Phishing for user security awareness

Ronald C. Dodge Jr.*, Curtis Carver, Aaron J. Ferguson

Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY, USA

Keywords:
Phishing
Email security
Social engineering
Security training
Information assurance
Spam
Computer user education

Abstract
User security education and training is one of the most important aspects of an organization's security posture. Using security exercises to reinforce this aspect is frequently done by education and industry alike; however these exercises usually enlist willing participants. We have taken the concept of using an exercise and modified it in application to evaluate a user's propensity to respond to email phishing attacks in an unannounced test. This paper describes the considerations in establishing and the process used to create and implement an evaluation of one aspect of our user information assurance education program. The evaluation takes the form of a exercise, where we send out a phishing styled email record the responses.

1. Introduction
The quest for information systems security has a significant, almost self cancelling facet—the user. User information assurance (IA) awareness is a random variable that is very difficult to characterize due to user's individual nature. Users create an open back door into our corporate networks through their internet enabled services, third party application use, and electronic interaction (i.e. email) with other users. This vulnerability is increased from mobile systems that join home and other commercial networks. While the application of host and network based security applications can provide some mitigation against malicious activity, there is no static technical defensive measure that can mitigate the threat introduced by user behavior. One of the most common interactions users have with entities outside control of our local networks is email. The July 2006 report issued by the Anti-Phishing Working Group reported 23,670 unique phishing attempts targeting over 14,191 websites used to commit identity theft, fraud and other malicious activity. These websites are very dynamic in nature, existing only for an average 4.8 days (Anti-Phishing Working Group, 2006). Security training and awareness programs have done a good job of mitigating this risk— but just how good? What measures exist to verify that users understand and consistently apply the best practices they are exposed to during periodic training?

The use of exercises to reinforce concepts in an educational setting has been written about frequently (Dodge et al., 2005). The United States Military Academy (USMA) has been very active in implementing hands-on exercises such as the Cyber Defense Exercise (Dodge et al., 2003). Typically, these exercises involve participation by knowing participants and involve a network attack/defense scenario. The United States Military Academy took the concept of an active learning and developed an email phishing exercise with the intent of evaluating the efficacy of our user IA training. The exercise first ran as a prototype in the spring of 2004 and has since been run two additional times. The most recent exercise (at the time of this writing) ended in November 2005.

The exercise was named Carronade after the Navy cannon used in the early 1770s. The inventors, Charles Gascoigne, Lt. General Robert Melville, and Patrick Miller, designed the
cannon in 1759 while working at the Carron Iron Works Company on the Carron River in Stirlingshire, Scotland. The short cannon weighed about 68 pounds. They initially called it the “Smasher,” but it was not adopted until 1779, and was then known as the Carronade. The Carronade although possessing limited range, was destructive at close quarters (less than 0.6 miles). It is important to note that in offensive operations during the 1700s, the objective was not to sink an enemy vessel but rather to avoid damaging the hull so as to capture it as intact as possible, so it would be retained as a “prize”.

In keeping with this military theme, this exercise was named the Carronade because: (a) while the email had the potential to be destructive, the intent was to get the attention of cadets, not to cause damage to the Academy network or to penalize the cadets; and (b) the exercise was short range – conducted inside the USMA security perimeter – only cadets with a usma.edu domain name could launch the embedded link.

In this paper, we will present a background discussion on the exercise, describing its origin and planning considerations. We will further describe the evolution of the exercise from a prototype to a multi-email exercise designed to evaluate different forms of phishing and the efficacy of training. We will provide results from each exercise and offer some assessment of our awareness and training program. We then conclude with a look toward future exercises.

2. Background and previous work

West Point has two primary mechanisms for reaching out to our students with information assurance training and education. The first is through our curriculum for those students enrolled in our information assurance focused courses. The second is through a series of required training provided to every student. The curriculum leads to our capstone informatics project, where each student has a specific suite of software. While they are allowed to install third party applications that are not part of the official suite, they must purchase them on their own and the computer staff at USMA will not support them. Given these limitations virtually all students have the same basic configuration. In addition, email is a very heavily relied upon management and information dissemination tool.

2.1. General considerations

Depending on your organization, the specific implementation of an email phishing exercise might vary. However, certain general considerations are transparent and are important to address. The most important consideration is to define the objectives of the exercise. The exercise needs to have a clearly defined goal that is consistent with the awareness and training program in place.

A second consideration is to devise a mechanism for assessing IA awareness programs that is non-punitive and not directly involve the institution computer security staff. We feel that the trust between the security staff and the end user is very important and we want to avoid compromising the relationship. Given the student run IA program, we elected to organize the event at the staff level; however, it is implemented by the student chain of command. The student ISO’s provided any corrective training immediately at and forwarded only statistical analysis to the Academy leadership. This no-threat, local resolution policy is a key aspect of the
exercise. As described by David Jevans, chairman of the Anti-Phishing Working Group in Bank (2005), exercises like this might develop into a lack of trust of company emails.

The third consideration is to involve all stakeholders. In our environment this included the Academy officer leadership and the students responsible to implement the security awareness and training program. We decided that to meet the objective of our first consideration, the student group involved would implement the exercise with faculty oversight on the design. An unexpected benefit of exercising the real security response team arose from initiating the exercise at the student level. No information about the exercise initiation was passed on to the campus computer security team. When incidents of large amounts of phishing started to be reported, the staff had to execute just as if it were initiated externally. The Academy leadership saw this as a good opportunity to review and evaluate academy responses.

A fourth consideration that should be included regardless of the agency is involvement of the legal staff. There are two important facets that legal can provide opinions and guidance on; human subject research requirements and assessment on personal privacy.

The final general consideration is to construct the exercise to coexist with the organizational structure. We want the emails to be believable, but not lose their validity due to the nature of the organization. For example given the military nature of USMA, our students operate under a strongly enforced military hierarchy; however, they must be able to discern the difference between an appropriate and inappropriate request.

2.2 Specific considerations

Once the general considerations are accounted for in the exercise design, we determined the specific requirements to make the exercise successful. Our first consideration was devising an email that a student would definitely be interested in opening, reading, and complying with. The objective is to provide the students with an email that they are enticed to open, however, if they read it carefully, they would realize it is not valid. One of our design decisions was to avoid common phishing email contents such as financial or services emails. We decided for our final email prototype that the student would be instructed to visit a website (hyperlink) to validate course grades. The second specific consideration, timing, fit nicely with the email content. For the prototype we constructed the email near the end of the semester when students would be most concerned about grade correctness. In general, the timing should be such that the test can accurately assess the defined objective. For example, if you are testing the long-term retention of security practices, the exercise should be conducted after a “cool down” period. Further if you are evaluating the increase in awareness over a time period, the exercise should be conducted at similar times for each implementation. The email in Fig. 1 is an example of the prototype.

The third specific consideration focused on the target. Prior to the exercise, a target population needs to be identified. For our prototype, a very small sample population across all classes was selected. The prototype (Carronade I) was limited in nature. The email referenced above was sent to 512 students at USMA (roughly 12% of the student body). Lastly, our fifth consideration, post event notification and follow-up mechanism, needed to be defined. Examples include, no notification, delayed notification to all “targets” (that may or may not include the rest of the student body), or immediate notification. In the prototype, immediate notification via an automated email was selected. In the next section we will discuss the evolution and addition of other email formats.

2.3 Carronade evolution

We conducted an assessment of the prototype and determined that the exercise could provide useful insights into the efficacy of our awareness and training program. Our focus for Carronade II was to develop a repeatable exercise that over time would serve as a yardstick to measure our programs. To that end, the exercise was conducted in September 2004. The timing of the exercise was set to ensure the new freshman class had an opportunity to become familiar with their computer and the email system at USMA. The exercise was conducted prior to any regularly scheduled IA training.

To validate that the email content was consistent with current training foci, we decided to seek input using a survey of information technology instructors. (This goes back to

![Fig. 1 – Example phishing email.](image)
including the relevant stakeholders.) The survey asked the instructors to identify the top information assurance-related negative behaviors of their students. Using the survey, we developed the following requirements for Carronade II, incorporating the following requirements and four different styles of emails:

- The system must be able to deliver an email to all students.
- Each of the emails should be questionable enough to raise the suspicions of the end user.
- None of the emails, if opened outside of the USMA domain, would collect, track, or transmit any user data.
- The first email type asks the student to click on an embedded link in an HTML-encoded questionable email to fix a problem with a fictitious grade report; clicking on the link records information readily available from the browser.
- The second email type is identical to the first email except that the email asks the student to open the corresponding .html attachment.
- The third email type asks the student to click on a link that takes them to a web form that asks for sensitive information (i.e., their social security number).
- The fourth email type asks the students to click on a link, download an application and run the application. (This was implemented, however, in each exercise technical difficulties arising from cross domain issues prevented the success.)

As noted, a significant difference in Carronade II was the number of cadets targeted with the emails. This time the scope increased to the entire student body (minus those involved in the planning and execution). Of the total number of 4155 in the student body, 4118 received the emails. The email breakdown by type was: 1010 embedded link emails, 1014 attachment emails, 999 sensitive information emails, and 1095 download emails were sent out.

Carronade III was implemented functionally with very few changes from Carronade II. A similar sample population was used (everyone minus the exercise coordinators), however, the timing was changed to more closely follow the required IA training that each student receives. The date was selected to assess whether the recently received training produced lower “violations”. The exercise was implemented in November 2005.

We chose a very similar email package – embedded link, attachment, sensitive information, and download emails. Unfortunately, different but similar problems plagued the download email and the results from this set are not included in the final analysis. The total emails sent 4136; were broken down as follows: 1006 embedded link, 1013 attachment emails, 1058 sensitive information emails, and 1059 download emails.

### 3. Technical implementation

We developed a generic design that is familiar to many web applications. The web application makes use of the Model-View-Controller design pattern separating data, display, and direction concerns within the program (Buschmann et al., 1996; Gamma et al., 1995). For our purposes we decided to use entirely open-source products to ensure that our work could be reproduced, as is, in any educational setting.

#### 3.1. Support architecture

We chose Tomcat from Apache as the Web App Container which serves up both static HTML pages and dynamic Java Server Pages (JSP) (Apache Tomcat Java Servlet Container). The email server uses Apache James, an open-source email server solution (Apache James Email Server). We decided to use an object-relational mapping solution in our project because the database schema and models were changing often and we wanted to mitigate some of the time involved in maintaining the code base (Nock, 2004). We chose Hibernate which seems to be a fairly popular and successful ORM implementation (Hibernate Object-Relational Mapping Software). For our database server, we chose, MySQL. The database server and web app container were on the same physical computer (Dual processor, 3.2 GHz, 4 GB RAM, Win2K3). Our email server was on a separate computer, but could have been co-located with the database server and the web app container. Fig. 2 shows the object diagram for the technical implementation.

#### 3.2. Phishing email construction

Our initial models were simple and evolved over time to represent the idea of a person which was used only for system administration reasons and the idea of a user’s information. The student body is broken down into four equal sub-organizations called regiments. Each regiment is further broken down into eight companies. Each company has a similar make-up across all regiments with about 25 students from each year group.

The information model contains fields that may or may not be filled in depending on the type of email the student received. The type of email was the scheme. Most of the attributes of the class were related to the information that could be retrieved from a web browser in this case the strings starting with IP and ending with mime types. The reported attribute stored whether or not the recipient of the email had reported the incident to one of the information security support personnel. The opened attribute records whether or not the recipient actually clicked on the link or opened the attachment. Each of these model conform to the Java Bean standard for web app with private class-level instance variables and public methods to get and set the values of the variables.

As we looked to design a more robust suite of emails (from the basic type we used in the prototype) we adopted the
recommendation described in Section 2.3. We selected four email phishing variants to employ; an embedded link, an attachment, a sensitive information request, and a download.

### 3.2.1. Embedded link

The first type of email which tried to get the user to click on an embedded link in an HTML-encoded email made use of a beacon, as shown in Fig. 1.

We define a beacon as a network link other than an anchor tag (i.e., \(<a>\)/) tags) in HTML over HTTP that when activated signals the existence and partial identity of a remote user. When the recipient selected the embedded link, their web browser (which is almost always Internet Explorer due to our homogenous software environment among students) opened and took them to an HTML page on the Web App Container. The link encoded their email address as a request parameter.

\(<a href='http://hostname:8080/carronade/GradeReport.html?Femail=x00000@usma.edu'>Grade Report</a>\)  

The HTML page was a modified version of a standard Internet Explorer HTTP 404 page-not-found error. The only difference is that we added a script to get the email address from the request parameter, append each of the browser properties (which include OS, IP address, etc.) and append it to the end of an image link tag which did not go to an image, but to a Java Server Page which redirected directly to a servlet. The “’” and “’” characters were added to help aid in parsing the request parameter on the receiving servlet.

\(<script\>
function submitInfo() {
    text = window.location.search + “&info = ”;
    for (var propertyName in navigator)
        text += propertyName + “= “ + navigator[propertyName] + “""; 
    document.images[0].src = document.images[0].src + text;
    return true;
}  
</script>\)

\(<meta http-equiv='refresh' content = ‘0; url = http://hostname:8080/carronade/GradeReport.html?email = x00000@usma.edu’/>\)

If the recipient opens the attachment, a web browser opens automatically and is redirected to the GradeReport.html file as described in the embedded link attachment above. An example of the attachment email is shown in Fig. 1.

### 3.2.3. Sensitive information

The third type of email (Fig. 3) tried to social engineer the student into submitting their social security number for questionable reasons over an insecure connection to a questionable website. The objective in this scenario was not to record whether the student clicked a malicious link, but if they entered sensitive information.

It should be noted that we did not actually store any sensitive data (social security numbers we used for this exercise). In fact, the HTML code did not even send the social security numbers to the servlet as indicated by the absence of the name attribute in the second input tag.

\(<form action="ssnServlet" method="post">\)

User Id:<input type="text" name="userId"/>
Social Security Number:<input type="text" name="ssn"/>
<input type="submit" value="Send Social Security"/>
</form>\)

At the servlet, this was only registered if the user correctly typed in their user id which matches their email address. Because of this privacy concern the results missed tracking many of false negatives. There is also the possibility that a student might enter another student’s user id which would lead to a false positive. Fortunately, the students who caught on to the fact that this was a bogus request typically entered in garbage in lieu of a friend’s user id.

From: sr1770@usma.edu [mailto:sr1770@usma.edu]  
Sent: Thursday, October 27, 2005 7:36 PM  
To: Cobb, M. MAJ EECS  
Subject: Account Administration Error!

Our records do not show an account verification word or pin associated with your account. This will allow you to access your account in the event you forget your password. You need to do two things:

Select this link [Update Account](mailto:sr1770@usma.edu) and follow the instructions to make sure that your information is correct; and Report any problems to me.

Charles Lidel  
LTC, AV  
Security Administration and Network Support Branch  
sr1770@usma.edu  
Olmstead Hall, 7th Floor, Room 7206

Fig. 3 – Sensitive information phishing email.
The fourth email type attempted to implement an email where the student was requested to download an application. Attempts were made in both Carronade II and III to implement this scenario, however, in each exercise technical difficulties arising from cross domain issues prevented the success.

4. Results

We elected to examine the results of the exercises in three facets. First, by overall percentage, by year, of the number of students that succumbed to the phishing emails. Second, we look at the distribution of failures by class for each exercise. Then finally, we look at the performance of a specific class over the two years.

4.1. Failure percentage by exercise version

As seen in Fig. 4, the failure rate in the prototype is very high. This is more than likely explained by the very small sample size (512). The results for 2004 and 2005 suggest minimal impact due to the recently conducted training. This, however, will require further data points to accurately draw this conclusion. It should be noted that in post exercise discussion with the students, the majority that did “fail” said they found the emails odd, however, responded anyway. The results indicate an 80% failure rate on the first prototype and approximately a 40% failure rate on the two subsequent exercises.

4.2. Distribution by email type

The breakout of failures (averaged over all Carronade interactions) by email type was interesting and proved to counter intuitive assumptions. The students were much more likely to open an attachment than they were to follow a link to a website or provide sensitive information. Fig. 5 shows that the failure rate was 38%, 50%, and 46% respectively. While the results do not indicate a significant propensity in any one area, they do provide a means to shape the discussion during email awareness training.

4.3. Distribution by class

The analysis of performance of each class as a whole provides some insight into how effect over time the training is. In the first full Carronade, each class presented similar susceptibility to phishing attacks, as shown in Fig. 6.

The two outcomes we hoped to see was a reduction in the propensity of a student to fall victim to a phishing attack and also an increase in reporting that the phishing attack occurred. In the training we stress that phishing is going to happen and that what is to be reported is phishing attacks that appear to be targeted toward the USMA population.

Given our first goal of seeing a reduction in falling victim, we should expect to see the rate of replying to the phishing attacks decrease the longer a student is at USMA (receiving the training). As shown in Fig. 7, the rate of failure shows the declining function we hoped for.

A more detailed view of the failure rate as broken down by class year and exercise iteration show the improvement by class as a function of time is shown in Fig. 8. The bars indicate by shading a given class. The scale label indicates which Carronade iteration (1, 2, or 3) the data is from. As shown, the results indicated a better performance on each subsequent exercise for each class year.
The second outcome was that the students would recognize a phishing attack that was specific to USMA, indicating a significant threat that warranted increased attention by the USMA staff. The initial statistics indicate that the longer a student is at USMA, the more likely they are to report phishing attempts. These results are shown in Fig. 9. Note that no specific questioning was done to determine if phishing attacks that are sent to the Internet population at large are also reported. However, anecdotal reports indicate that only USMA specific attacks are reported.

5. Conclusions and future work

Our students continue to disclose information that should not be disclosed to an unauthorized user and expose themselves to malicious code by opening attachments. For the United States Military, this is important given the future requirement for operational security once the students graduate and enter the Army. This information will help us not only modify the IA awareness program, but also provide input to the other areas where operational security is important. The results of the analysis, however, do provide promising feedback that the IA awareness programs in place are having an impact on our students security consciousness.

The phishing exercises served to provide an insight into the awareness levels of our students and help us better focus our IA and awareness training. The results are still very immature; however, they provide an opportunity to look at the effectiveness of our programs. One might look at the assessment of the programs using an exercise as “poisoning the well”, given the very fact that the exercises themselves may raise awareness, making it difficult to separate out any increased awareness due solely to the annual training. While this is true, when looking at the exercise from a bottom line – if our user’s awareness is increased, providing enhanced network security whatever the cause is a worthwhile cause.

We intend to continue the phishing email exercises, increasing the frequency to once every semester. One exercise will follow closely existing training; the second will be used to assess longer term retention. In addition to formalizing the scheduling of the exercise, we will expand the exercise to also include instant message (IM) traffic. The IM exercise will not occur in conjunction with the email phishing exercise.

References


Lt. Col. Dodge has served for over 19 years as an Aviation officer and is a member of the Army Acquisition Corps in the United States Army. His military assignments range from duties in an attack helicopter battalion during Operation Just Cause in the Republic of Panama to the United States Military Academy. Currently he is an Associate Professor permanently stationed at the United States Military Academy and the Director of the Information Technology and Operations Center (ITOC). Ron received his Ph.D. from George Mason University, Fairfax, Virginia in Computer Science, is a member of the ACM, IEEE, UPE, and IFIP, and is a CISSP. His current research focuses are Information Warfare, Network Deception, Security Protocols, Internet Technologies, and Performance Planning and Capacity Management. He is a frequent speaker at national and international IA conferences and has published many papers and articles on information assurance topics.

Lt. Col. Curtis A. Carver is an Army officer and Academy Professor at the United States Military Academy with over 20 years of service. He has served in a number of leadership positions including platoon leader, company commander, battalion operations officer, and division deputy G-6. His military awards include the Army Meritorious Service Medal with three oak leaf clusters, the Army Commendation with three oak leaf clusters, the Army Achievement Medal with three oak leaf clusters, and National Service Medal with star device. Curt holds a Ph.D. in computer science and is a member of the ACM, IEEE, UPE, and PKP. He has over 90 academic works and a researcher in information assurance, adaptive hypermedia and computer science education. He has been a keynote speaker at several conferences including, most recently, the 2003 National Collegiate Engineering Symposium. Curt won the 1995 EDSIG Best Overall Paper Award, 1996 Frontiers in Education Ben Dasher Best Paper Award, 1996 and 1997 EDMEDIA Outstanding Paper Award, 1997 AFCIA Best Paper Award, and EISTA 2003 Best Track Paper Award and an honorable mentions at CCSC 2001. He is the Program Chair of the FISSEA conference.

Curt has also led numerous software engineering projects within the Army and academia including development of the TACWEB, DPASS, and Adaptive Hypermedia CS383 systems.

Dr. Aaron J. Ferguson is currently a Program Manager in the Advanced Network Operations office at the National Security Agency. Prior to his current assignment, Dr. Ferguson was the National Security Agency Fellow in the Department of Electrical Engineering and Computer Science at the United States Military Academy at West Point where he taught Software System Design and other security-related courses. Dr. Ferguson is an Electrical Engineering graduate of Howard University where he focused on control systems. He received an M.S. in Operations Research from the University of New Haven where he focused on software reliability modeling. He earned an M.S. and Ph.D. in Applied Statistics from the University of Delaware where he focused on system simulation and modeling. Dr. Ferguson is a Certified Information System Security Professional (CISSP) and his research interests include Insider Threat Detection and Modeling, Security Awareness, Training, and Education (SATE), XML Security, Cross-Security Domain Information Exchange Architectures. Dr. Ferguson has taught Information Assurance course overseas in private industry and as a Senior Consultant for Price-waterhouseCoopers, LLC, has provided risk management consultancy to several Fortune 500 companies.