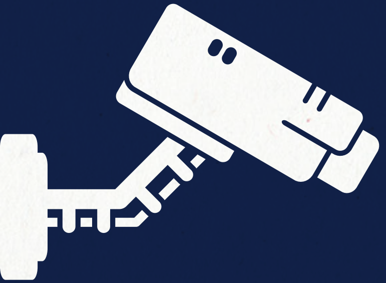


validity

How to Prevent Email Compromises with 24/7 Monitoring

Compromises can happen when you least expect them.

Your email program can be compromised at any time, from a slip in best practices to being maliciously attacked. Over the past couple of years, there have been significant leaps in technology that make it easier for bad actors to take advantage of companies who are not prepared.

If a compromise happens and goes unnoticed, it can very quickly wreak havoc on both your sender reputation and brand reputation. During these times, it can be difficult to know exactly what to do next, how to remedy the situation, and how to prevent future attacks.

Top issues uncovered

In today's cybersecurity landscape, swift action is essential to prevent potential disruptions and data breaches.

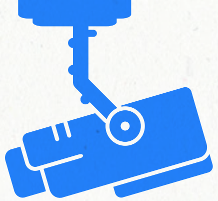
The fallout from data breaches and cyber-attacks can be devastating for businesses, leading to financial losses, reputational damage, and operational disruption. (The average cost of a data breach reached an all-time high of $4.45 million in 2023.) We also know that data compromises and exposure of sensitive information can lead to identity theft, fraud, and compliance violations.

Based on our extensive monitoring data from the past two years, we've identified the top security issues affecting businesses today:

Web form abuse	Illegitimate use of web forms to submit false, malicious, or excessive information, often leading to system vulnerabilities or data breaches.
Phishing attacks	Deceptive tactics used to trick individuals into divulging sensitive information (e.g., usernames, passwords, credit card details) through fraudulent emails or websites impersonating trusted entities.
Compromised user credentials	Unauthorized access to user accounts due to leaked, stolen, or guessed login credentials, posing significant risks to data security and privacy.
Spoofing incidents	Falsifying data, identity, or communication sources to deceive or gain unauthorized access. These include IP spoofing and email spoofing.

DID YOU KNOW?

70% of the critical issues Validity has identified for senders in the last two years fall into these categories!



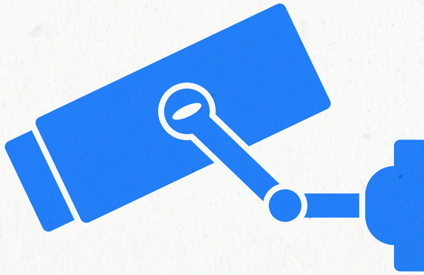
How to reduce risk

No company is infallible, but taking proactive measures can significantly reduce your risk of falling victim to harmful cybersecurity issues.

Here are key actions our clients take to fortify their defenses:

- **Enhance web form security:** Implement stringent validation measures and CAPTCHA protocols to mitigate the risks of web form abuse.
- **Heighten phishing awareness:** Conduct regular employee training on recognizing phishing attempts and adopt advanced email security solutions.
- **Strengthen authentication practices:** Enforce multi-factor authentication (MFA) and password hygiene policies to protect against credential compromises.
- **Implement anti-spoofing measures:** Use SPF, DKIM, and DMARC protocols to authenticate email senders and prevent spoofing attacks.
- **Practice proactive monitoring:** Leverage a service that offers continuous monitoring and rapid response measures.

Validity's Sender Certification program prioritizes swift action to address these critical threats and protect your business from potential consequences. Through continuous monitoring and rapid response measures, we're committed to safeguarding your organization's digital assets and ensuring operational continuity.



Other email issues on the rise

Bot Attacks – Compromised API Keys - Malware

Bot attacks

Automated and malicious activities performed by bots (software robots) with the intent to disrupt services, exploit vulnerabilities, or carry out fraudulent actions.

Compromised API keys

Unauthorized access or theft of API keys used for authentication and interaction with email services.

Malware

When someone clicks on a link or downloads content within a malicious email, it may contain viruses, ransomware, worms, malware or trojans. When that content is downloaded, it provides bad actors access to your network.

We've got your back.

Threats within the email landscape are increasing quickly—but you don't have to face them alone.

Completing Validity's Sender Certification program means you gain access to a team of experts who always have your back—literally. We monitor your email program 24 hours a day, 7 days a week, 365 days a year for any suspicious or unusual activity.

If unusual activity is detected, we notify you immediately and work with you through the resolution.

Learn more about Validity's 24/7 email monitoring capabilities.