AIM CYBER

High-touch services to help you navigate modern cyber threats.

CYBERSECURITY – WHY ISN'T IT MORE EFFECTIVE?

Statistics show that a high percentage of breaches, some say up to 95%, are caused by human error.

If tools were the answer, you would not read about cyber breaches and ransomware attacks every week. Cyber tools are good at many things but are not able to prevent all human errors.

If people are the cause, then they are also part of the cure. The common reaction is to provide training for users. And that makes sense, but it has not stopped people from making breach-causing errors.

Then what is the reason? The training is often ineffective. Users often view training as just another requirement, something necessary to keep their job. The focus is on getting through it to check the box and get back to their real job.

To make it more effective it needs to be taken seriously. People need to understand that cybersecurity is everyone's responsibility and fundamental to the continuation of their job and the business.

That takes training and more. The more is services to help people understand the role they play in cybersecurity, and to offer more than just training.

Making the training more interesting takes customization and an understanding of people, not just cybersecurity facts, and then, support to help them.

Making the training fun and challenging helps. Start easy to keep people's interest or you will lose them.

Keep the lessons short because interest spans are short. Shorter lessons are less of an interruption to the day and are easier to digest.

Create a culture where reporting a mistake is a positive. If people believe they will be punished, the mistake will go unreported, and the damage will proliferate. The faster the mistake is reported the better the chance to contain it.

Never forget you are dealing with people. That requires listening and flexibility. Failing to listen to the people who will use the program will ensure your new program fails. Being rigid and expecting everyone to behave the same way will also lead to failure.

People need to know they will not be punished if they clicked a suspect link or did anything else that might cause problems. They must know who to call for help or guidance.

That needs to be a person, not an app or other automated service. If people feel they are not valued, they will not bother reporting it.

Tools are important, people are essential. Ignore this at your own peril.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.