Making Email Security Smarter with Domain Intelligence

Posted on August 8, 2024

More than 4 billion people checking their emails daily represents a goldmine for attackers. No wonder phishing remains one of the biggest threats today, pushing email security to the top of organizations' cyber priorities.

But here's the kicker—90% of malicious emails can slip through email security standards, such as the Sender Policy Framework (SPF); the DomainKeys Identified Mail (DKIM); or Domain-Based Message Authentication, Reporting, and Conformance (DMARC).

While many email security providers are out there, those offering a multilayered approach can offer more.

The Domain Intelligence Layer

Anyone looking to make their mark online needs a domain name, and cybercriminals are no exception. They, after all, use email domains to send phishing emails. They also need domains to run their command-and-control (C&C) servers for malware distribution.

Therefore, keeping track of domain names is crucial for boosting email security. Specifically, it helps strengthen email security by spotting harmful domains and checking email sender legitimacy.

Identifying Shady Domains

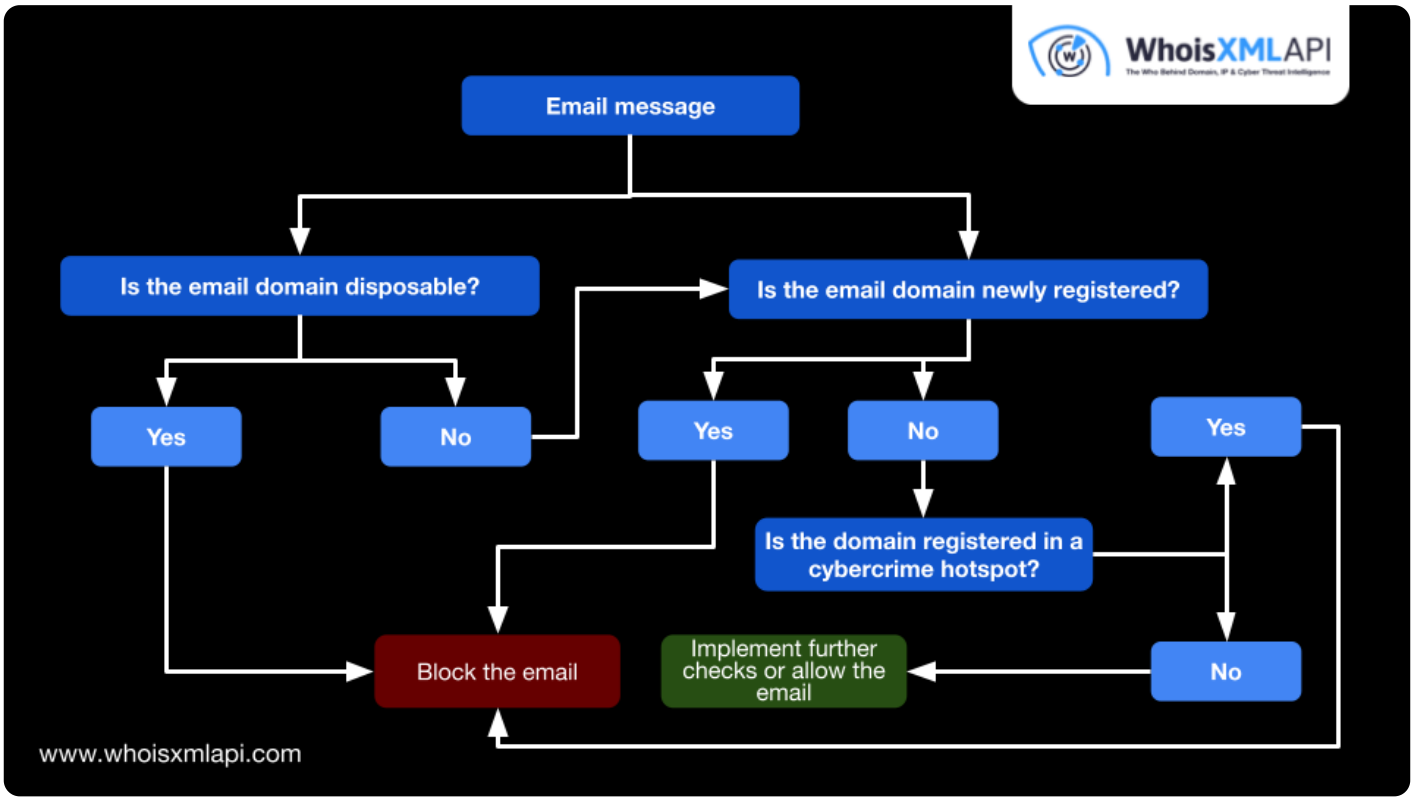
While all domains can be weaponized, threat actors often use newly registered domains (NRDs), disposable email domains, and domains registered in known cybercrime hotspots. Let's learn more about them below.

- **NRDs:** Attackers have been known to use domains within a few weeks or even hours of their registration. That's why it can be crucial for email security solutions, especially artificial intelligence (AI)-powered ones, to integrate with an NRD data feed to be able to detect and filter emails sent from NRDs.

- **Disposable email domains:** Indeed, disposable email addresses are great for privacy. But fraudsters are also riding this wave. They use these email domains to hide, and when caught, they can easily create new ones to continue their malicious activities. As such, email security solutions should be smart enough to detect disposable email domains.

- **Domains registered in countries known for phishing or fraud:** Domains from countries with a bad reputation for cybercrime are not always bad, but that still remains a red flag. For example, email security algorithms can be taught to block or quarantine messages from new email domains registered in countries with a history of cybercrime activity.

The email security workflow may look something like this after an email passes through standard security layers.



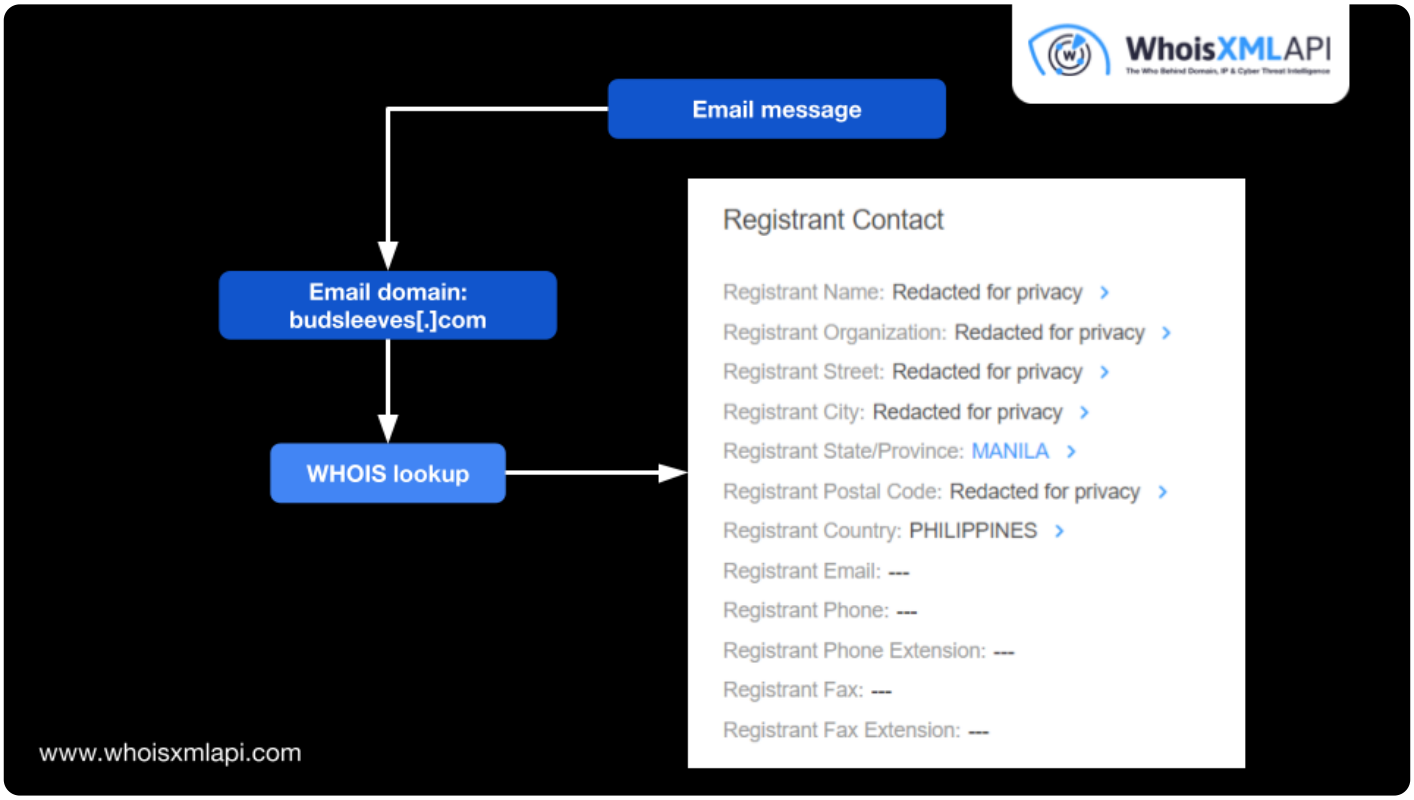
Checking If an Email Is Legit

While people can and should be trained to determine if an email message is genuine or fraudulent, relying entirely on recipients' ability to discern bad from good is risky due to the advanced techniques used in some phishing emails and the sheer number of scams being sent out.

That's why email security solutions must be able to run a variety of authenticity checks before the email arrives in a user's inbox. One way to do that is by looking at the WHOIS details of the domain from which the email originated. For instance, especially if the sender claims to work at a large enterprise, the registrant organization found in the WHOIS records of the email domain should typically be visible and matching.

If this information is not available because of redacted WHOIS records, the domain's registrant location should still be consistent with the sender's expected location. Say you receive a message from someone claiming to represent one of your European suppliers, but the email domain is

budsleeves[.]com (a confirmed phishing domain), which is registered in the Philippines, you should question it. Why would a European company register its domain in Asia?



In addition, a very new domain could be suspicious, especially when the entity you're supposed to be dealing with claims to have been in the business for a long time.

Wrapping Up

With cybercriminals getting smarter by the day and using emerging technologies like AI, multilayered email security intelligence is a must. Combining domain intelligence with spam filtering, malware detection, user awareness training, and other email security processes can help create a strong defense system.

Discover how you can add a domain intelligence layer to your email security solutions and processes. Contact us now for more information about our data solutions.