Legal Sector TOP 10 Security Directives for Client Protection

01

Use Encrypted Email for Sensitive Client Files

Always transmit confidential documents via your firm's secure channels, never personal email.

02

Lock Your Computer When Away from Desk

Prevent unauthorized access by locking your screen with Win + L (Windows) or Control + Command + Q (Mac).

03

Shred Printed Documents Containing Client Information

Dispose of case notes, contracts, and evidence securely—never discard unsecured.

04

Verify Suspicious Emails Even If They Appear Authentic

Call clients, courts, or opposing counsel to confirm before clicking links or attachments.

05

Avoid Using Personal Devices for Work Unless Authorized

Personal devices may lack sufficient security for handling legal data.

06

Keep Case Files Confidential in Shared Spaces

Protect files by not leaving them open or viewable on your desk or screen.

07

Steer Clear of Free Wi-Fi When Working Remotely

Always use a VPN or secured hotspot for firm system access offsite.

08

Access Only Authorized Files

Restrict usage to your firm's approved document management systems.

09

Apply Legal Software Updates Promptly

Timely updates include critical security patches vital for compliance.

10

Report Suspicions Immediately

Promptly escalate anything unusual to prevent breaches.

vyings

Contact **VYINGS** for fractional cybersecurity leadership.

www.vyings.com

info@vyings.com

Need help securing your organization?