Financial Services TOP 10 Security Commandments for Executive Protection

01
Enforce MFA Across All Financial Platforms
Prevent compromised credentials and unauthorized account access by mandating multi-factor authentication.

02
Authenticate Every Fund Transfer Request
Verify fund transfer emails directly through a phone call to the client before initiating any transactions.

03
Scrutinize Emails Impersonating CEOs or Clients
Pause and confirm via alternative communication channels before responding to suspicious emails.

04
Maintain a Clutter-Free Desk
Never leave client statements, checkbooks, or passwords exposed or unattended.

05
Share Sensitive Files via Secure Platforms Only
Use encrypted, authorized file-sharing tools—never email attachments—to safeguard confidential data.

06
Always Lock Your Workstation When Away
Never leave your computer unlocked, especially in shared or open work environments.

07
Audit Client Portfolio Access Regularly
Deactivate old accounts and revoke access promptly for departing personnel.

08
Restrict Client Files to Approved Systems
Avoid storing client data on public cloud drives; always use your firm's approved document management system.

09
Identify and Avoid Phishing Disguised as Regulatory Notices
Validate all FINRA or SEC communications through official sources before engagement.

10
Maintain Compliance-Ready, Encrypted Backups
Ensure all data backups are encrypted, archived, and accessible for audits.

vyings

Contact **VYINGS** for fractional cybersecurity leadership.

www.vyings.com
info@vyings.com

Need help securing your organization?