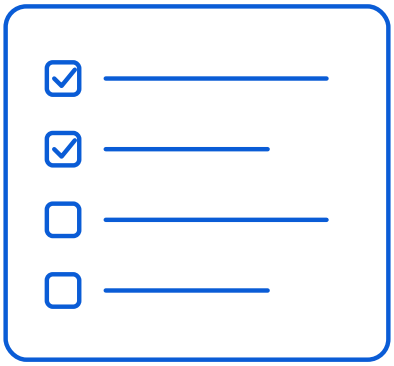
MMI | NYC

A FREE GUIDE FOR NYC SMALL BUSINESS OWNERS

You Turned On MFA. Good. Here's the Rest of the Picture.

A plain-English checklist for New York small business owners



getmmi.com · (646) 964-6501

Start here

If you've turned on multifactor authentication (MFA), the extra code or phone prompt when you sign in, you've already done something that matters. CISA, the federal cybersecurity agency, calls it "a simple, effective step that can block many common cyberattacks and significantly reduce the risk of account compromise."

MFA protects one thing very well: the moment someone signs in. A well-run office also covers what's around that moment:

- which accounts have MFA
- what kind of MFA you're using
- who has access
- how you'd recover if something went wrong

This guide walks through eight quick checks. None of them needs a big budget. Some take five minutes, and some are a single question to your IT person or provider. At the end there's a short list you can start this week.

> ✓ Whether you handle tech yourself, have someone in-house, or work with an outside provider, the goal is the same: **make sure you're getting the protection you think you have.**

CHECK 1:

Is MFA on everywhere that matters?

CISA notes that most people who use MFA have it on banking and financial accounts, but far fewer have it on work accounts. That's an easy gap to close, since your email is often what resets every other password.

CISA's advice to small and medium businesses is to "require MFA wherever possible." That means systems like **email, file storage, and remote access**, starting "with admin accounts and employees who handle sensitive data." The FTC adds that MFA should cover "all employees, contractors, and others who access your network and devices."

A practical list to check:

- Business email (Microsoft 365 or Google Workspace), for every user, not just you
- Admin accounts for those systems
- Online banking and payroll
- Accounting software
- Your website host and domain registrar
- Remote access tools and shared file storage

> **If your office runs on Microsoft 365:** Microsoft offers a baseline setting called "security defaults" at no extra cost. It requires everyone to register for MFA, requires MFA for administrators, and blocks older sign-in methods that skip MFA. Microsoft notes that offices on certain higher-tier plans usually use more tailored "Conditional Access" policies instead. Either way, it's worth asking which one you're on.

CHECK 2:

Is it the stronger kind?

Not all MFA is equal. CISA ranks the common options from strongest to weakest:

1. **Security key**, a small physical key that plugs in or taps your device
2. **Authenticator app with number matching**, where you type the number shown on screen
3. **Authenticator app with a one-time code**
4. **Biometrics** (fingerprint or face), best paired with another method
5. **Text or email code**, which CISA says "provides the weakest protection"

CISA is clear that "any MFA is better than none." The point isn't to worry about text codes. It's to know there's an easy upgrade.

NIST points out that phishing-resistant options are now often built into phones and laptops (passkeys). It says these tools "are often easier, faster, and more convenient than" text codes. A good first step is to move admin accounts and email to an authenticator app or a passkey.

CHECK 3:

Who still has access?

MFA confirms that the person signing in is the account owner. It doesn't decide whether that person should still have an account.

The FTC recommends that small businesses "restrict sensitive information access to only those who need it to do their jobs." For vendors, it recommends access "on a need-to-know basis, and only for the time the vendor needs to do the job."

A quick review:

- Are there accounts for people who've moved on?
- How many people have admin rights? Fewer is usually better.
- Do past vendors or contractors still have logins?

CHECK 4:

Are updates happening on their own?

CISA calls outdated software "one of the most significant security risks to your business." It recommends turning on automatic updates "where possible, including operating systems, applications and third-party software." It also recommends replacing devices and software that no longer get security updates.

Don't forget the office router and Wi-Fi. The FTC suggests changing the router's default username and password, and keeping its software current.

CHECK 5:

Is there a backup you've actually restored from?

The FTC recommends backing up regularly and making sure "those backups are not connected to the network," so you can restore if something goes wrong.

Also try a test restore. Pick one file and bring it back. New York's SHIELD Act lists "regularly tests and monitors the effectiveness of key controls" among its examples of reasonable safeguards. It's also the only way to know the backup works.

CHECK 6:

How does your office confirm money requests?

MFA protects your accounts. It doesn't stop a convincing email from someone pretending to be a vendor who "changed banks."

The FBI's Internet Crime Complaint Center recommends using "secondary channels and/or two-factor authentication to verify requests for changes in account information." CISA adds that staff should verify unexpected requests, "but not by replying or using any phone number or link in the message." Use a contact method you already have instead.

> The simple office habit: **any change to payment details gets a phone call to a number you already have on file.**

CHECK 7:

Is your email domain protected from look-alikes?

If your email uses your company's domain (you@yourbusiness.com), the FTC recommends that your email provider have three settings in place:

- **SPF**
- **DKIM**
- **DMARC**

Together, these make it "a lot harder for scammers to spoof your company's email." The FTC also notes these settings "take some expertise to configure." This is a good one to hand to whoever manages your email.

CHECK 8:

Are you getting what was promised?

If you pay an IT provider or software vendor, it's fair to ask them to show you their security work. The FTC's guidance for small businesses says to put security provisions in vendor contracts, and to "establish processes to confirm that vendors follow your rules. Don't just take their word for it."

New York's SHIELD Act includes the same idea among its examples of reasonable safeguards: "selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract."

Good questions to ask:

- "Can you show me which accounts have MFA, and which type?"
- "When was our last test restore?"
- "Who has admin access today?"

A good provider will be glad you asked.

Know which rules apply to you

Here's a short, conservative overview. Your attorney or accountant can tell you exactly where your business fits.

- **New York SHIELD Act (General Business Law § 899-bb).**
  - Who it covers: any person or business that "owns or licenses computerized data which includes private information of a resident of New York." For many offices, that includes customer or employee records.
  - What it requires: "reasonable safeguards," with administrative, technical, and physical examples listed in the law.
  - Scaling for small businesses: the law defines small businesses by employees, revenue, or assets. For them, safeguards should be "appropriate for the size and complexity of the small business," the nature of its work, and how sensitive the information is.
  - Private information now includes a username or email address combined with a password.
- **FTC Safeguards Rule (16 CFR Part 314).**
  - Who it covers: businesses the rule treats as "financial institutions." The FTC's examples include tax preparation firms, mortgage brokers, collection agencies, finance companies, and some financial advisors.
  - What it requires: among other things, MFA "for any individual accessing any information system," unless a designated Qualified Individual approves an equivalent control in writing.
  - The FTC has exempted businesses with customer information on fewer than 5,000 consumers from certain provisions. The FTC's page explains which ones.
- **Already regulated?** SHIELD treats businesses that comply with certain other security rules as compliant. Examples include HIPAA (healthcare), Gramm-Leach-Bliley (financial), and the NY Department of Financial Services cybersecurity regulation (23 NYCRR Part 500).

> ⚖ The common thread across all of these: know what information you hold, protect it in proportion to your size, and be able to show what you've done.

Start this week: the short list

- [ ] Make a list of your most important logins: email, banking, payroll, accounting, website/domain, file storage.
- [ ] Confirm MFA is on for each, for every user, starting with admin accounts.
- [ ] Switch at least your admin and email accounts from text codes to an authenticator app or passkey.
- [ ] Remove accounts for anyone who no longer needs access, and trim admin rights.
- [ ] Turn on automatic updates on computers, phones, and the browser.
- [ ] Restore one file from your backup to confirm it works.
- [ ] Set the office rule: payment changes get a call-back to a known number.
- [ ] Ask whoever manages your email whether SPF, DKIM, and DMARC are set up.

Sound familiar?

Most owners we talk to have done a good part of this already. The rest usually takes a free afternoon or a few good questions to the right person.

You can work through this list on your own, or we can do it for you. Call **(646) 964-6501** or visit **getmmi.com**.

MMI Integration, LLC · Queens, New York

This guide is general information, not legal advice. Talk to your attorney about how specific laws apply to your business.

Sources (all opened Oct 30, 2026)

1. **CISA**, "Require Multifactor Authentication" (small and medium businesses): https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication
   - Used for: "simple, effective step…"; most MFA users protect banking but far fewer protect work accounts (citing the National Cybersecurity Alliance survey); email, file storage, remote access; start with admin accounts; strongest-to-weakest ranking; "any MFA is better than none"; text codes "weakest protection."
2. **CISA**, "Implementing Phishing-Resistant MFA" (fact sheet, PDF): https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
   - Used for: background on phishing-resistant MFA and push bombing. Not quoted.
3. **CISA**, "Update Business Software": https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/update-business-software
   - Used for: "one of the most significant security risks"; automatic updates; replace end-of-life systems.
4. **CISA**, "Teach Employees to Avoid Phishing": https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/teach-employees-avoid-phishing
   - Used for: verify "not by replying or using any phone number or link in the message."
5. **NIST**, Small Business Cybersecurity Corner, "Multi-Factor Authentication": https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication
   - Used for: phishing-resistant authenticators built into phones and laptops; "often easier, faster, and more convenient."
6. **FTC**, "Cybersecurity for Small Business": https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
   - Used for: MFA for employees, contractors and others; limiting access; vendor access time limits; router passwords; offline backups; SPF/DKIM/DMARC; vendor contracts; "Don't just take their word for it."
7. **FTC**, "FTC Safeguards Rule: What Your Business Needs to Know": https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
   - Used for: examples of covered financial institutions; MFA requirement; the fewer-than-5,000-consumers exemption from certain provisions.
8. **eCFR**, 16 CFR 314.4: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4
   - Used for: 314.4(c)(5) MFA text.
9. **NY Attorney General**, SHIELD Act overview: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
   - Used for: safeguard examples; private information now includes username/email plus password.
10. **NY General Business Law § 899-bb**, statute text via FindLaw: https://codes.findlaw.com/ny/general-business-law/gbs-sect-899-bb/
    - Used for: who's covered; small-business scaling clause; testing and service-provider safeguards; the compliant-regulated-entity list (GLBA, HIPAA, 23 NYCRR 500).
    - The official nysenate.gov page blocked automated access, so FindLaw's copy was used.
11. **Microsoft Learn**, "Security defaults in Microsoft Entra ID": https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults
    - Used for: what security defaults do; no extra cost; P1/P2 licenses → Conditional Access.
12. **FBI IC3**, PSA I-091124-PSA, "Business Email Compromise": https://www.ic3.gov/PSA/2024/PSA240911
    - Used for: "use secondary channels and/or two-factor authentication to verify requests for changes in account information."