Annotated Bibliography

1) Legislation and Ethical Issues:


FERPA, or the Family Education Rights and Privacy Act, is a Federal law that protects the privacy of student education records, so long as the school is receiving funds under an applicable program of the United States Department of Education. As St. Olaf College does receive funds from the U.S. Department of Education, this law protects the privacy of student records. Although St. Olaf can disclose "directory" information (e.g. student's name, address, telephone number, date and place of birth etc.), St. Olaf is required to provide parents and students with the opportunity to request that this directory information not be shared.

Malicious data mining and other acts of social engineering, such as phishing, put student information, which is stored digitally on St. Olaf servers, at risk of being obtained illegally. By familiarizing ourselves with FERPA, we can appropriately suggest a security training program which prioritizes the safety of student education records.


GLBA, or the Gramm-Leach-Bliley Act, is a United States public law which requires financial institutions to provide a consumer with a privacy notice when the relationship is established and annually thereafter; the privacy notice must say what information has been collected about the individual, where that information is shared, how that information is used, and how that information is protected. St. Olaf is legally defined as a financial institution and it thereby must conform to this law in interaction with student and employee consumers.

Malicious data mining and other acts of social engineering, such as phishing, put student and employee information, which is stored digitally on St. Olaf servers, at risk of being obtained illegally. By familiarizing ourselves with the GLBA, we can appropriately suggest a security training program which will prioritize the safety of student and employee information.


HIPAA, or the Health Insurance Portability and Accountability Act, is a United States public law which, amongst other things, requires health care providers and organizations to develop and follow procedures that ensure the confidentiality and security of protected health information when it is transferred or handled. St. Olaf, as an organization which has both employee and student health information on file, may not disclose this information to outside parties without consent of the individual.

Malicious data mining and other acts of social engineering, such as phishing, put student and employee information, which is stored digitally on St. Olaf servers, at risk of being obtained illegally. By familiarizing ourselves with HIPAA, we can appropriately suggest a security training program which prioritizes the safety of student and employee health records.

This paper focuses on the unique problems that face universities in regard to managing and protecting the administrative, academic, and personal information of students and employees. This study provides a framework for approaching the management of professional and personal sensitive information given the unique requirements faced by higher education and overviews the best contemporary methods for managing and securing sensitive information within a large institution.

As an institution which retrieves personal, health, and financial information from its students, employees, and customers, it is important for St. Olaf College to have security systems and training programs in place to help users accurately detect security threats. We are hoping that this article will not only inform us about the variety of threats which exist but also proven methods for effectively managing legally protected information.

2) Social Engineering and Design Values for better Security Programs:


This article discusses a warning from AhnLab Inc, a leading provider of integrated security solutions, regarding the dangers of social engineering. Phishing and scam threats are increasingly common techniques that rely heavily on human interaction and user gullibility to break security protocols and infect victims’ PCs. The article discusses an android passed application, disguised as a London Olympics app, which sent messages at a premium rate without user permission while sending information from the phone to the attacker. This article concludes with a concrete list of six proven techniques that if applied will reduce vulnerability.

This article is important because it demonstrates how widespread phishing threats are; an event as large as the Olympics was made vulnerable by phishing scams, so it can certainly happen to any of us. However, what is most important to us is the list of tips that will help defend against phishing. Since AhnLab is a security firm, their advice will be very reliable for keeping St Olaf secure.


This study focuses on critical human factors that phishers exploit for criminal gain. Cranor has discovered that sending out anti-phishing mail to non-victims is virtually useless. They are just as likely to succumb to phishing attacks as non-victims who have gotten no anti phishing email. However, Cranor found that once someone became the victim, they were far more likely to not be heed anti-phishing warnings.

This article is important because it gives us a concrete example of effective and ineffective methods of phishing prevention and security training. This information could save us time and
resources down the road. Also, we are looking for a method of training employees in security measures. This article describes a game used to teach students how to avoid falling for phishing attacks. While, this might not be a professional enough program, it gives us a starting point for what attributes to look for.


This book provides an overview of phishing; Lance goes into depth about spam, cyber-crime, phishing, and covers a variety of relevant legal issues. He also talks about different phishing cons from the hacker’s perspective. By looking at the strategy used by hackers, we can better defend ourselves against the risks of being online.

This book is useful to us because it covers all the relevant aspects of phishing. It should not only give us a solid overview but also allow us to act as a springboard for finding other relevant articles.


An uncommon approach to solving phishing issues, this paper discusses the concept of emailing a phishing attack in an unannounced test as an exercise for phishing awareness. This unannounced test can provide insight into how phishing works, how effective it is, and how to better educate people about the digital risks.

This approach to evaluating security training programs would be very useful to our project. Not only is this a great idea that could possibly be implemented, but it also provides insight into how to better educate people about phishing and ultimately prevent it.


This paper details the effectiveness of two training methods—a simple comic-based approach and a more complicated video game program—in helping users to successfully identify phishing emails as untrustworthy. It also attempts to demonstrate connections between these different training techniques and individual attributes such as trust, impulsivity, and computer experience that affect susceptibility to phishing scams.

The programs themselves may be of interest to the St. Olaf Business office, and are certainly worth looking into. However, even if we ultimately choose to implement neither program, this paper demonstrates the use of “test” phishing attacks and the statistics involved in interpreting the results—methodology that will be invaluable if we decide to pursue that assessment strategy.


This article proves a brief summary of an Oakland University press release. In the release, the article talks about how University Technology Services warns students about a phishing scam. The scam is an email attack with a link to an external website. The website is sophisticated with the OU logo. Students are offered prizes for completing a survey. The Chief Information Officer at OU then gives some advice for how to handle a phishing scam.
This article is useful for several reasons; it gives detail into a real phishing attack on a college campus, which is what we are interested in. It shows the tactics and techniques of the phishing attempt, so we would know what to look for. It also gives preventative measures to prevent becoming a victim of phishing. We can use these techniques in our report. The only downside to this article is that it is in a newspaper, so there are no statistics as to the effectiveness of the preventative measures. Despite this drawback, the information is valuable enough for giving a basic overview of a phishing crisis.


This paper identifies and overviews the security threats associated with phishing, a social engineering technique which uses fraudulent email and web sites to trick unsuspecting users into submitting and revealing private personal, health, or financial information. In order to combat phishing, these researchers designed and tested a content-based system, called CANTINA, which uses a TF-IDF information retrieval algorithm, found to detect phishing websites 95% of the time.

As an institution which retrieves personal, health, and financial information from its students, employees, and customers, it is important for St. Olaf College to have security systems and training programs in place to help users accurately detect suspicious URLs. In looking at CANTINA, we are hoping to identify certain design values which may inform our final program proposal.

3) Security Training and Awareness Programs:


While the most common approaches to security awareness training involve online exercises, surveys, awareness, or all three, Albrechtsen and Hovden offer an analysis of a dialogue-based approach wherein participants actively share ideas about security threats and the best practices for combating them. Through collective reflection on the way employees treat data, actual behaviors can be significantly improved.

The training system proposed in this paper could be particularly useful for small institutions like St. Olaf, which is tasked with the collection and protection of a wide variety of student and employee personal information. In particular, the study includes quantitative evaluations of the program’s effectiveness via surveys, a technique that may be useful in diagnosing and auditing the state of security awareness at St. Olaf.


This article discusses common failures by IT organizations to apply security patches and configure security settings correctly. Timely patching of security issues is generally recognized as critical to maintaining the operational availability, confidentiality and integrity of IT systems.
These authors express how a study of all computers in a network and their patching schedules is crucial to keeping security at its highest.

In our project, it is important to confirm with IT that all security settings are up to date and properly patched. Being out of date with security patches is a dangerous problem if not considered and knowledge of this problem is half the battle. The article also proposes solutions to this problem that we could easily implement into a training program.


Banerjee and Pandey argue that individuals, rather than programs or databases, are often the first target for those seeking to gain access to sensitive information. This paper proposes that the process of handling data should be just as resilient as the software that organizes it; security awareness is critical to a complete software security solution.

The paper provides an invaluable review of research in the area of security awareness. It offers a myriad of different angles by which to address the security awareness problem, and it discusses some of the merits of each approach, such as interviews, surveys to educate project stakeholders, game simulations for training employees how to react to particular situations, online community forums for discussion of the issues, and routine tests of employee awareness to keep tabs on progress.


This qualitative study focuses on how human and organizational factors play a role in security vulnerabilities. The paper examines the interplay between human users and programmers and the software they work with, categorizing 9 areas of interest in particular: external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. It also summarizes the findings of two focus groups composed of five information security experts each, who identified a total of 50 pathways from human and organizational factors to security breaches.

For our purposes at St. Olaf, this article provides an important list of areas where security awareness has a direct impact on security. It will also provide detailed insight into the broader socio-technical system of information security.


This article offers the author's insights on how employees should be trained. Nixon states that in designing training programs, a set of goals should be clearly established. He also emphasizes the roles of the trainers in order to facilitate learning among employees. Moreover, he mentions that training should have certain degrees of competencies which are needed to be satisfied.
For our project, this source offers additional information on how employees should be trained in the best way possible, and how those training programs should be evaluated. This source especially covers employee and trainer relations.


This source gives a detailed description of standard training procedures used to train employees about security threats. Written by a former instructor in security education, this source thoroughly the entire process of how to train employees, including sections on how to motivate people to follow procedure, going steps beyond training and educations, how not to train employees, and evaluating security education programs.

For us, this source is immensely useful as it provides insight into how to educate employees about security issues in the most effective manner possible. The section about evaluating security education programs is particularly useful for our current project, as that is exactly what we are trying to do.

Semer, Lance J. (2012). Evaluating the employee security awareness program: regular audits of IT safeguards can reveal whether staff members are doing their part to protect the organization's data and networks. *Internal Auditor, 69*, 53-65.

This paper details the importance of auditing security awareness programs and provides a few tips on risks to watch out for in performing such audits. Specifically, the author discusses the importance of securing physical data storage device, the risks of accessing institutional mail or data systems from personal devices, and the dangers associated with paper media in addition to digital. He suggests that each area in the “security triad [of] technology, processes, and people” is equally vital in providing effective security coverage within an organization.

Our project—the refinement of St. Olaf security training—should benefit greatly from the author’s suggestions such as annual distribution of awareness and code of ethics documents to be signed by employees, recording and reviewing incident logs regularly, and making clear that security is everyone’s responsibility.