Why You Should Add Email Address Validation to Your Email Security Best Practices

Despite the emergence of instant messaging platforms, email is still the king of digital communication, particularly in the professional and business world. The number of email users globally is expected to reach 4.3 billion by the end of 2023, which accounts for more than half of the world's population. Also, the total number of emails sent and received every day is forecasted to rise to 347.3 billion by 2023.

Probably because of its vast userbase, email is also a common cyberattack vector. For instance, some 65% of cybercriminal groups use phishing as their primary infection vector, and almost 60% of IT professionals view phishing as a top security threat.

Spamming is another way by which threat actors enter an organization's IT network. Spam emails are not only annoying, but they can also be dangerous as

they may carry ransomware and other malware.

With that in mind, email security has become a top priority for organizations. And among the **email security best practices** is **email address validation**.

Email Address Validation as a Security Practice

Email address validation is the process of verifying the validity of an email address to make sure that the intended recipient receives the message. The process is commonly employed by email marketing professionals to reduce bounce rates and increase delivery rates. As part of this, one tool that they may find useful is Email Verification API.

Aside from checking email address validity, however, Email Verification API can also be used to spot and restrict the access of potentially dangerous email addresses to an organization's network. As an email security mechanism, it can filter out potential bad actors that use disposable addresses or homograph attack methods. And that, ultimately, mitigates email-based threats that could have dire consequences.

Effects of Email-Based Attacks

In a Barracuda study, IT stakeholders discussed the impact of email security attacks on their company. Below are the findings of the report:

- Loss of employee productivity – 48%
- Downtime and business disruption – 36%
- Hurts the reputation of the IT team – 28%
- Recovery costs – 20%
- Loss of sensitive, confidential, or business-critical data – 16%
- Direct monetary loss to cybercriminals – 10%

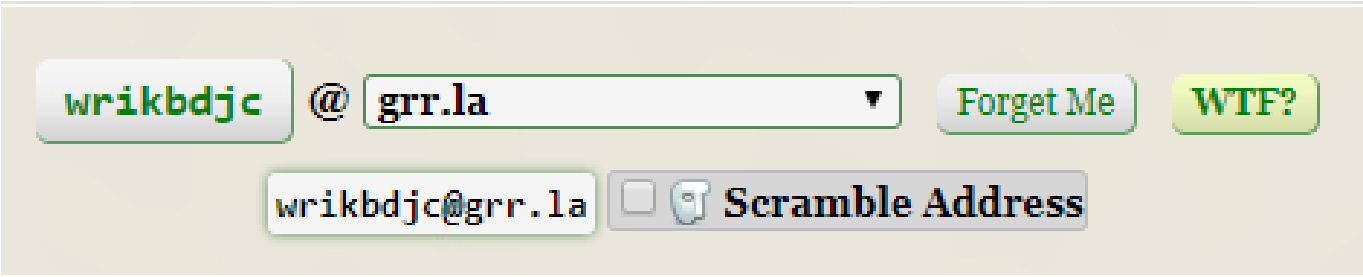
Overall, only 26% of the respondents said email security attacks had no impact. As such, email security is an essential component of an organization's overall IT security. Let's look at two cases to explore this point further.

Clamping Down on Users of Disposable Email Addresses

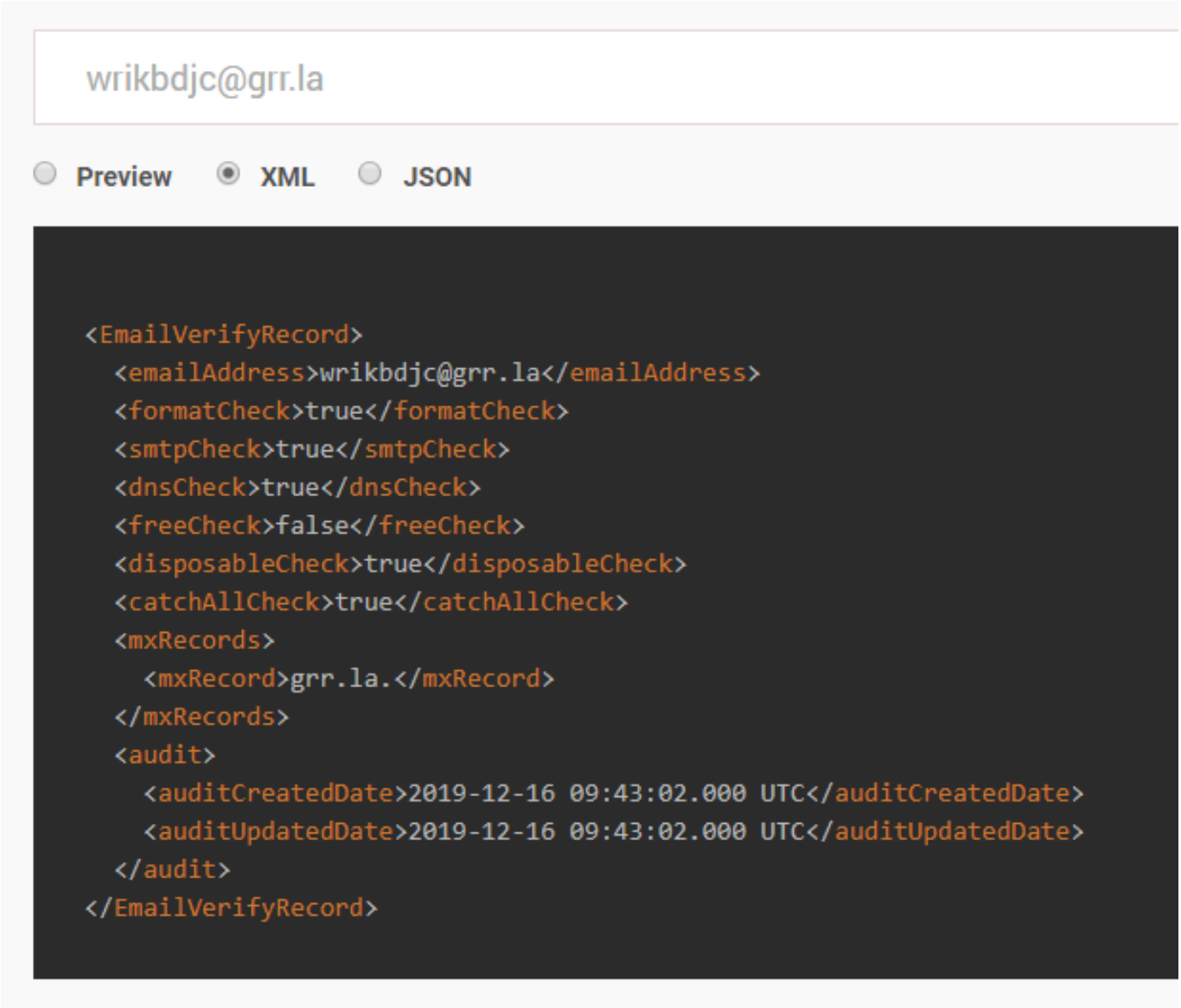
People may use disposable email addresses so they won't have to give out their real ones when taking advantage of freemium features. Aside from this purpose, however, disposable or temporary email addresses are also used by cybercriminals. Fraudsters can use temporary email services to create an account on your website, chat with customer support representatives, and access documents and pages that may give them insights on your overall IT infrastructure.

These temporary email addresses can also figure in phishing campaigns, which are difficult to trace as most disposable email service providers offer features that allow messages to self-destruct after a certain period.

Let us take a look at an example. We generated a temporary email address on GuerillaMail, a service provider of disposable email addresses. The disposable email address was wrikbdjc@grr[.]la.



We ran the email address on Email Verification API, and as expected, the tool detected that the email address is disposable (disposableCheck>true).



By preventing users with disposable email addresses from reaching your corporate inbox, you minimize the risk of threat actors gaining access to your website.

Detecting Homograph Attacks Masquerading as Typos

By definition, homographs are two or more words that are spelled the same but may have different pronunciations or meanings. The word “bow,” for example, can mean to bend the upper part of the body to greet another person, but it could also refer to a weapon used for shooting arrows. And it looks like fraudsters have found a way to use homographs in cyberattacks, too.

Since the Internet Corporation for Assigned Names and Numbers (ICANN) allows the use of non-Latin characters in domains, threat actors can potentially use homographs in their phishing campaigns. All they have to do is replace a character with a confusable one and pretend to be someone else. In a research paper proving that homograph attacks work, the researchers included their final list of confusable characters:

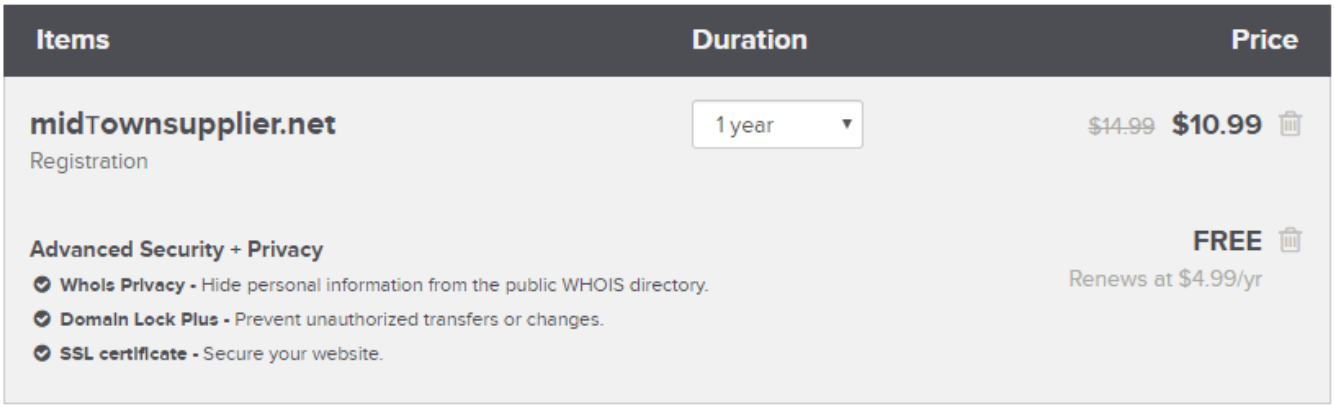
A	B	C	E	F	G	H	K	L	M	N	O	P	R	S	T	U	V	X	Z
A	B	C	E	F	G	H	K	L	M	N	O	P	R	S	T	U	V	X	Z
											O	P			T			X	
															T			X	

a	c	e	i	j	o	p	s	v	w	x	z
a	c	e	i	j	o	p	s	v	w	x	z
	c			j				v			
	c										

On the top row are the Latin characters. The succeeding rows show their confusable Unicode character counterparts.

Consider a scenario where phishers want to masquerade as someone from the accounting department of a company's supplier. They can just register a domain that replaces any character in the supplier's domain name with a confusable character, and send an email requesting for payment.

For example, bad actors can masquerade as midtownsupplier.net by replacing "t" with its Cyrillic equivalent, "т" so it becomes midтownsupplier[.]net. Such a domain can be bought with certain registrars:



At its simplest form, a homograph attack makes use of alphanumeric characters so that google.com becomes g00gle[.]com. In our illustration above, the “o” in midtownsupplier.net can also be replaced with “0”, thus becoming midt0wnsupplier[.]net.

Email Verification API can detect such misleading typos.

In short, while email remains a significant platform of communication, it is also a very common cyberattack vector. Organizations must, therefore, think through their current email security posture and include every possible process that can better protect them.

Email address validation using Email Verification API should be among a company’s **email security best practices** as it can help filter out potentially malicious emails used by hackers, spammers and phishers.