GARY ASHTON
RE/MAX
ADVANTAGE

Case Study: The Ashton Real Estate Group

Securing Hundreds of Dormant Domains
Through DMARC Monitoring

Website
www.sh.consulting

Email
hello@sh.consulting

01 Background

GARY ASHTON RE/MAX ADVANTAGE

The Ashton Real Estate Group owns and manages hundreds of domains, but actively sends customer-facing email from only a handful of them.

SH Consulting connected the full domain portfolio — 364 domains — to our DMARC monitoring platform to understand what traffic was actually flowing through them and identify domains that needed attention.

The goal was straightforward: identify unwanted or abusive traffic across a large, mostly dormant domain portfolio, protect those domains from unauthorized use, and properly configure the handful of domains with legitimate active sending.

02 The Challenge

GARY ASHTON RE/MAX ADVANTAGE

Of the 364 domains connected to monitoring:

81 showed traffic within a trailing 30-day window

2 of those 81 had a legitimate, active use case but were misconfigured, failing SPF and DKIM

The remaining 79 were supposed to be dormant, yet showed a slow, low-volume stream of unauthenticated traffic from IPs in Russia, China, Hong Kong, Greece, the UK, Korea, and other locations

None of the dormant domains had a DMARC reject policy in place, leaving them exposed to continued unauthorized use

02 The Challenge

GARY ASHTON RE/MAX ADVANTAGE

DMARC	DISPOSITION	DOMAIN	HOSTNAME	SOURCE IP	DKIM	SPF	REPORT ORIGIN
fail	none	tnrealestate.com	—	193.58.122.93	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	114.249.210.133	✗	✗	Mail.Ru
fail	none	tnrealestate.com	*.ttk.ru	176.115.89.218	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	130.49.122.9	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	114.252.189.114	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	180.165.55.28	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	105.27.180.194	✗	✗	Mail.Ru
fail	none	tnrealestate.com	*.nsfocus.cloud	212.58.132.5	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	114.241.201.180	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	147.45.66.117	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	114.249.225.232	✗	✗	Mail.Ru
fail	none	tnrealestate.com	*.voiceip.ru	176.106.233.236	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	141.133.39.32	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	147.45.218.117	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	1.231.81.166	✗	✗	Mail.Ru
fail	none	tnrealestate.com	*.vnpt.vn	113.168.17.42	✗	✗	Mail.Ru
fail	none	tnrealestate.com	—	183.243.104.234	✗	✗	Mail.Ru

One dormant domain, tnrealestate.com, showed repeated unauthenticated traffic from multiple sources. Every source shown in the DMARC data failed both SPF and DKIM.

02 The Challenge

GARY ASHTON RE/MAX ADVANTAGE

The core issue is that a domain does not have to be actively used to accumulate reputation damage. Unauthorized traffic can continue unnoticed for months on a dormant domain, potentially building a negative sending history with mailbox providers before the business ever begins using that domain legitimately. When the domain is eventually activated, that history can make it harder to establish strong deliverability from the start.

03 The Approach

GARY ASHTON RE/MAX ADVANTAGE

SH Consulting addressed the portfolio through two parallel tracks: fix what was actively misconfigured and lock down what was not supposed to be sending mail.

Track 1: Active Domain Remediation

Two domains showing traffic had legitimate active use cases but were failing email authentication. SH Consulting corrected their SPF and DKIM configuration so authentication passed properly.

This provided:

- Full authentication alignment for domains already in active use
- Removal of the immediate deliverability risk caused by misconfigured authentication
- Continued visibility into sending volume and sending sources

03 The Approach

GARY ASHTON RE/MAX ADVANTAGE

Track 2: Dormant Domain Lockdown

For the 79 dormant domains showing low-volume unauthorized traffic, SH Consulting is applying a security configuration that includes a strict DMARC p=reject policy along with supporting DNS controls.

MX	@	. (Priority: 0)	1 Hour
TXT	@	v=spf1 -all	1 Hour
TXT	*._domainkey	v=DKIM1; p=	1 Hour
TXT	_dmarc	v=DMARC1; p=reject; rua=mailto:ga@dmarc.sh; ruf=mailto:ga@dmarc.sh; adkim=s; aspf=s; fo=1:d:s	1 Hour

The lockdown record set applied to each dormant domain. A null MX tells receivers the domain does not accept mail; v=spf1 -all declares that no server is authorized to send for it; an empty wildcard DKIM key revokes any selector that might have existed; and DMARC p=reject with strict alignment instructs mailbox providers to discard anything that fails.

03 The Approach

GARY ASHTON RE/MAX ADVANTAGE

Phase 1: Applying DMARC reject policies and supporting security configuration across dormant domains showing unauthorized traffic

Expected outcome: Stopping ongoing unauthorized traffic from continuing to build negative sending history and damage the domains' future email reputation

Phase 2: Continuing passive DMARC monitoring so any future legitimate use can be identified and configured before sending begins

Success metric: Keeping dormant domains protected and better positioned for future legitimate use

04

Portfolio-Wide Visibility

GARY ASHTON RE/MAX ADVANTAGE

Monitoring the full portfolio gave SH Consulting and
The Ashton Real Estate Group visibility that did not exist before:

364 domains connected to DMARC monitoring

81 domains found to have email traffic

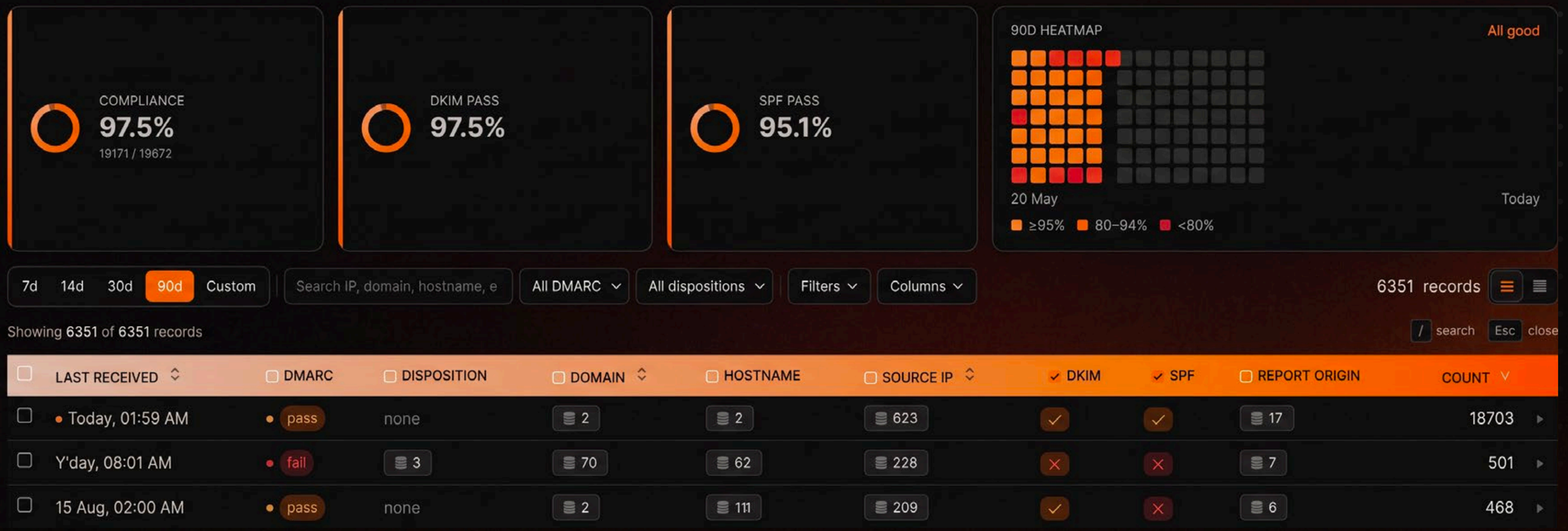
79 dormant domains identified as generating
low-volume unauthenticated or abusive traffic

2 domains identified as misconfigured despite legitimate
active use and subsequently corrected

04

Portfolio-Wide Visibility

GARY ASHTON RE/MAX ADVANTAGE



Portfolio-level view across all monitored domains: overall DMARC compliance, DKIM and SPF pass rates, and a 90-day heatmap showing where failures cluster.

04 Portfolio-Wide Visibility

GARY ASHTON RE/MAX ADVANTAGE

Instead of evaluating domains individually, the entire portfolio could now be viewed from one place, making it possible to identify which domains were sending, which were experiencing unauthorized activity, and which were completely quiet.

05

Example

GARY ASHTON RE/MAX ADVANTAGE

nashvillerealestate.com

The same monitoring also covers the client's active, high-volume domains.
For nashvillerealestate.com, the data showed:

- More than 99% DMARC/authentication compliance
- Sending sources clearly attributed across Mandrill, Google Workspace, and Follow Up Boss
- Approximately 72% of traffic coming from Mandrill
- Approximately 18% from Google Workspace
- Approximately 10% from Follow Up Boss
- No unexplained or suspicious sending sources identified

05 Example

GARY ASHTON RE/MAX ADVANTAGE

Over a 90-day period, the domain generated approximately 1.19 million messages with 99.69% DMARC compliance, while every sending IP was identified.

06 Key Insight

GARY ASHTON
RE/MAX
ADVANTAGE

DMARC aggregate data provides a centralized view of a domain's sending activity across multiple email services.

That visibility goes well beyond a simple pass/fail authentication rate. It makes it possible to identify which IPs and providers are sending mail, detect configuration problems before they become larger deliverability issues, and surface unauthorized activity on domains nobody may be actively watching.

At portfolio scale, that visibility becomes especially valuable.

07

The Value Delivered

GARY ASHTON RE/MAX ADVANTAGE

1. Reputation Protection at Scale

Monitoring and locking down dormant domains before unauthorized activity compounds helps protect their future sending reputation. If one of those domains is later activated for legitimate email, the goal is to start from a clean position rather than having to overcome a negative history that accumulated while nobody was watching it.

2. Early Detection of Unauthorized Activity

Low-volume abusive traffic on domains that were not expected to send email became visible through DMARC reporting, allowing it to be addressed before it developed into a larger problem.

3. Visibility Into Email Infrastructure

DMARC data shows exactly which services and IP addresses are sending mail on behalf of a domain.

For active domains, this gives the client a clear picture of platforms such as Mandrill, Google Workspace, Follow Up Boss, and other providers, including changes in sending infrastructure over time.

4. Clear, Ongoing Reporting

Live DMARC data provides a continuously updated view of domain health, authentication performance, sending volume, and source attribution.

That makes it easier for both the client and their IT team to understand what is happening across the portfolio without manually investigating hundreds of domains individually.

08 The Takeaway

GARY ASHTON
RE/MAX
ADVANTAGE

A dormant domain is not necessarily a harmless domain. If unauthorized mail is flowing through it while nobody is watching, the domain can accumulate a negative sending history long before the business ever decides to use it. The problem may only become visible later, when legitimate email is launched and the domain has to overcome reputation issues that could have been prevented.

08 The Takeaway

GARY ASHTON RE/MAX ADVANTAGE

The Ashton Real Estate Group's case demonstrates why visibility and policy enforcement need to work together at scale:

Monitoring creates visibility

Connecting the entire domain portfolio to DMARC reporting surfaces activity that would otherwise go unnoticed.

Policy limits unauthorized use

Strict DMARC policies on dormant domains make successful spoofing significantly more difficult.

Preparedness protects future deliverability

Domains that are monitored and locked down while dormant are better positioned to establish strong sender reputation when they are eventually activated.

For organizations managing dozens or hundreds of domains, the goal is not simply to secure the domains they actively send from. It is to understand and control the entire portfolio.

GARY ASHTON
RE/MAX
ADVANTAGE

Email Deliverability.
Security. Compliance.

SH Consulting

Website
www.sh.consulting

Email
hello@sh.consulting