SAFETY TIPS
TO PROTECT YOURSELF IN THIS DIGITAL AGE

Melissa F. Brown
Melissa F. Brown, LLC
145 King Street, Suite 405
Charleston, SC 29401
843.722.8900 (office)
843.722.8922 (fax)

Helping Individuals
Cross Thresholds
to New Lives

© 2009 Melissa F. Brown

Protect Yourself Against the Use of Spyware:

- Install good anti-spyware programs that seek out and destroy the spyware. Run the anti-spyware programs on your computer once a week.

- Install a firewall and spam clocker program to help combat spyware.

- Regularly update your operating system and web browsing software.

- Do not open the Web links found in email "spam" or other similar unsolicited messages.

- Only install software from Web pages you trust.

- If you install "free" software, carefully read the fine print in the license for any reference to collecting information from your computer and sending it elsewhere. (Be ESPECIALLY wary of popular "free" music and movie file-sharing programs.)

- When opening a Web Page, if a dialog box appears unexpectedly asking you to accept a download, the safest response is to click the red "X" in the upper corner of the box to close the window (clicking "no" may not close the box).

- Install software to detect, remove, and prevent the installation of spyware on your computer. Many internet service providers offer spyware protection software.[1]

- The following methods will NOT protect a computer against or make the user aware of active spyware:
    - Antivirus software will not protect against spyware.
    - Checking the list of installed computer programs will not reveal spyware on the computer.
    - Pressing control-alt-delete to review the programs currently running will not reveal spyware.

[1] "What You Need to Know about Spyware," *University of Washington*, http://www.washington.edu/computing/security/spyware/; Guilherme Roschke and Erica Olsen, "Maintaining Safety and Security in a Digital Age" ABA Section of Family Law, 2009 Spring CLE Conference.

© 2009 Melissa F. Brown

Safety Tips to Protect Your Cell Phones and Computers:

- Turn off your cell phone when it is not in use for location and privacy safety.
- Set Bluetooth to "hidden" and GPS to "911 only," especially in public areas such as airports and concert halls.
- Try to use a safe, public computer at a local library or internet café if you suspect your computer might be monitored.
- Avoid cordless phones. Use a new phone for personal calls. Beware of "gifts" of cell phones that may already have GPS and other technology downloaded on them.
- Consider activating the key-lock feature present on cell-phones to prevent autodialing.
- Contact your phone company and ask if location services were added to your service plans.
- Consider changing passwords and PINs to e-mail and bank accounts frequently.
- If possible, use anonymous e-mail accounts accessed from public computers.
- Have more than one email address, and avoid easy passwords. Change your password often.
- Avoid using e-mail to communicate sensitive and personal information.
- Caution family and friends from sharing addresses when sending or forwarding emails.
- NEVER use the BCC (Blind Copy) option when sending e-mails. Instead, forward the sent e-mail to others after you have sent it to the original recipient. Otherwise, if the BCC recipient chooses to "Reply All", their identity becomes known to all.
- Never open attachments from unknown sources and be skeptical of requests for information.
- Look for your name on the Internet and request government agencies such as the IRS, court systems, post office, etc. make your information confidential.[2] Victims can request to have their records sealed or restrict who can access their information.

[2] "Alternatives to Violence of the Palouse, Technology Safety and Cyber-stalking," http://community.palouse.net/ATVP/Material/Brochures/PDF_Brochures/General_-_Technology_Safety.pdf (Accessed May 20, 2009).

© 2009 Melissa F. Brown

- Always log off or sign out when you are finished.
- Save and document everything.
- Obtain a private mailbox, and do not give out your real home address.
- Search or have your car searched for signs of tampering or presence of cell phone monitoring devices.

Safety Tips About Hidden Cameras in Personal Life and at Work:

- Trust your instincts.
- When possible, hold meetings or conversations in locations where you will feel more confident of security.
- Know that there is camera detection equipment, but it is expensive.
- Ask law enforcement or private investigators to assist in searching if you feel like you are being watched.
- Understand the consequences and possible charges: criminal eavesdropping, stalking, or unlawful surveillance.

© 2009 Melissa F. Brown