TeleTrusT-EBCA "PKI-Workshop" 2021

Berlin, 30.09.2021

Streitgespräch: BIMI als Werkzeug zur Absenderverifizierung in E-Mails, Fluch oder Segen?

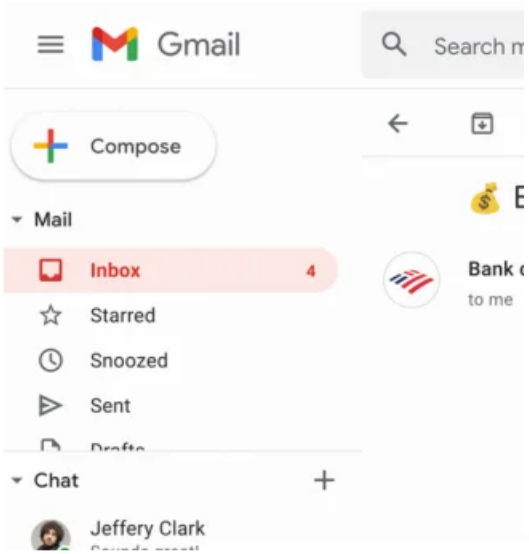
Stefan Cink, Net at Work
Sören Beiler, Net at Work

BIMI

Mit bunten Logos gegens Phishing: Gmail erhält BIMI

Gmail-Nutzer könnten künftig mehr Logos v
dieser sollen sie Phishing-Versuche direkt e

Lesezeit: 1 Min. In Pocket speichern



BIMI

Google will E-Mails mit Firmenlogos absichern

Nutzen Unternehmen bestimmte Sicherheitstechniken wie DMARC in E-Mails, zeigt Google in Gmail nun deren Logos an. Das soll Spoofing vorbeugen.

in Pocket speichern merken

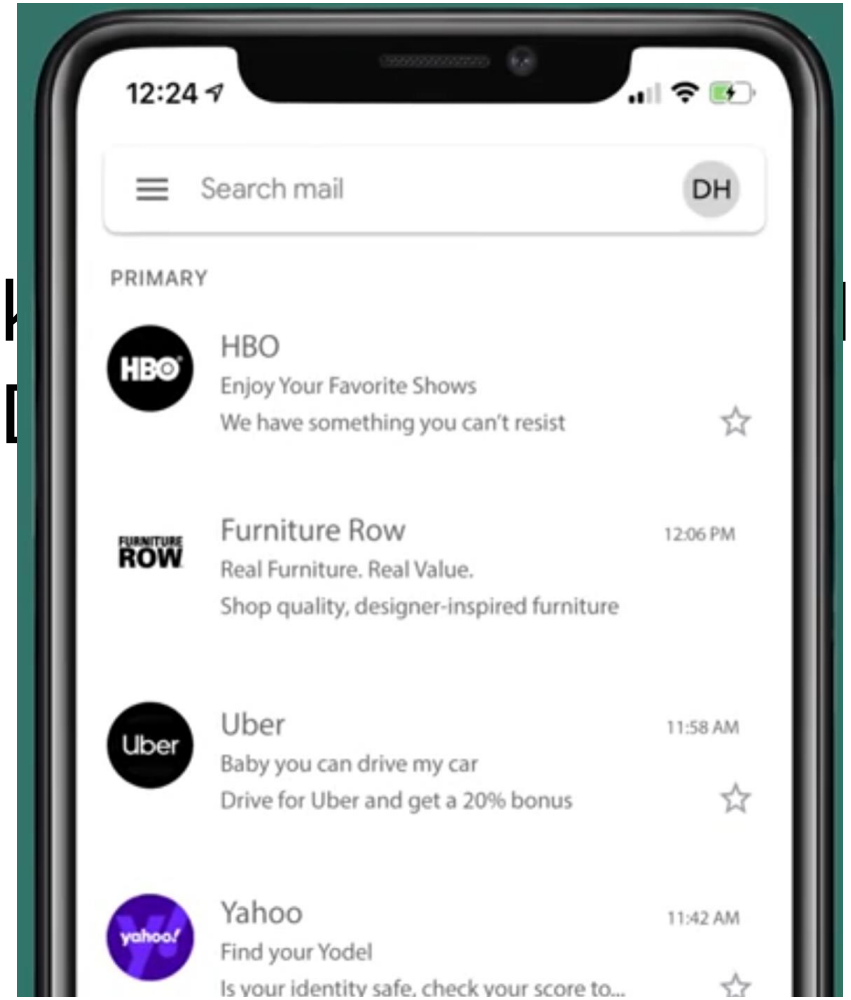
13. Juli 2021, 10:23 Uhr, Sebastian Grüner

Googles Gmail soll mit BIMI besser vor E-Mail-Spoofing schützen.

Google hat für seinen E-Mail-Dienst Gmail begonnen, den bisher noch nicht sehr weit verbreiteten Industriestandard Brand Indicators for Message Identification (BIMI) zu verteilen. Das kündigt das Unternehmen in seinem Cloud-Blog an. Wie der Name der Technik bereits andeutet, ist das Ziel, ein Unternehmenslogo für E-Mails anzuzeigen, was Phishing zumindest vorbeugen können soll, hofft das Unternehmen.

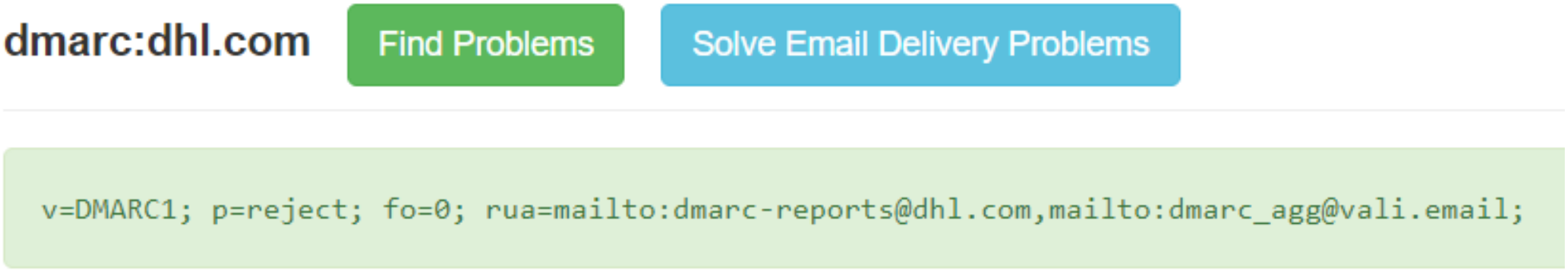
Was ist BIMI?

Anzeige eines Mark ail im E-Mail Client nach erfolgreicher



Anzeigen des Logo nur nach Sicherheitsprüfung

Schritt 1: Prüfung der DMARC Richtlinie des Domaininhabers am Beispiel von dhl.com



SPF Überprüfung

Schritt 2: Um DMARC prüfen zu können, müssen wir zuvor SPF von dhl.com validieren

spf:dpdhl._spf.dhl.com Find Problems Solve Email Delivery Problems

```
v=spf1 ip4:165.72.200.0/24 ip4:199.40.206.0/26 ip4:68.232.128.0/19 ip4:149.239.170.0/24 ip4:149.239.48.15 ip4:149.239.48.16 ip4:194.1.155.240
```

DKIM Überprüfung

Schritt 3: Um DMARC prüfen zu können, müssen wir ebenfalls DKIM von dhl.com validieren

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=dhl.com; l=214528; s=20140901; t=1631116831; h=date:from:to:message-id:subject:mime-version; bh=unE17ABNco2vES0+yQEJceU2bSIMnC5P7LjM6WwnD5w=;
b=EXe4IC+gaDKJxLZjMZUhb9e1sZ1Wxv4HBLR7i6/Qiiho6v1X8S525Tca  HTAqLb/BMTDH0Uj2EE1uV9OqZtUTf8fxF8LJk6eB2KKlF7wk5qvgj9ZvR  72u+ujHSeVsRFt7vVbxmmi6/RG9f5s+mXG1JUVha8DhhB05E/OsyiZfwZ
J5Z6tlfolKBLPfqQJ9P8xqvG4zJLjRI6SRWDkosUVEKQj1VC35mv0vodZ  LsAqKIi4vqjfLKgtgLwoqARW+cNfa4JO28dD3+Y1N8VyXCLrg6l5izoUS  jBj7gTq7SJmMphaVdKivTpUTWlxm+GMAEIjKDyGz6QxzlMwCneqM2jyEF  Q==;
```

dkim:dhl.com:20140901 Find Problems

dkim

```
v=DKIM1; t=s; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmasBmSPmXTRlDbfImRlAmSh1PmNcgfY/pVwjCAAyzO0h8S9nYv6Go1gYh+mZCwn1ropKzeibammK3yO8js1K21HenUnM2dClQ+VBI+K
lRmiYv/hVfJeKLO7zQZ7DAchUgt5XDyJfsFpnsE1MOjOTX41oHuARyOZ/d+AbICLLDGLmigzLTeivBFNusdYytUatV5dBj2UIU6CV+un+C+ZfCVtCeDtasvVqhozdJLvnnnFCb4B5l0dCVzvuJ16tT60ChiakWx/3tT
phzSkNXwHWzaWg6oC14zr0P8QTvIulrrfu0Wp7BrbVDLCjLO7xUU7X22g4GiEsh5lX9SlbCN5e+wIDAQAB;
```

DMARC erfolgreich bestanden

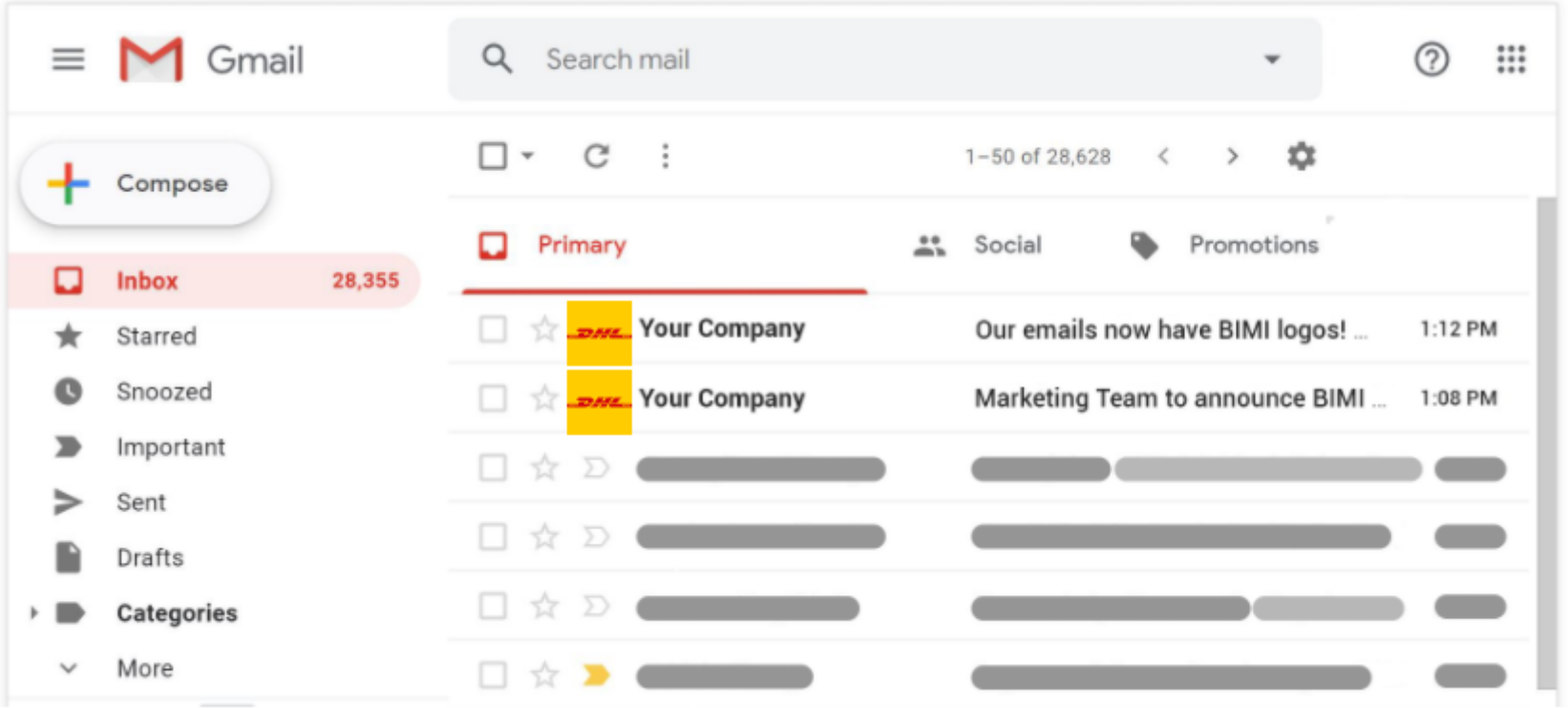
Schritt 4: DMARC ist bestanden, da SPF und / oder DKIM bestanden wurden

Schritt 5: Auflösung des BIMI Records im DNS

```
v=BIMI1;l=https://www.dhl.com/dhl-email-logo/dpdhl_bimi.svg
```

Tag	TagValue	Name	Description
v	BIMI1	Version	Identifies the record retrieved as a BIMI record. It must be the first tag in the record.
l	https://www.dhl.com/dhl-email-logo/dpdhl_bimi.svg	Locations	Comma separated list of base URLs representing the location of the brand indicator files.

Schritt 6: der E-Mail Client zeigt das Logo an



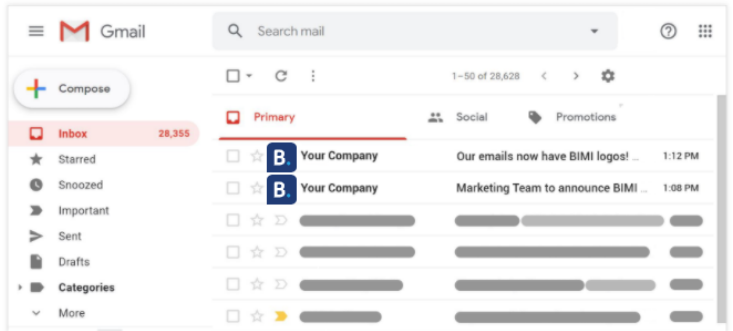
In die Diskussion

BIMI missbraucht

Was h en?

netshare.me BIMI Lookup

bimi:netshare.me Solve Email Delivery Problems bimi



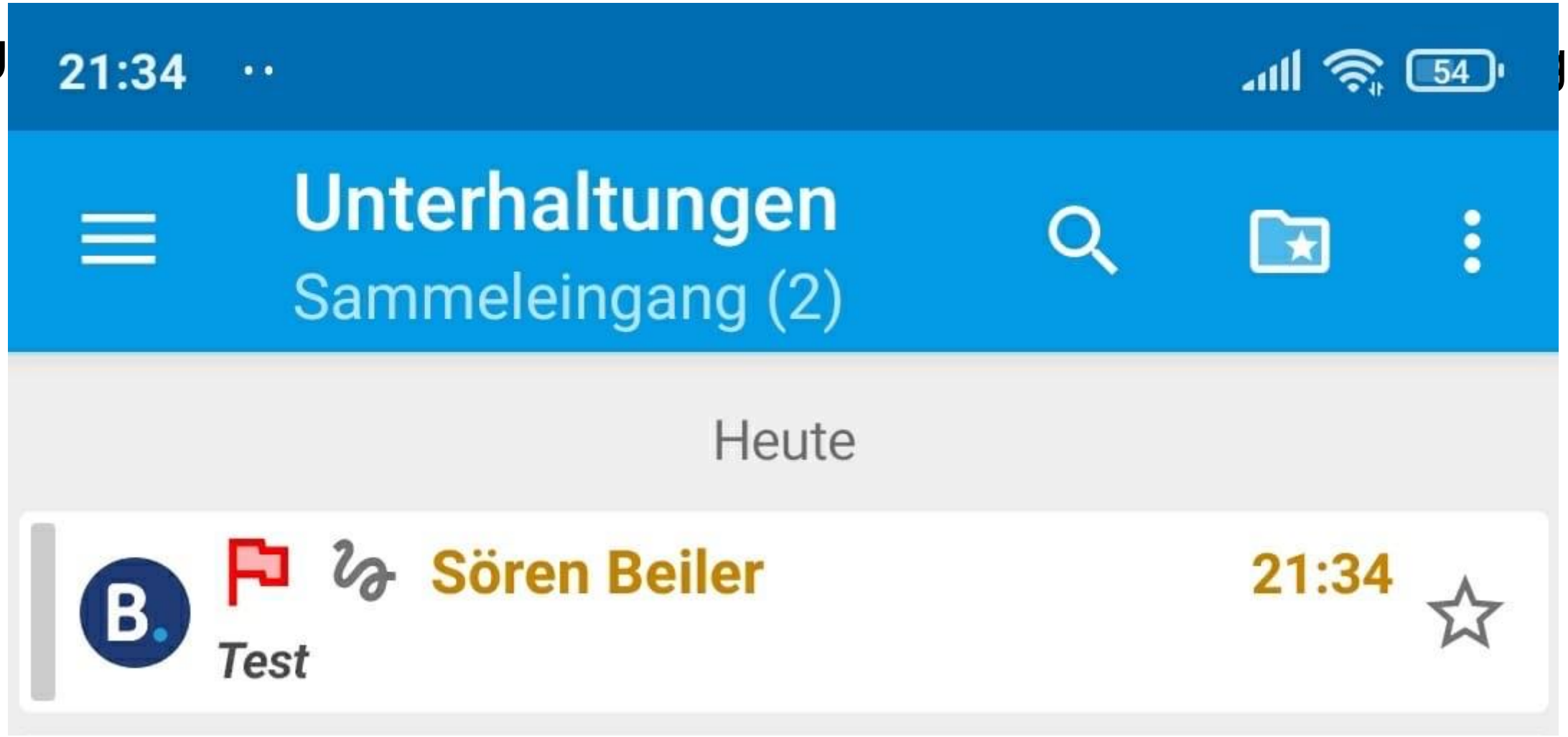
v=BIMI1; l=https://r.bstatic.com/static/img/newsletters/booking_bimi_icon_300.svg; a=https://r-xx.bstatic.com/data/mm/booking_com_202107.pem;

Tag	TagValue	Name	Description
v	BIMI1	Version	Identifies the record retrieved as a BIMI record. It must be the first tag in the record.
l	https://r.bstatic.com/static/img/newsletters/booking_bimi_icon_300.svg	Locations	Comma separated list of base URLs representing the location of the brand indicator files.
a	https://r-xx.bstatic.com/data/mm/booking_com_202107.pem	Trust Authorities	Optional Validation Information for verifying bimi locations.

	Test	Result
✓	BIMI Record Published	BIMI Record found
✓	BIMI Syntax Check	The Record is Valid
✓	BIMI Image Format	BIMI Image Format Correct
✓	BIMI Logo Validation	BIMI Logo Validation Valid
✓	DMARC Record Published BIMI Required	DMARC Record found - Valid for BIMI
✓	DMARC Policy Not Enabled BIMI Required	DMARC Quarantine/Reject policy enabled - Valid for BIMI

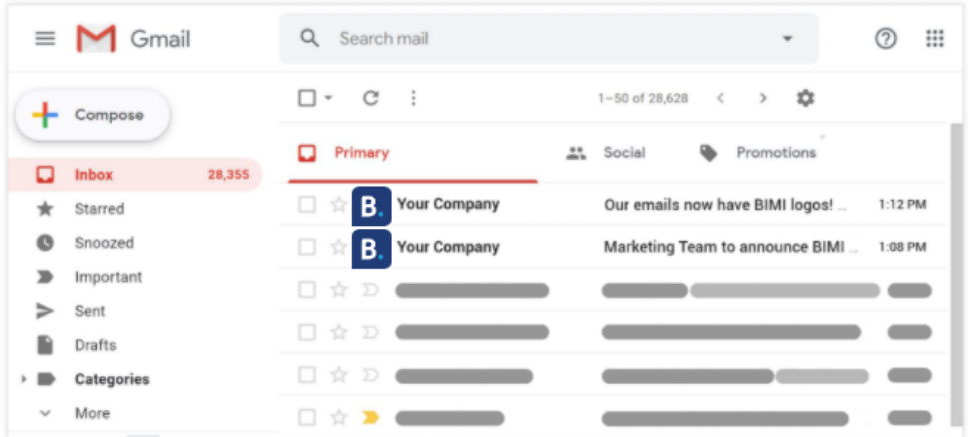
BIMI missbraucht

U



BIMI missbraucht

Kann man das denn nicht verhindern? Wie wäre es wenn wir da einfach noch eine Lage PKI drüber packen?!1!!




```
v=BIMI1; l=https://r.bstatic.com/static/img/newsletters/booking_bimi_icon_300.svg; a=https://r-xx.bstatic.com/data/mm/booking_com_202107.pem;
```

BIMI und die technischen Schwächen

1. Ein signiertes SVG ist nicht vorgeschrieben
2. Selbst wenn es vorhanden ist, muss es nicht zwingend überprüft werden
3. „Entwenden“ eines signierten Bildes kann nicht zu 100% vermieden werden