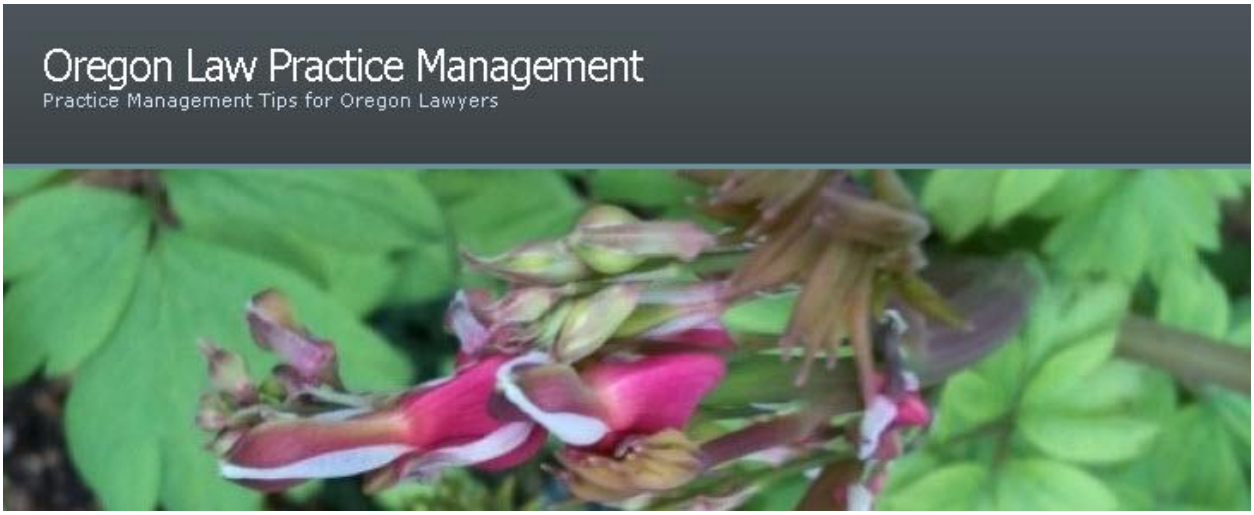

AirCards, Encryption, and Software! Oh My!

If you aren't a dedicated reader of Sharon Nelson and John Simek's Oregon State Bar Bulletin columns, you should be. This month, Sharon and John discuss secure mobile computing. Among their recommendations:

- Don't make a move without anti-virus, anti-spam, and anti-phishing software. Keep all three up-to-date and perform weekly scans.
- Use encryption to protect your valuable personal data. (John and Sharon use biometrics.)
- Always use a secure (https://) connection for remote access. A VPN (Virtual Private Network) is the best way to transmit sensitive data back to your home office.
- As a cloud alternative, consider AirCards. (Automatically secured and encrypted by your cell carrier).
- GoToMyPC or LogMeIn work, but leaving your home base computer powered-on may make it vulnerable in unanticipated ways.

- Public computer usage is a no-no. Keyloggers can track and record your every keystroke, such as user names, passwords, bank account numbers, or whatever you choose to enter. They are not secure!

Read the full article here.

Originally published March 8, 2010 at
http://oregonlawpracticemanagement.wordpress.com/2010/03/08/aircards-encryption-and-software-oh-my/