AttPro Snippets

Respected security professionals have compared e-mail to postcards written in pencil-they can be viewed or altered by third parties. Unfortunately, hackers are increasingly targeting law firms to mine sensitive client information. Email encryption can be an effective precaution to help prevent data theft. Encryption scrambles information according to a certain pattern, so that only the users who have access to that pattern or "key" can unscramble it and make it readable. Encryption technology is also effective in the event of a physical device theft since the data is unreadable without acquiring the key.

Client email accounts can also be hacked. Hackers can then send instructions from the client to the firm seeking confidential information, ordering disbursement of funds held, or instructing the lawyer to ask a third party to do something that ends up hurting the client. The key to avoiding most of these situations is to verify instructions directly with the client by telephone or one-on-one meetings. Before releasing funds, agreeing to settle, or taking any action adverse to a client based upon email instructions, call the client first.

A security breach can not only diminish the level of trust a client places in a law firm but could also have serious legal and financial ramifications. Using encrypted emails can help safeguard the attorney/client privilege.

For more information on encryption and other security resources please go to:

FYI: Playing it Safe With Encryption