DEVCORE
SECURITY
CONSULTING

I wanna know 你信不信 - 現代郵件詐術

高敏睿 (Mico)

戴夫寇爾股份有限公司

contact@devco.re

2023.03.11
DEVCORE Conference

中心思想

避免垃圾郵件阻擋

繞過郵件夾檔防火牆

如何構造一封實戰的釣魚郵件

繞過危險郵件警示

偽造網域寄信

DEVCORE SECURITY CONSULTING

攻擊導向的大綱

- 現在還能使用的攻擊招
- 現代有的 Email 欺騙偵測/防護機制
- 安全機制繞過方法
- 現代的 Email 攻擊技術方向
- 給網釣白帽的建議

Mail From

<高敏睿 / Mico>

現職

DEVCORE 紅隊演練專家

業餘經歷

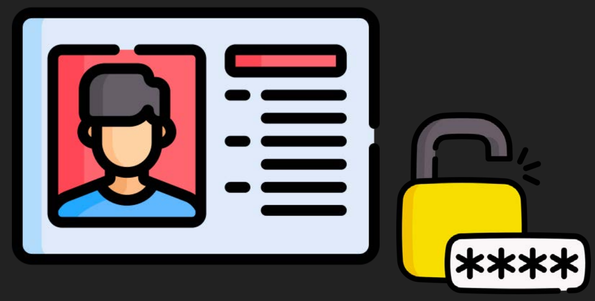
- WorldSkills 46th 網路安全職類 世界銀牌
- 2022 AIS3 網頁安全講師

內部演練畫面
僅公布於研討會

以下內容皆為與真實對等的虛擬情境

釣魚信件的秘密？

信寄的進



資料回的來

DEVCORE SECURITY CONSULTING

釣魚網站常見手法

- 假冒企業員工服務網站
  - 騙取企業員工登入憑證
- 假冒政府登記網站
  - 騙取個人身份資訊
- 假冒知名服務網站
  - 騙取常用帳號密碼

誘導下載惡意程式

騙取更多存取權限進而控制內網、勒索等...

平常可以蒐集的資訊素材

- 企業內網資訊、網址
- 蒐集已知或外洩的帳號、信箱帳號、工號及姓名
- 員工生活好友圈、飲食、生活足跡、常用軟體，打字、表情符號習慣
- 公司行程或活動日期，企業文化
- 通用客製化系統前端（帳務、人資、內訓服務、通訊系統、公文系統）
- 常用軟體資訊（VPN、WordPress、vCenter、共筆）

以貼近真實的來源，寄送假的內容

DEVCORE SECURITY CONSULTING

貼近真實的?

情境 (受害者)

員工 (Ben@devkors.lan)

攻擊情境 #1 (偽造不存在的域名)

駭客 -> 不存在 (notify@non-exist.gov.tw)

員工 (Ben@devkors.lan)

攻擊情境 #2 (偽造存在的域名)

駭客 -> 存在 (notify@google.com)

員工 (Ben@devkors.lan)

攻擊情境 #3 (偽造相似目標的域名)

駭客 -> 相似 (notify@devk0rs.lan)

員工 (Ben@devkors.lan)

攻擊情境 #4 (偽造相同目標的域名)

駭客 -> 相同 (notify@devkors.lan)

員工 (Ben@devkors.lan)

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

1　不存在

notify@non-exist.gov.tw

2　存在

notify@google.com

3　相似

notify@devk0rs.lan

4　相同

notify@devkors.lan

信件就只是個文字封包

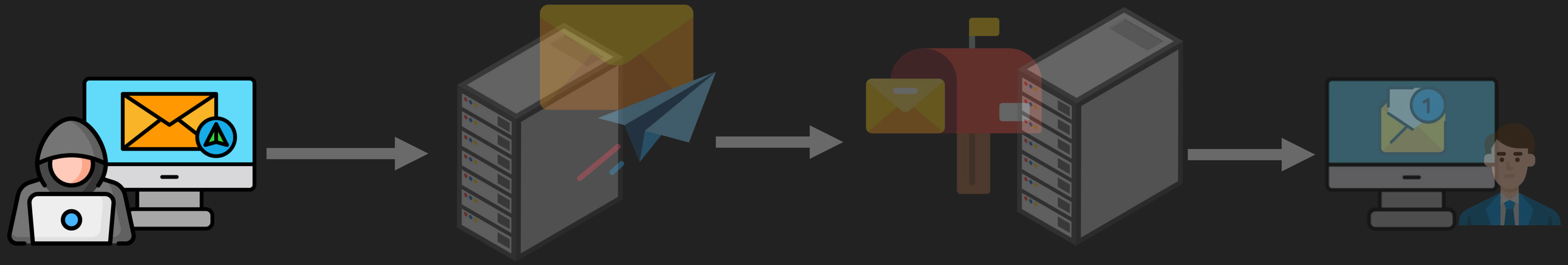
任何人，都可以修改成任意信箱

寄信給你

安全機制?

寄信角色介紹？

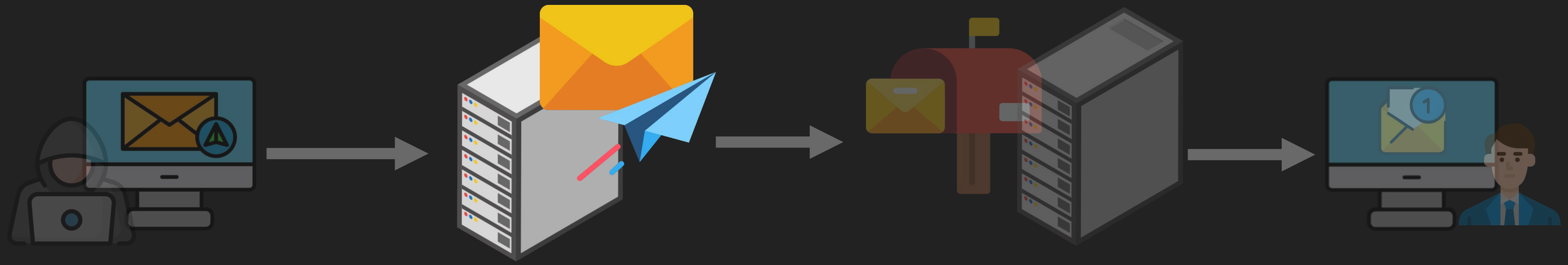
寄信用戶端



MUA MTA MRA MUA

寄信角色介紹？

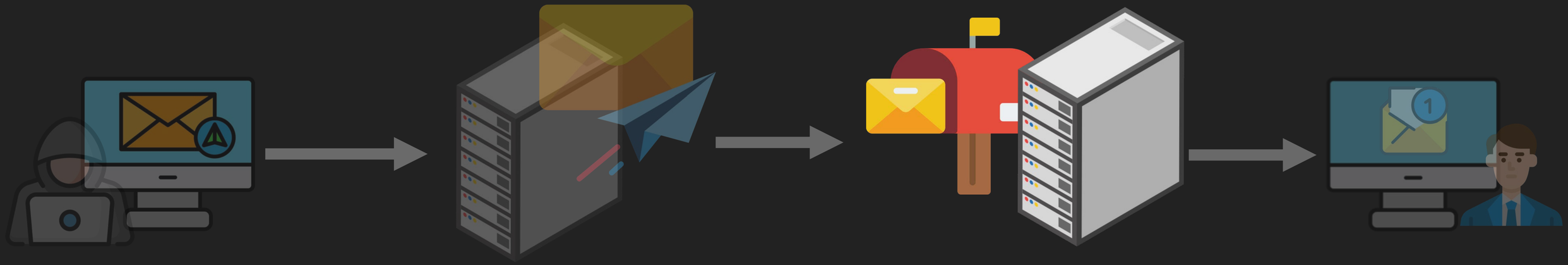
寄信伺服器



MUA　MTA　MRA　MUA

寄信角色介紹？

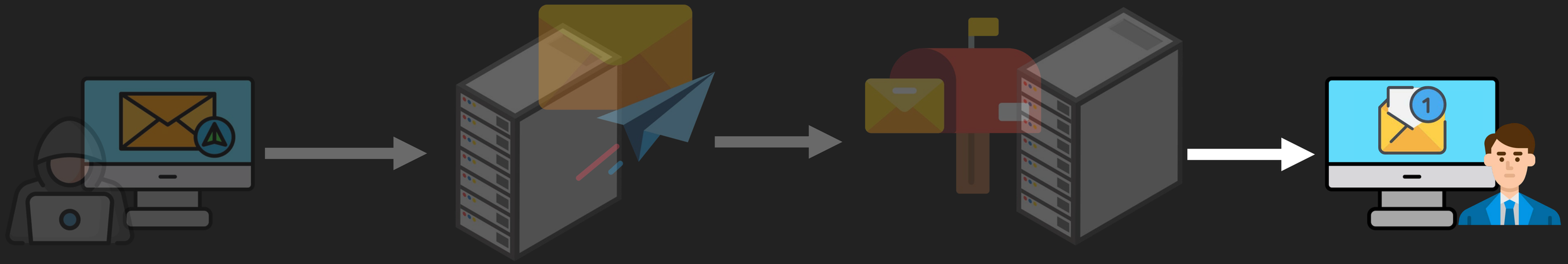
收信伺服器



MUA　MTA　MRA　MUA

寄信角色介紹？

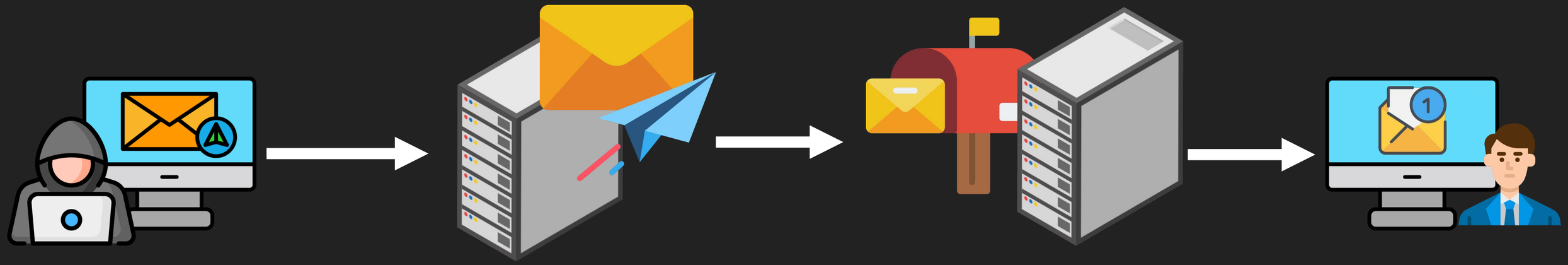
收信用戶端



MUA MTA MRA MUA

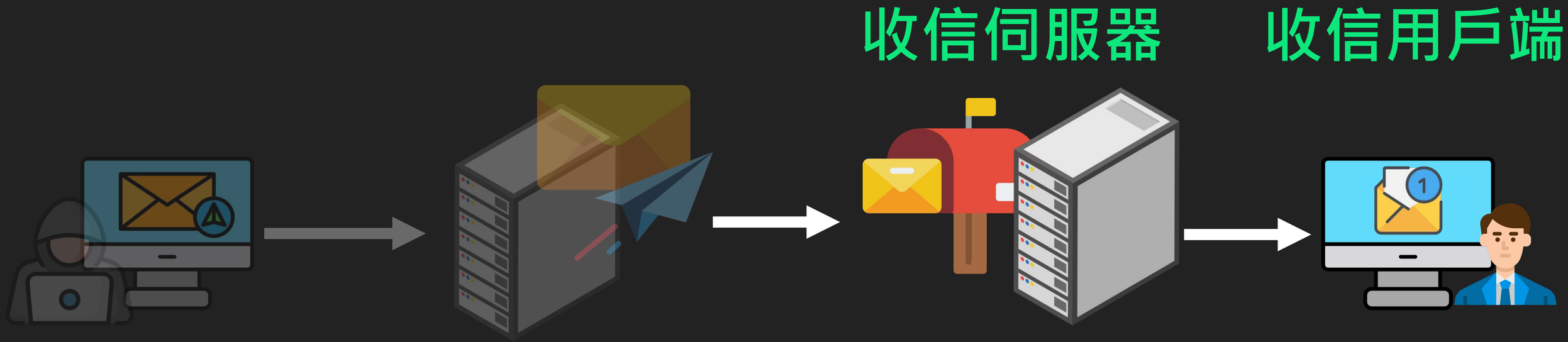
這次要講的安全機制在哪？

寄信用戶端　寄信伺服器　收信伺服器　收信用戶端



MUA　MTA　MRA　MUA

這次要講的安全機制在哪？



探討 收信端(Gmail) 上的就好

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC SPF DKIM

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC

防範網域被別人假冒，驗證以下兩項
(若都驗證不過，就讓對方把信丟了)

SPF

該網域寄信伺服器的 IP 白名單

DKIM

網域信件防竄改的驗證公鑰

DEVCORE SECURITY CONSULTING

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC  罰則

SPF  規則

DKIM  規則

DEVCORE SECURITY CONSULTING

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC  **罰則（若未設置）**

SPF  規則（沒罰則）

DKIM  規則（沒罰則）

DEVCORE SECURITY CONSULTING

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC 

dig txt _dmarc.devkors.lan

SPF 

dig txt devkors.lan

DKIM 

dig txt foo_domainkey.devkors.lan

DMARC、SPF、DKIM 懶人包 (Email 安全三劍客)

DMARC

dig txt _dmarc.devkors.lan

v=DMARC1; p=reject;

SPF

dig txt devkors.lan

v=spf1 ip4:203.0.113.13 ~all

DKIM

dig txt foo_domainkey.devkors.lan

v=DKIM1; k=rsa; p={PublicKey}

DEVCORE SECURITY CONSULTING

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1 不存在 (notify@non-exist.gov.tw)

目標無 SPF、DKIM、DMARC 紀錄

 # 2 存在 (notify@google.com)

 # 3 相似 (notify@devk0rs.lan)

 # 4 相同 (notify@devkors.lan)

DEVCORE SECURITY CONSULTING

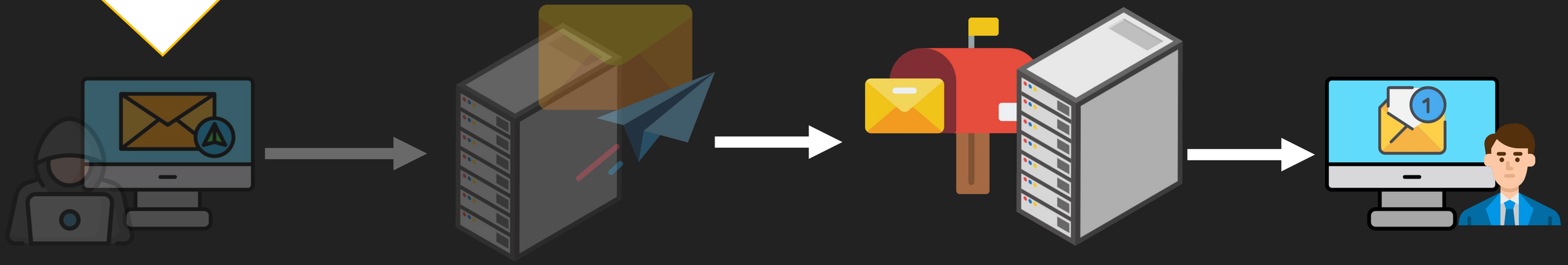
MAIL FROM: <notify@non-exist.gov.tw>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

1 不存在 (notify@non-exist.gov.tw)

MAIL FROM: <notify@non-exist.gov.tw>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

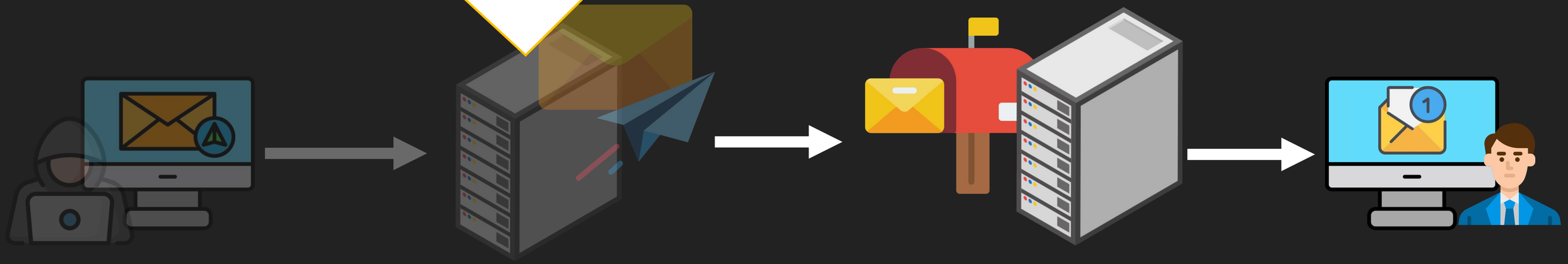


MUA MTA MRA MUA

1 不存在 (notify@non-exist.gov.tw)

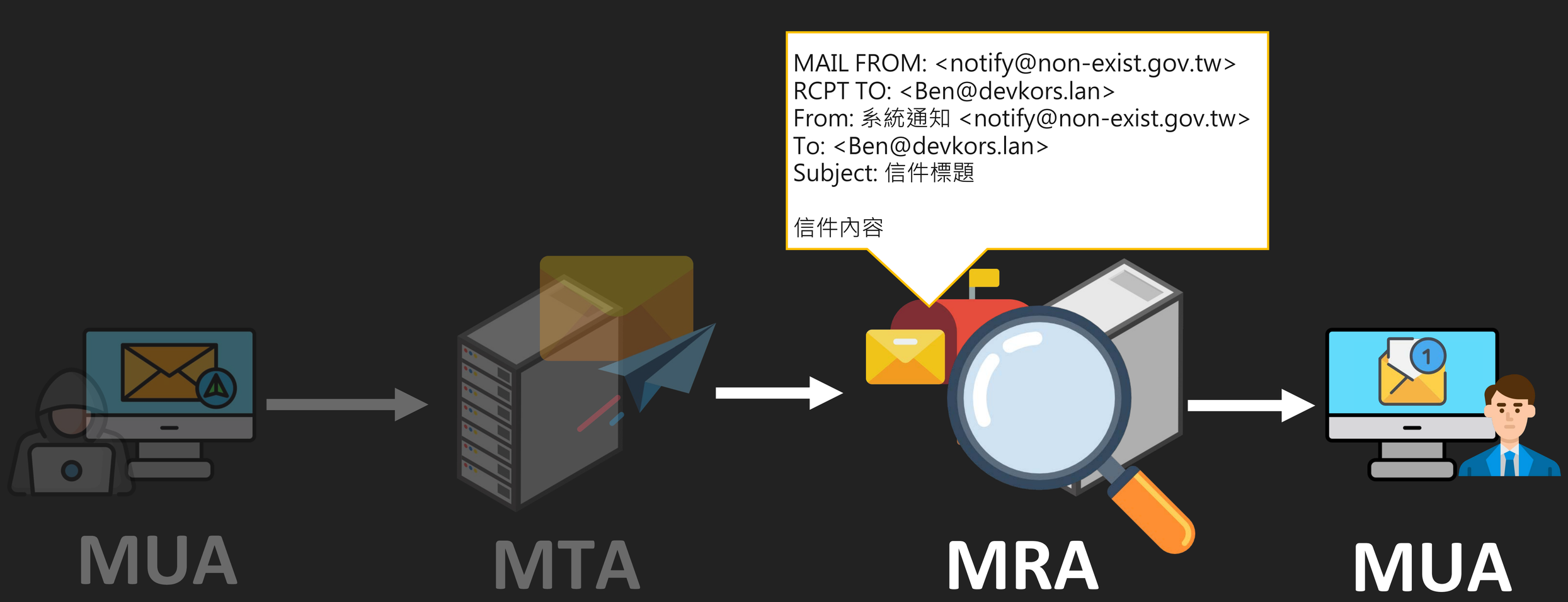
MAIL FROM: <notify@non-exist.gov.tw>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容



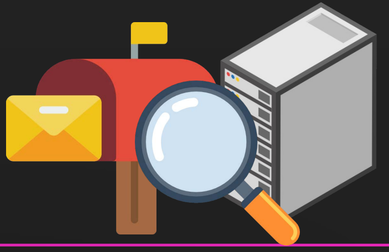
MUA MTA MRA MUA

1 不存在 (notify@non-exist.gov.tw)



1 不存在 (notify@non-exist.gov.tw)

安全機制

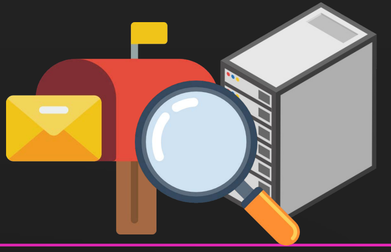
MRA 

垃圾信保護機制 (不存在 SPF 紀錄)

MAIL FROM: <notify@non-exist.gov.tw>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

安全機制

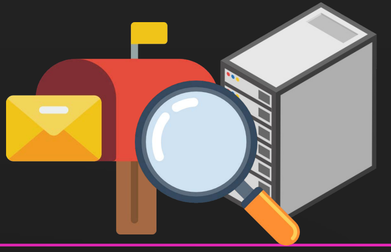
MRA 

SPF 驗證寄信來源 IP – 方法

```
dig txt non-exist.gov.tw
```

“查無 SPF 記錄”

安全機制

MRA 

SPF 驗證寄信來源 IP – 方法

```
dig txt non-exist.gov.tw
```

“查無 SPF 記錄”

NEUTRAL 😕

DEVCORE

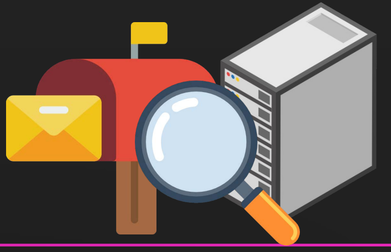
因為沒 DMARC ，沒罰則 (不丟信)

但 Gmail 還是會試圖保護受害者


信件標題
外部
收件匣 ×
notify@non-exist.gov.tw
寄給 Ben
信件內容.


垃圾郵件 ×
寄給 我
為什麼這封郵件被歸類為垃圾郵件？ 這封郵件的內容與先前歸類為垃圾郵件的郵件相似。
回報為非垃圾郵件

安全機制

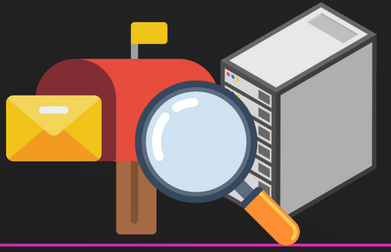
MRA 

垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

安全機制

MRA 

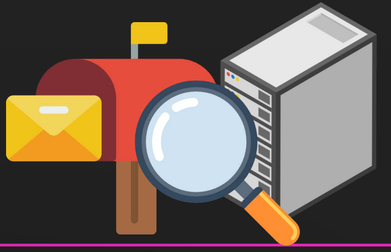
SPF 驗證寄信來源 IP (RFC 7208)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

（SPF 驗證看哪一個？）

安全機制

MRA 

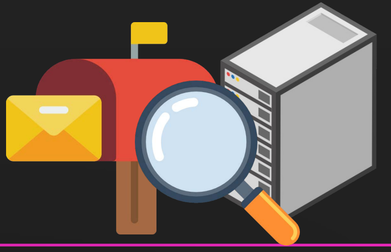
SPF 驗證寄信來源 IP (RFC 7208)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

（SPF 驗證看哪一個？-> MAIL FROM）

安全機制

MRA 

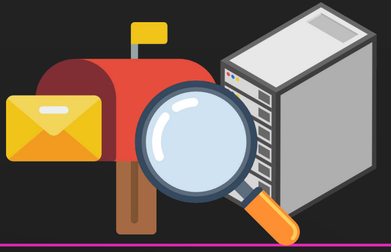
垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

(這樣不一樣也可以哦？)

安全機制

MRA 

垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

（這樣不一樣也可以哦？-> 可以）

安全機制

MUA 

垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

（實際收信顯示哪一個？）

安全機制

MUA 

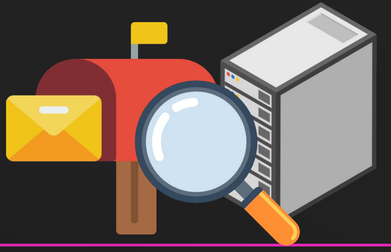
垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>

From: 系統通知 <notify@non-exist.gov.tw>

（實際收信顯示哪一個？-> From ）

安全機制

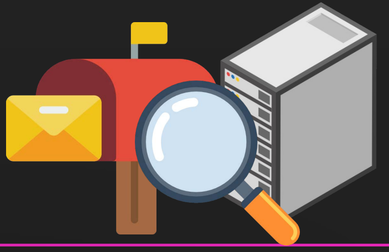
MRA 

SPF 驗證寄信來源 IP

MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

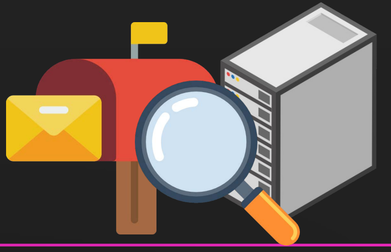
安全機制

MRA 

SPF 驗證寄信來源 IP – 方法

```
dig txt hacker.com
```

安全機制

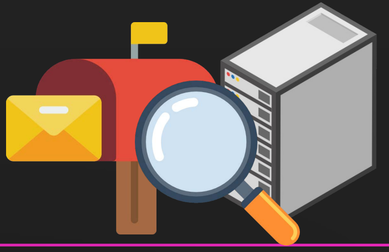
MRA 

SPF 驗證寄信來源 IP – 方法

dig txt hacker.com

“v=spf1 ip4:203.0.113.13 ~all” (hacker 完全可控)

安全機制

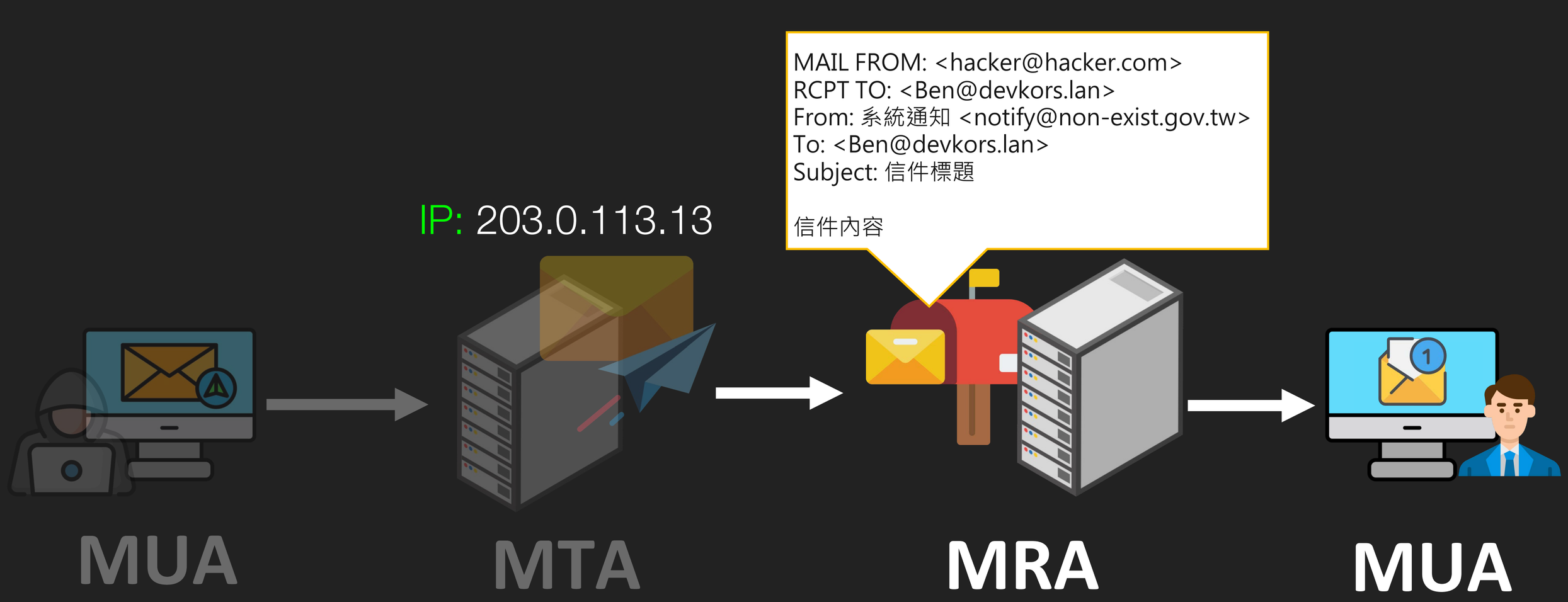
MRA 

SPF 驗證寄信來源 IP – 方法

dig txt hacker.com

“v=spf1 ip4:203.0.113.13 ~all” (hacker 完全可控)

PASS 203.0.113.13 (MTA)

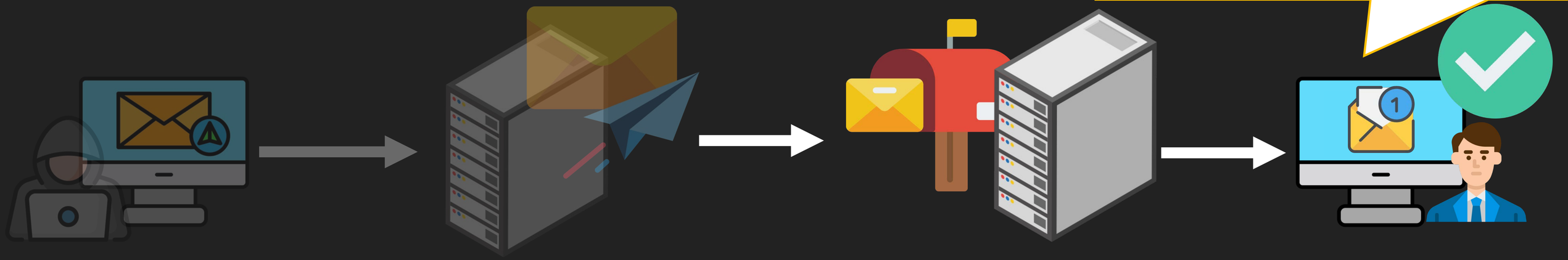


1 不存在 (notify@non-exist.gov.tw)

MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@non-exist.gov.tw>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

IP: 203.0.113.13



MUA MTA MRA MUA

1 不存在 (notify@non-exist.gov.tw)

MUA

信件標題 外部 收件匣 ×

系統通知 notify@non-exist.gov.tw 透過 hacker.com

寄給 Ben

信件內容

SPF： PASS，IP 203.0.113.13 瞭解詳情

MUA

信件標題 外部 收件匣 ×

系統通知 notify@non-exist.gov.tw 透過 hacker.com

寄給 Ben

信件內容

SPF： PASS，IP 203.0.113.13 瞭解詳情

如何去除掉這個 tag？

1. 手機版 Gmail 不會顯示

1. 手機版 Gmail 不會顯示
2. 透過郵寄清單轉發 (Remailing) 殺招

透過郵寄清單轉發 (Remailing) 殺招

駭客 -> 不存在 (notify@non-exist.gov.tw)

員工群組 (staff@devkors.lan)

透過郵寄清單轉發 (Remailing) 殺招

駭客 -> 不存在 (notify@non-exist.gov.tw)

員工群組 (staff@devkors.lan)

員工 (Ben@devkors.lan)
員工 (...@devkors.lan)
員工 (...@devkors.lan)

MUA

信件標題 外部 收件匣 ×

系統通知 <notify@non-exist.gov.[redacted]

寄給 staff

信件內容

MUA

信件標題 外部 收件匣 ×

系統通知 <notify@non-exist.gov.tw>

寄給 staff

信件內容

MUA

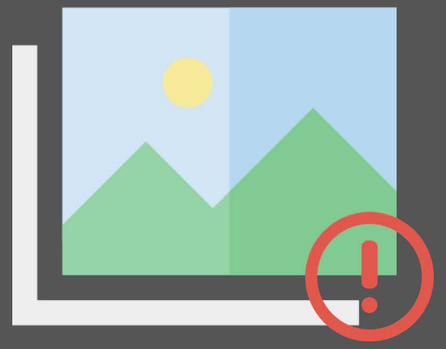
信件標題 外部 收件匣 ×

系統通知 <notify@non-exist.gov.tw>

寄給 staff

信件內容

I WANNA KNOW 你信不信



內部演練畫面
僅公布於研討會

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1 不存在 (notify@non-exist.gov.tw)

目標無 MX、SPF、DKIM、DMARC 紀錄

 # 2 存在 (notify@google.com)

目標有 SPF、DKIM、DMARC 紀錄

 # 3 相似 (notify@devk0rs.lan)

 # 4 相同 (notify@devkors.lan)

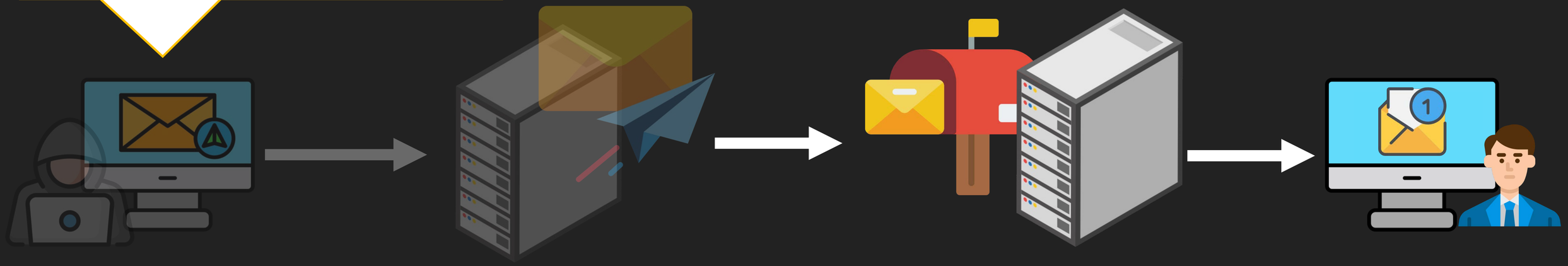
MAIL FROM: <notify@google.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

 # 2 存在 (notify@google.com)

MAIL FROM: <notify@google.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

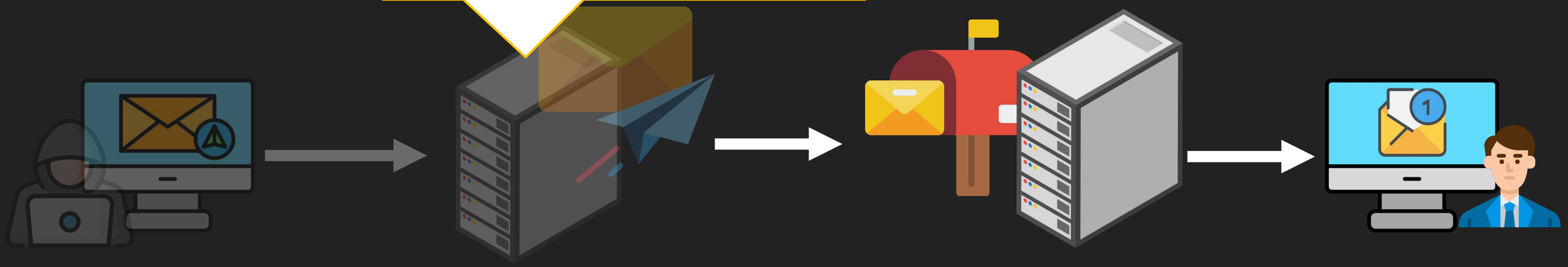


MUA MTA MRA MUA

2 存在 (notify@google.com)

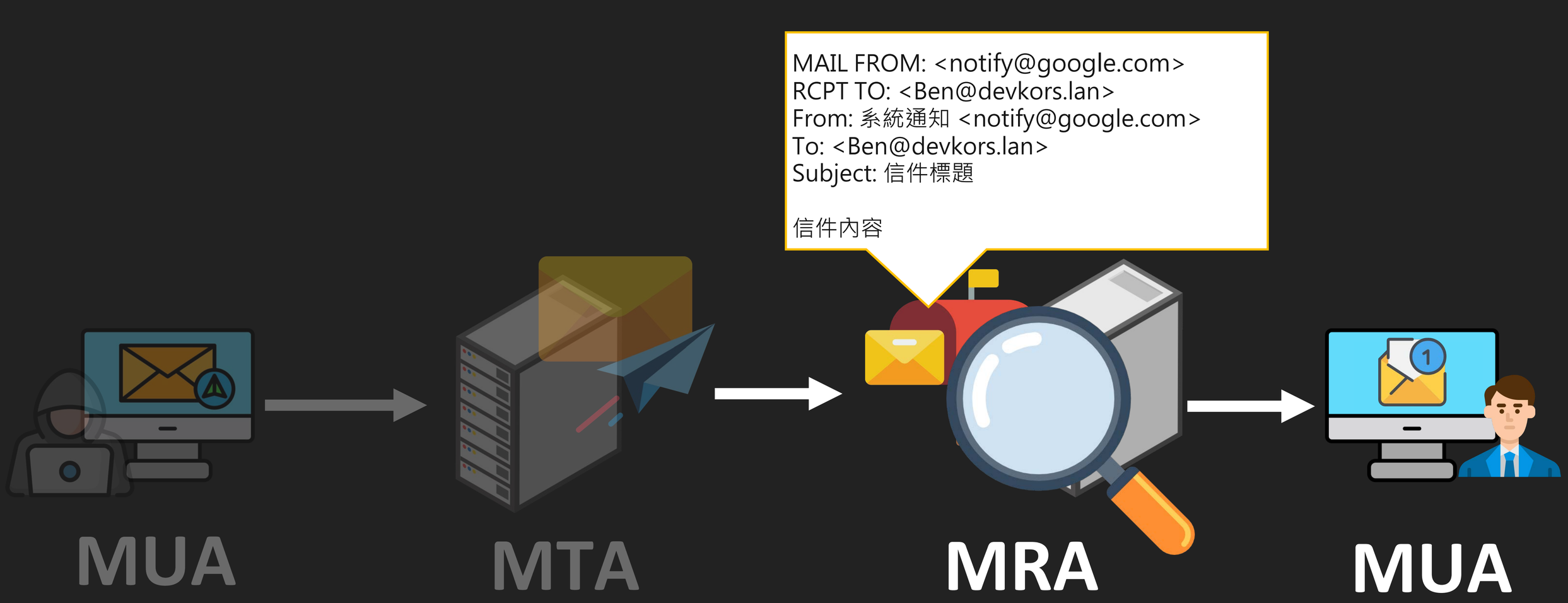
MAIL FROM: <notify@google.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容



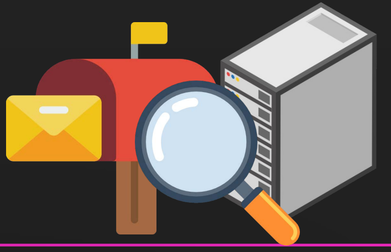
MUA MTA MRA MUA

2 存在 (notify@google.com)



2 存在 (notify@google.com)

安全機制

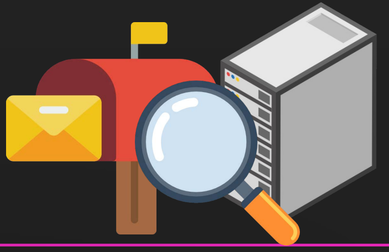
MRA 

SPF 驗證寄信來源 IP

MAIL FROM: <notify@google.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

安全機制

MRA 

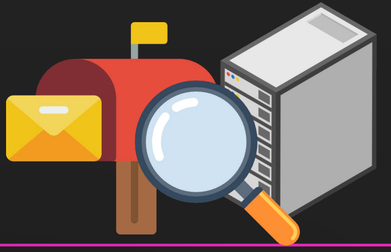
SPF 驗證寄信來源 IP – 方法

```
dig txt google.com
```

“v=spf1 include:_spf.google.com ~all”

SOFTFAIL 😕

安全機制

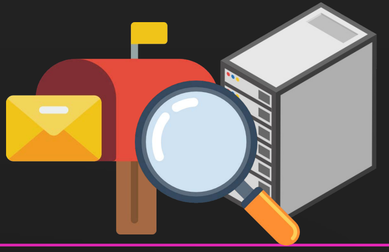
MRA 

垃圾信保護機制 (改個存在 SPF 紀錄的)

MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容

安全機制

MRA 

SPF 驗證寄信來源 IP – 方法

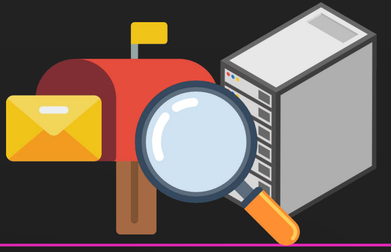
dig txt hacker.com

“v=spf1 ip4:203.0.113.13 ~all” (hacker 完全可控)

PASS 203.0.113.13 (MTA)

但 google.com 還有 DKIM 和 DMARC 機制

安全機制

MRA 

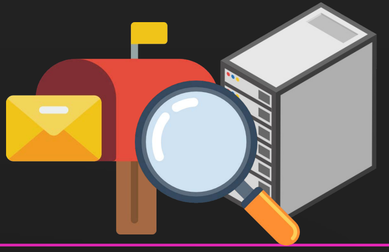
DKIM 保護完整性機制 – (原始信件)

- **DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/relaxed; **d=google.com; s=20210112;** h=to:from:subject:message-id:feedback-id:reply-to:date:mime-version:from:to:cc:subject:date:message-id:reply-to; bh={hash};b={signature}

信件內容

DEVCORE

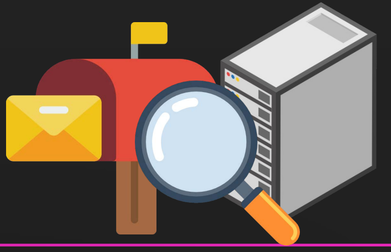
安全機制

MRA 

DKIM 保護完整性機制 – 方法

```
dig txt 20210112_domainkey.google.com
```

安全機制

MRA 

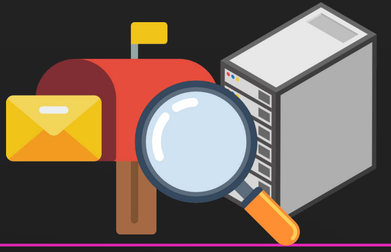
DKIM 保護完整性機制 – 方法

dig txt **20210112**_domainkey.**google.com**

“v=DKIM1; k=rsa; p={PublicKey}”

但 DKIM-Signature 自改 domain 也可

安全機制

MRA 

DKIM 保護完整性機制

- **DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=**hacker.com**; s=**20210112**; h=to:from:subject:message-id:feedback-id:reply-to:date:mime-version:from:to:cc:subject:date:message-id:reply-to;
  bh={new-hash};b={new-signature}

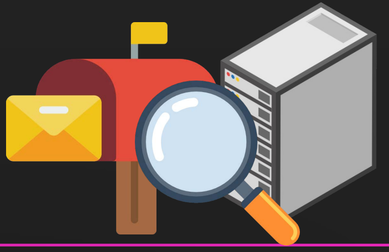
（domain 自改自簽，不也會過嗎）

DEVCORE

SPF & DKIM PASSED

但 google.com 有 DMARC 機制

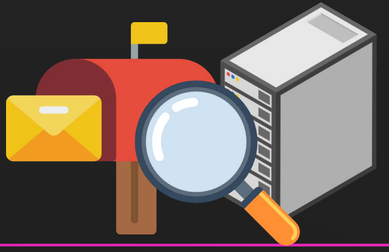
安全機制

MRA 

DMARC 保護機制 – 方法

```
dig txt _dmarc.google.com
```

安全機制

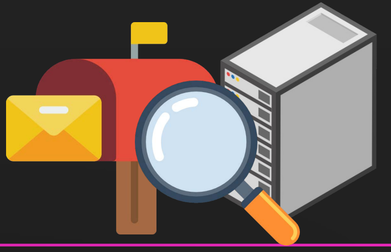
MRA 

DMARC 保護機制 – 方法

```
dig txt _dmarc.google.com
```

```
“v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com”
```

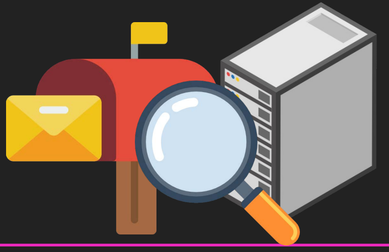
安全機制

MRA 

DMARC 保護機制 – 方法

- v： 必須為 DMARC1
- p：none = 不處理，quarantine = 進垃圾郵件，**reject = 拒收**
- rua：mailto:mailauth-reports@google.com，有人違規的話，MRA 就會打小報告到這裡

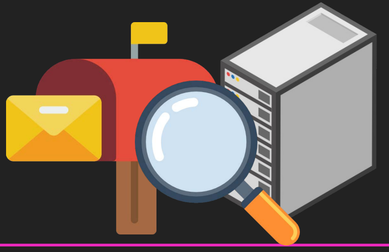
安全機制

MRA 

DMARC 保護機制

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)

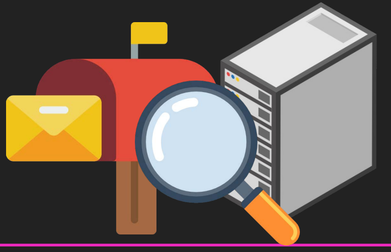
安全機制

MRA 

DMARC 保護機制

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)
- 且 SPF 或 DKIM 與 From 必須相同 Domain

安全機制

MRA 

DMARC 保護機制

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)
- 且 SPF 或 DKIM 與 From 必須相同 Domain

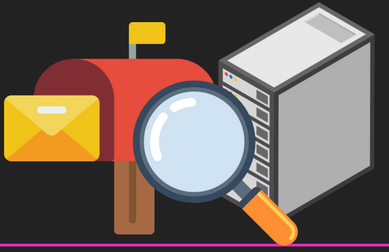
MAIL FROM 網域不同

```
MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容
```

DKIM 網域不同

```
•DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=hacker.com; s=20210112; h=to:from:subject:message-
id:feedback-id:reply-to:date:mime-
version:from:to:cc:subject:date:message-id:reply-to;
bh={new-hash};b={new-signature}
```

安全機制

MRA 

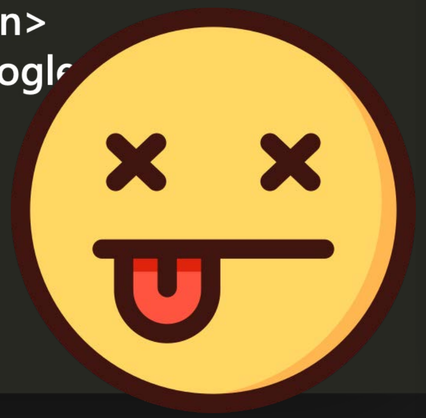
DMARC 保護機制

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)
- 且 SPF 或 DKIM 與 From 必須相同 Domain

MAIL FROM 網域不同

MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容



DKIM 網域不同

•DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=hacker.com; s=20210112; h=to:from:sub
id:feedback-id:reply-to:date:mime-
version:from:to:cc:subject:date:message-id
bh={new-hash};b={new-signature}

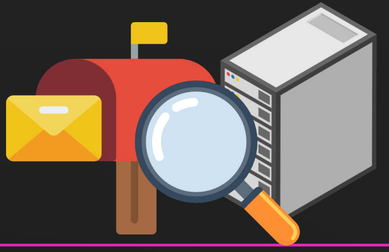
怎麼繞？

Inconsistencies DKIM (Fixed)

https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun

```
@inproceedings{chen-email,
author = {Jianjun Chen and Vern Paxson and Jian Jiang},
title = {Composition Kills: A Case Study of Email Sender Authentication},
booktitle = {29th {USENIX} Security Symposium ({USENIX} Security 20)},
year = {2020},
isbn = {978-1-939133-17-5},
pages = {2183--2199},
url = {https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun},
publisher = {{USENIX} Association},
month = aug,
}
```

安全機制

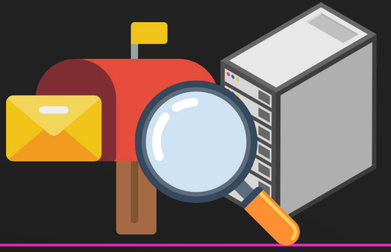
MRA 

DKIM 保護完整性機制

- **DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/relaxed; **d=google.com; s=20210112;** h=to:from:subject:message-id:feedback-id:reply-to:date:mime-version:from:to:cc:subject:date:message-id:reply-to; bh={hash};b={signature}

DEVCORE

安全機制

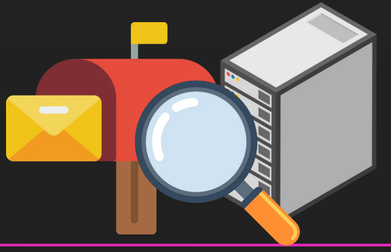
MRA 

DKIM 保護完整性機制 – 方法

dig txt **20210112**_domainkey.**google.com**

“v=DKIM1; k=rsa; p={PublicKey}”

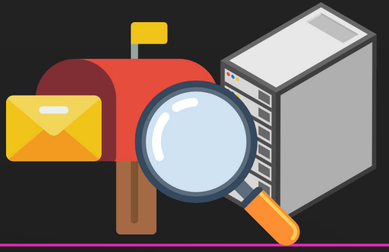
安全機制

MRA 

DKIM 保護完整性機制 – 解析問題

- **DKIM-Signature:** v=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=hacker.com.\x00.20210112;
h=to:from:subject:message-id:feedback-id:reply-to:date:mime-version:from:to:cc:subject:date:message-id:reply-to;
bh={hash};b={signature}

安全機制

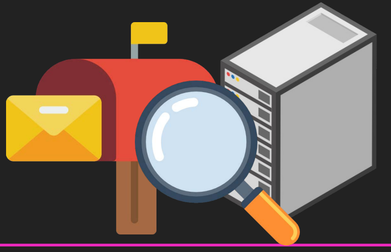
MRA 

DKIM 保護完整性機制 – 駭客可控

dig txt hacker.com.

“v=DKIM1; k=rsa; p={PublicKey}”

安全機制

MRA 

DMARC 保護機制 – 不一致攻擊

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)
- 且 SPF 或 DKIM 與 From 必須相同 Domain

MAIL FROM 網域不同

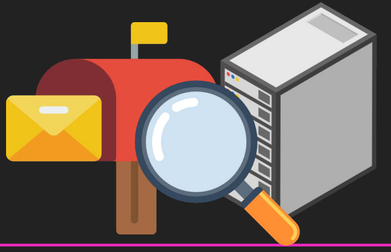
```
MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google.com>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容
```

DKIM 網域相同

```
•DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=hacker.com.\x00.20210112;
h=to:from:subject:message-id:feedback-id:reply-to:date:mime-
version:from:to:cc:subject:date:message-id:reply-to;
bh={hash};b={signature}
```

安全機制

MRA

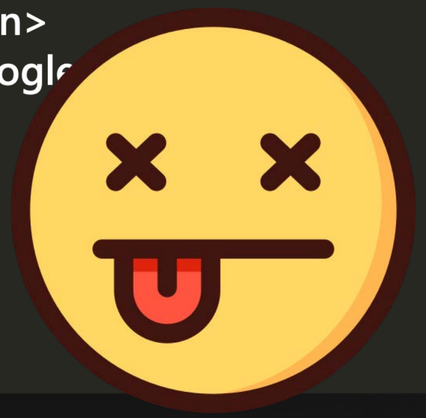


DMARC 保護機制 – 不一致攻擊

- 你一定得通過 SPF 或 DKIM 保護機制 (已過)
- 且 SPF 或 DKIM 與 From 必須相同 Domain

MAIL FROM 網域不同

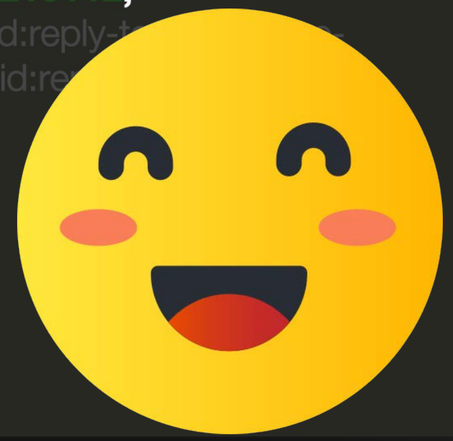
```
MAIL FROM: <hacker@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@google
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容
```



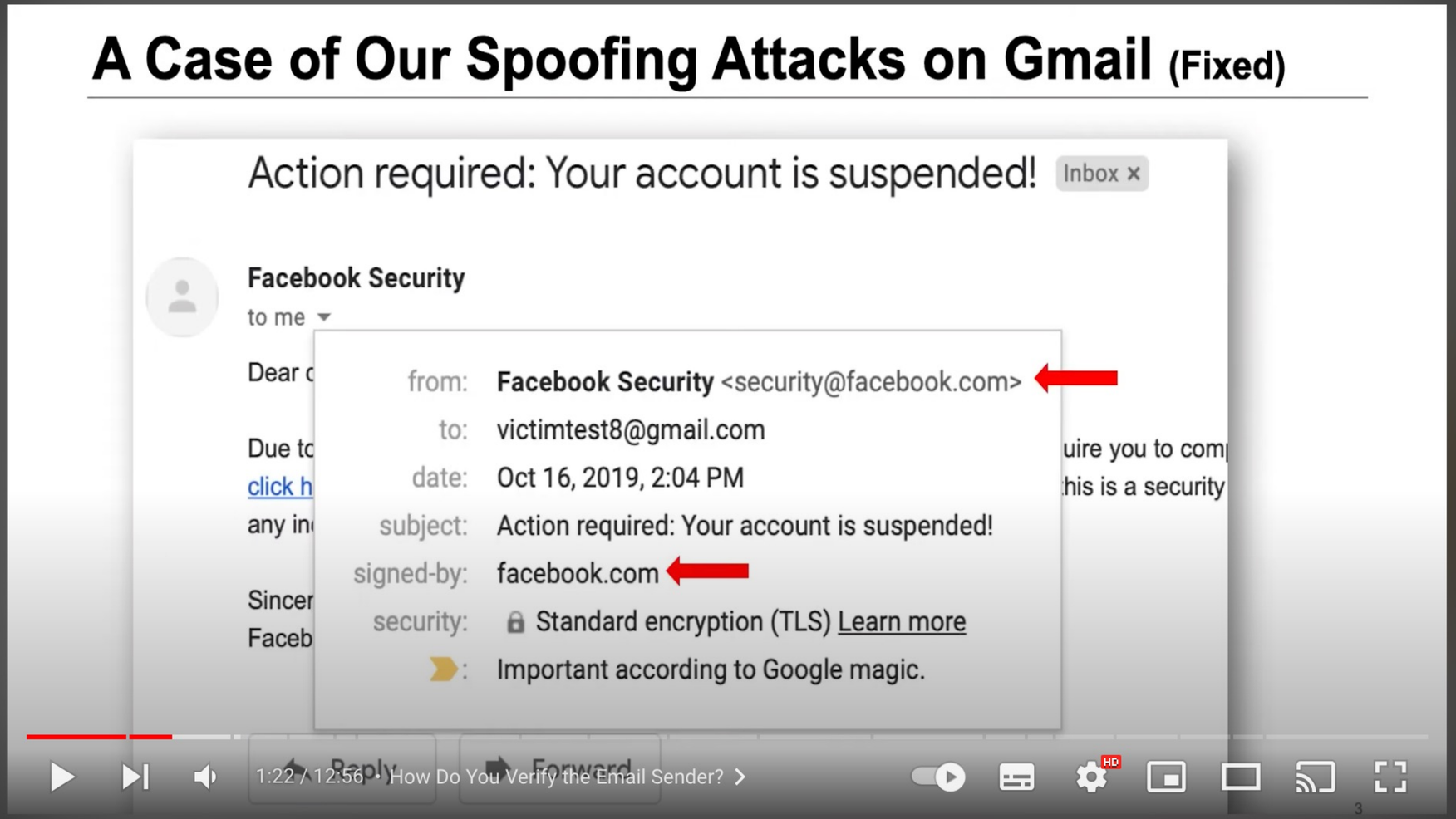
DKIM 網域相同

```
•DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=google.com; s=hacker.com.\x00.20210112;
h=to:from:subject:message-id:feedback-id:reply-
version:from:to:cc:subject:date:message-id:re
bh={hash};b={signature}
```

d=google.com



https://www.usenix.org/conference/usenixsecurity20/presentation/chen-jianjun



USENIX Security '20 - Composition Kills: A Case Study of Email Sender Authentication

USENIX
2.74萬位訂閱者
訂閱
4
分享
下載

But Fixed

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1 不存在 (notify@non-exist.gov.tw)

目標無 SPF、DKIM、DMARC 紀錄

 # 2 存在 (notify@google.com)

目標有 SPF、DKIM、DMARC 紀錄

 # 3 相似 (notify@devk0rs.lan)

目標無 SPF、DKIM、DMARC 紀錄

 # 4 相同 (notify@devkors.lan)

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1 不存在 (notify@non-exist.gov.tw)

目標無 SPF、DKIM、DMARC 紀錄

 # 2 存在 (notify@google.com)

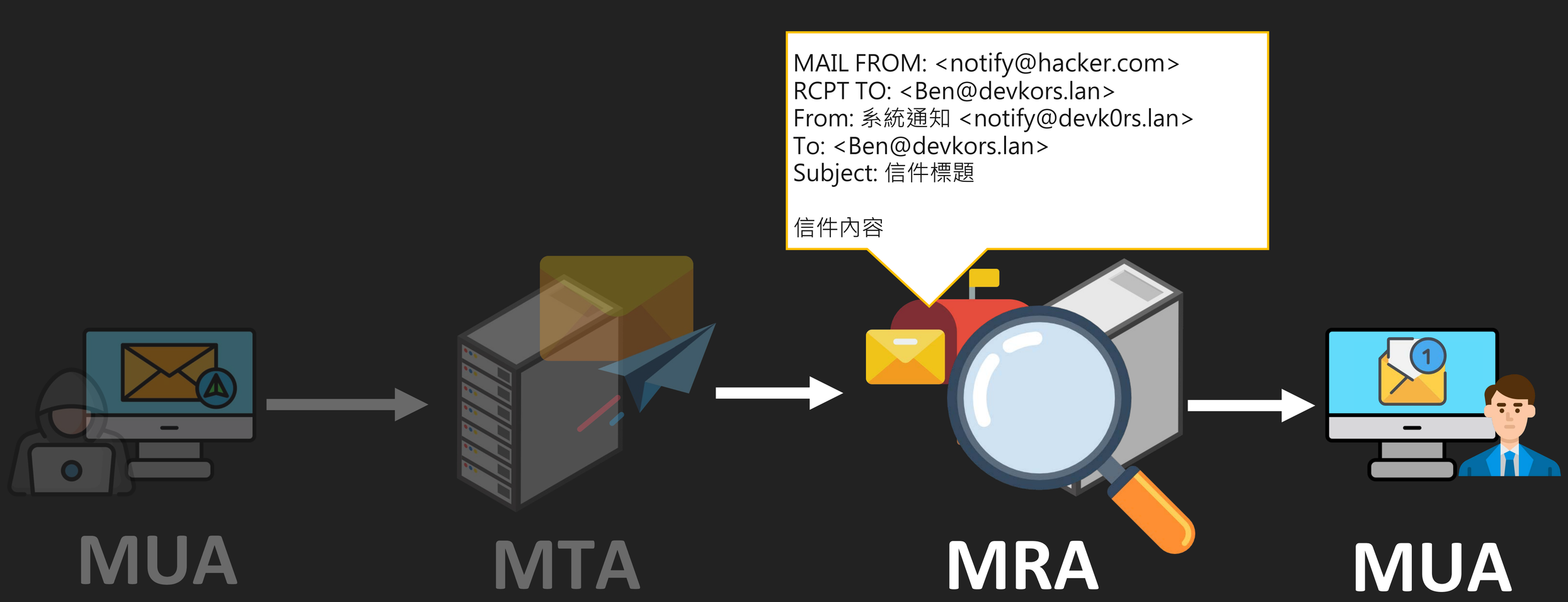
目標有 SPF、DKIM、DMARC 紀錄

 # 3 相似 (notify@devk0rs.lan)

目標無 SPF、DKIM、DMARC 紀錄

 # 4 相同 (notify@devkors.lan)

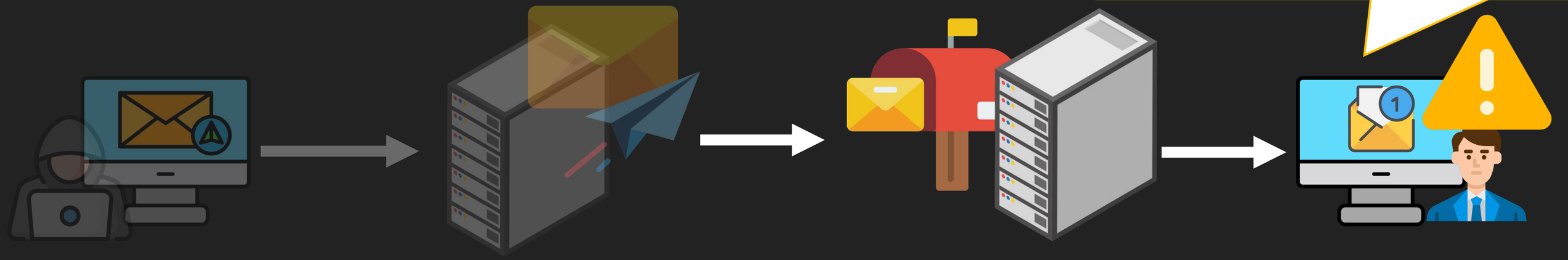
網域不存在，作法一樣



3 相似 (notify@devk0rs.lan)

MAIL FROM: <notify@hacker.com>
RCPT TO: <Ben@devkors.lan>
From: 系統通知 <notify@devk0rs.lan>
To: <Ben@devkors.lan>
Subject: 信件標題

信件內容



MUA MTA MRA MUA

3 相似 (notify@devk0rs.lan)

MUA

notify@devk0rs.lan

寄給 Ben

這封郵件似乎很危險

這位寄件者的電子郵件地址使用了不正常的字元，可能是試圖假冒實際存在的地址。請勿點選郵件中的連結、下載附件，或回覆這封郵件。

信件內容

網域評分信用分數等等...

成本高，完全不建議

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1不存在 (notify@non-exist.gov.tw)

目標無 SPF、DKIM、DMARC 紀錄

 # 2 存在(notify@google.com)

目標有 SPF、DKIM、DMARC 紀錄

 # 3 相似 (notify@devk0rs.lan)

目標無 SPF、DKIM、DMARC 紀錄

 # 4 相同 (notify@devkors.lan)

目標 ？？？ 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄

目標 有 SPF 無 DKIM 無 DMARC 紀錄

目標 無 SPF 有 DKIM 無 DMARC 紀錄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

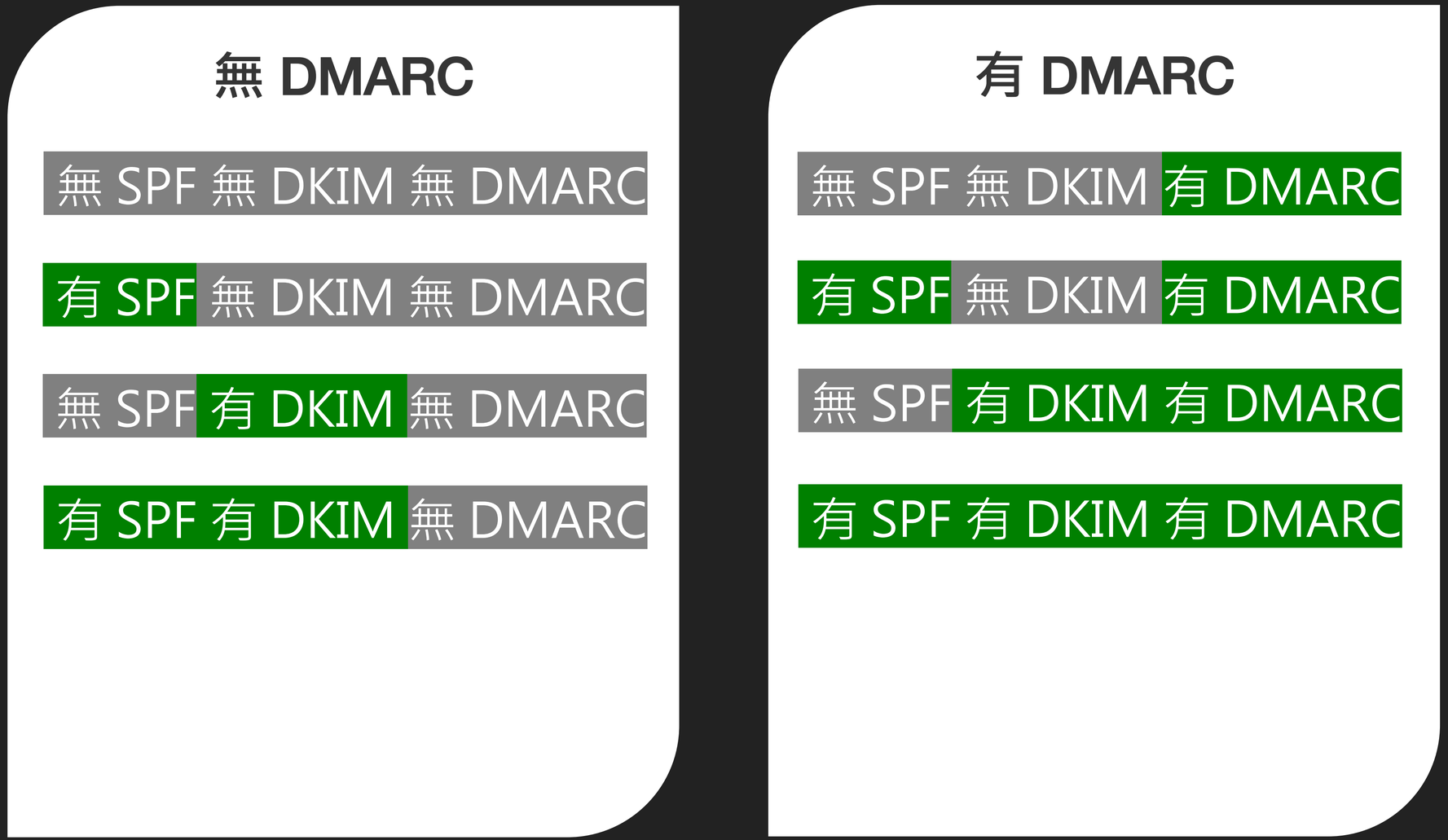
目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4 (對駭客來說)


無 DMARC
無 SPF 無 DKIM 無 DMARC
有 SPF 無 DKIM 無 DMARC
無 SPF 有 DKIM 無 DMARC
有 SPF 有 DKIM 無 DMARC
有 DMARC
無 SPF 無 DKIM 有 DMARC
有 SPF 無 DKIM 有 DMARC
無 SPF 有 DKIM 有 DMARC
有 SPF 有 DKIM 有 DMARC

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄

目標 有 SPF 無 DKIM 無 DMARC 紀錄

目標 無 SPF 有 DKIM 無 DMARC 紀錄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄

目標 無 SPF 有 DKIM 無 DMARC 紀錄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

駭客可以自己改 MAIL FROM 網域通過 SPF

但 Gmail 會嘗試保護你！

MUA 會嘗試保護你

MUA 

(來信的網域，只設 SPF 沒設 DMARC)

信件標題 收件匣 × 公司內部 ×

notify@devkors.lan 透過 hacker.com
寄給 Ben

請謹慎處理這封郵件

寄件者並未驗證這封郵件，因此「DEVKORS 郵件」無法確認郵件是否確實由對方寄出。請勿點選郵件中的連結、下載附件，或在回覆郵件時提供個人資訊。

回報為垃圾郵件　看起來沒有問題

信件內容

但釣魚信，其實就不該點？

哎呀 哪那麼多 0 day，有種針對我！
我已經可以獨當一面，面對釣魚網站了

醋！

第一次駭客偽造寄過來

MUA

MUA 會嘗試保護你 (來信的網域，只設 SPF 沒設 DMARC)

第 N 次駭客偽造寄過來 (點開數次，沒人回報)

MUA

第 N 次駭客偽造寄過來 (點開數次，沒人回報)

MUA

難怪學校老師會說不要點開釣魚信件

不開哪知道，薛丁格釣魚信?

不開哪知道，薛丁格釣魚信?

記得 回報為垃圾郵件 就好

攻擊思路：
拿下企業其中一個信箱帳號
一直狂點釣魚信

攻擊思路 2：用那個殺招！

透過郵寄清單轉發 (Remailing) 殺招

駭客 -> 相同 (notify@devkors.lan)

員工群組 (staff@devkors.lan)

員工 (Ben@devkors.lan)
員工 (Cody@devkors.lan)
員工 (David@devkors.lan)

透過郵寄清單轉發 (Remailing) 殺招

給 Google 轉發一次，有如神靈護體

透過郵寄清單轉發 (Remailing) 殺招

給 Google 轉發一次，有如神靈護體

I WANNA KNOW 你信不信

內部演練畫面
僅公布於研討會

甚至還可以

透過郵寄清單轉發 (Remailing) 殺招

駭客 -> Ben (Ben@devkors.lan)

員工群組 (staff@devkors.lan)

員工 (Ben@devkors.lan)
員工 (Cody@devkors.lan)
員工 (David@devkors.lan)

透過郵寄清單轉發 (Remailing) 殺招

信件標題 收件匣 × 公司內部 ×

Ben <ben@devkors.lan>

寄給 staff

信件內容

回覆 回覆所有人 轉寄

透過郵寄清單轉發 (Remailing) 殺招

信件標題 收件匣 × 公司內部 ×

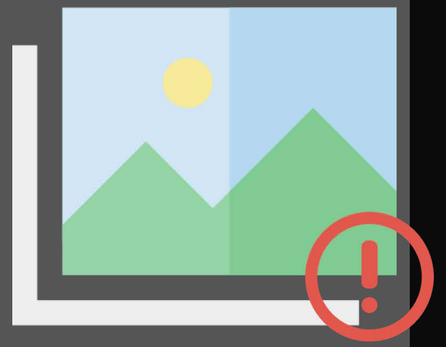
Ben <ben@devkors.lan>

寄給 staff

信件內容

回覆 回覆所有 轉寄

I WANNA KNOW 你信不信



內部演練畫面
僅公布於研討會

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

主動：查驗 SPF

主動：查驗 DMARC

被動：信裡面有 DKIM 才查驗

MRA

DEVCORE SECURITY CONSULTING

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄 => 根本沒人收的到 they 的信

目標 有 SPF 無 DKIM 有 DMARC 紀錄

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄 => 根本沒人收的到 they 的信

目標 有 SPF 無 DKIM 有 DMARC 紀錄 => 難偽造，除非特殊攻擊案例

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

安全機制

SPF 驗證寄信來源 IP – 方法

dig txt devkors.lan

“v=spf1 ip4:203.0.113.13 ~all”

PASS 203.0.113.13 (MTA)

DEVCORE

安全機制

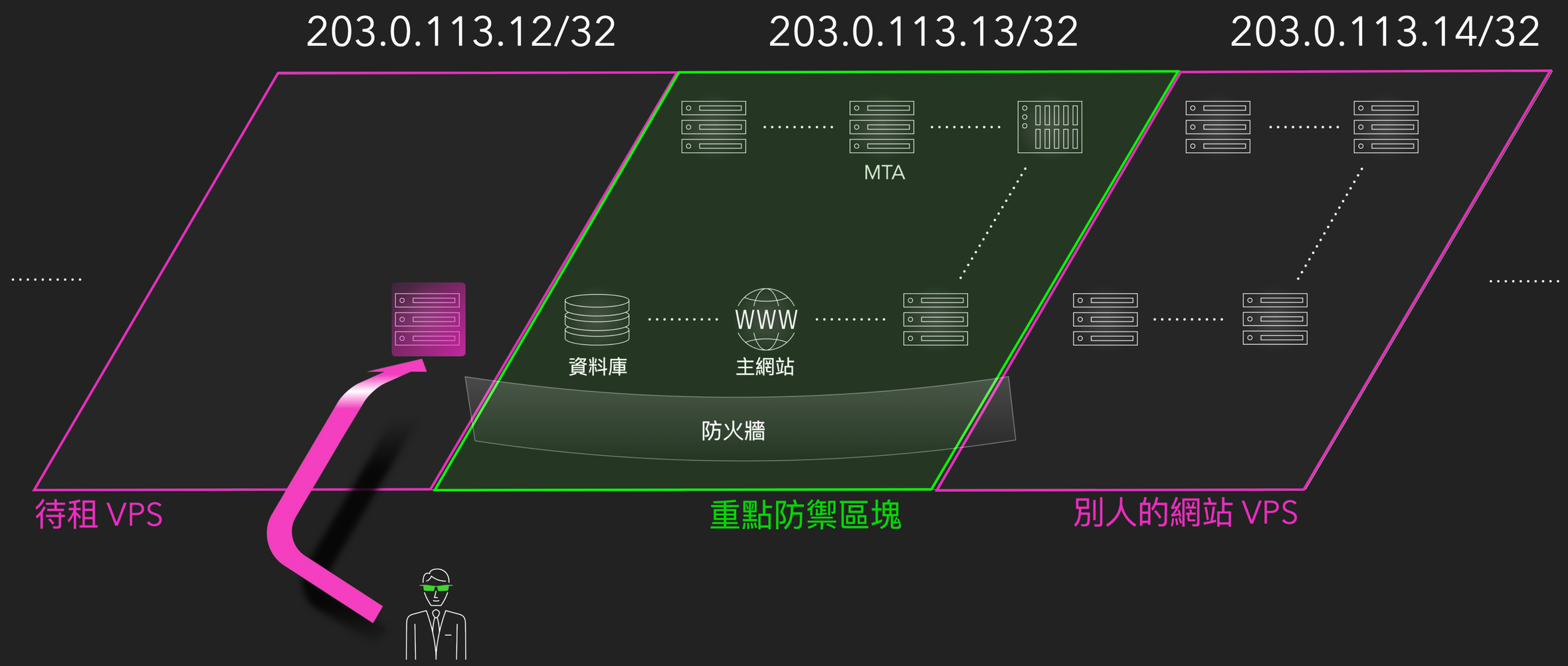
SPF 驗證寄信來源 IP – Misconfiguration

dig txt devkors.lan

“v=spf1 ip4:203.0.113.13/24 ~all”

PASS 203.0.113.13/24 (MTA)

VPS 網站託管商 (203.0.113.0/24)



安全機制

SPF 驗證寄信來源 IP – Misconfiguration

dig txt devkors.lan

“v=spf1 ip4:203.0.113.13/24 ~all”

PASS 203.0.113.12 (MTA)

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄 => 根本沒人收的到 they 的信

目標 有 SPF 無 DKIM 有 DMARC 紀錄 => 特殊攻擊案例 (Misconfiguration)

目標 無 SPF 有 DKIM 有 DMARC 紀錄

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄 => 根本沒人收的到 they 的信

目標 有 SPF 無 DKIM 有 DMARC 紀錄 => 特殊攻擊案例 (Misconfiguration)

目標 無 SPF 有 DKIM 有 DMARC 紀錄 => 只能把私鑰打下來 (超出命題範圍)

目標 有 SPF 有 DKIM 有 DMARC 紀錄

攻擊情境 #4

目標 無 SPF 無 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 無 DKIM 無 DMARC 紀錄 => 進入攻擊技巧

目標 無 SPF 有 DKIM 無 DMARC 紀錄 => 隨便你寄

目標 有 SPF 有 DKIM 無 DMARC 紀錄 => DKIM 可無視，同只有 SPF

目標 無 SPF 無 DKIM 有 DMARC 紀錄 => 根本沒人收的到 they 的信

目標 有 SPF 無 DKIM 有 DMARC 紀錄 => 特殊攻擊案例 (Misconfiguration)

目標 無 SPF 有 DKIM 有 DMARC 紀錄 => 只能把私鑰打下來 (超出命題範圍)

目標 有 SPF 有 DKIM 有 DMARC 紀錄 => 駭客覺得你是討厭鬼

攻擊情境 #4 (對駭客來說)

無 DMARC

無 SPF 無 DKIM 無 DMARC

有 SPF 無 DKIM 無 DMARC

無 SPF 有 DKIM 無 DMARC

有 SPF 有 DKIM 無 DMARC

有戲

有 DMARC

無 SPF 無 DKIM 有 DMARC

有 SPF 無 DKIM 有 DMARC

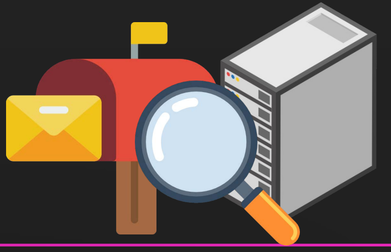
無 SPF 有 DKIM 有 DMARC

有 SPF 有 DKIM 有 DMARC

很難有戲

Policy = reject

安全機制

MRA 

DMARC 保護機制 – 方法

dig txt _dmarc.TARGET.COM

domain 能不能被偽造，看這就好

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1 不存在 (notify@non-exist.gov.tw)

目標無 SPF、DKIM、DMARC 紀錄

 # 2 存在(notify@google.com)

目標有 SPF、DKIM、DMARC 紀錄

 # 3 相似 (notify@devk0rs.lan)

目標無 SPF、DKIM、DMARC 紀錄

 # 4 相同 (notify@devkors.lan)

目標 ？？？ 紀錄

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

1　不存在

notify@non-exist.gov.tw

2　存在

notify@google.com

3　相似

notify@devk0rs.lan

4　相同

notify@devkors.lan

攻擊情境 #1 ~ #4 (駭客偽造哪個，最不被阻擋？)

 # 1　不存在

notify@non-exist.gov.tw

 # 2　存在

notify@google.com

 # 3　相似

notify@devk0rs.lan

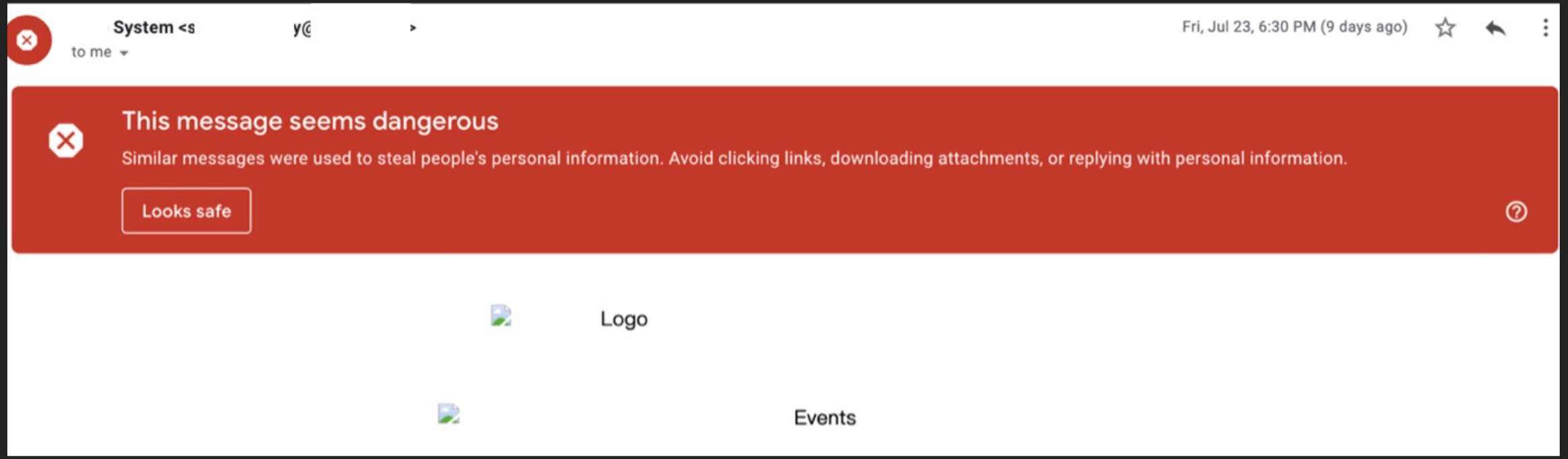
 # 4　相同

notify@devkors.lan

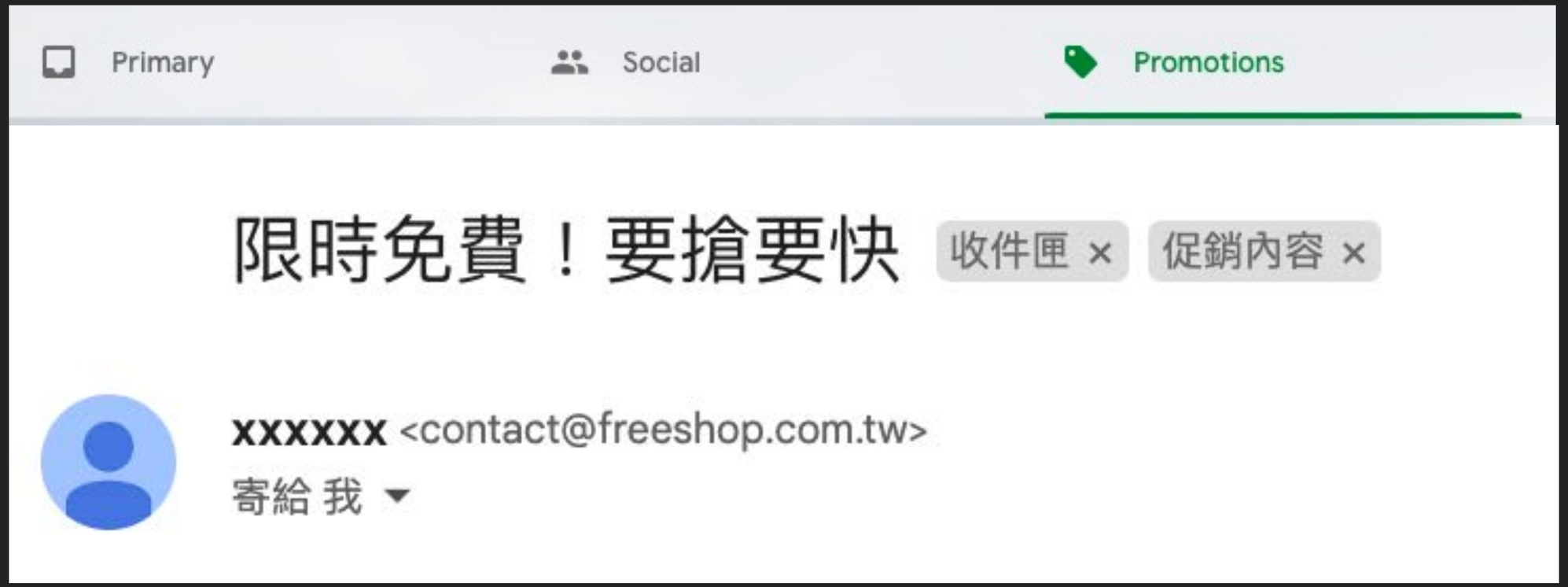
DEVCORE SECURITY CONSULTING

提升信件評分/ 垃圾信?

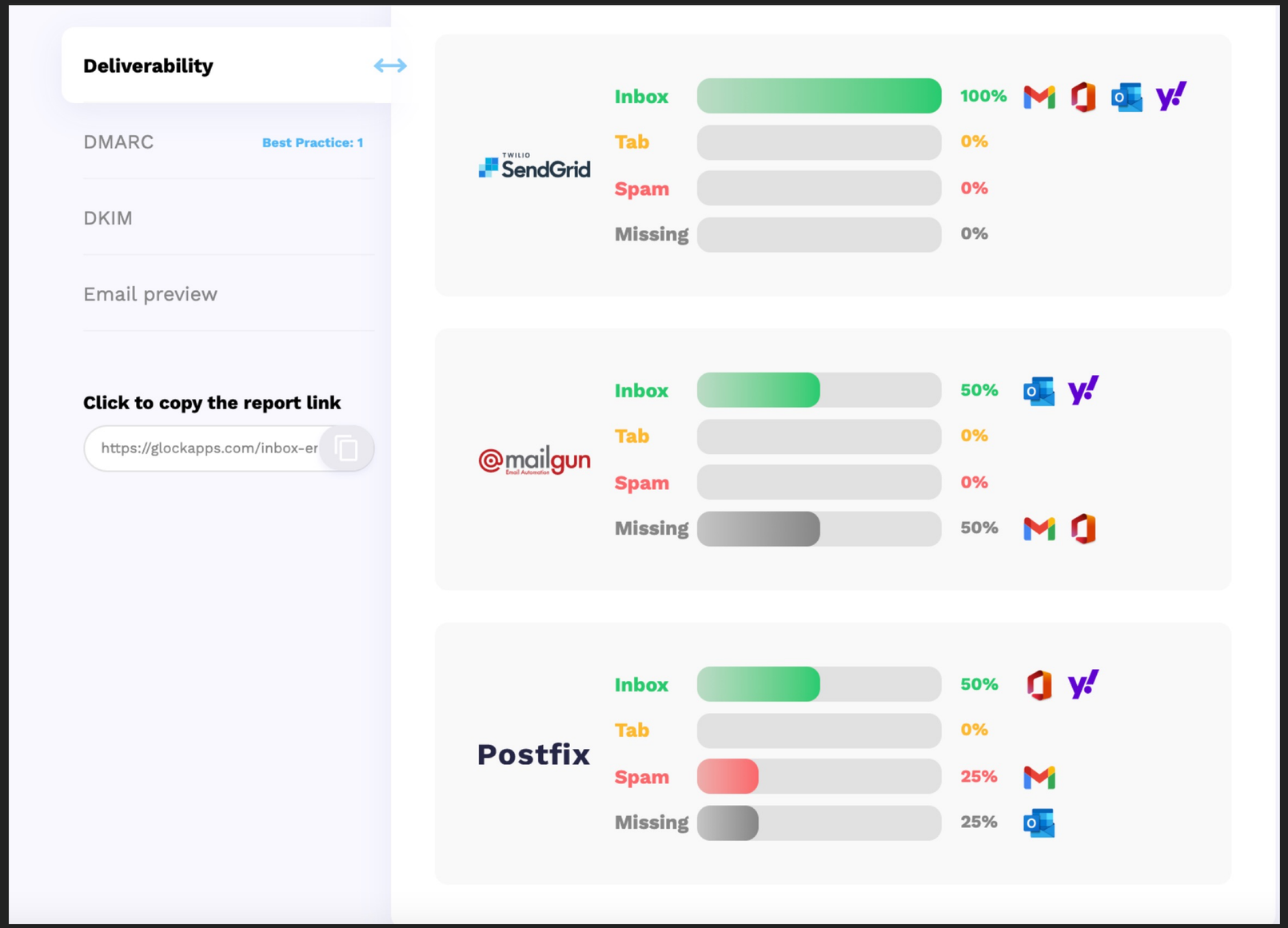
駭客最害怕的事情


System <s y@ >
to me
Fri, Jul 23, 6:30 PM (9 days ago)
This message seems dangerous
Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.
Looks safe
Logo
Events

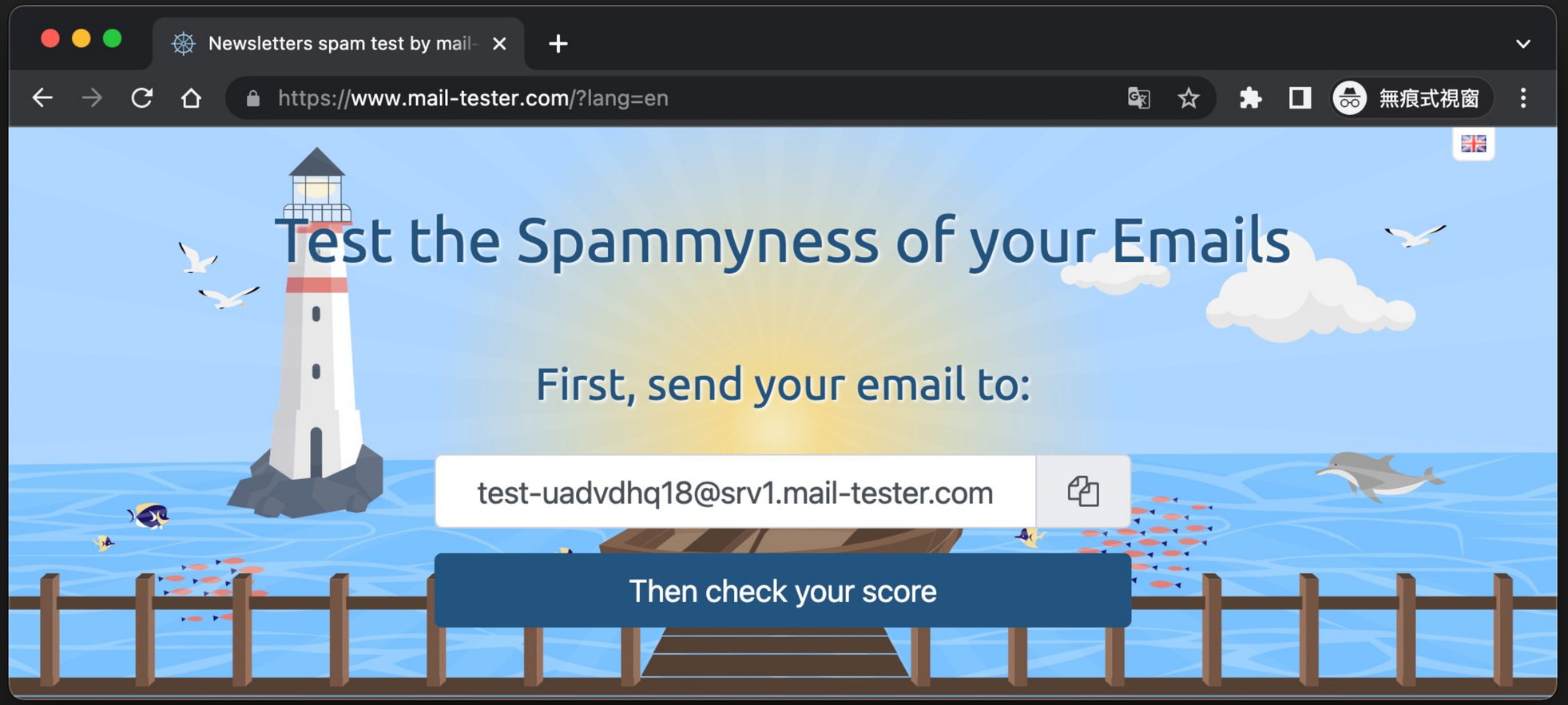
垃圾/促銷郵件觸發詞


Primary
Social
Promotions
限時免費！要搶要快
收件匣 ×
促銷內容 ×
xxxxxx <contact@freeshop.com.tw>
寄給 我

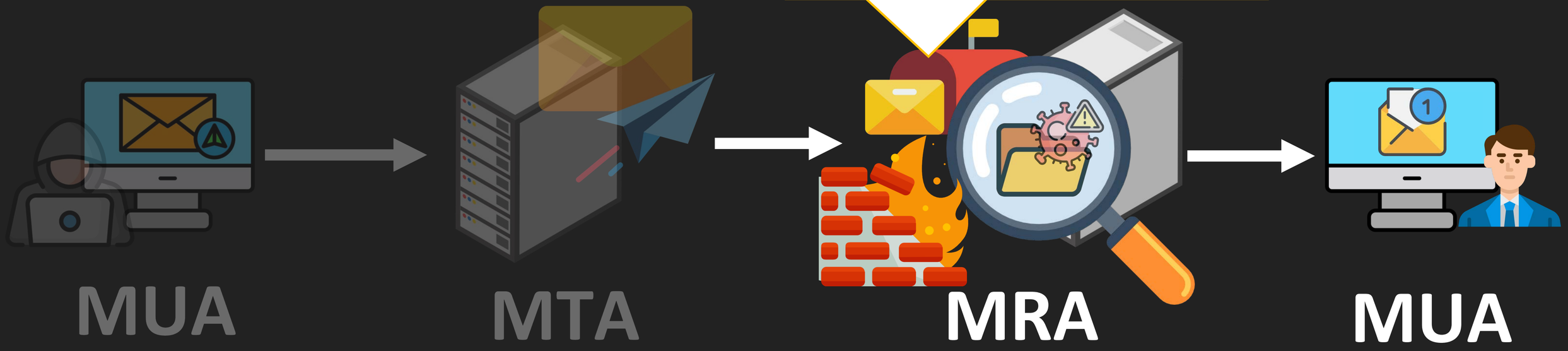
垃圾郵件抵達測試服務 (glockapps.com)



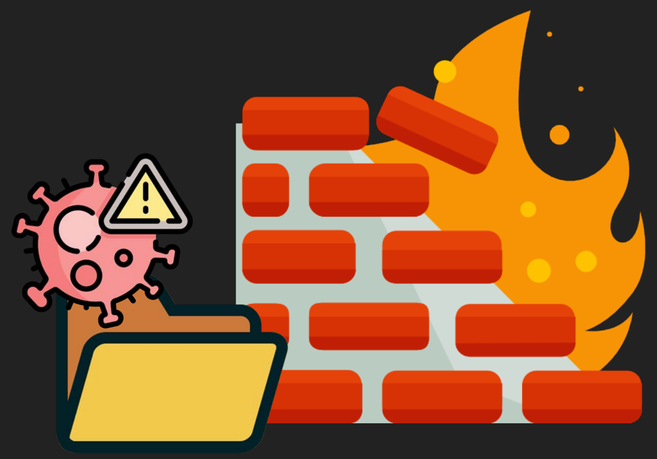
信件評分及修改建議服務 (www.mail-tester.com)



檢查信件夾檔
連結檔案安全性

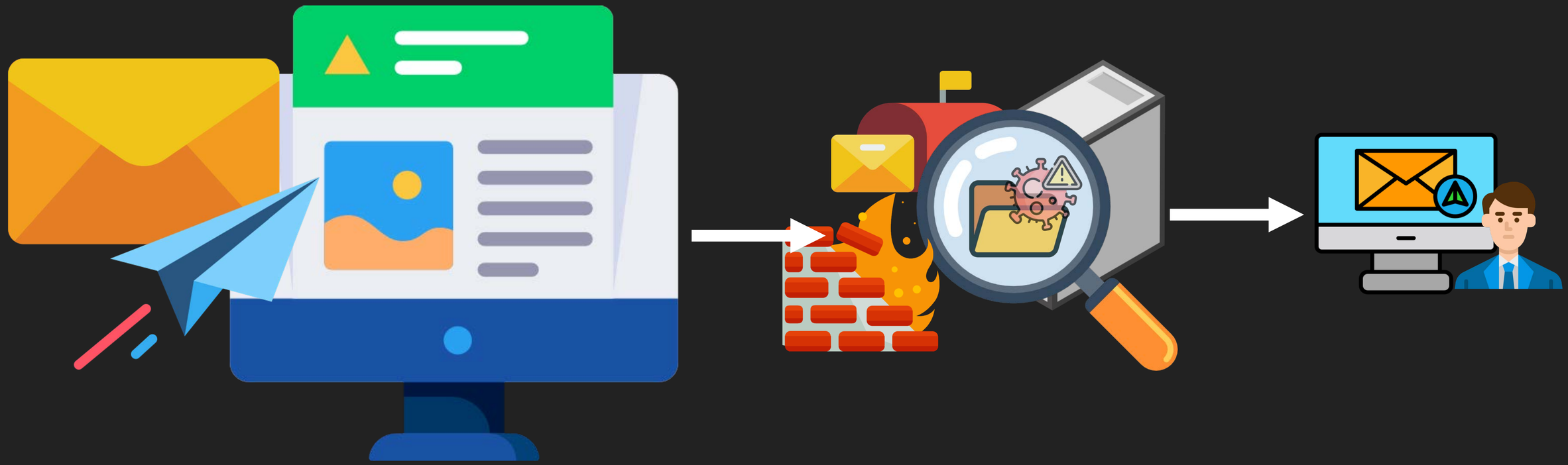


MUA MTA MRA MUA



繞郵件夾檔防火牆

URL LINK

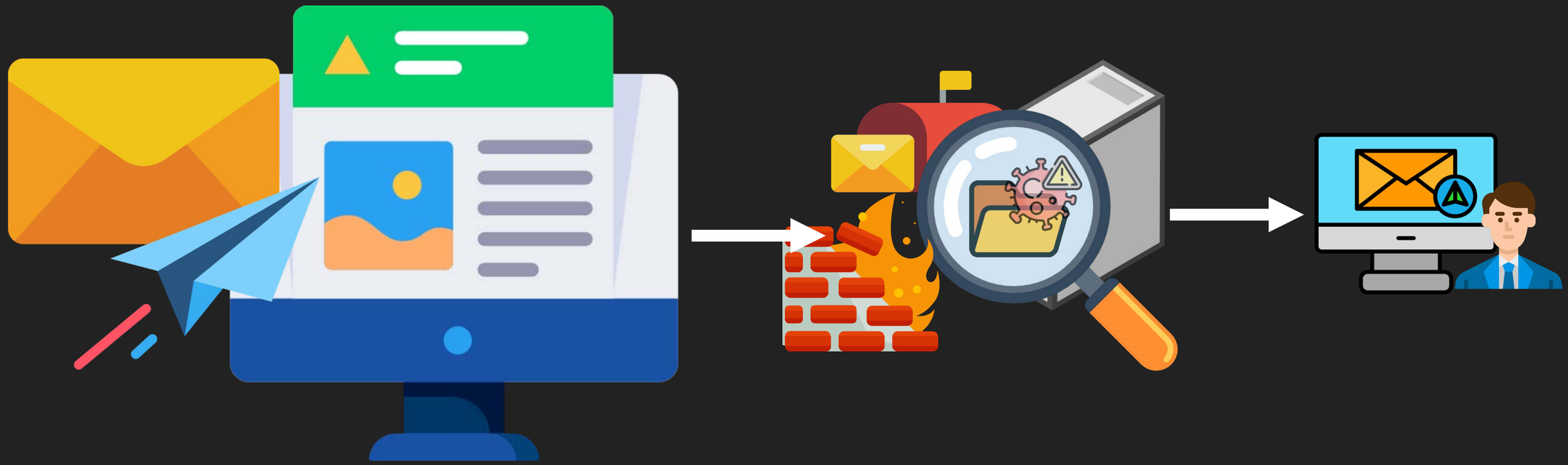


Content-Disposition:
form-data; name="fieldName"; filename="evil.exe"

URL LINK

Content-Disposition:
form-data; name="fieldName"; filename="evil.exe"

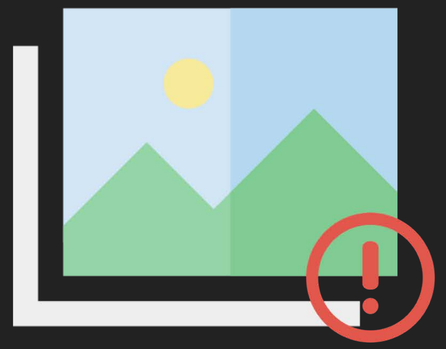
URL LINK



File in the HTML?

DEVCORE SECURITY CONSULTING

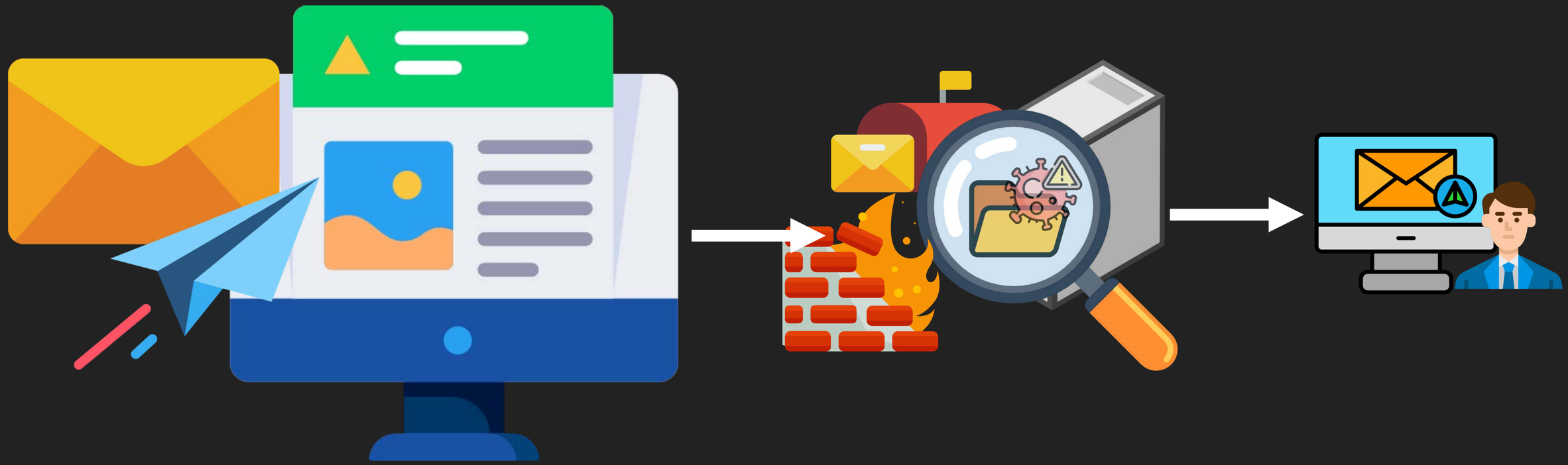
1.檔案 in the script (blob)：



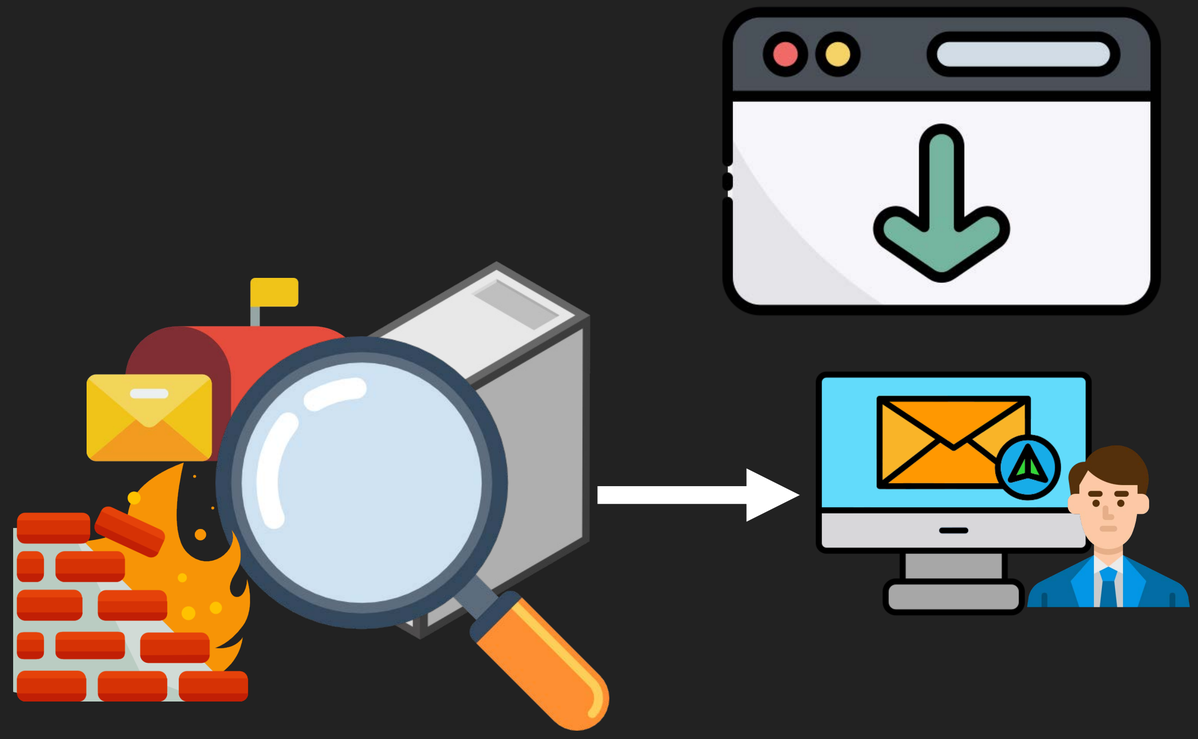
2.觸發瀏覽器下載：

內部演練畫面
僅公布於研討會

URL LINK



組成檔案、另存新檔



給白帽駭客的建議

核心問題，詐術

心理學名詞

蔡加尼效應

暈輪效應

認知失調

登門檻效應

自證控制

DMARC 設置普及率？

From: domain
其實不要太爛都還好

例如： xxxuyaxyx.xyz V.S autoalert-service.com

別用 Gmail 寄釣魚信

準備好了嗎

DEVCORE
SECURITY
CONSULTING

You gonna know
別懷疑你自己的本領

Thank

特別鳴謝

Linwz
Crystal