Executive Summary

CIOs and IT managers need to mitigate the risks to information and IT assets arising from deception-based attacks. Common examples of deception are “social engineering” and phishing, both aimed at getting people to divulge information that will enable unauthorized access to computer systems. One well-known hacker has claimed it is easier to ask people for the required information than to employ highly technical hacking techniques.

Mitigating deception threats is not easy because people are not very good at detecting deception—the overall success rate is only just over 50%. However, our research has shown that training—and especially e-training—can improve people’s knowledge about deception and their ability to recognize it.

There are two types of deception training: tactics-based and cue-based. Tactics-based training teaches people to look for the tactics deceivers commonly use to hide the truth. However, the tactics employed are very domain specific – for example, they will be different in the accounting and HR domains.

Deception cues are not context-specific, and people can easily be taught how to recognize them. The cues fall into three categories: (1) Physiological (sweating, increased heart rate); (2) Psychomotor (eye contact, gesturing); and (3) Linguistic (such as limited use of the personal pronoun).

In two studies carried out a year apart with United States Air Force officers in the communication and information career field, we showed that appropriate training can improve deception detection. The studies also showed that those who used an e-training system performed better than those who participated in conventional classroom learning. One of the studies was designed to test the effectiveness of adding additional interactive capabilities to the e-training system. It showed that including features that require students’ continued engagement and interactivity (such as quizzes to reinforce the learning) are well worth the small additional investment.

Four actions for CIOs and IT managers in organizations at risk of losing valuable information from deception-based attacks arise from our research: (1) Provide employees with training on what deception is and how to recognize it; (2) Focus the training on how to detect the deception cues that “leak” from deceivers; (3) Use a well-designed e-training system that allows trainees to go at their own pace; and (4) Enhance e-training with features such as a navigable outline, search tools, and tools that involve practice and feedback.

DECEPTION-BASED ATTACKS ARE A SERIOUS THREAT TO INFORMATION SECURITY

A recent survey shows that many white-collar employees routinely violate their companies’ information technology (IT) policies. One in six admitted they use peer-
to-peer file sharing at work, while 74% believed it was acceptable to download personal software onto a work machine, and 63% were not concerned about the security of their information at work. Such practices compromise information security, but the risks are exacerbated because there are many who know about slack IT policy enforcement and take advantage of it.

In his book, well-known computer hacker Kevin Mitnick explains how he used “social engineering” to get people to do things they normally wouldn’t do for a stranger. He describes how he can deceive unsuspecting victims into handing over social security numbers or passwords that he can then use to gain access to their computer systems. Mitnick’s targets were often employees with IT access or knowledge who unwittingly shared with him information that enabled him to compromise the security of the systems he targeted. He notes that it was easier for him to simply ask people for needed information than to employ highly technical hacking methods to compromise a system.

Another example of a common method for taking advantage of lackadaisical employees is phishing. Most people are familiar with phishing attacks aimed at providing information about bank or credit card accounts, but phishing is also used to gain access to network-computer and server accounts.

Both social engineering and phishing are instances of deception practices designed to gain illicit access to computer systems through employee naivety rather than through sophisticated hacking techniques. While IT security staff commonly deploy advanced technology to thwart sophisticated attempts to compromise systems, they often do not pay much attention to low-tech methods that use deception to gain illicit system access. However, since CIOs and their IT staffs are responsible for protecting their companies’ information and IT assets, the task of mitigating deception threats falls within their purview.

Unfortunately, mitigating deception threats is not easy because people are not very good at detecting deception. A recent analysis of studies involving over 23,000 subjects found that people were only 54% accurate in detecting deception. That is why social engineering and phishing attacks are so successful. Hackers and others wishing to get access to critical information assets don’t have to employ sophisticated attacks; they merely have to ask for the information they want. Fortunately, there is some good news.

**USING E-TRAINING TO COMBAT DECEPTION-BASED ATTACKS**

In two research studies we conducted with IT specialists in the U.S. armed forces, we found that an e-training system we developed can be used successfully to both teach managers and employees about deception and to improve their ability to accurately detect deception when it is present. Our approach focuses on Web-based training that teaches people how to recognize the “cues” that deceivers unwittingly give out. People can also be trained to recognize the tactics deceivers might use to hide the truth. Deception tactics are domain-specific, but deception cues are not context-specific. This means that cue-based training is applicable in a wide variety of organizations. Moreover, our Web-based approach makes it easy to deploy the training to multiple locations.

The remainder of this article describes the two approaches to training people to recognize deception (tactics-based and cue-based), describes our Agent99 Trainer e-training system, presents the results of two field experiments, and draws conclusions about the feasibility of training IT and non-IT managers in how to detect attempts at deception. We conclude with lessons learned from our studies and actionable items for CIOs and IT managers.

**APPROACHES TO DECEPTION DETECTION TRAINING**

With a 54% accuracy rate, an individual’s chances of successfully detecting an attempt at deception are only slightly better than flipping a coin. McCornack and Parks suggest that people suffer from a “truth bias”—they are overly confident in their ability to detect deception, and they tend to believe what others are telling them is the truth. In a recent study in which a deceiver intentionally led a group of decision makers away from making an optimal decision, those deceived were reluctant to challenge the deceptive member

---


of the group. They could not believe the deceptive person deliberately tried to mislead the group, and even when they became suspicious, no one wanted to challenge the deceiver.

People’s poor natural ability at detecting deception and their truth bias mean that deceivers have a built-in advantage even before they begin their efforts to deceive. Over the years, several approaches to deception detection have been developed, including polygraphs, voice stress analysis, and behavior analysis interviews, but they all require a significant amount of specialized training and equipment, and sometimes do not produce results that justify their large overhead cost. It is possible, however, to train people to improve their deception detection ability without the use of specialized techniques or equipment.

There are two types of deception detection training, one based on helping people to recognize deception tactics and the other based on helping them to recognize cues to deception.

**Tactics-based Training**

Tactics-based training teaches people to look for the tactics deceivers might use to hide the truth. For instance, deceivers might use the tactic of “inventing,” which means they add new information to suggest an incorrect representation. Or they might provide “decoy” information that hides the truth.

A third tactic is “mimicking,” where deceivers change the attributes of a situation to support an incorrect decision. In the HR domain, for example, a deceiver might modify attributes of a resume to suggest that he or she is the best candidate for a job. Thus a deceptive applicant might use the acronym “MIT” when referring to a degree supposedly obtained from the “Milican Institute of Technology” (which doesn’t exist). In the accounting domain, the mimicking tactic might look very different. The deceiver might add misleading narrative of a company in a financial statement, slightly adjusting information to manipulate the reader’s impression of the company.

In both these examples, domain-specific knowledge is needed to train an individual to identify the deception.

An HR specialist needs to know that deceptive applicants may use acronyms to mislead hiring decision makers. But an accountant must learn to compare the financial data and the statement narrative to defeat the mimicking tactic.

Training people in how to recognize deception tactics has had limited success in some domains (such as accounting), but therein lies the problem. Deception tactics are very context-specific and may be very different in other domains.

**Cue-based Training**

Unlike deception tactics, cues to deception are not context-specific. Training people to successfully recognize deception cues hinges on two key ideas:

1. Deceivers inadvertently provide cues to their deception while they deceive.
2. A person being deceived can detect those cues and realize they are indicators of deception.

One of the earliest hypotheses in the deception literature was that the act of trying to deceive causes a variety of internal physiological responses in the deceiver that give rise to external behavioral manifestations that are displayed involuntarily and/or inadvertently. These displays are called “leakage cues” because indicators of deception and true feelings “leak” out of the body unbidden and become telltale signs that separate deceivers from truth-tellers. The cues fall into three categories:

1. Physiological, such as sweating or increased heart rate.
2. Psychomotor, as in eye contact and gesturing.
3. Linguistic, as with avoiding the use of first person speech so as to distance oneself from the event.

Some technologies, like the polygraph and voice stress analysis, measure the physiological cues but, as noted above, they require expensive equipment and training to operate successfully. There is still a need for people to become better at credibility assessment and deception detection, and training them to identify deception cues is a good way of improving the ability to do this. Many reliable cues to deception have been identified, and people can be easily taught how to recognize them and thus improve their ability to detect deception. Moreover, these reliable cues are

---


8 “Credibility assessment” is the term used by the military and law-enforcement agencies to describe the process of determining if a person is telling the truth or lying. It is synonymous with deception detection.
potentially present in many deceptive situations. Recognizing them does not depend on understanding the context and knowledge base of a particular domain or work situation.

Previous research has shown that cue-based training can improve people’s deception detection abilities,9 and our two studies were designed to provide additional evidence. We were also interested in determining whether there was a difference in the effectiveness of training provided by instructors or by a computer-based e-training system. We now describe the cue-based deception detection curriculum we developed for our experimental studies and then introduce our e-training system, Agent99 Trainer.

THE CUE-BASED TRAINING CURRICULUM

We developed a cue-based deception detection training course in accordance with the United States Air Force (USAF) Air Education and Training Command (AETC) guidelines. The course was aimed at Air Force officers in the communication and information career field, and the training curriculum focused on cues to deception and how they could be detected. A former Air Force technical training “master instructor” developed learning objectives for the subject matter and linked the cues to the objectives.

For example, one objective was to instruct students in how to identify psychomotor cues such as eye contact and use of hand gestures. Then, following standard USAF curriculum development guidelines, the master instructor developed a standardized training plan for use in instruction. The plan included topic areas to be covered, examples of various cues, and training scenarios to show students how cues might materialize in a domain relevant to them. While the cues were not domain-specific (for example, eye contact cues and linguist cues like personal pronoun usage are the same across domains), the curriculum was developed in the communications and information domain, as it was meaningful to the students and consistent with their curriculum.

Two seasoned Air Force officers with considerable experience in communications and information developed realistic scenarios for use in the curriculum. These included cases of social engineering used to gain access to organizational computer systems and examples of unauthorized personnel attempting to collect sensitive information. Other examples came from past studies of deception detection, which involved experimental subjects trying to deceive their interviewers.

The standardized curriculum was delivered both by a traditional training program (lecturer in front of the class) and by the Agent99 Trainer e-training system. The training teaches about the cues, using the scenarios to illustrate the cues in context. An example from the cue-based deception detection training with a related scenario from the training materials is included in Appendix A.

E-TRAINING: AGENT99 TRAINER

We designed and developed a prototype e-training system called “Agent99 Trainer” to deliver our cue-based deception detection training curriculum.10 Agent99 Trainer provides a variety of synchronized features, including instructional videos, presentation slides, course lecture transcripts, and navigational and search capabilities. Two screenshots of Agent99 Trainer are provided in Figure 1. In the upper-left corner of both screenshots is a videotaped lecture by an instructor, while the lower-left portion of the screen provides a complete transcript of the lecture as well as two search features. One feature allows the user to search the lecture on key words; the other, called “Ask-a-Question,” lets the user search by posing a natural language question. In the upper right corner of the screen is a navigable lecture outline, while the lower right portion of the screen provides presentation slides. An additional feature, visible in the screenshot on the right, provides pop-up quizzes to test users on their subject matter knowledge, thereby actively engaging trainees. Agent99 Trainer was used to deliver cue-based deception detection training for the two studies described below.

THE TWO STUDIES

We conducted two experiments at a large USAF facility located in the U.S. The studies were conducted approximately one year apart. While the career communication and information officers involved in both studies take their immediate orders from their

---


10 We borrowed the name from the old “Get Smart” TV show. Agent 99 was Maxwell Smart’s partner. Agent99 Trainer is a prototype research tool, unavailable commercially. However, the content of the deception detection cue-based training curriculum can be requested from Dr. Jay F. Nunamaker Jr. (jnunamaker@cmi.arizona.edu).
local commanders, they receive their policy guidance and instructions from the Air Force’s CIO. These officers are IT professionals charged with developing, maintaining, and protecting Air Force information and information assets. The first study involved 119 officers whose normal role involved building computer networks and conducting information management duties. A total of 190 officers participated in the second study. The demographics on the participants in both studies are given in Figure 2.

In both studies, the USAF AETC assigned participants to “blocks,” each consisting of up to 16 officers. Each block was randomly assigned to one of several test configurations (described below). This environment provided an excellent opportunity to determine if we could improve students’ ability to detect deception, and the relative effectiveness of e-training and conventional classroom training.

<table>
<thead>
<tr>
<th>Variables</th>
<th>Military Participants</th>
<th>Percentage of Total</th>
<th>Military Participants</th>
<th>Percentage of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Study 1</td>
<td>Study 1</td>
<td>Study 2</td>
<td>Study 2</td>
</tr>
<tr>
<td>Male</td>
<td>103</td>
<td>86.6</td>
<td>159</td>
<td>83.7</td>
</tr>
<tr>
<td>Female</td>
<td>16</td>
<td>13.4</td>
<td>31</td>
<td>16.3</td>
</tr>
<tr>
<td>Rank</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Civilian</td>
<td>8</td>
<td>6.7</td>
<td>2</td>
<td>1.1</td>
</tr>
<tr>
<td>2nd Lieutenant</td>
<td>99</td>
<td>83.2</td>
<td>177</td>
<td>93.2</td>
</tr>
<tr>
<td>1st Lieutenant</td>
<td>5</td>
<td>4.2</td>
<td>4</td>
<td>2.1</td>
</tr>
<tr>
<td>Captain</td>
<td>4</td>
<td>3.4</td>
<td>5</td>
<td>2.6</td>
</tr>
<tr>
<td>Major</td>
<td>1</td>
<td>0.8</td>
<td>2</td>
<td>1.1</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>1.7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Age (years)</td>
<td>28</td>
<td>N/A</td>
<td>27.6</td>
<td>N/A</td>
</tr>
<tr>
<td>Average Years in Communication Career Field</td>
<td>3.0</td>
<td>N/A</td>
<td>2.5</td>
<td>N/A</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>112</td>
<td>94.1</td>
<td>14</td>
<td>7.4</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>6</td>
<td>5.1</td>
<td>159</td>
<td>83.7</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>0.8</td>
<td>17</td>
<td>8.9</td>
</tr>
</tbody>
</table>
The basic procedure and timeline for the training sessions for both studies are shown in Figure 3. Timing and length of sessions were constrained by USAF facility management.

Participants reported to their regular block classroom at the USAF facility. They began by completing pre-training tests of their knowledge about deception and deception detection accuracy (or judgment). The pre-training knowledge test measured how much of the subject matter the trainees understood as they began the session. Both tests were repeated after the training had been delivered but in slightly different forms.

The knowledge tests consisted of multiple-choice questions drawn from the deception detection curriculum materials. The same questions were used in both pre- and post-training tests but in a different order. There were 12 questions in the first study and 10 in the second. Appendix B shows details of the post-training knowledge test.

The judgment tests measured participants’ ability to detect deceptive behavior. These tests consisted of examples in video, audio, or text formats, showcasing either deceptive or non-deceptive behavior. Participants were asked to judge if the behavior in the example was truthful or dishonest. There were six judgment items in the first study and 10 in the second. The pre- and post-training judgment tests were similar but consisted of different examples.

All participants in both studies received feedback on the correct responses to the pre- and post-training knowledge and judgment tests.

The experimental designs for the two studies are shown in Figure 4. In the first study, participants were assigned to either a control group, where they took the same pre- and post-training tests but did not have any training, or to a group that received training either from a live lecturer or through the same configuration of Agent99 Trainer. Participants sat through three training sessions: an introduction, a session on cues to deception, and a session on heuristics related to deception and its detection.

In the second study, the control group was trained via a videotaped lecture. Each of the other groups was exposed to one of four different configurations of Agent99 Trainer, each with successively more features. Participants received only two training sessions—the introduction to deception and the session on cues.

### Study Results

One of our main objectives was to determine whether training on deception and its detection could improve people’s ability to successfully detect deception. The results from both studies provide evidence that appropriate training can improve deception detection. In the first study, as expected, we found that participants who were exposed to the e-training

---

11 We based the cues for this study on those found in DePaulo, B., Lindsay, J., Malone, B., Muhlenbruck, L., Charlton, K., and Cooper, H. “Cues to deception,” *Psychological Bulletin* (129), 2003, pp. 74-118.
The Role of E-Training in Protecting Information Assets Against Deception Attacks

Figure 4: Experimental Designs for Both Studies

<table>
<thead>
<tr>
<th>Training Session</th>
<th>Attended Lectures</th>
<th>Used Agent99</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Deception</td>
<td>60%</td>
<td>59%</td>
</tr>
<tr>
<td>Cues to Deception</td>
<td>57%</td>
<td>63%</td>
</tr>
</tbody>
</table>

Participants using e-training performed better than the traditional classroom-trained participants on the cues-to-deception material presented in the training session. This is encouraging because it demonstrates that even a subject as cognitively demanding as deception detection can be taught in an e-training format.

In the second study, all experimental groups, whether exposed to the videotaped lecture or to one of the four configurations of Agent99 Trainer, increased their knowledge about deception and its detection, and their ability to detect deception (judgment). Figure 6 shows the results for the pre- and post-training judgment tests. Prior to the instruction, all groups performed at less than the 50% success rate known in the literature; after training, all groups except those who had watched the videotaped lecture performed at a 60% success rate or better.

Our second research question, tested in the second study, was whether the delivery method mattered. To understand the training effectiveness of the various delivery system did just as well in both the knowledge and judgment tests as those who took the traditional classroom training version. Figure 5 shows the deception detection accuracy rates for the first study, as measured by the post-training judgment test scores.

Figure 5: Post-training Judgment Test Scores for Detecting Deception in the First Study

© 2008 University of Minnesota
Agent99 Trainer configurations, we conducted a planned comparison analysis using Helmert contrasts. This statistical technique tests whether the additive features are differentially effective by comparing the results of each configuration with the average results of the remaining, more sophisticated configurations.\(^\text{12}\)

We found that delivery method had an effect on judgment test scores, or participants’ ability to correctly distinguish between truth-tellers and deceivers. In short, participants who used more feature-laden versions of Agent99 outperformed those who used simpler versions. The Helmert contrast results that underpin the findings detailed below are set out in Appendix C.

For the second study’s “Introduction to Deception” session, students using the three versions of Agent99 Trainer with more features outperformed students using the basic Agent99 Trainer configuration. Also, users of the Agent99 Trainer configuration with the most features outperformed those who used the similarly configured version that did not include quizzes.

As Figure 6 shows, all students in the second study improved their performance on the judgment tests,\(^\text{13}\) but students who used any configuration of Agent99 Trainer improved more than those who were exposed only to the videotaped lecture. Looking at results across the entire training period for the knowledge tests, we also found that users of Agent99 Trainer with the most features outperformed those who used the similar configuration but which lacked quizzes.\(^\text{14}\)

### LESSONS ON DECEPTION DETECTION TRAINING

The objective of our research program was to determine if training could improve people’s ability to detect deception. Previous studies have, at best, had limited success in determining this issue, but our research demonstrated that training can improve IT professionals’ abilities to detect deception, which in turn helps them to better protect critical information assets. We found that, given the right training content and the right delivery methods, it is possible to make people more knowledgeable about deception and its detection. Given this, organizations should consider providing their employees with deception detection training as a means to prevent security breaches perpetrated by social engineering. We offer the following suggestions to CIOs and IT managers.

**Lesson 1: People Can Be Taught to Be Better Detectors of Deception**

Even though most people have a limited innate ability to tell when they are being deceived, they can be taught to be better at it. We provided our students with knowledge of the deception domain and taught them how to identify the cues that are indicators of deception. The training we provided increased their knowledge of deception and ability to detect deception. The students in our study were all military officers in a career field that includes duties such as IT administration, network security, and computer security.

---


\(^{13}\) To make this comparison, we compared pre-training test scores before the introductory session to post-training test scores after the cues session.

\(^{14}\) While we found that users of the Agent99 Trainer with the most features outperformed those in groups using configurations with less features, we did not record how much the students actually employed the additional features. However, we believe the additional features may be useful for distance-learning situations.
and information assurance. Their duties require them to protect information and information systems from attack. Deception is often a characteristic element of such attacks.\textsuperscript{15} Organizations with a need to protect sensitive information should consider including this type of training in their information security strategies. As we have noted, failure to educate employees on deceptive practices such as social engineering risks neutralizing other organizational security mechanisms.

**Lesson 2: Online Deception Detection Training Can Produce Better Results Than Traditional Training**

A primary focus of our research was to determine if a topic as cognitively challenging as deception detection can be effectively taught online. While traditional classroom training is often desirable when challenging topics are taught, it can be costly, especially in a geographically distributed organization. E-training enables courses to be delivered remotely, and our studies showed that training in deception detection can be effectively delivered in this way. Further, since e-training typically costs less than traditional training and can be delivered in forms that can accommodate various learning styles, providing deception detection e-training can be a good investment.

**Lesson 3: Media Variety and Interactivity are Worth the Extra Small Investment**

Online training often fails because it lacks variety or interactive capabilities. Everyone learns differently. This is especially true for subjects like deception detection where the curriculum is cognitively difficult. However, if the e-training made available to employees allows them to ask a question or view more content or take periodic quizzes, then the training becomes student-centered, which can result in more learning. Especially valuable is the inclusion of features that require students’ continued engagement and interactivity (as the quizzes did). Such additional features are inexpensive to develop, yet they can potentially yield excellent returns in the form of increased learning.

\textsuperscript{15} For more information on attack characteristics, see Denning, D. E. *Information Warfare and Security*, Addison-Wesley, 1999.

** ACTIONS FOR CIOS AND IT MANAGERS**

Our research results and lessons learned lead to four actions for CIos and IT managers.

**Action 1: Assess Your Current Deception Detection Training**

Are you training your employees about deception? How? Do you know if the training is effective? Deception is common in the IT workplace so CIOs should provide employees with training about what it is and how to detect it. Our research shows that training can improve people’s ability to successfully detect deception.

**Action 2: Focus on Cue-based Deception Detection Training**

Tactics-based training teaches employees how to spot the domain-specific tactics deceivers might use. Tactics are part of a topic-specific strategy for manipulating information. If you can learn the strategy, you can learn to detect the tactics that are used to implement it. However, the deceiver’s tactics are targeted at a particular domain.

On the other hand, cue-based training teaches employees how to detect the non-domain-specific physiological, psychomotor, and linguistic cues that “leak” from deceivers. Cue-based training focuses on the characteristics of deceivers’ communication, and, in many cases, deceivers are not even aware that they are exhibiting them. Cue-based training is applicable to any context and helps people understand why certain behaviors indicate deception so they can recognize those behaviors and avoid falling victim to the deception. Our research shows that a cue-based training approach can improve people’s ability to successfully detect deception.

**Action 3: Consider E-training**

Use an e-training system, such as Agent99 Trainer, to effectively train employees about deception detection. Such a system can be Web-based, which means it is inexpensive (no need for travel or live instructor; content can be easily updated as necessary) and convenient (can be done any place, any time). Furthermore, because e-training can be designed to provide greater learner control and other supportive features not available in traditional training, it can result in more effective training—that is, better learning performance. A well-designed e-learning
system allows trainees to go at their own pace, focus on the content that addresses their individual learning objectives, and tailor the learning experience to their individual learning styles. Our research shows that e-training is as good as, or more effective, than traditional training.

**Action 4: Enhance E-training with More Features For Better Learning**

E-training can be effective at improving people’s deception detection skills, but some bundles of e-training features work better than others. Trainees become more accurate judges of deception when the e-learning system:

- Has features, such as a navigable outline and search tools, that facilitate self-directed learning strategies.
- Involves practice and feedback of skills (for example, through quizzes and scenario analysis).

Quizzes and testing features seem to be particularly effective. In our research, participants using the version of Agent99 Trainer with the most features often outperformed participants using less feature-rich versions. For the best possible results, CIOs should therefore choose e-training that provides trainees with self-direction as well as practice, quizzes, and feedback.

**E-TRAINING IN DECEPTION DETECTION HELPS TO PROTECT INFORMATION AND SYSTEMS**

Deception-based attacks on information and information systems are hard to defend against. Those intent on causing harm have found ways to deceive in all realms of life and have become very successful at it. Furthermore, people are not very good at detecting deception, and there is no current technology capable of easily and inexpensively identifying a deceiver. Thus the only immediate solution is to train people to be better at detecting deception. While providing this type of training has been problematic in the past, we have demonstrated that people can be trained to detect the cues that leak out from deceivers. More importantly, we have shown that such training can be successfully delivered online. Organizations at risk of losing valuable information due to deception-based attacks should therefore provide online training for their employees in how to detect deception. Our research has shown that such training certainly can be effective.

**APPENDIX A: EXAMPLE OF CUES TO DECEPTION TRAINING CONTENT**

PRESENTER: The fourth category of reliable indicators of deception relates to memory processes. When truth-tellers are asked to respond to questions, they search memory for real details. Deceivers have no such memory to rely on and must invent details. Real and familiar events, places, or information that can be retrieved from memory usually produce richer language or content than imagined or fabricated ones. Due to fabricated events being made up on the moment, it would be difficult to describe them in detail. Therefore deceptive utterances are often shorter, less specific, less complex, use less varied language, and end up being less coherent. Because people are typically unaware of how they translate their thoughts into words, they do not monitor their own behavior nor are they readily able to manipulate such behavior. That makes these memory-based indicators especially reliable in separating truth from deception.

First, deceptive utterances are often shorter in terms of the number of syllables, words, sentences, or amount of talking time.…

A second memory-related class of indicator is specificity, which includes both content and linguistic specificity. Content specificity relates to a statement being rich in details, such as specific descriptions of place, time, people, objects, or events. Because truth-tellers have real memories that they are accessing, their messages should include more details and more specific details. This is what content specificity is all about. Many of these details should be sensory in nature, related to things seen, heard, smelled, and touched. There should also be details related to space and time: “The green car was parked diagonally so it took up two parking spaces.” The details in a truthful message may also be unusual or unexpected—things that would be hard to make up. Truthful messages may also contain spontaneous corrections of details. People telling the truth often correct themselves as they talk, making their stories more accurate. Deceivers include far fewer details and have no need to correct errors from memory because they are not drawing on actual memory.
Take a look at this example [on the PowerPoint slide] that shows the kinds of details present in a truthful response.

POWERPOINT SLIDE: “Alrightie here we go ... so I got to class and talked to my UTA for a few minutes just about whatever, and then I sat down and did my homework that was due that day (shhh!), and then I waited for class to start. Oh, and I stepped out to go to the bathroom, which I did not put on the form I filled out previously b/c I forgot about it. Then about five minutes before class started, a woman came into the classroom and placed four black wallets around the room—one on the chalkboard ledge of each of the four chalkboards in the room. Then class began and students were giving speeches. I kept my eye on the wallet throughout class. I’ll be totally honest with you, I was feeling very tired b/c I didn’t sleep the night before so I wasn’t concentrating too hard on the wallet, but I know that after the speeches were finished and I turned in my homework and left, the wallet was still here.”

PRESENTER: Did you notice the specific visual details, such as number of wallets, the number of references to place and time, the mentions of her feeling states, and the unusual detail of going to the bathroom? Plus, she spontaneously corrects her previous written report.

APPENDIX B: SECOND STUDY POST-TRAINING DECEPTION KNOWLEDGE TEST

1. What would be a reliable kinesic indicator of deception?
   a. The speaker is leaning forward
   b. The speaker has stiff, wooden posture
   c. A highly expressive face
   d. Relaxed posture

2. Under what conditions are deceivers likely to produce longer messages than truth-tellers?
   a. When they have time to plan, rehearse, or edit their communication
   b. When they are trying to be persuasive
   c. When the communication medium has time delays, such as with e-mail
   d. All of the above

3. A physiological indicator that might tip off a deceiver to a polygraph (lie detection machine) would be:
   a. Decreased blinking
   b. Increased pulse rate
   c. Negative speech
   d. Increased stuttering

4. The theory that suggests that deceivers strategically and intentionally alter their messages to avoid detection is:
   a. Interpersonal deception theory
   b. Indicator theory
   c. Leakage theory
   d. Cognitive effort theory

5. Which of the following would NOT be a reliable cue pointing toward deception?
   a. Lower voice pitch
   b. Poor detail in a particular message
   c. Non-ah nonfluencies [a silent pause in speech; contrasts with ah nonfluencies, where the speaker fills the pause with sounds like “ah,” “um,” and “er.”]
   d. Fewer pauses

6. It is possible that deceivers are having a difficult time lying if we notice that they:
   a. Respond immediately after being asked a question
   b. Behave in a normal manner
   c. Drop the names of others into conversation
   d. Stop gesturing

7. A ________ may be used by deceivers to mask their negativity toward others.
   a. non-ah nonfluency
   b. Self-grooming behavior
   c. Feigned smile
   d. Long response latency

8. The increased difficulty associated with lying while conveying a consistent story to others is known as _____________.
   a. Cognitive effort
   b. Leakage theory
   c. Arousal
   d. Deceptive stress and strain
9. Truthful messages are more likely to contain:
   a. Fewer personal pronouns (I, we, etc.)
   b. Use of vague verbs like “could” and “would”
   c. Qualifiers like “perhaps” and “possibly”
   d. Definitive words like “definitely” and “absolutely”

10. If writing or e-mailing a truthful message to others, an honest person is likely to use:
   a. More punctuation
   b. Simple sentence structure
   c. Limited vocabulary
   d. More misspelled words

APPENDIX C: HELMERT CONTRAST RESULTS FROM THE SECOND STUDY

To understand the relationship between the different combinations of system functions and training effectiveness, we conducted planned comparison analyses using Helmert contrasts. Helmert contrasts test whether treatments with additive features are differentially effective, by comparing each level or group with the average of the more sophisticated remaining levels. We used Helmert contrasts to compare the different configurations of Agent99 Trainer for each of the two sessions the participants were involved in—the introduction to deception session and the cues to deception session.

For the introduction to deception session, the configuration of Agent99 a trainee used made a significant difference in his or her performance, as measured by the post-test judgment tests (F (1,175) = 2.682, p < .033). The Helmert contrast results show that trainees who used the basic Version 1 of Agent99 Trainer (with linear navigation only) for the introduction to deception lecture performed differently from those who used the successively more sophisticated Versions 2, 3, and 4 (p < .035), and that the effectiveness of Version 3 was different from Version 4 (p < .033). However, for the cues to deception lecture, performance differences were not related to the configuration of the Agent99 Trainer trainees used.

Differences in performance across the entire training period—i.e., across both training sessions—were also evaluated using Helmert contrasts. The configuration of the Agent99 Trainer used also made a difference in performance on judgment tests across both training sessions (F (1,167) = 3.226, p < .014). Trainees who experienced only a video lecture did not improve as much at detection judgment as those who used any of the more sophisticated Versions 2, 3, and 4 of Agent99 Trainer (p < .002).

ABOUT THE AUTHORS

Joey F. George
Joey George (jgeorge@cob.fsu.edu) is a professor of information systems and the Thomas L. Williams Jr. Eminent Scholar in Information Systems in the Management Information Systems Department in the College of Business at Florida State University. His research interests include deceptive computer-mediated communication, computer-based monitoring and group support systems. George currently serves as editor-in-chief of *Communications of the Association for Information Systems*. He is co-author of four textbooks for Prentice Hall and editor of a fifth book.

David P. Biros
David Biros (david.biros@okstate.edu) is Assistant Professor in the Management Science and Information Systems Department in the Spears College of Business at Oklahoma State University. He earned his Ph.D. from Florida State University in 1998. He retired as a Lt. Colonel from the United States Air Force in 2005. His final duty assignment was as Chief Information Assurance Officer for the Air Force’s CIO. His research interests include deception detection and information system trust. He is an associate editor for the *Journal of Digital Forensics, Security and Law*. He currently serves as a review panel member for the NSA Centers of Academic Excellence in Information Assurance Education Program.

Judee K. Burgoon
Judee Burgoon (judee.burgoon@gmail.com) is Professor of Communication, Family Studies and Human Development at the University of Arizona, where she is Site Director for the Center for Identification Technology Research and Director of Research for the Center for the Management of Information in the Eller College of Management. Burgoon has authored seven books and monographs.
The Role of E-Training in Protecting Information Assets Against Deception Attacks

Jay F. Nunamaker Jr.

Jay Nunamaker (jnunamaker@cmi.arizona.edu) is Regents Professor and Director of the Center for Management of Information at the University of Arizona. He was a faculty member at Purdue University prior to founding the MIS department at the University of Arizona in 1974. Nunamaker received his Ph.D. in systems engineering and operations research from Case Institute of Technology. In 1992, he received the Arthur Andersen Consulting Professor of the Year award. In 1996, he received the DPMA EDSIG Distinguished IS Educator Award.

Janna M. Crews

Janna Crews (jcrews@unr.edu) is an assistant professor in the Department of Accounting and Information Systems at the University of Nevada at Reno. She received her Ph.D. in Management Information Systems from the University of Arizona. Her research interests include computer-assisted instruction (CAI) design, e-learning and multimedia training, collaboration to improve business processes and system analysis, and design issues, including human computer interaction and usability.

Jinwei Cao

Jinwei Cao (jcao@lerner.udel.edu) is an assistant professor in the Department of Accounting and Management Information Systems at the University of Delaware. She received her Ph.D. in Management Information Systems from the University of Arizona. Her research interests include technology-supported learning, multimedia information systems, human computer interaction and usability, and knowledge management. She has published in the Journal for Management Information Systems (JMIS), the International Journal of Technology and Human Interaction, and the Journal for STEM Education. She has also presented over 14 papers at prestigious international conferences, including AMCIS, ICIS, and HICSS.

Kent Maret

Kent Marret (lkm2@msstate.edu) is an assistant professor of Management Information Systems at Mississippi State University. He holds a Ph.D. in MIS from Florida State University. His primary research interests include deceptive communication in computer-based media, user security and privacy in online environments, and the use of technology in individual and group decision making.

Mark Adkins

Mark Adkins (m.adkins@accenture.com) is a chief solution owner at Gestalt, now a part of Accenture. In this role, Adkins focuses on issues and developmental architectures relating to command and control service level management. He has also initiated research into inter-enclave communication amongst secure networks across the defense enterprise. He is an authority on network centric operations (NCO), collaboration, group decision making, human communication, information systems, and elements of humanitarian assistance/disaster relief (HA/DR). Adkins earned a Ph.D. from the University of Arizona and is a thought leader as well as an action officer with over 80 publications in peer-reviewed journals, book chapters, and conference articles/proceedings.

John Kruse

John Kruse (kruser@gmail.com) is a lead information systems engineer at the MITRE Corporation. He was previously the Director of Systems Development at the University of Arizona’s Center for the Management of Information. His primary field of interest is decision support. In pursuit of this, he has worked extensively in the field of network-centric military operations and automated deception detection.

Ming Lin

Ming Lin (jerry.minglin@gmail.com) is a software architect at WorldEvolved Services, LLC. Before joining WorldEvolved, he was a software engineer at Google Inc. Lin received his Ph.D. from the University of Arizona. During his Ph.D. studies, his research areas included natural language processing, video indexing and retrieval, knowledge management, and computer-assisted learning. He has published more than 16 papers in top MIS journals and conference proceedings.