Idea 05 ms-final

Podcast script: Prof Margit Scholl, TH Wildau
Topic: Scam Alert! Raising Employee Awareness of CEO Fraud Attacks
Reference: https://link.springer.com/chapter/10.1007/978-3-031-33258-6_40

Hello and welcome to ResearchPod. Thank you for listening and joining us today.

In this episode, we'll delve into the research of Margit Scholl, Professor of Business and Administrative Informatics at TH Wildau, Germany. Carried out in cooperation with corporate partners, her work explores a novel approach to giving business employees a greater awareness of fraud. Since 2013, a pernicious form of corporate cyberattack has surfaced in Germany. In it, the scammer impersonates a company CEO and convinces employees to transfer large sums of money outside the organization and into their hands. But how can employees be made alert to such a scam? She analyzed the current scientific literature and, together with her research team and two corporate partners, developed both an analog and a digital game-based learning scenario geared to this topic to determine what methods of awareness raising can best protect businesses from this costly threat.

Across institutions, both small and large, and in all areas of life, digital has become destiny. A range of organizations are reaping the efficiency gains of digital integration, but the transition brings new threats to security. In the modern digital environment, top managers must implement a cohesive strategy to ensure operational security. A technical infrastructure should be built to first filter out any known cyberattacks. But the second and most significant line of defense is staff—after all it will be one such individual who clicks a link or makes a call that completes the final step in a scammer's plan. Therefore, staff must be trained to identify and respond to cyberattacks in a smooth and seamless protocol. But raising employee awareness is easier said than done. The process of learning requires sufficient understanding and investment in the lesson itself. Training in digital security will need to meet these psychological demands to make employees alert to scams.

Phishing is an industry worth billions, and CEO fraud is an especially lucrative scam that operates in around 140 countries. In this scam, attackers impersonate the CEO and contact employees responsible for accounts payable, tricking them into sending money to the attacker's bank account. Social engineering techniques are used to create a sense of urgency. For example, employees could be made to worry that failure to transfer the funds would result in catastrophe for the corporation. In Germany, some businesses have sought damages from the banks that process fraudulent payments, claiming that they should have recognized and prevented the fraud. However, few cases go to court because the fear of reputational damage outweighs the potential for financial gain.

CEO fraud can also target HR departments in a bid to obtain personal information for identity theft or bank fraud. Such attacks can result in financial loss, damage to brand reputation, litigation costs, and even staff redundancies. The dangers posed by CEO fraud have dramatically increased as manipulation methods have become more sophisticated and tools for creating counterfeit identities more accessible. Under threat of this damaging deception, businesses need to keep their employees aware of the signs of potential cyberattacks and the appropriate action to take. Indeed, the survival of the company is at stake.

// Pause for music //

Just *distributing* information is not the same as raising awareness. If proper risk assessment is to be implemented, employees must be fully engaged with the subject of digital security. After all, learning is an active process which asks participants to draw on their own knowledge and experience in order to build new understanding. Efforts in personnel development should therefore make information meaningful, helpful in work, and linked to existing knowledge. Consideration should also be given to time demands. Chief Information Security Officers have found that employees learn best with shorter modules. Short-burst training, they argue, serves as a manageable reminder of corporate cybersecurity.

But what about the content of training? *Stories* are a powerful means of raising security awareness. They make facts more accessible by contextualizing abstract details in emotional experiences. Indeed, government agencies and organizations are already in the process of incorporating well-crafted stories into their lessons on cybersecurity. But while short stories, including serious comics, can convey complex information in an entertaining way, they must be effectively tailored to hold social and occupational salience for a range of audiences. Meanwhile, game environments can immerse people in an endless array of contexts and situations. This gives them great potential as vehicles for storytelling, and ultimately for learning. However, striking the right balance in such games between entertainment value and educational purpose requires careful design and development.

A project was established to create a space where methods of storytelling and game-based learning could be trialed in the development of digital security training. Funded by the German Federal Ministry for Economic Affairs and Climate Action, the “ALARM Information Security” project aims to develop education and training for small to medium-sized enterprises, otherwise known as SMEs. Pilot companies were invited to take part in interviews and an online survey, and responses were used to customize training material to the specific needs of working groups.

The ALARM Information Security project created two game-based learning scenarios on CEO fraud—one analog and the other digital. Developed by the subcontractor known_sense, a firm based in Cologne, the analog scenario uses a board-game approach. The board is split into five phases, each subdivided into process steps around the perimeter. The players are given cards showing sample phishing emails or the situation at different stages of the scam, as well as decoy cards that represent no threat whatsoever. Players must place their cards on the appropriate areas of the board, which may represent the scammer's research phase, their process of maintaining contact, or the point of attack, with bonus points given for correct chronological placement *within* the phases. A stopwatch is used to emulate the sense of urgency created by attackers, as they fabricate threats of imminent company failure to undermine critical thinking and encourage instant employee action.

The digital version of the CEO Fraud learning scenario was developed by the subcontractor Gamebook Studio, an enterprise in Berlin. It uses storytelling and a visual novel format, allowing players to navigate through a decision tree as a security detective. The game allows players to make decisions that affect their progression through the scenario. The players' efficiency and social skills are evaluated, and feedback is given at the end. Both the analog and digital learning scenarios offer interactive and engaging ways to educate SMEs on the importance of security measures and how to mitigate risks.

The learning scenario in each game, both analog and digital, has been developed and iterated in three stages. The first stage involved the university team testing the subcontractor's proposal. In the second stage, improved scenarios were tested with pilot companies. Feedback from these tests was used to create new versions, which were then tested with participants in public events. The final versions are now available in German on the ALARM project website, where they can be downloaded for free for noncommercial use.

The analog game is designed to be fifteen minutes in duration. This design feature aligns with the above finding that employees value short-form learning, which they can undertake quickly during breaks. However, the game is designed to be modular, so that with the proper interest, experience, and discussion, it can be extended; the instructions delivered provide the moderator with appropriate information. Conducting quizzes after modules was regarded as a means to strengthen the contextual focus. It was also considered crucial for the training material to be adapted to the local context and language, despite the evident challenges involved in doing this. Other insights include the recommendation to restrict presentations about the games to around fifteen to twenty minutes to maintain learners' attention.

In contrast to the analog version, the digital learning scenario involves solo play. This limits the learner's experience to the path chosen from the options made available. Such a narrow perspective makes the design of the game a delicate art, in which players should be encouraged to take action and think about ways to expose themselves to new information in a sensible but compelling way. Alongside this challenge, the solo digital format also has the potential to embed new insights even deeper in the learner's memory. Debriefings remain an important check-in time during which digital players can seek clarification and elaboration on their security questions.

The ALARM Information Security project has shown that short interactive game-based learning scenarios can raise awareness of CEO fraud and other security threats, helping to develop appropriate risk assessment and ultimately saving companies from potential catastrophe.

// Pause for music //

That's all for today's episode. For more about Professor Scholls research, read the original article linked to in the show notes for this episode. And, as always, be sure to stay subscribed to ResearchPod for more of the latest science. See you again soon.