Jakub Bouček

E-maily technicky

aby vaše zprávy došly do cíle

Plzeňský Barcamp 16. 4. 2016
https://goo.gl/RCx0nR


Jakub Bouček

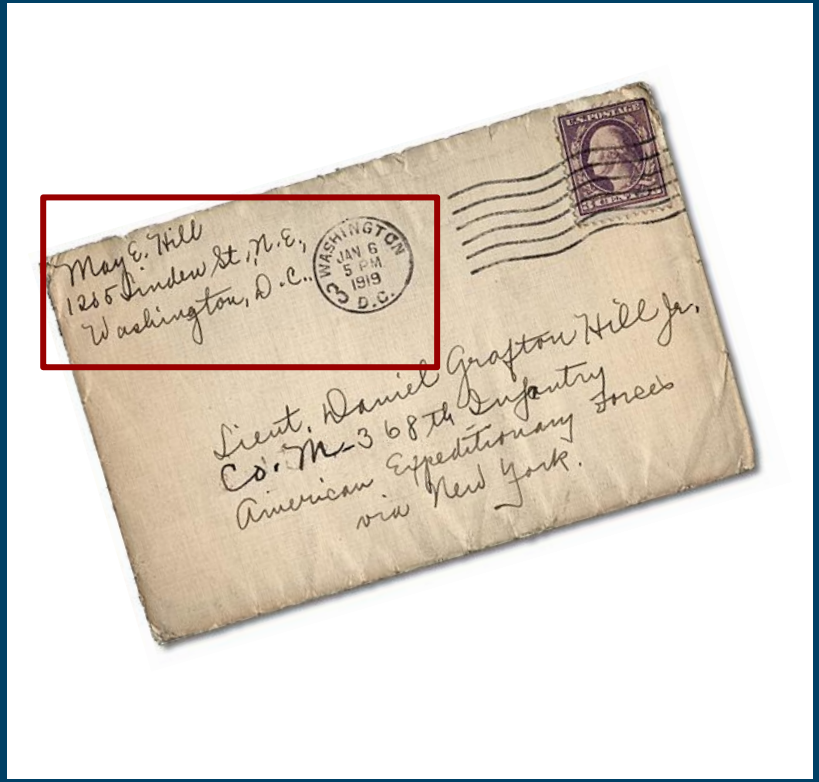
SPAM

Obálka

Analogie

Obálka

Analogie



SPF

Sender Policy Framework

SPF záznam

```
v=spf1 a ~all

v=spf1 ip4:31.31.79.103 ip4:12.34.56.78 ~all

v=spf1 include:_spf.google.com ~all

v=spf1 include:_spf.google.com -all

v=spf1 -all
```

Google → “Google Apps SPF” / “Office 365 SPF” / …

SPF – cesta mailu

```
6         Wed, 30 Mar 2016 06:06:02 -0700 (PDT)
7  Received: from mail-wm0-x236.google.com (mail-wm0-x236.google.com. [2a00:1450:400c:c09::236])
8         by mx.google.com with ESMTPS id ys8si892467wjc.210.2016.03.30.06.06.01
9         for <pan@jakubboucek.cz>
10        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
11        Wed, 30 Mar 2016 06:06:01 -0700 (PDT)
12 Received: by mail-wm0-x236.google.com with SMTP id 20so70363758wmh.1
13        for <pan@jakubboucek.cz>; Wed, 30 Mar 2016 06:06:01 -0700 (PDT)
14 X-Received: by 10.28.224.212 with SMTP id x203mr24025897wmg.75.1459343161599;
15        Wed, 30 Mar 2016 06:06:01 -0700 (PDT)
16 Received: from Koldas-MacBook-Air-3.local ([194.213.48.4])
17        by smtp.googlemail.com with ESMTPSA id s66sm19798026wmb.6.2016.03.30.06.06.00
18        (version=TLSv1/SSLv3 cipher=OTHER);
19        Wed, 30 Mar 2016 06:06:00 -0700 (PDT)
20 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:38.0)
```

SPF

- **Vymezuje** seznam firem (serverů), které mohou vaším jménem posílat e-maily
- **Brání** zneužívání dobrého jména spamy
- **Nezaručuje** autenticitu skutečného odesílatele

Zkuste si to:

www.emkei.cz

DKIM

DomainKeys Identified Mail

DKIM

```
google._domainkey.kolarik.cz. 1799 IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCOxui+SY48G2/09fJ5…"
```

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=kolarik.cz; s=google;
  h=subject:to:references:cc:from:message-id:date:user-agent
   :mime-version:in-reply-to;
  bh=GZx10t0tR7R3k9tNVwu5XPsH2qA+hbtsZCytv6Uys2I=;
  b=0HeROz9rkxRAgRIR2SoiPI4u3wluYLJwEPe4NXSrhtO3BwIFuij9lkbwPaLiq…
```

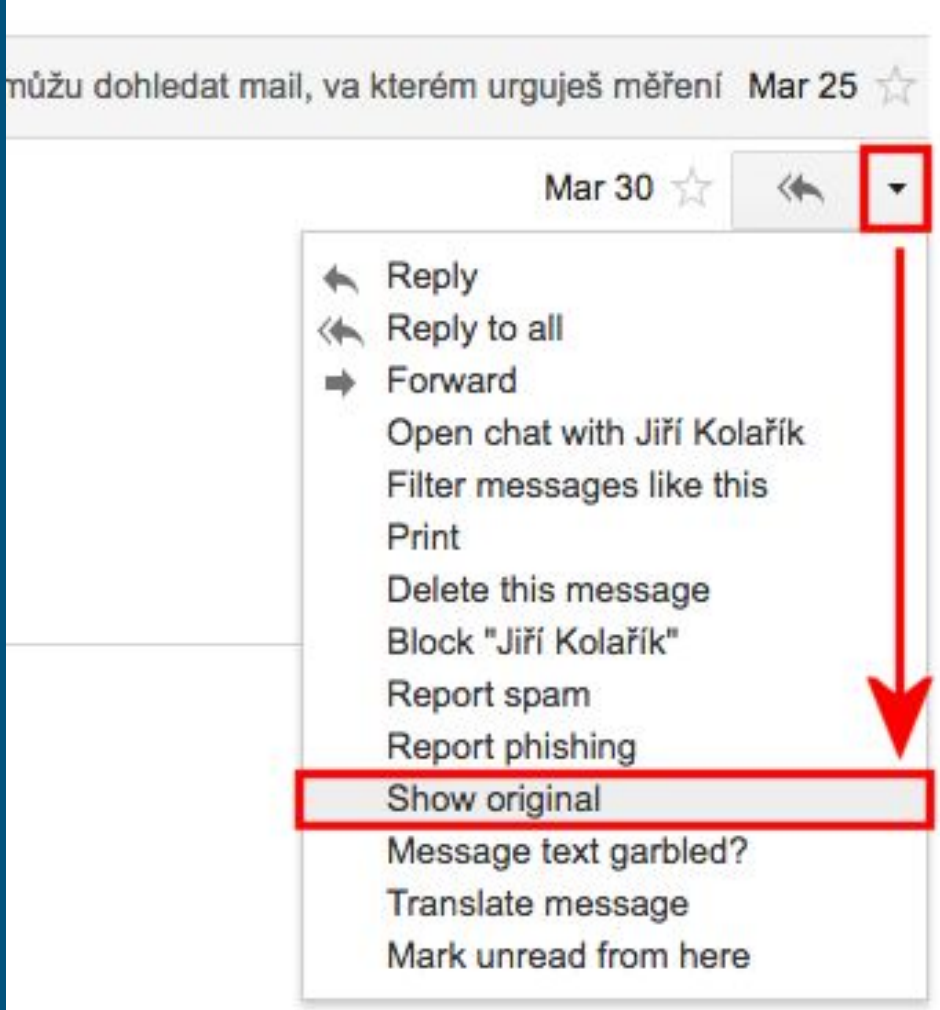
DKIM

- **Zaručuje** autenticitu zprávy
- **Zaručuje**, že mail byl odeslán z prostředků schválených vlastníkem domény
- Nemá přímé **právní důsledky**
- **Nezaručuje**, že zprávu poslala jmenovaná osoba
- **Nenahrazuje** ani nedoplňuje klasický elektronický podpis osob.
- **Nešifruje** obsah zprávy

Diagnostika

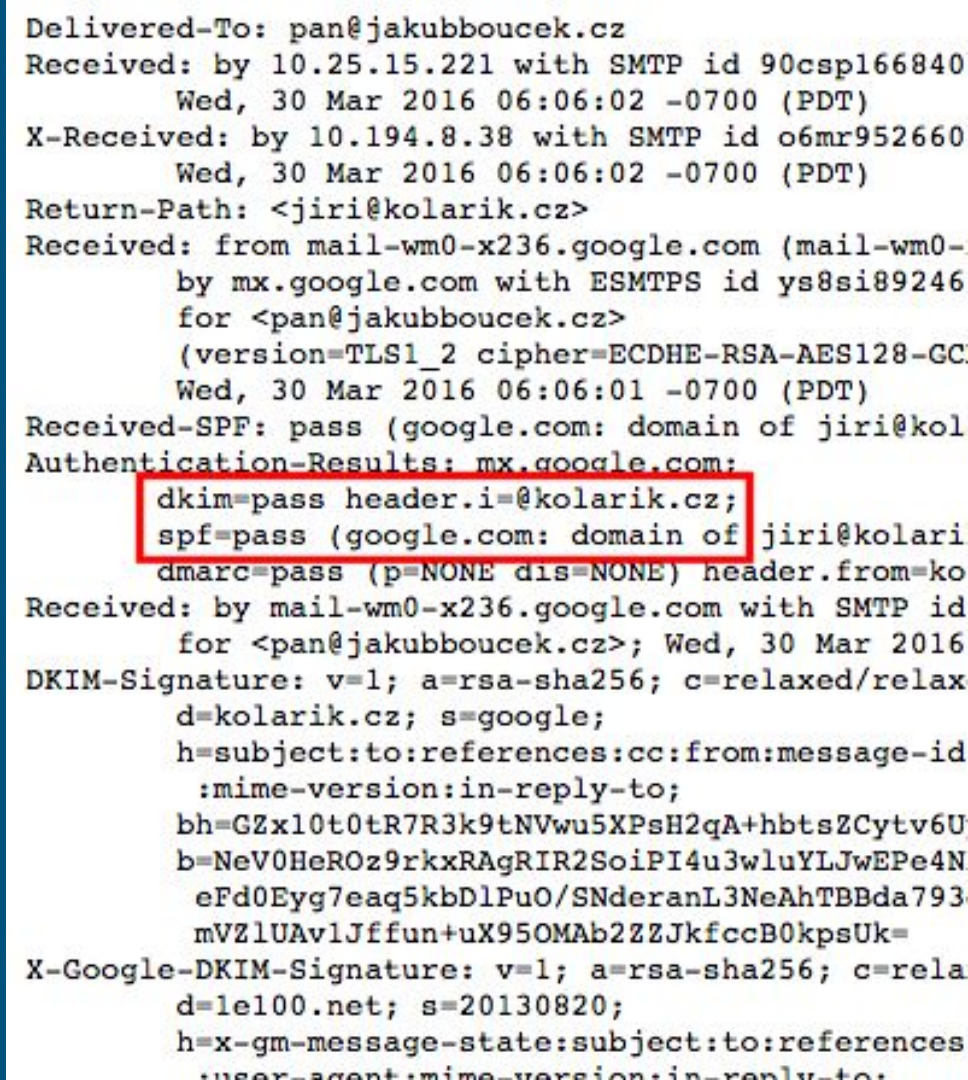
Diagnostika

Gmailem



Diagnostika

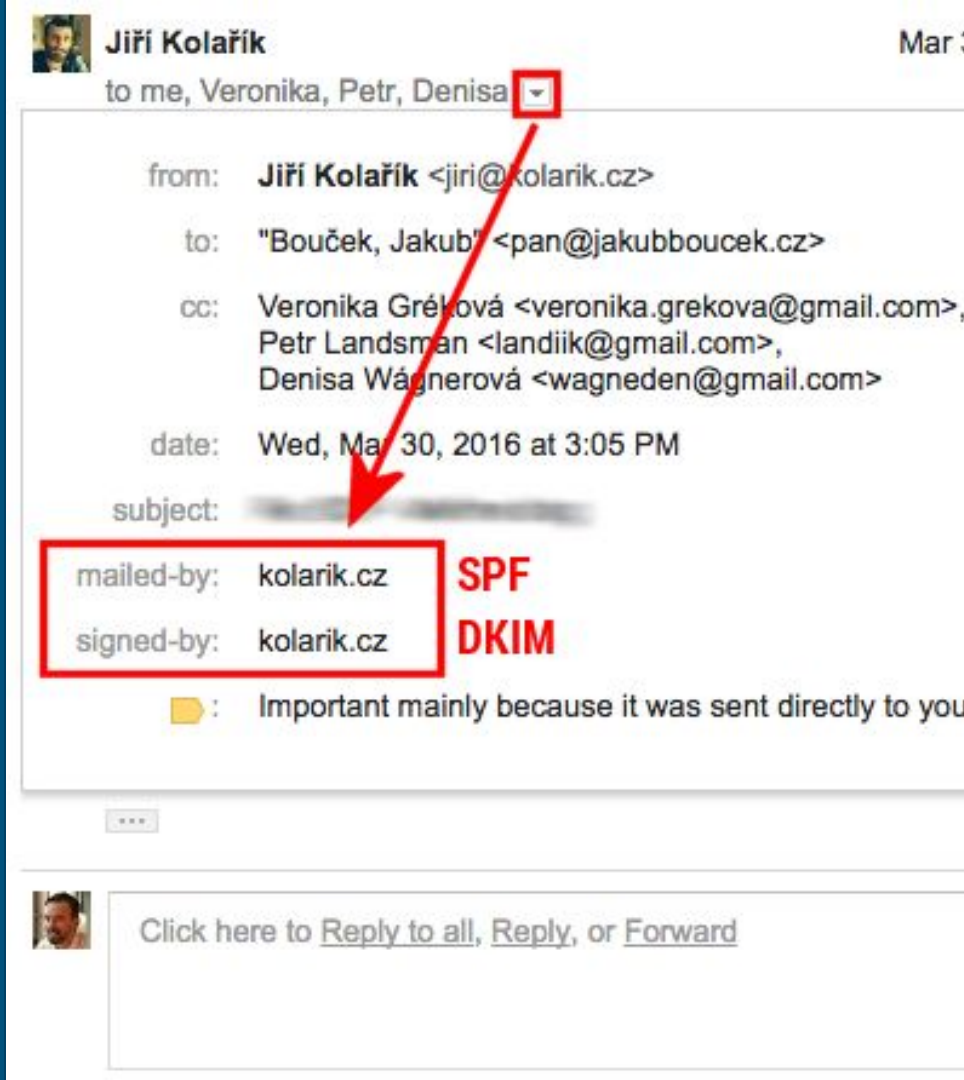
Gmailem



```
Delivered-To: pan@jakubboucek.cz
Received: by 10.25.15.221 with SMTP id 90csp166840
        Wed, 30 Mar 2016 06:06:02 -0700 (PDT)
X-Received: by 10.194.8.38 with SMTP id o6mr952660
        Wed, 30 Mar 2016 06:06:02 -0700 (PDT)
Return-Path: <jiri@kolarik.cz>
Received: from mail-wm0-x236.google.com (mail-wm0-
        by mx.google.com with ESMTPS id ys8si89246
        for <pan@jakubboucek.cz>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GC
        Wed, 30 Mar 2016 06:06:01 -0700 (PDT)
Received-SPF: pass (google.com: domain of jiri@kol
Authentication-Results: mx.google.com;
       dkim=pass header.i=@kolarik.cz;
       spf=pass (google.com: domain of jiri@kolari
      dmarc=pass (p=NONE dis=NONE) header.from=ko
Received: by mail-wm0-x236.google.com with SMTP id
        for <pan@jakubboucek.cz>; Wed, 30 Mar 2016
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relax
        d=kolarik.cz; s=google;
        h=subject:to:references:cc:from:message-id
         :mime-version:in-reply-to;
        bh=GZx10t0tR7R3k9tNVwu5XPsH2qA+hbtsZCytv6U
        b=NeV0HeROz9rkxRAgRIR2SoiPI4u3wluYLJwEPe4N
         eFd0Eyg7eaq5kbDlPuO/SNderanL3NeAhTBBda793
         mVZlUAv1Jffun+uX95OMAb2ZZJkfccB0kpsUk=
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=rela
        d=1e100.net; s=20130820;
        h=x-gm-message-state:subject:to:references
```

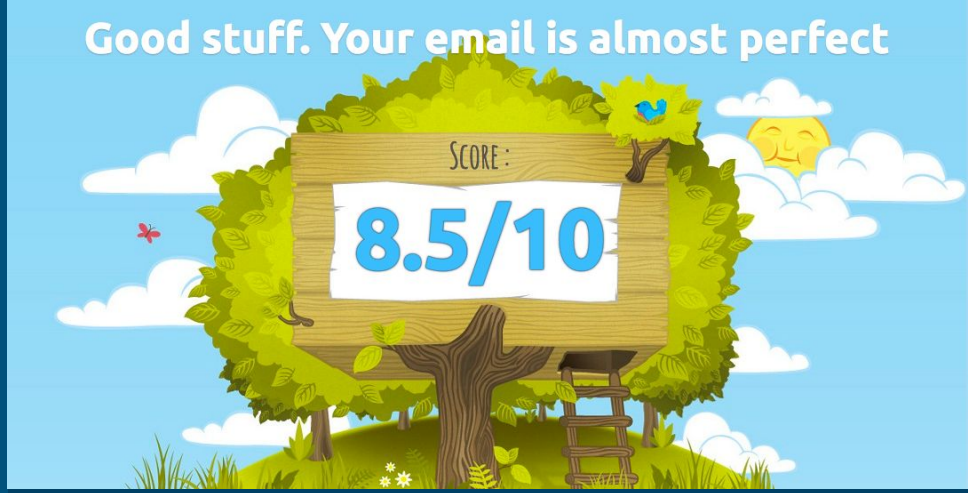
Diagnostika

Gmailem



Diagnostika

Mail tester



www.mail-tester.com

Diagnostika

Další zdroje

- dkimvalidator.com
- toolbox.googleapps.com

Negativa

Negativa

- Přesměrování

Negativa

- Přesměrování
- Cizí SMTP (např. u Telefonicy)

Negativa

- Přesměrování
- Cizí SMTP (např. u Telefonicy)
- Nahodilé chyby
- DKIM není vynutitelné

DMARC

Domain-based Message Authentication, Reporting & Conformance

DMARC

- Vynucení SPF a DKIM
- Reportování chyb
- Debugování

DMARC záznam

```
_dmarc.jakubboucek.cz. 1799 IN TXT
    "v=DMARC1;p=none;rua=mailto:pan@jakubboucek.cz;
    ruf=mailto:pan@jakubboucek.cz;fo=1;adkim=r;aspf=r;pct=100;
    ri=604800;rf=afrf;sp=none"
```

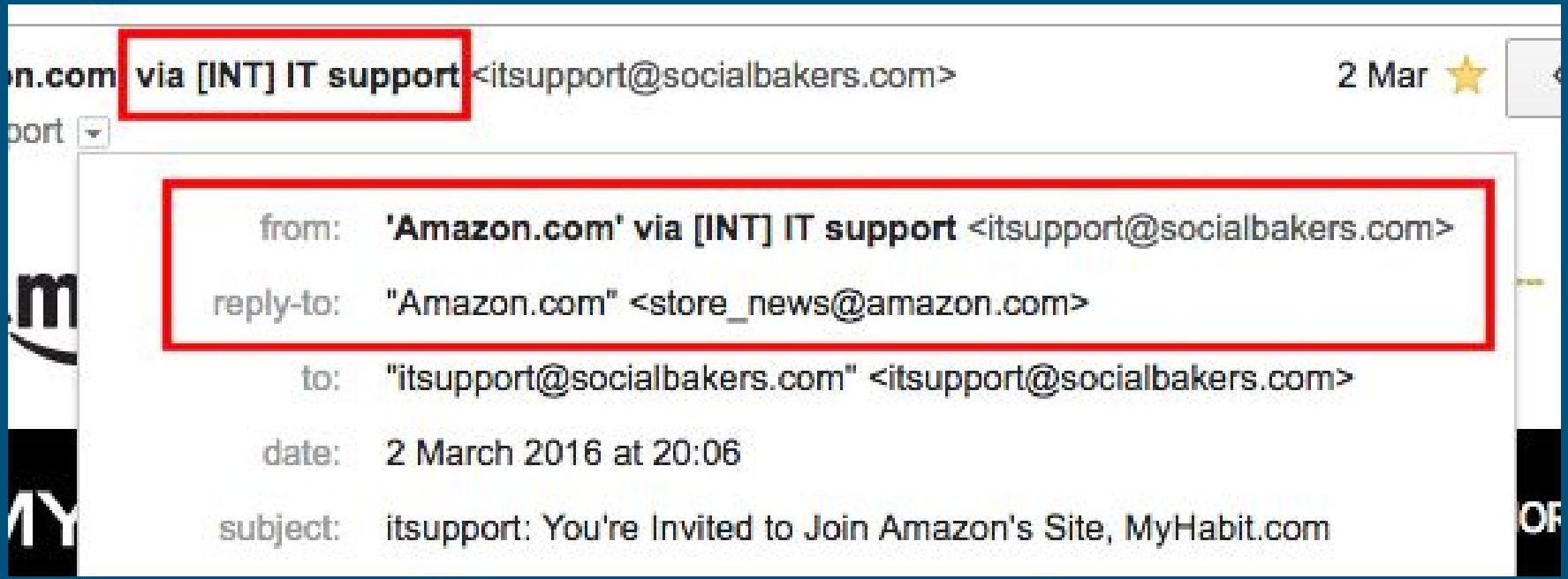
DMARC report

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>  <record>    <row>
    <source_ip>2a02:598:a::78:125</source_ip><policy_evaluated>
      <disposition>none</disposition>
     <dkim>pass</dkim>
     <spf>fail</spf></policy_evaluated> </row>
  <identifiers> <header_from>plzenskybarcamp.cz</header_from></identifiers>
  <auth_results><dkim><domain>seznam.cz</domain><result>pass</result>
  </dkim><dkim><domain>plzenskybarcamp.cz</domain><result>pass</result>
```

Podmínky

Vlastní doména (ne free-mail)

Jak na přesměrování



Osobní mailovka

Použijte některého z velkých:

- Google Apps
- Office 365
- Zoho (!)
- Mojedomena.seznam.cz

Tuzemské hostingy:

- Gigaserver

mail( )

Použijte velkého poskytovatele:

- Amazon AWS SES
- Mandrill
- SendGrid
- …

Tuzemské hostingy:

- Gigaserver

Dotazy?

Jakub Bouček

E-maily technicky

aby vaše zprávy došly do cíle

Plzeňský Barcamp 16. 4. 2016
https://goo.gl/RCx0nR