Read or listen to this article online

Scan the QR code to open this article on XO.PL

Article source:

https://xo.pl/it-made-fun-inet-mail

INTERNET

Email: the postman, the sorting office and the parcel nobody wants to accept

A scandal erupted at the Main Post Office of Mr Postfix. Greg sent an email, then five seconds later demanded proof that the recipient had read it, understood it and completed the task. The postmaster calmly put down his stamp. “Greg, we're a postal service, not a machine for reading other people's minds.” 📬🤣

I clicked Send. Where is my letter?

— I sent a message to Agnieszka — Greg announced.

— We've accepted it for sending — replied the SMTP clerk.

— So she got it?

— I didn't say that.

— THEN WHAT DID YOU ACTUALLY DO?!

— Accepted the parcel from the customer. Now we have to deliver it to the recipient's post office.

Email is a service for sending messages between mailboxes, commonly hosted by different providers. A mail application — such as Thunderbird, Outlook or a phone app — lets you compose messages, but doesn't normally deliver them directly to distant recipients' servers.

A message contains a sender, one or more recipients, a subject, a body and possibly attachments. When you click Send, the client usually submits it to an outgoing mail server that handles the next steps.

— So clicking Send doesn't teleport the letter?

— Afraid not. Otherwise we'd have far less work here.

— Isn't less work a good thing?

— Don't say that where the postmaster can hear you.

SMTP: the sorting office works while everyone sleeps

Trolleys of letters lined the back office. Each carried the name of a destination mail server.

— SMTP department, collect the mail! — Greg called.

— We already have it — replied the mail carrier. — Now we're sending it onward.

SMTP is the protocol used for outgoing email: from a user's application to a submission server and between mail servers. A mail client often submits messages on port 587 with authentication and STARTTLS; port 465 with TLS from the beginning of the connection is also used. Server-to-server delivery usually uses port 25.

— Three different service windows for one letter?

— Different jobs, Greg. One accepts customer submissions; others talk to fellow post offices.

— And where is Postfix?

— Postfix is mail-server software, not the name of a postman. Though the manager has already ordered a nameplate.

Postfix, Exim and Microsoft Exchange are examples of mail server software. SMTP is the shared language for transferring messages, not a particular program's name.

How does the postman find the correct sorting office?

The envelope was addressed to `agnieszka@example.net`. The carrier studied it.

— I have her name and town. But where is her post office?

— Look in the address book — suggested the postmaster.

For the recipient's domain, the sending server normally looks up **DNS MX records**. These identify mail exchangers that accept email for that domain. With multiple records, priority values help decide which servers to try first; that doesn't guarantee any one of them will always be reachable.

— It says MX 10 here and MX 20 there. Are those bus numbers?

— No. Lower values generally indicate higher priority.

— What if number ten doesn't answer?

— We can try another suitable server, if the domain's configuration allows it.

— Why do we need IP addresses then?

— To actually reach the server named in the records. Knowing a sorting office's name won't transport the van.

Greg sighed. Once again, the DNS address book had rescued the entire Packet Highway.

Queues, retries and five hundred and fifty

The carrier returned with an undelivered letter.

— Doors locked. The recipient's server is temporarily unavailable.

— Throw it away? — asked a new clerk.

— NO! — the postmaster shouted. — It's not a takeaway menu!

When a problem is temporary — perhaps a `4xx` response or a failed connection — the sending server may put the message in a **queue** and retry delivery later. Timing and retry schedules depend on configuration. After the configured delivery period expires, the sender may be notified that the message couldn't be delivered.

— What if the recipient doesn't exist?

— The server may reject it permanently, usually with a `5xx` response.

— Such as `550`?

— Yes, although the number alone doesn't always explain the reason without the full response.

— If my server accepts the message, does that mean Agnieszka received it?

— No. It confirms only the particular handoff that succeeded.

— I want a stamp saying READ!

— We don't sell those, even for extra money.

Submission accepted, message placed in a mailbox and actual human reading are three different events.

The mailbox is waiting. Who collects it?

At the receiving post office, the mail carrier placed the letter in the right mailbox.

— Delivered — he reported.

— Now show it on my phone and laptop — Greg demanded.

— That's a different department.

IMAP lets mail applications work with mailboxes held on the server: viewing folders, changing message flags and synchronizing state between devices. **POP3** is mainly for retrieving messages from a mailbox into an application; depending on client settings, copies may be left on the server or removed. It isn't as simple as “new good versus old bad” — the protocols support different approaches to email.

— So IMAP is a reading room where the documents stay in the office?

— Good analogy.

— And POP3 is the fellow who drives up with a sack to collect the letters?

— Exactly.

— He can take them away?

— If configured to do so.

— And SMTP?

— Still handles sending. Please don't ask the postman to manage your folder structure.

Webmail, meanwhile, lets people use email through a web browser. Mail infrastructure still runs behind the website, but users don't have to set up SMTP or IMAP manually.

An attachment is a parcel strapped to a letter

Greg arrived with an envelope, a bag of photos, three videos and an image of an entire hard drive.

— Please attach these — he said.

— To the letter?! — exclaimed Agnieszka.

— There's an Attach File button.

Email uses standards such as **MIME** to combine plain text, HTML and attachments. Binary files need suitable transfer encoding; Base64, for example, increases the encoded size by roughly one third before other overhead. Providers and servers also impose limits on the size of an entire message.

— Why can a twenty-megabyte file fail when the limit is twenty megabytes?

— Because the parcel may grow when it's packaged.

— Then I'll zip the entire server.

— Still a poor idea.

For large files, a link to a properly secured file-sharing service is often more practical than turning email into a moving company.

Postmaster! Someone is impersonating the sender!

A hooded stranger approached the counter.

— I am your bank director. Please email me your password immediately.

— Credentials? — asked the postmaster.

— I wrote the bank's name in the From field.

— THAT'S NOT PROOF OF IDENTITY!

The displayed sender address can be forged, so mail servers use domain authentication mechanisms. **SPF** checks whether a sending server is authorized for the domain used in the technical SMTP sender identity. **DKIM** adds a cryptographic signature that can verify selected message elements and a signing domain. **DMARC** connects those results to the domain visible in the From field and provides policy and reporting options.

— Three stamps, and no scammers?

— Not so fast. Passing SPF, DKIM or DMARC doesn't prove the message itself is trustworthy. A fraudster can send email from a properly configured domain they control.

— Does DKIM encrypt the message?

— No. A signature isn't a safe.

— How do I defend myself?

— Check the addresses, content and unusual requests. Don't trust a displayed name alone.

The hooded stranger left. He took a pen with him. The postmaster filed an incident report.

Spam, filters and the guest blacklist

A truck labeled “AMAZING OFFER!!!” pulled up outside. Then another: “CLAIM YOUR PRIZE!!!”. A third carried investment proposals from a prince nobody had heard of.

— Put it all in the bin! — Greg ordered.

— Careful — said Agnieszka. — Sometimes a genuine message looks suspicious.

Spam filters use many signals, including sender reputation, authentication results, message content and server behavior. They may reject a message, move it to spam or accept it normally. No filter is perfect: legitimate mail may be wrongly caught, and some junk gets through.

— Why did my invoice go to spam?

— The automatic checks found something suspicious. We'd need to inspect the details.

— I'd like a filter that never makes mistakes.

— Please queue for the Miracles Department.

Even a message accepted by the receiving server may not appear in Inbox. It might go to Spam or be processed by other mailbox rules.

Is the letter secret? And who can read it?

Greg pushed his letter into an envelope.

— Sealed. Now nobody can peek?

— Not quite — replied the clerk.

TLS may encrypt connections between a mail client and server, and between mail servers when both endpoints use it. That protects transmission over particular links; it doesn't automatically encrypt the message from sender all the way to recipient. On servers, the message may be accessible for processing.

— So the truck drives sealed, but a sorting office can open the parcel?

— Roughly.

— Can we **encrypt the actual letter**?

— Yes. Methods such as OpenPGP and S/MIME exist, but both parties need to set them up appropriately.

— Why is this so complicated?

— Because writing SECRET on the envelope is not a security mechanism.

Sensitive messages can be protected further, but recipients, keys and devices still matter. Email is a delivery system, not a magical guarantee of confidentiality.

The delivery report

At the end of the day, the postmaster called the crew into the briefing room.

— SMTP?

— Messages accepted, transferred and queued where necessary.

— DNS?

— Mail exchanger addresses checked.

— IMAP?

— Mailboxes ready to synchronize.

— POP3?

— Sack packed.

— Spam filter?

— One advertisement stopped. Unfortunately it was from the manager.

Email combines several cooperating systems. SMTP transfers messages, DNS helps locate the domain's servers, and IMAP and POP3 support different ways of accessing mailboxes. Queues help cope with temporary failures, while SPF, DKIM, DMARC and filtering reduce abuse. None of these mechanisms can promise that a person will read the message.

— Postmaster, what about my email to Agnieszka?

— Delivered to her server.

— Did she read it?

— I don't know.

— WILL SHE REPLY?!

— Greg, not even Postfix can predict that.

Outside, another mail van drove past. Its sign read “RETRY IN FIVE MINUTES”.

Management of the Main Post Office of Mr Postfix reports: the sorting facility is operational, the SMTP carriers are back from their routes, IMAP mailboxes are synchronized, and the POP3 employee refuses to return his sack because “another letter might arrive”. Greg filed a complaint: “I SENT AN EMAIL AND NOBODY ANSWERED!”. The inquiry found that the message had been delivered correctly. Agnieszka's reply was: “I saw it. I'm busy.” 📬📮🤣❤️