The Human Aspect of Data Security and Phishing Prevention

by BJ Bouschor, Vice President of Information Technology, FireKeepers Casino Hotel

In today's world, everything is done with technology. While this trend has greatly increased productivity, technology has also made it easier for criminals to steal personal information, as well as obtain access to vital company data. The most common way one may gain access to an individual's or company's data is through email. Due to the high effectiveness and ease of access, email is a primary communication medium through which many people conduct their business. However, the very same benefits that make email popular also make it more vulnerable to attack.

Phishing is the most common form of a social engineering attack – a method used to steal personal information, such as user data – and it is extremely sophisticated. Posing as a trusted entity, a phishing attack is an email sent with malicious attachments or links which can compromise the user's system if clicked on or opened. These attacks are becoming more and more specialized and precise, allowing criminals to take advantage of employees through very realistic emails that appear to come from within their organization. To combat phishing, individuals and companies alike utilize a variety of anti-phishing software, but these programs are only as strong as the weakest link – i.e. the human factor.

Humans, as a whole, operate on a seeing-is-believing mentality, which makes them trust their own eyes too easily and makes it difficult for them to avoid sophisticated schemes, such as phishing. Proper training to recognize these disguised attacks involves identifying how the attackers work and how one may avoid falling into the just-click-it mentality. That is to say, during this training, employees are made to pause before clicking on an email and its contents, which is a simple form of operant conditioning that counteracts the just-click-it mentality. Initial training should be completed during a new employee's hiring process and company orientation, and refresher training should be available throughout the year. However, proper training for all employees is only the first step. Companies also have to know who is more at risk during phishing attacks and make sure these individuals receive extra training. At-risk users can be identified through the use of targeted emails – fake phishing attempts – to determine the likelihood that they will automatically open emails without verification. Those who open emails without any caution and thus fail this test should then be assigned additional training to improve their comprehension of the problem. This, in short, is how companies could prevent their data from being stolen, but how does a company get its employees to implement these precautions? It all depends on how one packs and sells such a solution to management.

In most scenarios, management is willing to listen to informed individuals when it comes to IT security and the hardware or software they wish to implement to guarantee a company's continued wellbeing. However, even if one encounters an open ear, there is no assurance that management can set aside company funds for additional employee training; budgeting is often either minimal or non-existent. Due to the difficulty of gaining appropriate funds for the training of all personnel, to minimize successful phishing attacks, management needs to be reminded that the human factor, while the greatest liability, is also the greatest asset a company has against social engineering attacks. As aforementioned, without proper training, the door stands wide open to phishing attacks, which allows for a possible breach of data, a very costly mistake. This is one point that management will understand and agree with. However, investing in proper phishing training, while costly, greatly decreases the likelihood of a possible breach or loss of personal data – i.e. it greatly decreases company funds being wasted on data loss. Graphs that show the number of attacks that occur each month within an untrained business vs. the number of attacks that occur each month within a trained business can greatly enhance management's understanding of the problem and the worth of the investment.

Overall, well-trained employees make fewer mistakes, which decreases the amount of man-hours a company's IT division spends on fixing problems or trying to recover data. Moreover, it decreases costs and increases the positive productivity of the IT staff. In addition, contrary to some studies, the majority of employees who receive proper training are more apt to remain employed at their current location. In other words, properly training

employees in an ongoing manner not only adds to the overall security of a company by decreasing the security risk from phishing attacks, which decreases corrective costs, but it also leads to an increase in employee performance. As one may observe, the benefits of phishing training for employees far outweighs the costs a company may incur due to a successful phishing attack, which is why it should be a part of a company's annual budget.

In closing, the human factor is present in all areas of life, not just IT security. However, by recognizing the fact that humans are adaptable and can be trained for almost all situations, one may establish an argument that can help convince management to support employee phishing training. After all, in the end, the investment costs for phishing training are minimal in comparison to the costs of a lack of training.