



Cybersecurity for Small Business

Email Authentication

Some web host providers let you set up your company's business email using your domain name (which you may think of as your website name). For example, your domain name might look like yourbusiness.com, and your email may look like name@yourbusiness.com. Without protections in place, scammers can use your domain name to send phishing emails that look like they're from your business.

You can help protect your business and customers by using email authentication technology, which makes it a lot harder for scammers to spoof your company's email. It works by allowing a receiving server to verify emails from your company. Emails from imposters are either blocked or sent to a quarantine folder for further review.

What to know.

- If your business email uses your company's domain name, make sure your email provider has these three email authentication tools:
 - **Sender Policy Framework (SPF).** SPF verifies that a mail server is allowed to send email for a given domain.
 - **Domain Keys Identified Mail (DKIM).** DKIM puts a digital signature on outgoing mail so servers can verify that an email from your domain was sent from your organization's servers and hasn't been tampered with in transit.
 - **Domain-based Message Authentication, Reporting & Conformance (DMARC).** DMARC is the third essential tool for email authentication. SPF and DKIM verify the address the server uses "behind the scenes." DMARC verifies that this address matches the "from" address you see. It also lets you tell other servers what to do when they get an email that looks like it came from your domain, but the receiving server has reason to be suspicious (based on SPF or DKIM). You can have receiving servers reject the email, flag it as spam, or take no action. You also can set up DMARC so that you're notified when this happens.

- It takes some expertise to configure these tools so they work as intended and don't block legitimate emails. Choose an email provider that can set them up if you don't have the technical knowledge.

What to do if your email is spoofed.

Email authentication lets you know you if someone spoofs your company's email. If you get a notification that your email has been spoofed:

- **Report it.** Report the scam to local law enforcement, the FBI's Internet Complaint Crimes Center at [IC3.gov](https://www.ic3.gov), and the FTC at [ReportFraud.ftc.gov](https://www.reportfraud.ftc.gov). You can also forward phishing emails to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies).
- **Notify your customers.** If you find out scammers are impersonating your business, tell your customers as soon as possible. If you email your customers, send an email without hyperlinks. You don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers' data was stolen, direct them to [IdentityTheft.gov](https://www.identitytheft.gov) to get a recovery plan.
- **Alert your staff.** Give your staff guidance on how to respond to customers. Take this opportunity to update your security practices and train your staff about cyberthreats.