Pensinger Financial's Cyber Security Policy

The policy is to:

Password protect any documents containing sensitive information (for example: SSNs, account numbers, or driver's license numbers). This applies to not just emailed attachments, but also files on the company's hard drive(s).

Treat any client communication requesting money movements, information requests, and other data requests with caution. And to always verify with a phone call anything that seems suspicious or out of the ordinary.

To understand that no amount of money needs to be moved immediately (thereby bypassing cyber security protocols due to the immediacy of the need).

Any request for wired money needs to be verified with a phone call where Pensinger Financial verbally confirms the request, the destination, and identifying numbers of the wire.

Look for impersonating email addresses (i.e. the name of client is in the email sender address line, but the email address is a bogus one).

Be wary of any client requests to click on a link or open an attachment. Again, a phone call to be certain is the best precautionary measure.

Utilize AVG Internet Security and Anti-Virus software. My AVG software automatically has updates and patches sent to it from AVG, and those updates will run automatically behind the scenes. The virus and malware scan across my operating system, and applications automatically runs once a week. I can also perform ad hoc virus and malware scans. The AVG software protects: "computer," "web & email," "hacker attacks," and "personal data." After completing AVG's virus scan, it provides me with a report showing: issues and threats I need to address, as well as:

- Protection status of all browser-stored passwords
- Protection status for webcam privacy
- Protection against remote desktop protocol exploit attacks
- Protection level of sensitive documents
- Protection status against fake websites
- Finding outdated computer drivers

Once a year complete a cyber security training course.