Protecting yourself on social media

MANAGING YOUR SECURITY ONLINE

Advice

Social media is a fact of modern life and when it is used successfully can be a powerful communication tool. Unfortunately, given the very public and unregulated nature of social media, there are also risks such as account hacking, identity theft and breach of professional conduct obligations.

Here are some tips for lawyers to keep their social media accounts secure and their reputations intact.

Tips

- Keep your password secure, change it regularly.
- Sign out of your account after you use a publicly shared computer.
- Manage your account information and privacy settings from the ***Profile*** and ***Account*** sections of your Settings page.
- Keep your antivirus software up to date.
- Don't put your email address, address or phone number in your profile's ***Summary***.
- Only connect with people you think you can trust.
- Stay vigilant - never give out your sensitive information if you feel something isn't right.
- When accessing social media in a wi-fi hotspot check the browser bar for a secure connection. If you see **https://** in the browser's address bar, it's a good indication the connection is protected.
- Report any suspected breach of privacy issues to the platform's customer service.
- Avoid posting at times when your judgment may be impaired (for example after Friday night drinks!).
- Be suspicious of a message from a host that contains bad spelling or grammar, or a threat of some kind. Example: your account will be deleted unless you act right away.

- Know and observe the Law Institute of Victoria's Guidelines on the Ethical Use of Social Media .See also the Law Institute of Victoria (Ltd) Professional Conduct and Practice Rules. Contact the LIV Legal Ethics Manager (9607 9515) if clarification is required.

Traps

- Opening links in an e-mail message from the host (LinkedIn, Twitter, Facebook etc) telling you to open an email attachment or install a software update. Hosts will ***never*** ask you to do this.
- Don't open attachments or click any links in an e-mail that seems suspicious or is from a person or company you don't know. If in doubt, move your cursor to hover over the link. If the address has no relation to the alleged sender of the e-mail, delete the e-mail. See below the picture example of what these fake emails look like.

For more information

Please contact the LIV's social media department.

E: socialmedia@liv.asn.au

T: 03 9607 9347