Top 10
Security Tips to Keep You and Your Clients Safe

1 Use Encrypted Email for Client Files
Always use your firm's secure tools to send sensitive documents—never personal email.

2 Lock Computer Before Leaving Your Desk
A client file left open is a liability. Press **Win + L** (Windows) or **Control + Command + Q** (Mac).

3 Shred Printed Documents with Client Info
Don't toss case notes, contracts, or evidence into the trash—shred it.

4 Verify Suspicious Emails Even If They Look Legit
Hackers impersonate clients, courts, and opposing counsel. Call before clicking.

5 Don't Use Personal Devices for Work (Unless Approved)
Your phone or laptop might not be secure enough to handle legal data.

6 Keep Case Files Private in Shared Spaces
Don't leave folders open on your desk or screens visible in meetings.

7 Avoid "Free" Wi-Fi When Remote
Always use a VPN or secured hotspot when accessing firm systems offsite.

8 Only Access Files You're Authorized To View
Stick to your firm's approved document management system.

9 Update Legal Software Promptly
Those reminders aren't annoying—they're protection. Many software updates include necessary security updates.

10 Report Anything Suspicious Immediately
If something feels off—say something. Fast action can stop a breach in its tracks.

Learn more at
phinsecurity.com