BITRALYNX
SOLUTIONS

FREE CHECKLIST FOR LAW FIRMS

Client File Security Checklist

A 30 minute self check for small New York law firms: email, sign in, remote access, closings, backups, AI use, and proof for clients and insurers.

Bitralynx Solutions
Managed IT, cybersecurity, AI governance, and fractional CIO services for New York nonprofits and law firms
October 2026 | bitralynx.com

Work through this with your office manager or IT contact. Allow about 30 minutes. Check what is true today, not what you plan to do. Every "no" is a conversation worth having.

This checklist helps you find gaps. It does not verify your systems, and it is not legal advice.

1. Email and sign in

- [ ] Every person has their own email account. Nobody shares a login.
- [ ] Two step sign in is on for every email account.
- [ ] Partners, the office manager and anyone who handles escrow use passkeys or security keys, the strongest kind of sign in.
- [ ] Our domain has SPF, DKIM and DMARC set up, so others cannot easily send email that looks like it came from us. (Ask your IT provider: "Is our DMARC set to reject?")
- [ ] Someone checks our email settings at least once a year.

2. Calls, remote access and visitors

- [ ] Staff know the one real way to reach IT, and that number is on every desk and phone.
- [ ] Our rule: if someone calls claiming to be IT, hang up and call back on the number we already have.
- [ ] Remote support only starts from a request we made, with the one tool our IT provider uses.
- [ ] Firm computers block or alert on unknown USB drives.
- [ ] Nobody touches a firm computer unless they are expected and verified.

3. Money and closings

- [ ] Clients are told in writing, early, that we never change wiring instructions by email.
- [ ] Every wiring instruction and every change is confirmed by phone, using a number already on file.
- [ ] We note in the file who confirmed the wire, and when.
- [ ] We have a written same hour plan if money goes to the wrong place: call the bank, request a recall, report at ic3.gov.

4. Devices and updates

- [ ] Every firm laptop and desktop has its drive encrypted, so a lost laptop does not mean lost client files.
- [ ] Updates install on their own, and someone checks that they actually did.
- [ ] We keep a list of every device that holds client files, and who has it.
- [ ] Lost or stolen devices can be locked or wiped remotely.

5. Backups and recovery

- [ ] Client files and email are backed up, including Microsoft 365 or Google Workspace.
- [ ] At least one backup copy cannot be changed or deleted, even by someone using a stolen password.
- [ ] We have restored a real file from backup in the last 6 months, and it worked.
- [ ] We know backups help us recover, but they do not stop someone from leaking stolen files.

6. Vendors and apps

- [ ] We have a list of every app and vendor that holds client data, and who can get into each one.
- [ ] Former staff and old vendors lose access the day they leave.
- [ ] We know which vendors would tell us if they had a breach.

7. AI use (see ABA Formal Opinion 512)

- [ ] We have a short, written list of approved AI tools.
- [ ] Staff know what never goes into an AI tool: client names, documents and financial details, unless the tool is approved for that use.
- [ ] A person reviews anything AI helped write before it goes to a client or a court.

8. Proof for clients and insurers

- [ ] We can show, in writing, what safeguards are in place.
- [ ] We can answer a cyber insurance questionnaire without guessing.
- [ ] We know who to call first if something goes wrong: our IT provider, our insurer and our counsel.

What your answers mean

- **Mostly checked:** You have a solid base. Keep it current and test it.
- **A few gaps:** Start with sections 2 and 3. They cover the two scams the FBI has warned law firms about.
- **Many gaps:** You are not alone, and most of this can be fixed step by step. Start with one conversation.

We are an IT company, not a law firm. This checklist is not legal advice.

Built from: FBI alerts on the Silent Ransom Group (2025, 2026); CISA phishing and multifactor guidance; FBI, FinCEN, CFPB and ALTA guidance on closing wire fraud; New York Rule of Professional Conduct 1.6(c); ABA Formal Opinions 477R, 483 and 512. Full list: bitralynx.com/research-sources

NEXT STEP

Talk it through with us

Bitralynx Solutions offers a free 30 minute Technology Readiness Review. It is a conversation, with no access to your systems needed. Bring this guide and your questions. You leave with a short list of what is solid and what to fix first.

Keep your staff working and your services running.

info@bitralynx.com | (516) 855-5353 | bitralynx.com/how-we-start

This guide is general information for nonprofit and law firm leaders. It is not legal advice, a security certification, or a full risk assessment. Facts were checked in October 2026; threats and rules change, so confirm current guidance before you act. Bitralynx Solutions is an IT company, not a law firm.