

Educating your staff

Mark James, ESET IT Security Specialist, answers a few questions about why it's important to teach your staff about cyber security and make them your primary line of defence against potential breaches.

How can businesses improve staff cyber security awareness?

Having good internet security with regularly updating operating systems and application is very important but if your staff are just going to click every link or surf the web with no thought or regard for security then sooner or later you will be compromised.

Making your staff aware of the current threat landscape including measures used and possible scenarios could help educate them in combating this very real threat, they also need to understand why it's important to be part of your security.

Why isn't training being provided?

Cost, time and availability would be the bigger reasons. Of course training comes at a cost and it's ongoing: to properly train in the very quickly changing landscape of cyber threats takes time, money and highly knowledgeable training personnel.

Finding the right resource to deliver effective training at a level that can be easily digested is a big problem as well: training can easily become overwhelming for the average user, so delivery is very important.

Are upper management and other users with high levels of access a particular problem?

Quite often upper management have enough to worry about without getting involved in what "might" happen. Having someone who understands the importance of effective training as well as a good understanding of current attack methods with the ability of delivering that information at a level the average user can understand is a job all in itself.

Effective training should be given to all levels of staff including the board, everyone in the company could be a target and some would argue that the higher level employees are even more at risk than some others due to their "required" data or network access.

How else can breaches be prevented?

Good internet security software that updates on a regular basis along with the latest operating systems that are patched in a timely manner is critical in protecting your company systems.

All applications installed should be vetted to ensure they are actually needed and updated on a regular basis, data monitoring and good company policies will all help to keep your staff and data safe at all times.