

Small Business Email Security Checklist

From the dotbm workshop "Stop fake emails from your business". Hand it to whoever manages your email and domain; the last column is the question to ask them.

DOMAIN	EMAIL PROVIDER	CHECKED BY AND DATE
CHECK	WHY IT MATTERS	WHAT TO ASK YOUR IT PROVIDER
☐ SPF: exactly one record, listing every service that sends as you, ending in -all or ~all.	Tells receivers which servers may send for you. Missing or broken, your real mail looks less trustworthy.	Do we have one SPF record covering every system that sends as us (accounting, booking, website forms), within the 10-lookup limit?
☐ DKIM: signing switched on for your own domain, in every service that sends as you.	A seal that survives forwarding. Needed for DMARC to recognise your genuine mail.	Is DKIM signing enabled for our domain in our mail provider and every other sending service? Which selectors do we use?
☐ DMARC: a valid record at _dmarc.yourdomain, with reports going somewhere someone reads.	Ties SPF and DKIM to the From address customers see, and reports who is sending as you.	Do we have a valid DMARC record? Where do the reports go, and who reviews them?
☐ DMARC enforcement: policy at quarantine or reject, applying to all mail.	Monitor (p=none) blocks nothing. Only enforcement asks receivers to stop forged mail.	When can we move from p=none to quarantine, then reject? Which genuine senders still fail?
☐ Two-step sign-in (MFA) on every mailbox, including shared and unused ones.	A stolen password alone is no longer enough to get in.	Is MFA enforced on every account, admins included? Are older sign-in methods that skip it turned off?
☐ Admin accounts kept separate from everyday email, with strong MFA.	A phished daily mailbox should not hand over control of the whole system.	Who has admin rights on our email and domain? Are those accounts separate from day-to-day logins?
☐ A password manager. No shared or reused passwords.	Passwords leaked from other sites are tried against business mailboxes automatically.	Can we set up a business password manager, with shared vaults for logins we must share?
☐ Payment changes verified by phone, on a number already on file, and approved by a second person.	Catches every kind of fake invoice, including lookalike domains and hacked mailboxes.	Can our mail system tag outside senders and warn on lookalikes of our regular suppliers? (Ask the bank about dual approval for new payees.)
☐ Suspicious invoices have a named person to go to, and holding a payment to check is expected.	If money has moved, the first hours matter most for getting it back.	How do staff report a suspicious email, and how quickly can you check who else received it and block the sender?
☐ Recovery phone numbers, recovery emails and the domain registrar login belong to the business.	Whoever controls recovery controls the account. Whoever controls the domain controls all of your email.	Who is listed as recovery contact and domain administrator for us? Can we have that written down?
☐ Everyone who handles email knows the four kinds of fake email and the bank-details rule.	Settings stop forgeries of your exact domain. People stop the rest.	Can you add an "External" tag to outside mail and give us a short guide to reporting phishing?

Check your domain's public settings at dot.bm/security-check. This checklist covers common protections; it is not a full security assessment. dotbm, October 2026.