tenha um vazamento de dados provocado por um ataque deverá demonstrar à Autoridade Reguladora que tomou os cuidados necessários para evitá-lo ou minimizá-lo. De acordo com o art. 52 da LGPD as penalidades podem ser amenizadas com a demonstração que a empresa aplica melhores práticas de proteção. Havendo indícios de negligência, pode ocorrer a aplicação da penalidade máxima que é a multa de até R$ 50 milhões de reais por infração.
Os custos potenciais de roubo de dados e perda de serviços continuam aumentando, mas medidas simples como o DMARC podem salvar organizações de milhares, senão de milhões, em prejuízos.

Melhore a capacidade de entrega de e-mail

Os provedores de e-mail, como Gmail, Yahoo e Hotmail, estão se tornando mais protetores das caixas de entrada de seus usuários. Um provedor de e-mail pode se recusar a enviar um e-mail para a caixa de entrada de um usuário se ele não tiver uma assinatura SPF e/ou DKIM.

Com o DMARC, os e-mails são autenticados de forma confiável, melhorando, assim, a capacidade de entrega de e-mails legítimos para a caixa de entrada de um usuário.

Nutrir confiança

As organizações que não tomam as precauções necessárias para impedir a falsificação de e-mails provavelmente serão consideradas menos confiáveis. Os clientes não podem confiar em e-mails que pretendem vir de tais organizações e podem ser impedidos de usar o e-mail para se comunicar com eles, o que pode afetar a capacidade dessas organizações de se comunicarem efetivamente com seus clientes.

Identifique e remova o shadow IT

Não é fácil encontrar todos os serviços em nuvem "shadow IT". Por exemplo, se alguém no Marketing configurou uma conta com um complemento do Salesforce anos atrás que ninguém na TI conhece e envia e-mails para os clientes, você precisa verificar se os DPAs (Contratos de processamento de dados) estão em vigor. Implementando o protocolo de e-mail, o DMARC descobre todos os serviços de e-mail que enviam e-mails do seu domínio, quer você saiba ou não sobre eles oficialmente.

Os custos de roubo de dados como resultado de e-mails de spam continuam aumentando, mas a adoção do **DMARC** pode salvar uma organização de milhares, se não milhões, de reais.

Respondendo a objeções comuns

- **Por que devemos priorizar a adoção do DMARC?**

  O DMARC é fundamental para a segurança cibernética. O Centro Nacional de Segurança Cibernética do Reino Unido declarou que ***"A adoção generalizada do protocolo DMARC é essencial para se defender contra ameaças cibernéticas específicas."*** [8] Uma organização que gasta dinheiro em medidas de segurança sofisticadas e caras, mas não implementa o DMARC, é análoga ao proprietário que instala um alarme de alta tecnologia, mas que deixa a porta da frente destrancada.

- **Por que devemos pagar por algo que é um padrão aberto?**

  Você pode implantar o DMARC sem nenhum custo, configurando seus próprios relatórios, interpretando os resultados e, em seguida, ajustando suas configurações de SPF e DKIM de acordo. No entanto, os relatórios XML do DMARC são muito demorados e exigem recursos da equipe para interpretar os dados e fazer os ajustes necessários. Os provedores do DMARC, como o ***OnDMARC***, fornecem suporte na interpretação desses relatórios e orientações sobre a configuração apropriada do DMARC para chegar ao estágio de poder implementar p = quarentena ou p = rejeitar políticas mais rapidamente.

- **Ainda não implantamos o SPF e/ou o DKIM. Não precisamos fazer isso primeiro?**

  Você não precisa ter implantado o SPF e/ou o DKIM para começar a usar o DMARC. Na verdade, a percepção dos seus relatórios do DMARC ajudará você a implantar e configurar corretamente o SPF e o DKIM.

- **O DMARC parece ser realmente complexo de implantar com base em nossa experiência com outros provedores de segurança cibernética.**

  A implementação do DMARC deve ser um processo lógico e iterativo, mas ele depende de um certo nível de conhecimento sobre segurança de email. Um bom provedor DMARC, como o ***OnDMARC***, simplificará enormemente esse processo e ajudará você a alcançar o modo de proteção total.

- **Temos a preocupação que a implementação do DMARC afete nossa atual capacidade de entrega de e-mails.**

  O DMARC irá melhorar significativamente a capacidade de entrega de e-mails, desde que seja configurado corretamente. O OnDMARC ajudará você a alcançar o modo de proteção total com muito mais rapidez, minimizando os problemas operacionais diários de e-mail e ajudando sua organização a alcançar um nível muito maior de capacidade de entrega de e-mail.

- **Já temos o Mimecast / Messagelabs - isso não funciona?**

  A maioria das soluções de segurança de e-mail atualmente disponíveis não oferece às organizações proteção total contra a personificação de e-mail. Isso ocorre porque eles se concentram na prevenção de violações de segurança que resultam no envio de emails spam dentro dos limites da rede de uma organização. Eles não impedem ataques originados fora da rede da organização e que não ultrapassem o limite da rede. O protocolo DMARC é a única maneira de fechar essa lacuna ao cercar o domínio de uma organização e impedir que os spammers se façam passar por ela.

Os custos potenciais de roubo de dados e perda de serviços continuam aumentando, mas medidas simples, como o ***DMARC***, podem salvar organizações isoladas, milhares, senão milhões de reais.

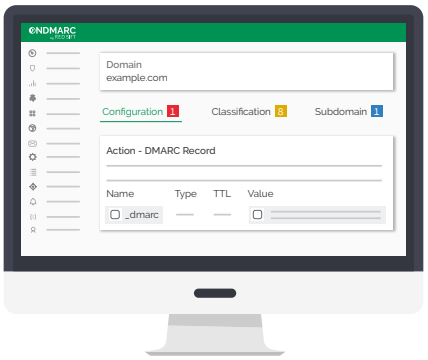
7. Qual o próximo passo?

Esperamos que você tenha achado este guia útil para começar a desenvolver seu próprio conhecimento sobre o DMARC e seus benefícios de segurança de maneira clara e fácil para possa transmitir esse conhecimento para outras pessoas na empresa.

Recomendamos que você confira a Parte 2 da série DMARC Digest, encontre seu provedor DMARC perfeito para obter uma lista de verificação clara e concisa de tudo o que você precisa saber para identificar um fornecedor confiável e comprovado do DMARC para sua organização.

Quer ver o DMARC na prática?

Um provedor DMARC fácil de usar, como o ***OnDMARC***, ajudará você a alcançar o modo de proteção total muito mais rapidamente. Teste as águas para ver como é simples navegar no seu cenário de e-mail e dar os primeiros passos para proteger seu domínio contra a falsificação de identidade inscrevendo-se em nossa avaliação gratuita em:
https://www.ondmarc.com.br .



Fique seguro!

Time OnDMARC

Referências

1. http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf
2. https://techcrunch.com/2018/11/01/half-fortune-500-dmarc-email-security/
3. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
4. http://www.newsweek.com/origins-nigerias-notorious-419-scams-456701
5. https://enterprise.verizon.com/resources/reports/dbir/
6. https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda
7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
8. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Entre em contato hoje mesmo!

www.ondmarc.com.br

ONDMARC

O Red Sift Open Cloud é uma plataforma de análise de dados desenvolvida especificamente para os desafios da segurança cibernética. Ao aproveitar o poder da IA, podemos coletar, computar e visualizar dados de milhares de sinais individuais com segurança para ajudar as organizações a otimizar sua segurança cibernética.

Nosso primeiro produto na plataforma Red Sift é o OnDMARC, um produto SaaS que ajuda a implementar e manter o DMARC. Este protocolo de autenticação de e-mail bloqueia efetivamente ataques de phishing e aumenta a capacidade de entrega de e-mails genuínos.

www.ondmarc.com.br
contato@managerone.com.br