SafePoint IT

› Cybersecurity Brief

Is Someone Pretending to Be Your Agency?

A plain-language guide to email impersonation risk for creative agency owners.

The short version: If your domain doesn't have proper email authentication in place, attackers can send emails that look exactly like they came from you — your clients, vendors, and team have no easy way to tell the difference. Most agencies don't know they're exposed until it's already happened.

Why This Matters For an Agency Like Yours

Creative agencies live in email. You send proposals, invoices, file links, NDAs, and "quick favor" requests every day. That's exactly what makes you a high-value target — and what makes the impersonation risk so quiet.

An attacker doesn't need to hack into your systems. They just need to send an email that *looks* like it came from you. If your domain isn't locked down, most email systems will let it through.

SIMPLE ANALOGY

Think of it like a return address. Anyone can write your studio's address on the back of an envelope — that doesn't mean the letter actually came from you. Email works the same way by default. Email authentication (the technical setup we're talking about) is what tells the post office to refuse mail with a forged return address. Without it, the forged letters get delivered.

What Happens When You're Exposed

RISK 01

Fake Invoices

A client receives an "updated invoice" from your domain with new wire instructions. They pay it. The money's gone before anyone notices.

RISK 02

Wire Fraud Requests

A vendor or freelancer gets an email "from the owner" asking for a quick payment or gift cards. The tone is right. The signature looks right.

RISK 03

Malicious File Links

Clients receive a "revised brief" or "project files" link from your address. One click installs malware on their network — and your name is attached to it.

The damage isn't only financial. It's reputational. Once a client gets burned by a fake email "from your agency," explaining the technical details after the fact rarely repairs the trust.

How To Tell If You're Exposed (Without a Technical Background)

There are three records that need to exist on your domain: **SPF**, **DKIM**, and **DMARC**. You don't need to understand how they work — just whether they're properly configured.

- ✓ **SPF** — Lists who's allowed to send email as your domain
- ✓ **DKIM** — Adds a tamper-proof signature to your outgoing mail
- ✓ **DMARC** — Tells receivers what to do with mail that fails the first two
- ✓ **The catch** — All three need to exist *and* be set correctly

Many agencies have one or two of these in place but with weak settings (e.g. DMARC set to "monitor only" instead of "reject"). That's the equivalent of installing a security camera but never turning it on.

A 5-Minute Self-Check You Can Do Today

This won't replace a proper assessment, but it'll tell you whether the topic deserves more of your attention.

1. **Go to mxtoolbox.com.** It's a free public tool — no login required.
2. **Enter your domain** (e.g. *youragency.com*) and run a DMARC lookup.
3. **Read the result.** If you see "No DMARC Record found," you're fully exposed. If you see *p=none*, you're partially exposed (monitoring but not blocking). If you see *p=quarantine* or *p=reject*, you're protected — but it's still worth verifying SPF and DKIM are aligned.
4. **If anything looks wrong, don't try to fix it yourself.** Misconfigured records can break your legitimate email overnight — your team stops sending, your campaigns stop landing. Get someone who's done it before.

What This Looks Like When It's Done Right

A properly hardened email setup does three things, quietly, in the background:

- **Blocks impersonation attempts** at the receiving server, before they ever hit your client's inbox.
- **Sends you a report** every time someone tries to spoof your domain — so you actually know it's happening.
- **Improves your real deliverability.** Authenticated domains land in inboxes more reliably. Your proposals stop landing in spam.

For most small agencies, the full setup is a one-time configuration project (typically a few hours of work) plus light ongoing monitoring. It's not expensive. It's just rarely prioritized — until it has to be.

Common Misconceptions

"We use Google Workspace / Microsoft 365 — aren't we covered?"

No. Those platforms make it *possible* to set up authentication, but they don't do it for you. Out of the box, your domain is not protected.

"We're too small to be a target."

Small agencies are *preferred* targets. Less mature security, smaller IT budgets, fewer people checking, and clients who already trust your brand. Attackers automate this — they don't pick targets, they scan for them.

"Our IT person handles email."

Worth verifying. Email authentication sits in DNS, not in the email platform itself, and it's commonly missed by generalist IT support unless someone's specifically asked them to address it.

> **Bottom line:** Whether or not you ever work with us, this is worth checking. The 5-minute lookup above will tell you where you stand. If you're exposed and want it handled cleanly, that's a conversation we have often.

Want to know exactly where your agency stands?

Our Security & Access Risk Assessment includes a full audit of your email authentication posture — plus the other quiet exposures most small businesses don't know to look for.

Alek Pirkhalo
alekp@safepointit.com
(847) 499-1500

This document is for informational purposes. Specific configurations should be reviewed by a qualified IT or cybersecurity professional based on your business's actual environment.