



EMAIL

SECURITY 101

FOR SMALL BUSINESSES

*Why Email Is Your Biggest Risk & How To
Lock It Down*



READ MORE



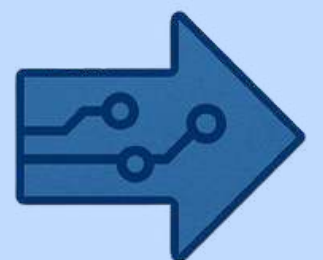
EMAIL IS THE #1 ENTRY POINT FOR CYBER THREATS

*Email is more than just communication—it's a gateway
to your business.*

RANGING FROM PHISHING AND SPOOFING
TO DATA LEAKS AND MALWARE. IT'S
WHERE BUSINESS HAPPENS, AND WHERE
BREACHES BEGIN.



LISTEN TO THESE TIPS TO SECURE YOUR
EMAIL, AND YOUR BUSINESS

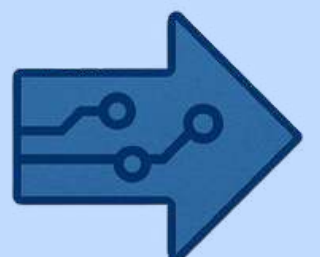


Tip #1

USE STRONG AUTHENTICATION

Passwords alone aren't enough. MFA adds a critical layer of protection to every inbox.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA) FOR ALL EMAIL ACCOUNTS. IT'S ONE OF THE SIMPLEST WAYS TO BLOCK UNAUTHORIZED ACCESS.

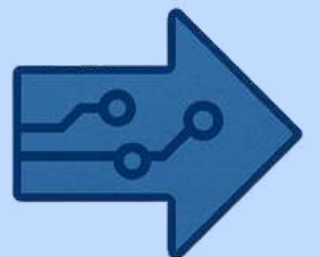
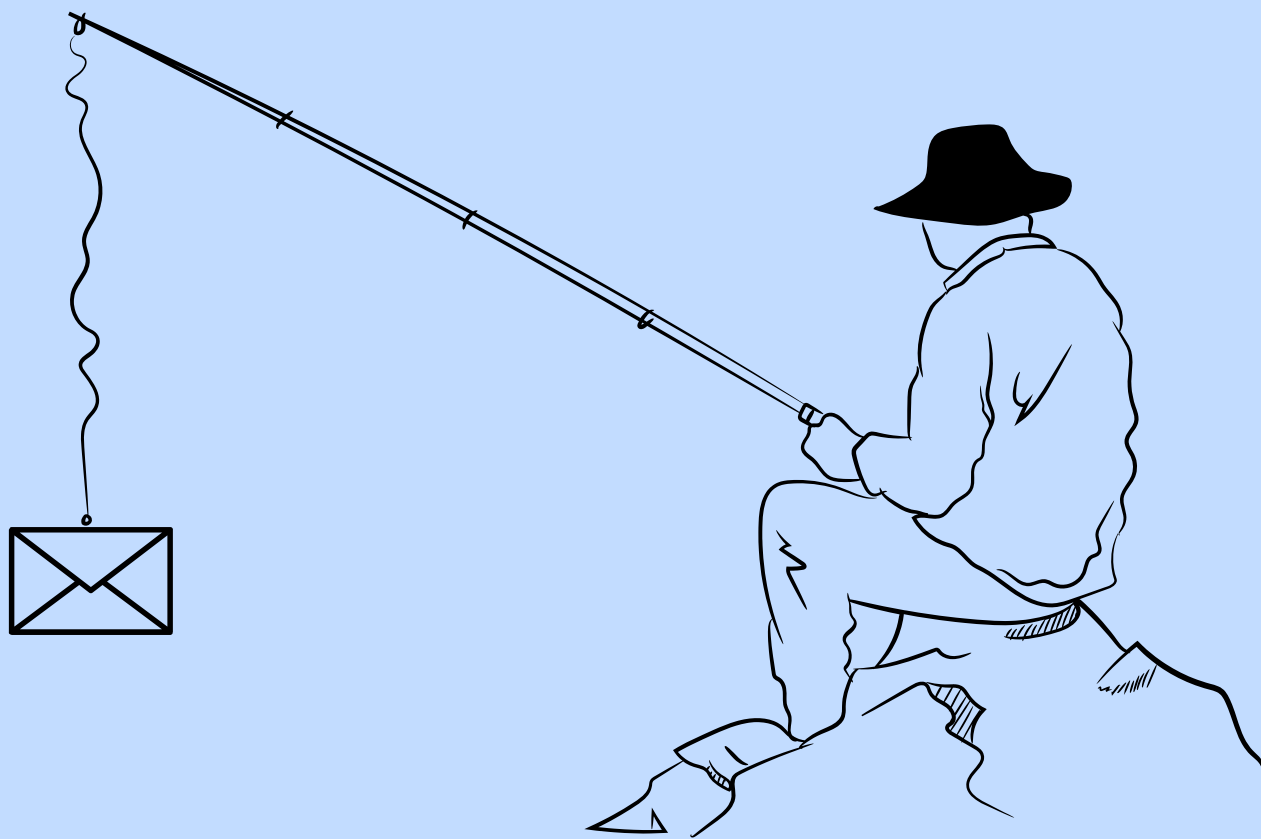


Tip #2

LEARN HOW TO SPOT PHISHING

Most phishing emails look real. Train your team to pause before they click.

- LOOK FOR MISSPELLINGS, STRANGE URLS, AND URGENT LANGUAGE.
- ENCOURAGE REPORTING SUSPICIOUS MESSAGES.

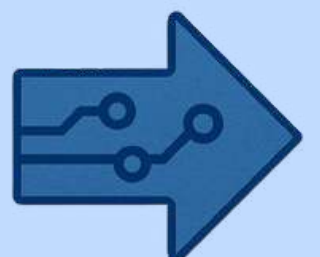


Tip #3

SECURE YOUR DOMAIN

Without proper tools attackers can impersonate your business. These records help keep your brand—and your customers—safe.

SET UP SPF, DKIM, AND DMARC
RECORDS TO PREVENT SPOOFING AND
PROTECT YOUR BRAND FROM
IMPERSONATION ATTACKS.

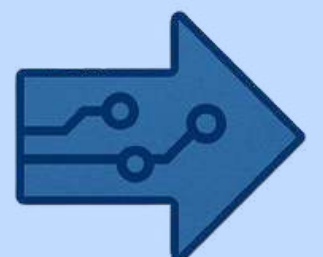


Tip #4

TRAIN YOUR TEAM

Your employees are your first line of defense. Regular training helps them spot threats before they become problems.

REGULARLY EDUCATE EMPLOYEES ON EMAIL SAFETY—HOW TO SPOT SUSPICIOUS LINKS, VERIFY SENDERS, AND REPORT THREATS.



WANT MORE SIMPLE, NON-TECHNICAL WAYS TO PROTECT YOUR BUSINESS?

JOIN OUR NEWSLETTER AND DOWNLOAD OUR **FREE SMB IT CHECKLIST** TO START SECURING YOUR EMAIL, AND YOUR BUSINESS TODAY.



JOIN AT

A search bar with a magnifying glass icon on the left and an 'X' icon on the right. The text 'WWW.SBTPARTNERS.COM' is entered into the search field.