dnsbelgium

CENTRE FOR CYBERSECURITY BELGIUM

Cyber Tips: Email Under Attack

#	Question	Answer Kristof
1	What signals do you use to detect compromised email accounts that still pass SPF/DKIM/DMARC?	If an attacker gains full control of a mailbox, every outbound email will successfully pass SPF, DKIM, and DMARC checks because the messages originate from a legitimate account. In such cases, detection must rely on behavioral, contextual, and technical anomaly indicators rather than authentication results. Examples: unusual geolocations for that user, new or risky IP ranges (VPNs, Tor exit nodes, cloud-hosted IPs), new devices or browsers, sudden spike in outbound email volume, emails sent at unusual hours, endpoint security warnings, etc. Advice: only allow connection to mail service from managed devices and only via corporate VPN
2	What caused the jump in early 2019 (SPF/DMARC graph)?	Increase in DNSSEC adoption due to some large registrars configuring it by default for their customer base
3	We've configured DMARC to reject, and SPF/DKIM so that failing messages are blocked or sent to quarantine. Since doing this, we've noticed that a lot of legitimate communication is affected because other organizations have not correctly implemented SPF, DKIM or DMARC on their side. I started reaching out to those organizations, but this is becoming never-ending work. Do you have any suggestions or best practices on how to handle this situation?"	Chasing every sender to fix their configuration is a battle you can't win (unfortunately). Focus on senders that break critical workflows, high-value senders (customers, suppliers, government), high-volume senders (if not spam/scam/...) Implement ARC (Authenticated Received Chain) ARC can "preserve" authentication results across intermediaries (forwarders, helpdesks, mailing lists). See also: https://arc-spec.org/
4	how can you easily check if the SPF/DKIM/DMARC setings have been implemented for a (your) domain ?	If you use M365, send an email to yourself and then use https://mha.azurewebsites.net to check the headers More general, you can also use https://mxtoolbox.com/emailhealth/
		Tools to check your status: https://internet.nl/test-mail/ and https://mecsa.jrc.ec.europa.eu/
5	Hello does CERT recommends a specific dmarc aggregate platform or possible buy-in for shared platform use?	All commercial products, so no advice on this: Dmarcian, EasyDMARC, OnDMARC, Valimail, Agari.
6	Why is it not possible that https://www.dnsbelgium.be/ does not validate the registration till these setups are not in place?	We are the top level domain registry for .be. We only manage the 2th level domain names, not the underlying configuration. Furthermore, configurations can be altered (in a good or bad way) during the registration period.
7	if your domain name is a .com, are the same standards valid?	Yes they are. There are universal standards. But of course .be is the better/safer/more secure choice ;-)

8	Which KPIs most accurately reflect the effectiveness of an organization’s email security program?	Phishing simulation failure rate => I'm not a fan of that. In my view, a well-crafted phishing email has the potential to deceive almost anyone into clicking on it. Phishing report rate & time to report => How do you measure what's not being reported? DMARC enforcement across all domains Inbound malicious emails blocked => Depends on the quality of the filters; how do you measure that? False negatives (malicious emails that got through) => Depends of the quality of reporting by the users Mean time to remidiate for email-related incidents => What about the severity of the incidents? How can you be sure that you have remediated successfully? Number of compromised mailboxes => I hope you have implemented MFA and secured the network so that this is zeo Executive impersonation attempts detected => Doesn't say anything about the undetected attempts (blind spots) User-submitted suspicious emails vs. actual confirmed threats Conclusion: very hard to come up with a KPI that is unbiased ... Tune in to the current maturity level and adjust annually
9	We see a lot that SPF/DKIM/DMARC are configured way too relaxed (p=none, allow all IPs etc), which means organisations started on the journey but never finished it to end in the ‘full secure/blocking config’. Is there plan idea to validate this for the domains by the TLDs and provide suggestions to companies to secure it better?	We hold awareness campaigns to promote the use of secure protocols and to inform about how to properly implement them. But we don't make suggestion for improvements on an individual basis.
10	What do we do with the pitfalls of this setup:	
	SPF fails	Sender uses an IP not listed in your SPF record (e.g. direct marketing platform). Forwarding breaks SPF because the forwarder’s IP isn’t authorised. Fix this by checking the DMARC reports and learning from the failed attempts.
	→ DKIM signed by ERP fails	ERP system doesn’t sign emails or uses a different domain for DKIM. => enable DKIM signing on ERP or route mail through your main mail gateway Misconfigured selector or expired key. => validate DKIM keys regularly Alignment fails because d= domain doesn’t match the “From” domain. => align ERP’s sending domain with your organisational domain (sorry, I'm not an ERP specialst, just thinking out loud)
	→ DMARC rejects	Before enforcing p=reject in DMARC, use phased approach: 1) Start with p=none + reporting. 2) Fix SPF & DKIM alignment issues for all senders. 3) Move to p=quarantine (partial enforcement; 25% - 50% - 100%). 4) Onyl then: p=reject when all sources comply. Use DMARC reports (RUA/RUF) to identify misaligned senders. = configure, verify, adapt, verify, etc.
	→ Customer never receives invoice"	There can be a lot of hops between the sending and the receiving server. IPs and domain names can show up on blacklists -even when security is correctly configured- preventing the mail from showing up at the receiving end.
		For those using M365 on the legacy mail.protection.outlook.com MX domain, time to switch to v1.mx.microsoft. The process is explained here: https://learn.microsoft.com/en-us/purview/how-smtp-dane-works
11	Which tools or services would you recommend for DNS integrity monitoring?	We like to use https://dnsviz.net/ for DNSSEC Also for DNSSEC: https://dnssec-debugger.verisignlabs.com/

13	Just checked 12 banks, active in Belgium. Only *2* have DNSSEC for their domain. Wouldn't you say they are quite negligent in offering protection for their customers?	I think NIS2 (and implicitely DORA) covers this with the state-of-the-art statement. The EU Commission just published the call for participation at the Multi-Stakeholder Forum on Internet Standards Deployment. https://digital-strategy.ec.europa.eu/en/news/european-commission-seeks-participants-multi-stakeholder-forum-internet-standards-deployment is going to start some interesting work: The Forum's main objective is to develop multi-stakeholder guidance identifying the relevant Internet standards and best practices, describing the corresponding deployment techniques, and defining suitable timeframes for fulfilling the selected network security requirements under Implementing Regulation (EU) 2024/2690. And I'm still a big fan of the comply or explain approach in the Netherlands (https://www.forumstandaardisatie.nl/en/netherlands-standardisation-forum)
14	Is the null MX a good practise? Would it not be better to have a way to receive postmaster and security emails to be informed about misuse / impersonation?	A Null MX record (RFC 7505) explicitly signals that a domain does not accept email. It's considered best practice in the scenario I mentioned during the webinar, because it makes the intent clear to senders and MTAs. This domain is phased out ... forget about it (indeed, the internet "never" forgets, so this is the best attempt). On top of that it prevents unnecessary SMTP retries.
15	MFA for all email accounts does that include service/technical accounts? If so, how to implement that?	Employee accounts: always enforce MFA (CyFun2025 = key measure) Service accounts: replace password-based login with certificate or token-based auth Never exempt admin accounts from MFA Golden rule: if you can't secure it, don't use it There are more secure/modern/flexible/... means of communication than email
16	Are there specific tools or platforms effective for monitoring SPF/DKIM/DMARC compliance?	See question 5
17	Besides the CCB suggestion, is it recommended to apply additionally S/MIME to email accounts?	S/MIME is useful for end-to-end protection of the data part of an email. For data protection, you need S/MIME, PGP, or platform-based content encryption. Again, you could argue that if you want to share sensitive/confidential data, email is (probably) not the communication tool you want to use.
18	Would it be possible to build a report about SPF/DKIM/DMARC & DNSSEC adoption by belgium companies (per company segment size) ?	It should be doable, if there is sufficient and accurate public company data available (which I don't think is the case today)
19	To diminish sending sensitive information via e-mail, do you have an overview of alternatives? Or a link to overviews?	Some options with potential use cases Encrypted file-sharing / secure file transfer services:services that encrypt files on the client side (zero-knowledge or end-to-end) before storing or sharing. Recipient gets a secure link instead of an attachment. -> be careful with free commercial services that offer this Secure messaging / encrypted chat apps: use end-to-end encryption (E2EE) so that messages or attachments are only readable by sender and recipient. Useful for real-time or asynchronous exchange of sensitive info Secure portal: a controlled web portal where users (internal or external) can securely upload/download documents rather than sending them over email. Sharepoint (if you use M365) can also be structured for this usage. Client-side encrypted email (PGP / S/MIME): if both parties support it: encrypt the email content (and attachments). This keeps the data confidential even if email transport is compromised. -> but it's not user friendly (certainly PGP isn't) Secure File Transfer platforms: especially for business-to-business (machine to machine) or partner exchanges — encrypted transfer with authentication and logging. Good for large files, compliance, or regulated sectors. SFTP or rsync over SSH are examples.

20	can you do the spf dkim dmarc strictiness with rejects in a phased approach?	Yes, implementing SPF, DKIM, and DMARC with strict enforcement (including rejects) is best done in a phased approach to avoid mail flow disruptions and to learn from your specific data flows. 1) Ensure SPF exists for all sending domains. Enable DKIM signing everywhere you can. Publish DMARC with p=none and enable RUA/RUF reporting. Monitor reports for x days to identify all legitimate senders. Validate SPF and DKIM alignment for each source. 2) Fix SPF & DKIM alignment. Move DMARC to p=quarantine (e.g. %=25 initially). Gradually increase pct to 100% as confidence grows. Continue monitoring reports. 3) Switch DMARC to p=reject once all legitimate sources comply. Maintain SPF and DKIM strict alignment (aspf=s, adkim=s) for maximum protection.Keep reporting active (and check them) for ongoing visibility. General notes For SPF: ensure all authorised IPs/services are listed; avoid +all; no excessively long SPF (>10 lookups) For DKIM: one DKIM selector per major system/service (keep control&flexibility), ensure all outbound mail (so also 3th party providers sending on your behalf) is signed For SMARC: don't enforce strict DMARC until all alignment issues are solved
21	What about BIMI Brand Indicator Message Identification, do you see it as an efficient layer of protection ?	It can be effective. Adoption rate is under 0,5%. It's still in draft phase (https://datatracker.ietf.org/doc/draft-brand-indicators-for-message-identification/)
23	Anyone using the domain guard service?	Yes there are users for the service(s). Domain Guard is more popular than Domain Shield because it's more flexible and has less overhead ... trade-off between usability and security. /https://www.dnsbelgium.be/en/secure/domain-guard https://www.dnsbelgium.be/en/secure/domain-shield