

이메일 DNS 보안 취약사항 점검 가이드

≡ Task ID	
↗ 프로젝트	<u>Development_명재환</u>
↗ 상위작업	
↗ 담당그룹	 <u>DevSecOps</u>
↗ Work Type	<u>Documentation</u>
↗ Task 현황	 <u>Closed</u>
≡ 작업 년/월/주	2022년/9월/3주
↗ Technical Tags	<u>#Microsoft 365</u>
👤 작업자	⑦ 명재환
⬇ 우선순위	Normal
≡ 유형	Documentation
# 진척도	100%
📅 기간	
Σ 소요시간	D 0H
≡ 작업 내용 요약	전자메일(이메일)과 관련된 보안 가이드 내용을 정리하여 공유합니다.
👤 생성자	⑦ 명재환
👤 최종 편집자	⑦ 명재환
🕒 최종 변경일시	@2022년 9월 23일 오후 1:34
↗ Requestor - Cloocus	
↗ Requestor - Customer	
↗ Parent item	

메일은 고객 또는 관계사와의 업무 협업을 위한 창구로써 필수적으로 사용될 수밖에 없기 때문에, 업무 관련된 내용으로 첨부 파일이나 메일 내용을 작성하여 이를 사용자가 실행하게 되면 멀웨어에 감염되도록 악용하는 사례가 잇따르고 있습니다.

이를 방지하기 위한 메일 보안을 위한 여러 기술들이 있는데요. 대표적으로 SPF, DKIM, DMARC로써 이메일 보안 국제 표준 기술입니다.

각 기술별요약

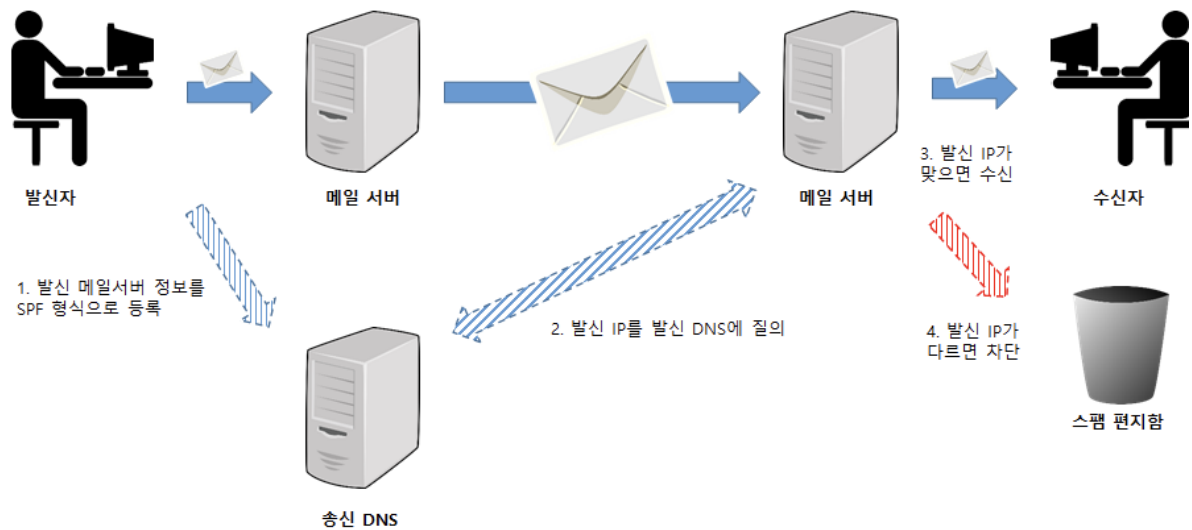
구분	SPF	DKIM	DMARC
인증 대상	발송 서버	메시지 발신자	발송 서버 & 메시지 발신자
인증 방법	메일 발송 IP 비교	전자서명	SPF & DKIM 검사 결과 조합
발신자 요구사항	DNS(메일 도메인)에 SPF 정책 설정 (별도 SW 설치 없음)	DNS에 공개키 등록 및 전자 서명 기술 적용	DNS에 DMARC 정책 설정
수신자 요구사항	메일 수신시스템(메일서버 등)에 SPF SW 설치 필요	메일 수신시스템(메일서버 등)에 DKIM SW 설치 필요	메일 수신시스템(메일서버 등)에 DMARC SW 설치 필요

출처: [이메일 보안을 위한 기술 SPF, DKIM, DMARC 에 대하여 알아보기 \(itsandtravels.blogspot.com\)](https://itsandtravels.blogspot.com).

1. SPF(Sender Policy Framework)

발신측에서 DNS에 SPF 레코드를 설정하고 SPF 레코드에는 메일서버 IP 정보, 사칭 메일에 대한 필터링 정책을 담고 있습니다. 수신측에서는 발신자 DNS에 SPF 레코드를 조회하여 사칭 여부를 확인합니다.

1. SPF 인증 절차



출처: [이메일 보안을 위한 기술 SPF, DKIM, DMARC 에 대하여 알아보기 \(itsandtravels.blogspot.com\)](http://itsandtravels.blogspot.com).

SPF 레코드는 다음과 같은 형식입니다.

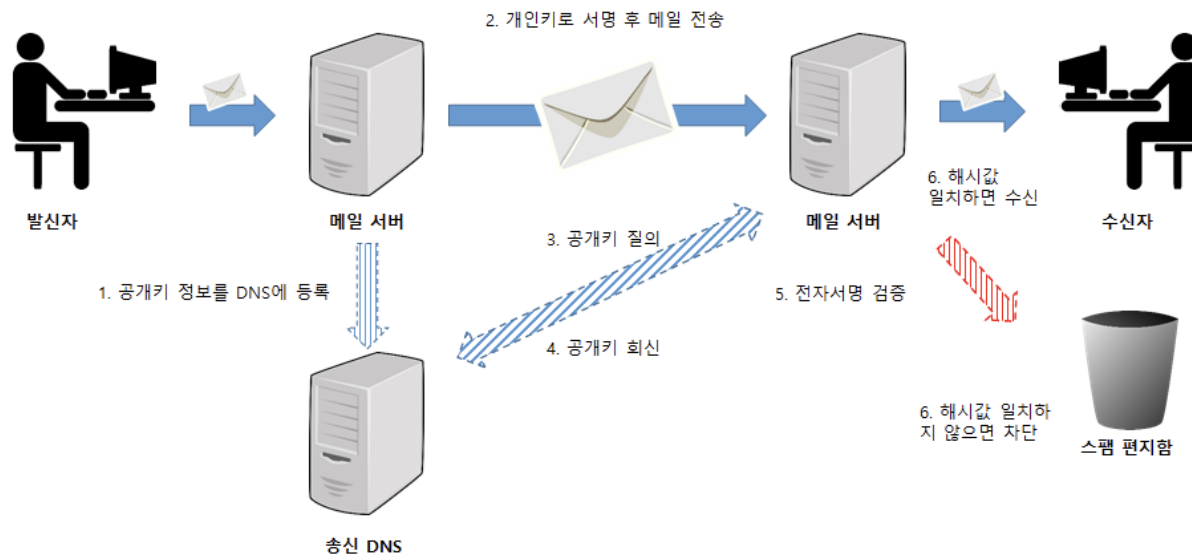
```
"v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.123 include:_spfblocka.example.com -all"
```

1. v: SPF 버전
2. +, ?, ~, -(퀄리파이어): SPF 인증을 통과하거나 실패한 이메일을 어떻게 처리할지 정의. +는 PASS, ?는 NEUTRAL 중립, ~는 가벼운 실패로써, 실패지만 수신될 것을 원하며 수신 서버에서 의심스러운 메일로 처리될 수 있다. -는 실패로 SPF 레코드에 등록되지 않는 서버에서 발송된 모든 메일은 수신이 거부될 수 있다.

2. DKIM(Domain Keys Identified Mail) 도메인 키 인증 메일

발신 측에서 자신의 DNS에 공개키를 등록하고, 메일에는 개인키로 서명한 뒤 전송합니다. 수신 측에서 발신자 DNS로부터 공개키를 받아 해시값과 메일에 포함된 해시값을 비교하여 일치여부를 확인합니다.

2. DKIM 인증 절차



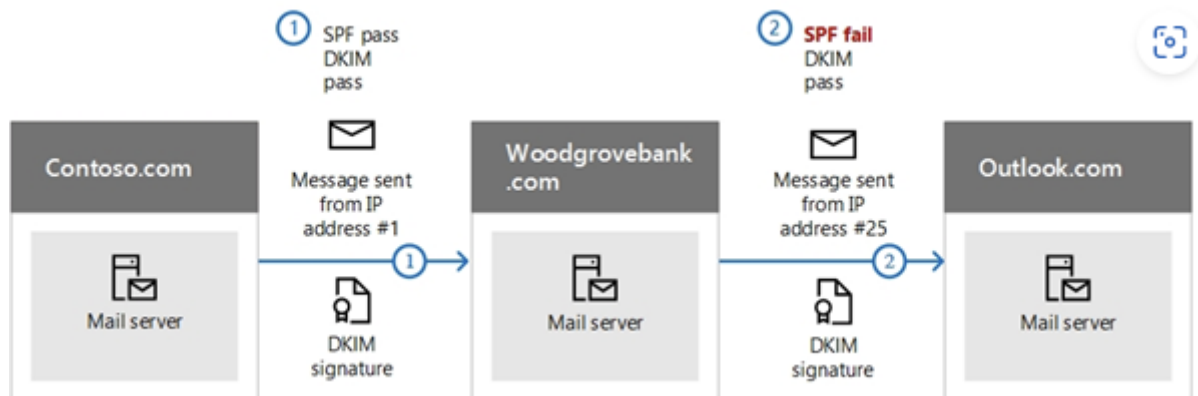
출처: [이메일 보안을 위한 기술 SPF, DKIM, DMARC 에 대하여 알아보기 \(itsandtravels.blogspot.com\)](https://itsandtravels.blogspot.com).

DKIM-Signature는 다음과 같은 형식으로 이메일 헤더(DKIM-Signature 헤더)에 추가됩니다.

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=toast;
t=1117574938; x=1118006938;
h=from:to:subject:date;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVyoFAKcdLXdJ0c9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

1. v: 버전 정보
2. a: DKIM 서명 알고리즘
3. d: 도메인 정보. DKIM 서명을 검증하기 위해 DNS에서 DKIM 레코드를 조회할 때 사용함
4. s: Selector 지정자. 발송 도메인은 여러 개의 DKIM을 사용할 수 있음. DKIM-Signature 헤더에서 어떤 공개키를 이용해 인증해야 하는지를 알려줌
5. bh: 이메일 본문 서명 값
6. b: 서명할 헤더에 정의된 헤더 서명 값

SPF와 DKIM을 예를 들어 설명한 그림을 살펴보면 이해하기 쉽습니다.

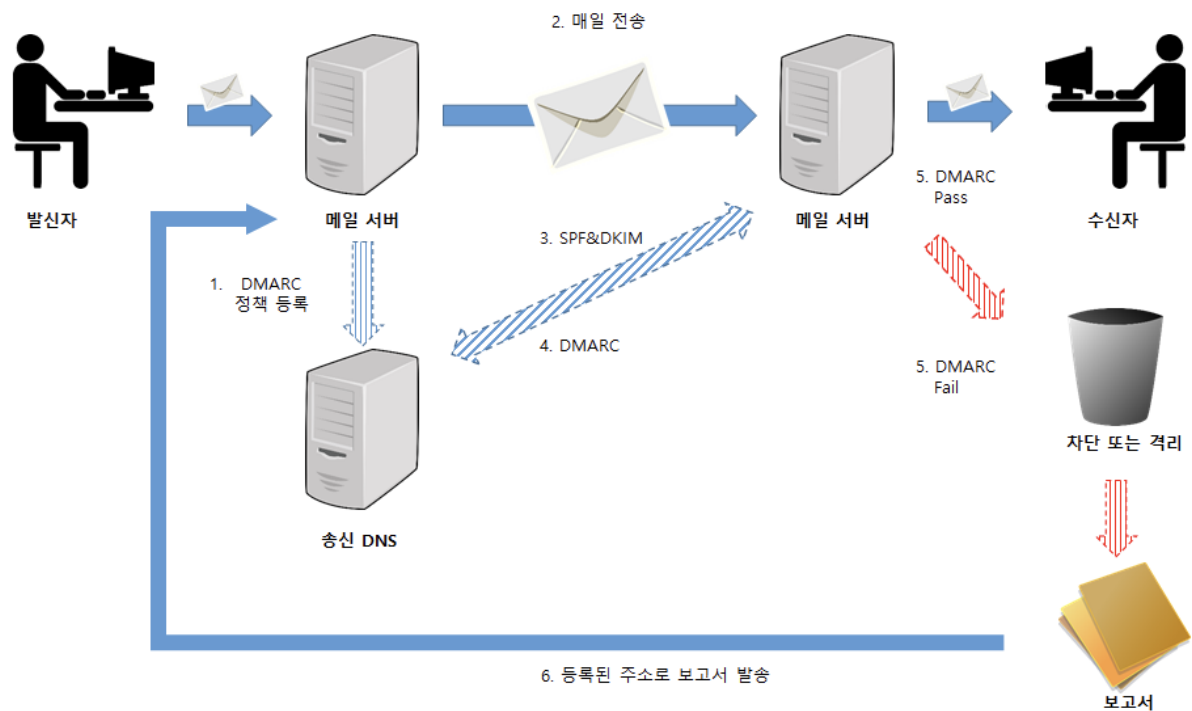


SPF는 메시지 봉투에 정보를 추가하는 방식이라 본다면, DKIM은 메시지 헤더에 서명을 하는 방식입니다. SPF 방식은 메시지 전달 시 여러 메일 서버를 거치면서 메시지 봉투가 제거될 수 있습니다. 하지만, DKIM 방식은 메시지 헤더의 일부로써 메일 메시지와 함께 목적지까지 유지됩니다.

3. DMARC(Domain-based Message Authentication, Reporting&conformance)

DMARC는 SPF와 DKIM을 사용하는지, 각각의 인증 수단이 실패했을 때 메일 처리 방법이 어떻게 되는지로 구성됩니다. 필수 기능은 아니지만, 대부분의 메일 서비스들은 DMARC를 사용합니다.

3. DMARC 인증 절차



DMARC DNS 레코드는 다음과 같은 형식입니다.

```
"v=DMARC1;p=none;sp=quarantine;pct=100;rua=mailto:dmarcreports@example.com;"
```

1. v: 버전 정보
2. p: 실패 시 처리에 대한 정책
3. sp: 서브 도메인에 대한 실패 처리 정책
4. pct: 정책을 적용할 이메일 비중. 예로 50인 경우 수신된 이메일 중 절반이 DMARC 정책에 의해 인증
5. rua: 주기적으로 집계한 실패 보고서를 수신할 주소 ex)mailto:demarc-report@example.com
6. ruf: 실패 보고서를 수신할 주소 ex)mailto:demarc-report@example.com
7. fo: 실패 보고서를 생성한 기준 ex)1, d, s
8. ri: 실패를 집계한 기간. 설정된 주기마다 실패 보고서(rua)가 발송됨. ex)86400(초, 기본값)

p(실패 정책)는 좀더 자세하게 구분됩니다.

none은 수신 서버에서 아무 처리도 하지 않을때를 상징하고, quarantine는 수신 서버는 실패한 메일을 스팸으로 처리함입니다. reject는 수신 서버에서 DMARC 실패가 발생한 메일을 반송합니다.

주의할 점은 DMARC는 수신 서버가 DMARC 정책에 맞게 처리하는 것을 완전히 보장하지 않는 것입니다. 즉, 발송 서버가 수신 서버에게 정책을 제안하는 수준으로 이해해야 합니다. 예를 들어 p실패 정책은 none으로 설정해야 수신 서버는 인증이 실패된 이메일을 스팸처리할 수 있습니다.

4. 점검 가이드:

앞서 설명한 SPF, DKIM, DMARC 정책을 조직이 적용하고 있는지, 있지만 취약사항이 어떻게 되는지를 살펴볼 수 있는 방안들에 대하여 다뤄보겠습니다.

1) 사이트(내부)에서 확인하는 방법

```
>nslookup
```

```
>set type=mx
```

>도메인 입력

```
2018014@N8-NAP002 ~ % nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=mx
> telus.co.kr
Server:      8.8.8.8
Address:     8.8.8.8#53
MX레코드
Non-authoritative answer:
telus.co.kr mail excha
SPF정책
Authoritative answers can be found from:
> set type=txt
> telus.co.kr

Non-authoritative answer:
telus.co.kr text:
telus.co.kr text:
telus.co.kr text:
telus.co.kr text:
telus.co.kr text:

Authoritative answers can be found from:
Dmarc정책
> _dmarc.telus.co.kr

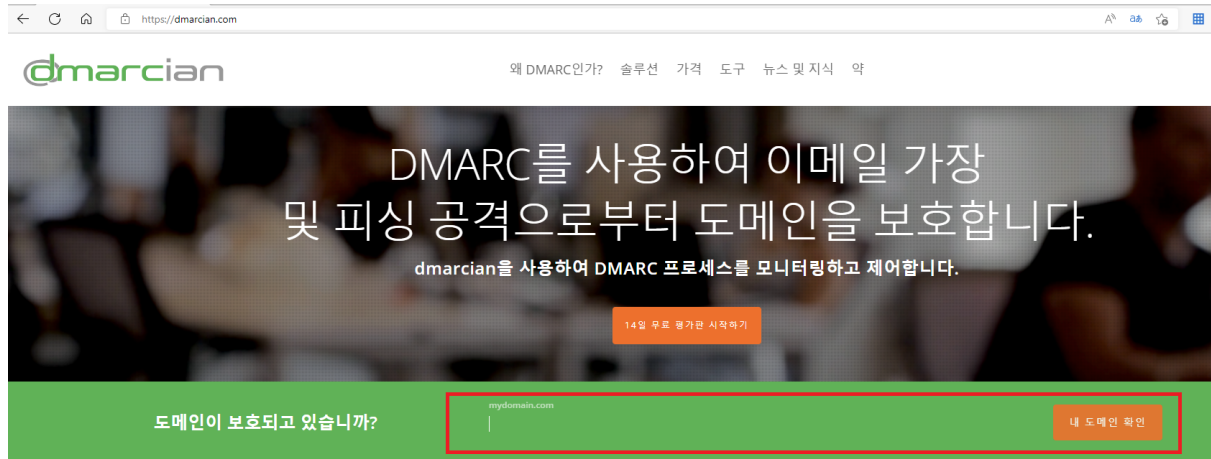
Non-authoritative answer:
_dmarc.telus.co.kr text = "v=DMARC1; p=none;"

Authoritative answers can be found from:
DKIM selector와 publickey
> selector1._domainkey.telus.co.kr

Non-authoritative answer:
|
```

2) 사이트에서 검색

<https://www.dmarcanalyzer.com/>, <https://dmarcian.com/> 에서 SPF, DMARC, DKIM 레코드를 조회



DMARC SaaS 플랫폼
애플리케이션이 인증 값(SPF/DKIM)과 도메인의 무단 사용을 노출하는 방식으로 DMARC 데이터를 처리하고 시각화할 수 있도록 합니다.

배포 서비스
자신감을 갖고 배포 관리자가 프로젝트 기반 접근 방식을 안내할 수 있도록 하여 DMARC 프로젝트 타임라인을 신속하게 처리할 수 있습니다.

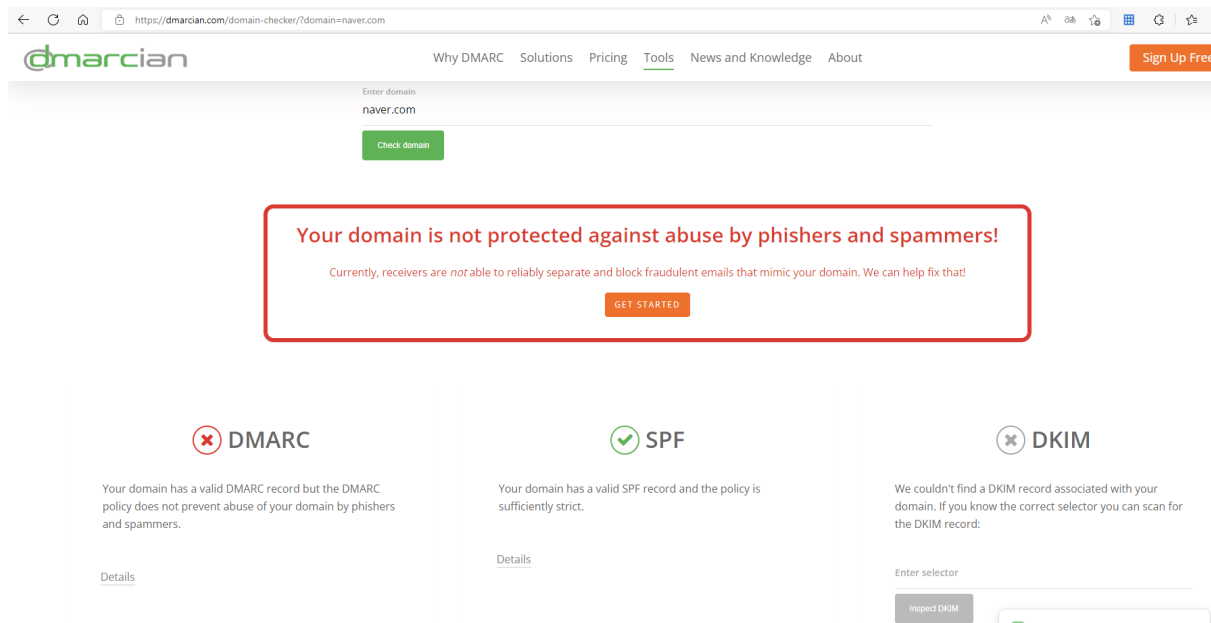
전담 지원
필요할 때 주문형 지원을 받으십시오. DMARC 관련 인시던트 검토, 지속적인 규정 준수 및 DMARC를 일상 업무에 임베드할 수 있습니다.

모든 규모와 DMARC 요구 사항의 조직에 적합합니다.

DMARC를 처음 접하거나 변화를 가져오는 도움이 필요한 조직에 이상적입니다.

위시드트 대륙 보충 또는 가형적 지휘이 필요한 조직에 기

dmarcian.com 무료 도메인 검사 사이트



naver로 검색 시 DMARC, SPF, DKIM 정보를 확인할 수 있다.

Details를 누르면 상세 정보를 확인할 수 있습니다. DMARC에서는 유효 레코드가 있지만, p 실패 정책이 없기 때문에, 피싱 및 스팸에 의한 도메인 남용을 방지 않는다고 확인할 수 있습니다. SPF는 유효한 SPF 레코드가 적용되고 있기 때문에 충분하다고 확인되었습니다.

❌ DMARC

Your domain has a valid DMARC record but the DMARC policy does not prevent abuse of your domain by phishers and spammers.

Details

v=DMARC1; p=none;
rua=mailto:dmARC_reports@worksmobile.com

For more insight into your DMARC record we recommend our [DMARC Inspector](#).

✅ SPF

Your domain has a valid SPF record and the policy is sufficiently strict.

Details

v=spf1 ip4:111.91.135.0/27 ip4:125.209.208.0/20
ip4:125.209.224.0/19 ip4:210.89.163.112
ip4:210.89.173.104/29 ip4:117.52.140.128/26 ~all

For more insight into your SPF record we recommend our [SPF Surveyor](#).

DKIM에서는 nslookup을 통한 명령어가 아니라면, 위에서 소개한 사이트에서 조회가 어려울 수 있습니다. 다음은 outlook 메일 속성을 통한 DKIM 헤더 정보를 확인하는 방법입니다.

outlook에서 파일 > 정보 > 속성을 선택합니다.

정보


저장

다른 이름으로 저장

첨부 파일 저장


인쇄

닫기


암호화

이 항목 암호화


이 항목에 대한 제한을 설정합니다. 예를 들어 이 전자 메일 메시지를 받은 사람(다른 사용자에게 전달하지 못하도록 제한할 수 있습니다.


폴더로 이동

다른 폴더로 항목 이동


이 항목을 다른 폴더로 이동 또는 복사합니다.

- 현재 폴더: 받은 편지함


배달 보고서 열기


메시지 배달 보고서

메시지가 배달된 시간과 메시지에 적용된 규칙(있는 경우) 등 이 전자 메일 메시지에 대한 배달 보고서를 검토합니다.


다시 보내기 또는 회수

메시지 다시 보내기 및 회수

이 전자 메일 메시지를 다시 보내거나 받는 사람으로부터 회수합니다.


속성

속성

이 항목의 고급 옵션 및 속성을 설정하고 확인합니다.

- 크기: 2 MB

인터넷 머리글을 모두 선택하고 notepad에 붙여넣기 하면 됩니다.

속성

설정

중요도(P) 중간

우편물 종류(Y) 보통

☐ 이 항목 자동 보관 안 함(U)

보안

☐ 메시지 내용과 첨부 파일 암호화(E)

☐ 보내는 메시지에 디지털 서명 추가(S)

☐ 이 메시지에 대한 S/MIME 확인 요청(T)

추적 옵션

☐ 메시지를 배달했을 때 알림(D)

☐ 메시지를 읽었을 때 알림(R)

배달 옵션

회신 대상 선택(T)

☐ 다음 날짜 이후에 만료(X) 없음 오전 12:00

연락처(C)...

범주(G) 없음

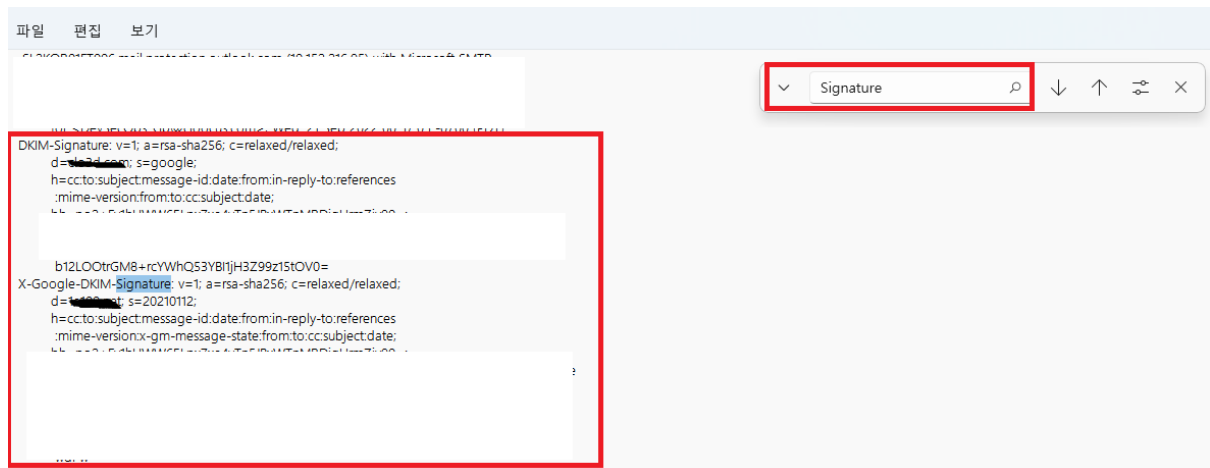
인터넷 머리글(H)

Received: from SL2P216MB0604.KORP216.PROD.OUTLOOK.COM (2603:1096:100:1e::9) by SLXP216MB1177.KORP216.PROD.OUTLOOK.COM with HTTPS; Wed, 21 Sep 2022 07:57:10 +0000

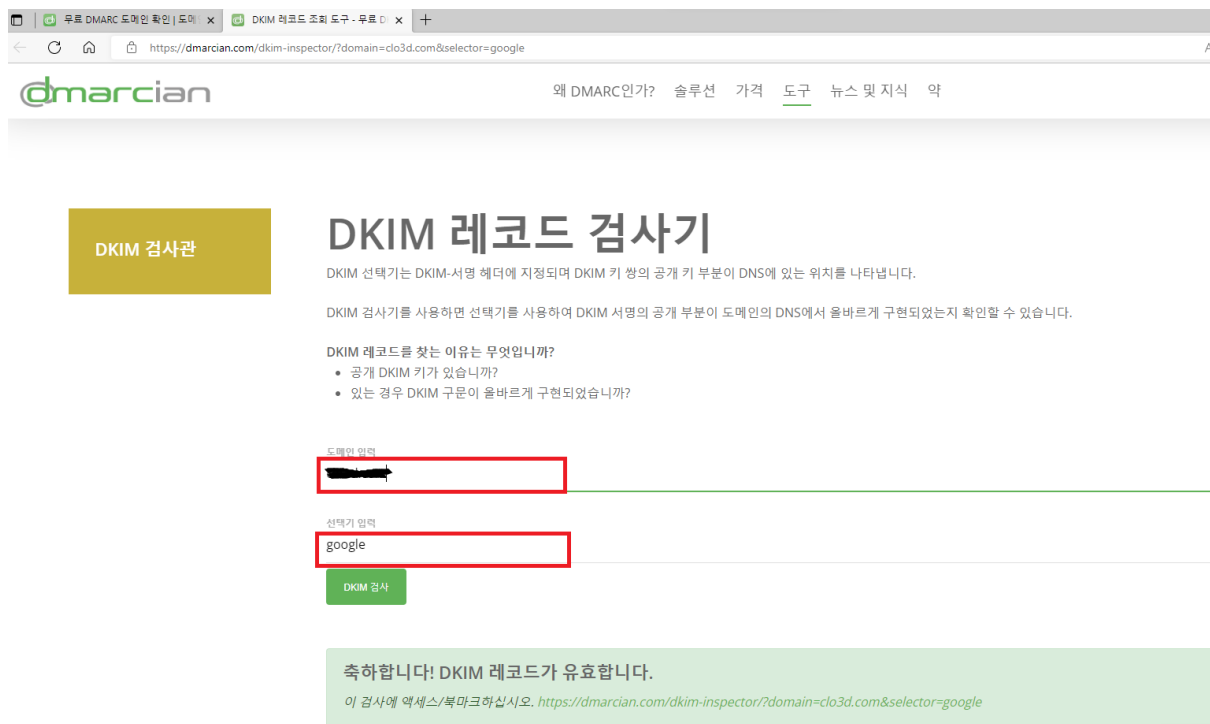
Received: from SL2P216CA0194.KORP216.PROD.OUTLOOK.COM (2603:1096:101:1b::19)

닫기

Signature로 검색하면 DKIM 정보를 확인할 수 있습니다.



해당 정보를 토대로 다시 dmarcian 사이트에서 DKIM 레코드 검사기(DKIM 레코드 조회 도구 - 무료 DKIM 체크 | 드마르시안 (dmarcian.com))로 이동합니다. 확인한 도메인 정보를 입력하고 선택기를 입력합니다. 선택기는 s=xxxx로 표현되는데, 위에서는 google로 검색되었네요. 확인 결과 DKIM레코드가 유효하다고 검색되었습니다.



Microsoft에서는 이와관련된 솔루션이 몇 가지 있습니다. Microsoft Defender for Office 365라는 제품으로 EOP(Exchange Online Protection)라는 솔루션도 있지만 Office

365(Outlook, SharePoint, OneDrive등) 보안에 좀 더 전문적인 제품이라고 할 수 있습니다([Office 365용 Microsoft Defender - Office 365 | Microsoft Learn](#))

해당 솔루션을 잠깐 살펴보면, 스푸핑 인텔리전스를 사용하여 SPF, DKIM, DMARC 검사를 통과하지 않는 도메인을 식별하고, 사서함 인텔리전스 기능은 보낸 사람이 합법적인지 스푸핑 되었는지 구분하는데 도움을 줍니다. 이 밖에 MITRE Attack 보안 프레임워크를 통한 공격 시뮬레이션 도구를 제공하고, SIEM 솔루션인 Microsoft Sentinel과 통합하여 상관 관계를 파악할 수도 있습니다.

이렇게 DKIM, SPF, DMARC 레코드에 대한 간략한 정보와 해당 레코드를 토대로 보안 점검을 수행할 수 있는 방안들에 대하여 살펴보았습니다.

긴글 읽어주셔서 감사합니다. 다음에 좀 더 유익한 정보로 찾아뵙겠습니다.

참고 사이트:

[Email 보안 강화 기능 소개\(SPF\) : NHN Cloud Meetup \(toast.com\)](#)

[이메일 보안을 위한 기술 SPF, DKIM, DMARC 에 대하여 알아보기 \(itsandtravels.blogspot.com\)](#)

[위키백과, 우리 모두의 백과사전 \(wikipedia.org\)](#)