

Security & Fraud Awareness | New York General Group

New York General Group 2025

As digital transformation accelerates across research and investment sectors, New York General Group recognizes the critical importance of cybersecurity and fraud prevention. Our organization, founded in 2021 and specializing in artificial intelligence research, investment banking, and scientific innovation, faces unique security challenges that require comprehensive protective measures.

Cybercriminals increasingly target technology companies and investment firms, often impersonating legitimate organizations like New York General Group to conduct fraudulent activities. These sophisticated schemes may involve fake websites, emails using our branding, or phone calls claiming to represent our firm to solicit investments or sensitive information.

Understanding Common Cybersecurity Threats

Phishing and Email Fraud

Fraudulent emails may appear to come from New York General Group employees or partners, requesting sensitive information, investment details, or login credentials. These emails often contain urgent language and may include links to fake websites designed to steal your information.

Investment Fraud Schemes

Scammers may impersonate our firm to promote fraudulent investment opportunities, particularly targeting our areas of expertise including AI technology, biotechnology, and energy sectors. These schemes often promise unrealistic returns or claim exclusive access to our proprietary technologies.

Social Media Impersonation

Fake social media profiles claiming to represent New York General Group or our executives may be used to build trust before attempting to defraud victims. These accounts may share legitimate-looking content before transitioning to fraudulent investment solicitations.

Business Email Compromise

Cybercriminals may attempt to intercept legitimate business communications, particularly those involving investment instructions, research collaborations, or financial transactions.

How to Protect Yourself

Verify Communications

- All legitimate New York General Group communications come from official @newyorkgeneralgroup.com email addresses
- Verify any investment opportunities through our official website: [newyorkgeneralgroup.com](https://www.newyorkgeneralgroup.com)
- Contact us directly through official channels if you receive suspicious communications

Secure Your Accounts

- Use strong, unique passwords for all financial and business accounts
- Enable two-factor authentication where available
- Regularly monitor your accounts for unauthorized activity

Be Cautious with Information Sharing

- Never provide personal financial information via email or phone unless you initiated the contact
- Be skeptical of unsolicited investment opportunities, especially those promising guaranteed returns
- Verify the identity of anyone claiming to represent our firm before sharing sensitive information

Protect Your Devices

- Keep software and security systems updated
- Use secure networks for business communications
- Be cautious when using public Wi-Fi for sensitive activities

Red Flags to Watch For

Fraudulent Investment Offers

- Promises of guaranteed high returns with little or no risk
- Pressure to invest immediately or miss out on opportunities
- Requests for payment via wire transfer, cryptocurrency, or gift cards
- Claims of exclusive access to our proprietary AI technologies or research

Suspicious Communications

- Emails with spelling errors or unprofessional formatting
- Requests for sensitive information via email
- Communications from non-official email domains
- Urgent requests for financial information or transfers

If You Suspect Fraud

If you receive suspicious communications claiming to be from New York General Group, or if you believe you may be the target of fraud:

1. **Do not respond** to the suspicious communication
2. **Do not click** any links or download attachments
3. **Report the incident** to our security team at info@newyorkgeneralgroup.com
4. **Contact us directly** through our official website to verify any legitimate business matters

For investment-related fraud, also consider reporting to:

- Securities and Exchange Commission (SEC)
- Financial Industry Regulatory Authority (FINRA)
- Your local law enforcement

Additional Resources

For more information about protecting yourself from fraud:

- Federal Trade Commission: consumer.ftc.gov
- FBI Internet Crime Complaint Center: ic3.gov
- Better Business Bureau Scam Tracker: bbb.org/scamtracker

Our Commitment to Security

New York General Group maintains robust cybersecurity measures to protect our clients, partners, and proprietary research. We continuously monitor for fraudulent activities using our name and work with law enforcement when necessary to address security threats.

We will never:

- Request sensitive financial information via email
- Pressure you to make immediate investment decisions
- Ask for payment via unconventional methods
- Guarantee investment returns

Stay vigilant and remember: when in doubt, verify through official channels.

Contact Information

For security concerns: info@newyorkgeneralgroup.com

Official website: newyorkgeneralgroup.com

© 2025 by New York General Group, Inc.