CYBERSECURITY FOR
SMALL BUSINESS

EMAIL AUTHENTICATION

Email authentication technology makes it a lot harder for a scammer to send phishing emails that look like they're from your company.

Using email authentication technology makes it a lot harder for scammers to send phishing emails. This technology allows a receiving server to verify an email from your company and block emails from an imposter — or send them to a quarantine folder and then notify you about them.

WHAT TO KNOW —

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). Your domain name might look like this: yourbusiness.com. And your email may look like this: name@yourbusiness.com. Without email authentication, scammers can use that domain name to send emails that look like they're from your business. If your business email uses your company's domain name, make sure that your email provider has these three email authentication tools:

Sender Policy Framework (SPF)

tells other servers which servers are allowed to send emails using your business's domain name. So when you send an email from name@yourbusiness.com, the receiving server can confirm that the sending server is on an approved list. If it is, the receiving server lets the email through. If it can't find a match, the email can be flagged as suspicious.

Domain Keys Identified Mail (DKIM)

puts a digital signature on outgoing mail so servers can verify that an email from your domain actually was sent from your organization's servers and hasn't been tampered with in transit.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

is the essential third 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 other 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 that they work as intended and don't block legitimate email. Make sure that your email hosting provider can set them up if you don't have the technical knowledge. If they can't, or don't include that in their service agreement, consider getting another provider.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION
Homeland Security
NIST National Institute of Standards and Technology U.S. Department of Commerce
SBA U.S. Small Business Administration

CYBERSECURITY FOR
SMALL BUSINESS

WHAT TO DO IF YOUR
EMAIL IS SPOOFED

Email authentication helps keep your business's email from being used in phishing schemes because it notifies you if someone spoofs your company's email. If you get that notification, take these actions:

Report it

Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at IC3.gov, and the FTC at FTC.gov/Complaint. You also can forward phishing emails to spam@uce.gov (an address used by the FTC) and 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 — by mail, email, or social media. 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. And if your customers' data was stolen, direct them to IdentityTheft.gov to get a recovery plan.

Alert your staff

Use this experience to update your security practices and train your staff about cyber threats.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration