

Laptop Safety Alert!

Increased laptop theft causes concern for theft of confidential client data!

Sensitive client information should ALWAYS be encrypted as soon as it is uploaded onto a laptop. Software programs should ensure that every data field that contains information pertaining to personal identity is also encrypted. Additionally, physical security should be kept in your laptop case, such as a locking device to attach to a desk or stationary object.



Some encryption programs are built into popular financial and database software programs. Additionally, your broadband provider may include encryption on your wireless network as part of your service. In some cases, a separate program will be needed to properly encrypt sensitive data, especially for laptops, BlackBerries and other portable media. The transmission of confidential information by email should ALSO always be encrypted.

Remote Laptop Security (RLS) features can prevent access to protected files in the event a computer device has been lost or stolen. Protected files are encrypted, and the program periodically authenticates the identity of the user, shutting down when the user is unable to provide authentication (password, fingerprint, voice, etc.). Some RLS programs will even track laptops when they are connected to the internet. Inquire with your software and internet providers and get your "house in order" today!

Insurance Partners Agency, Inc.
26865 Center Ridge Road
Westlake, OH 44145-4042
phone 440.835.9600
fax 440.835.9614

4 Locations to Serve You
Westlake • Solon • Mentor • Elyria

* Excerpt from the Business Insurance Tips & Safety (BITS) series at Insurance Partners

Please contact Sharon Francz, ext. 127 or sfrancz@inspartners.com at Insurance Partners today for a no-cost consultation of your business insurance needs. You can also submit a request by going to www.clearlinesolutions.com/lipa2. It's the right choice to protect yourself and your valued assets.