Email Reputation detects if criminals have access to an email inbox, and if so, when it was first compromised. It also quantifies the likelihood that a given email address was created solely for the purposes of fraud (e.g., for use with a synthetic identity).

150 THOUSAND

newly-compromised email account credential pairs are added to our database daily

EMAIL REPUTATION FIGHTS ATO/MALICIOUS CONDUCT

Email Reputation is delivered via an easy-to-use API with straightforward responses that can be integrated into other business systems. Early detection of a high-risk email—or one with no reputation—is a valuable signal that enables your organization to thwart many types of attacks and prevent ATO by knowing:

- Is an email authentic or synthetic?
- Is the email actively compromised? We see live data compromise.
- What is the risk the email could be compromised?

BUSINESS USE CASES

Identify Business Email Compromise

Trust and reputation around an email address is paramount when it centers around B2B transactions and business users. Business email compromise (BEC) leads to misdirected payments and other issues, especially when the email of one of your organization's leaders is taken over. myNetWatchman's *Email Reputation* can provide indication of whether or not that email account is compromised, mitigating the threat of misdirected payment.

myNetWatchman proved the value of *Email Reputation* working with a cyber insurance provider who received an insurance claim related to a misdirected payment. After making a call to the *Email Reputation* API, they discovered that the email address of the company's CEO was compromised and had been actively accessed by a fraudster over a two-month period leading up to the misdirected payment.

Identify Compromised Emails at Password Recovery

A consumer's email inbox is the key to their online castle. If that email account is taken over by a bad actor, other user accounts associated with that email are vulnerable to ATO as well. If you rely on email to send one-time passcodes (OTPs) or use email to complete password recovery or resets, it is critical to have an indication of the level of risk associated with that email address. *Email Reputation* helps you prevent handing these digital keys to a fraudster who has taken over a legitimate user's email inbox.

Protect new accounts from being created for malicious use in synthetic identities

17	MILLION COMPROMISED EMAILS IN OUR EVER-EXPANDING DATABASE
15	MILLION NEWLY-COMPROMISED CREDENTIAL PAIRS ADDED DAILY TO OUR DATABASE
35+	BILLION UNIQUE, COMPROMISED CREDENTIAL PAIRS IN OUR EVER-EXPANDING DATABASE

Assess Email Risk at Account Creation

When new user accounts are created and an email address is supplied (or when an existing account changes their associated email address), your call to the *Email Reputation* API quantifies the quality of that email address. No trace or prior use of that email indicates it may be synthetic—a useful signal to help determine if the user is legitimate, or if they created the provided email address for the purposes of committing fraud.

Identifying bad new accounts early on saves the time and resources of further vetting them. myNetWatchman clients using *Email Reputation* are able to reduce operational costs by not conducting further identity authentication, verification, or manual reviews on junk data or on malicious actors using synthetic emails for nefarious purposes.

myNetWatchman

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech