

**Why is
EMAIL so
broken?**





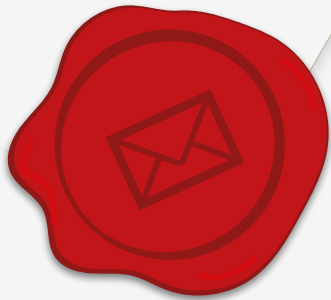
Hello! I'm...

Jaymon Lefebvre CET ISP CISSP CCSP CEH

Director IT Services

Wild Rose School Division

Western Alberta School District with ~4500 students ~1100
faculty

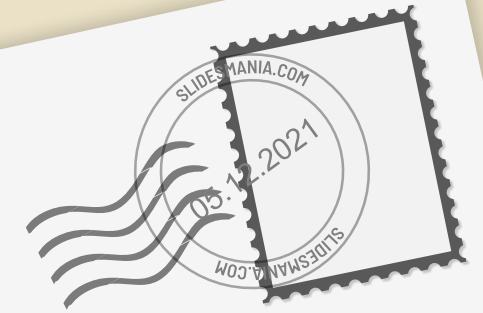


Is SMTP still simple?

SMTP turned 40 this year!

Over 40 years as the Internet shifted from being obscure, the inherent trust email was built on is no longer sufficient.

So what'd we do?



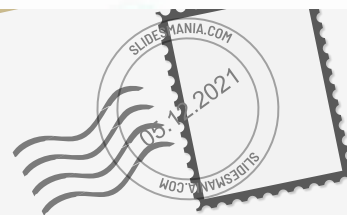
John K. Smith
123 Main st.

Did you know?

- SMTP AUTH was only published in 1995?
- The Internet Mail Consortium (IMC) reported that 55% of mail servers were open relays in 1998,[\[5\]](#) but less than 1% in 2002.[\[6\]](#)
- SMTP as specified by Jon Postel had no passwords; each server was by design an open relay!



'UNKNOWN_SENDER!'
(No subject)



*John K. Smith
123 Main st.*



Message Filter: Inbound All Reading Pane: Right Bottom Off

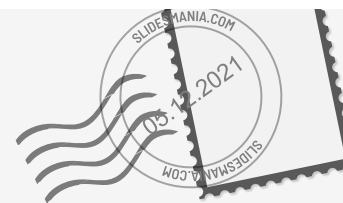
Search: All domains 2 days Search Advanced Search Saved Searches

Allow List Recategorize Export Deliver

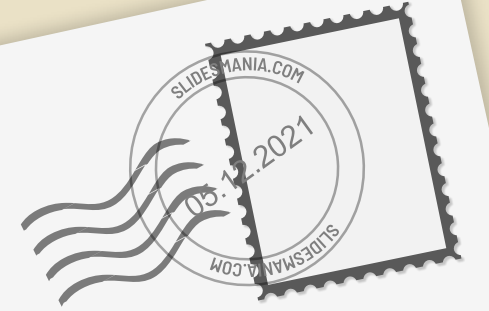
<input type="checkbox"/>	From	To	Subject	Date	Size	Delivery	Reason	Score
<input type="checkbox"/>	DataBreachToda...	sbanks@cuda36...	» Shifting Cloud Security Left with Infrastructure as Code	08:33AM	32 KB	Not Delivered	Bulk Email	0.46
<input type="checkbox"/>	your name	admin@cuda36...	» urgent new purchase order	08:12AM	868 KB	Not Delivered	Barracuda Repu...	
<input type="checkbox"/>	Mark Bomstein ...	sbanks@cuda36...	» This we can't ignore...	08:09AM	9 KB	Not Delivered	Bulk Email	0

Did you know?

- In 2006 Indiana Uni. carried out a study to quantify the effectiveness of phishing email messages.
- Phishing user credentials had a 72% success rate when the email came from an attacker impersonating a friend of the victim!



Sender Policy Framework (SPF)



John K. Smith
123 Main st.

Along comes DKIM



*John K. Smith
123 Main st.*

Did you know?

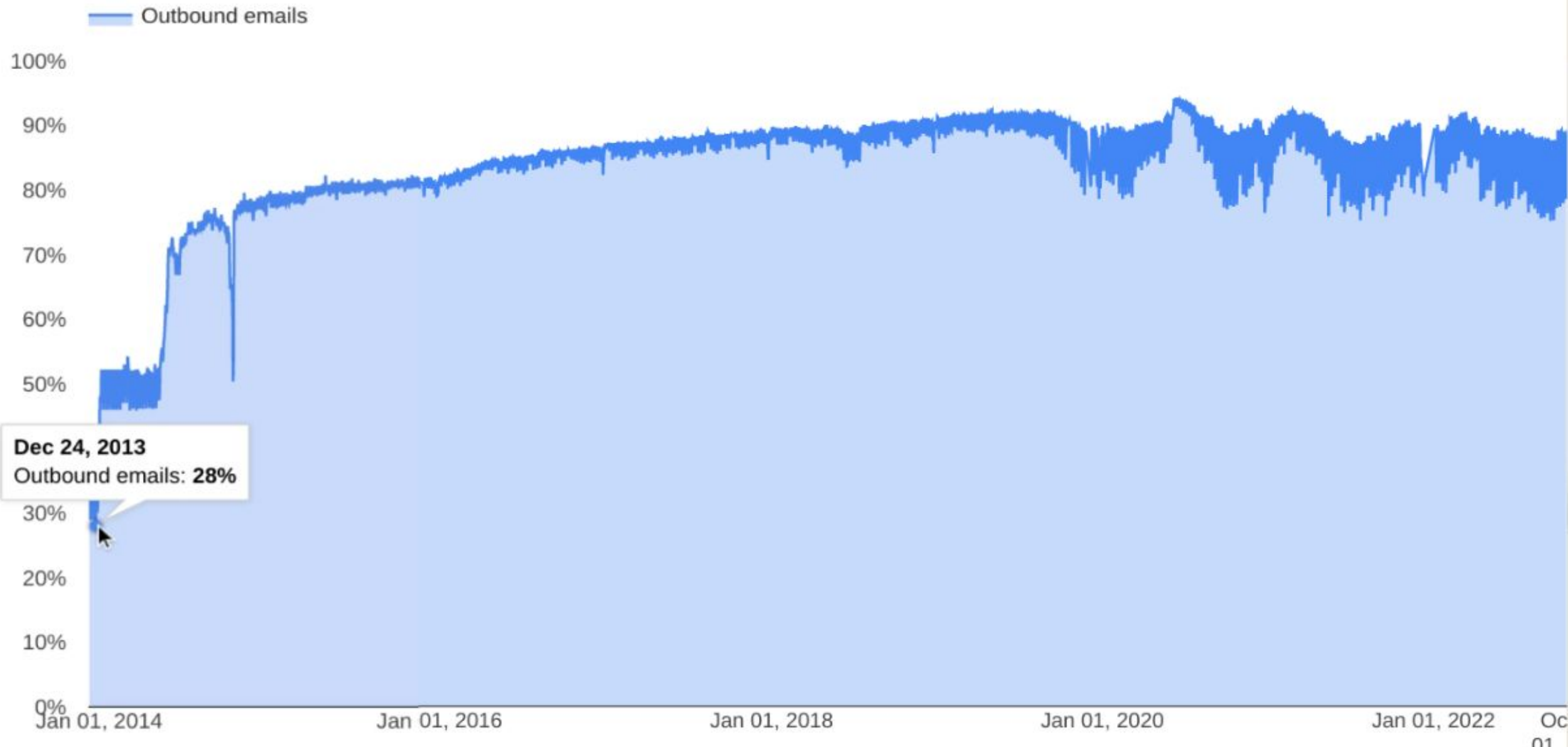
- Gmail was one of the first major email providers to finally start making TLS the default in 2014.
- <https://transparencyreport.google.com/safer-email/overview?hl=en>
- Before that, email was mostly “simple”



*John K. Smith
123 Main st.*



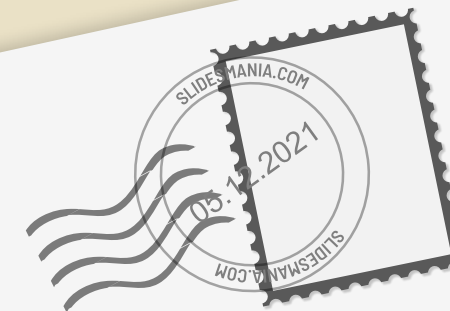
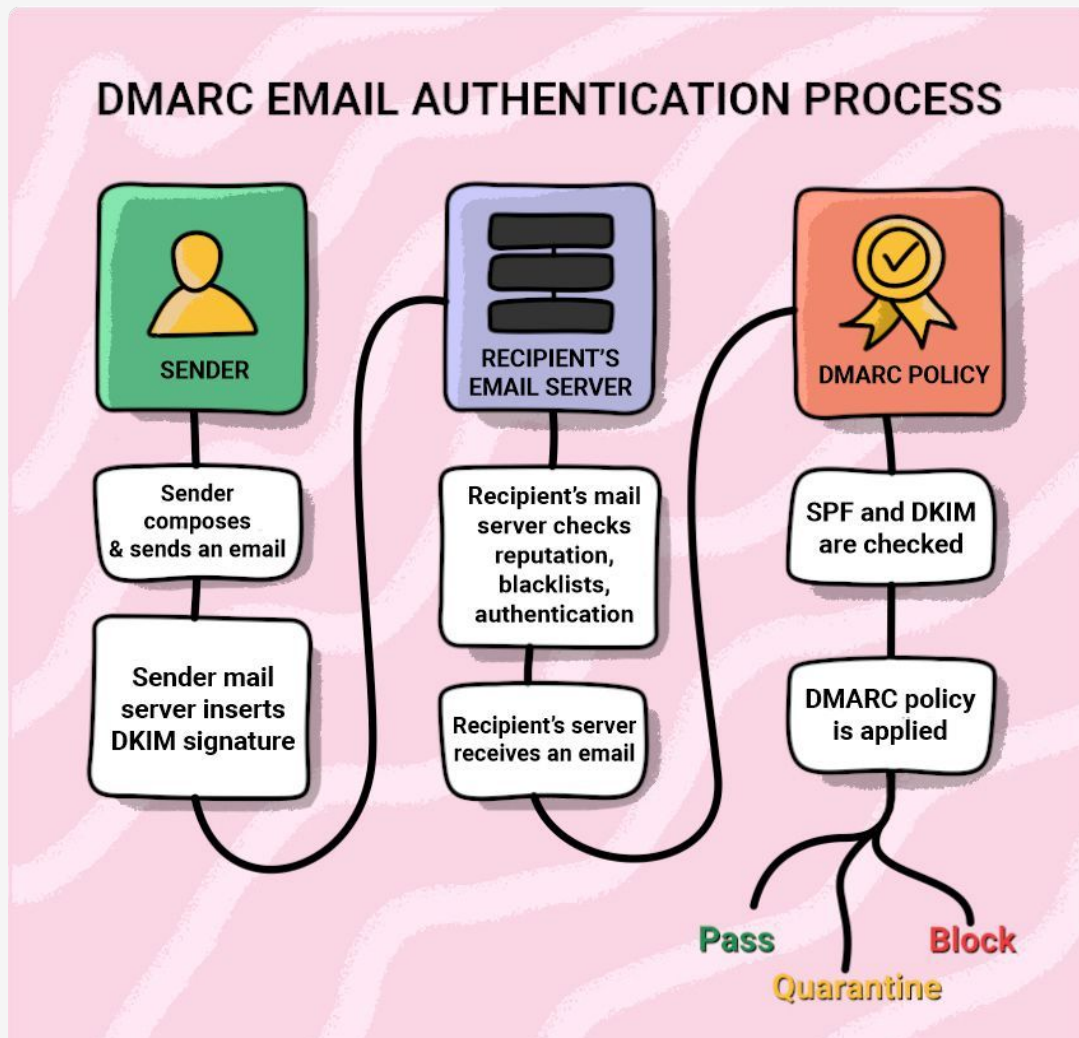
Start  12/31/2009 End  10/27/2022



Dec 24, 2013
Outbound emails: **28%**

And we finally get to DMARC!

SPF pass & / || DKIM pass = DMARC pass



John K. Smith
123 Main st.



Who cares, Jaymon?



gov.ab.ca

DMARC Lookup

dmARC:gov.ab.ca

Find Problems

Solve Email Delivery Problems

```
v=DMARC1; p=none; rua=mailto:dmarc@gov.ab.ca;
```

wrsd.ca

DMARC Lookup

dmARC:wrsd.ca

Find Problems

Solve Email Delivery Problems

```
v=DMARC1; p=reject; rua=mailto:dmarc@t5ma41cb.uriports.com; fo=1:d:s
```



*John K. Smith
123 Main st.*

<https://mxtoolbox.com/DMARC.aspx>

New Message

To *jaymon.lefebvre@wrsd.ca*

Subject *Earning Statement For Jaymon B Lefebvre*

EARNING STATEMENT FOR JAYMON B LEFEBVRE



payroll@wrsd.ca

to JAYMON.LEFEBVRE ▾

Your Earning Statement is attached

Original Message

Received-**SPF**: **pass** (google.com: domain wrsd.ca configured 64.46.59.92 as internal address)

Authentication-Results: mx.google.com;

spf=pass (google.com: **domain wrsd.ca configured 64.46.59.92 as internal address**)

smtp.mailfrom=payroll@wrsd.ca



Send




1


Story Time



I guess we're just stuck then, sigh.

You're Invited! Attend Operations Webinar External Trash x The Vital Role of Security Print Share

 **Kevin** kevinp@ via mailchimpapp.net 7:59 AM (2 hours ago) Reply More
to me ▾

 **Be careful with this message**

Kevin is similar to a name in your organization, but the email address does not belong to your domain or wrsd.ca Mail couldn't verify that it actually came from kevinp@[REDACTED]. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

Report phishing Looks safe Help

SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain psd-ca.20210112.gappssmtp.com



How do we even get started?

1. **Subscribe to a DMARC aggregate reporting service (they are many, your cloud partner can also recommend one)**
2. **Simply implement a DMARC *p=none* and direct the reports to the aggregate service**



*John K. Smith
123 Main st.*

Next...

- 1. Identify sending services that would have failed DMARC from your service catalog**
- 2. Work with the business unit to determine whether it needs to send as the primary domain suffix**



*John K. Smith
123 Main st.*

And then...

- 1. If the business determines it NEEDS the primary domain, configure it correctly if possible**
- 2. Services you identify that can pass DMARC and don't need the primary domain can be broken out**



*John K. Smith
123 Main st.*

Such as...

Can the business adjust from
payroll@wrsd.ca to
noreply@payroll.wrsd.ca

v=dmARC1; p=none, sp=reject rua=mailto:jaymon@wrsd.ca



*John K. Smith
123 Main st.*

Other suggestions...

- **Avoid allowing your domain to use relay services approved by SPF / IP address.**
- **Avoid the use of the quarantine policy (**p=quarantine**)**



How we handled a recently phishing incident that targeted Dropbox

// By Dropbox Security Team • Nov 01, 2022

<https://dropbox.tech/security/a-recent-phishing-campaign-targeting-dropbox>

We know it's impossible for humans to detect every phishing lure. For many people, clicking links and opening attachments is a fundamental part of their job. Even the most skeptical, vigilant professional can fall prey to a carefully crafted message delivered in the right way at the right time. This is precisely why phishing remains so effective—and why technical controls remain the best protection against these kinds of attacks. As threats grow more sophisticated, the more important these controls become.



Call to action...

- **Consider adding DMARC as an approved vendor and RFP response requirement.**
- **DMARC is a repeatable technical control. Focus as much or more on DMARC than user based phishing training.**
- **Phishing Fatigue is a real thing.**





Thank you!

Do you have any questions?

jaymon.lefebvre@wrsd.ca