# Security Education

## A Phishing Approach

Matthew Johson (johnsma@stolaf.edu) and Ben Le Cam (b.lecam@gmail.com)

# Executive Summary

According to our research on St. Olaf students, there is a need for increased Security Education at St. Olaf in order to improve the safety of St. Olaf's online community and also to prepare students for the threats they will face in the workforce and in their personal lives.

The overall goal of our project was to investigate how significant of an issue phishing at St. Olaf is or has the potential to be. In order to determine this, we conducted research on non-Computer Science St. Olaf students by observing and interviewing them about how they read email. All of the students involved in the study fell for some type of phishing. The methodology of our study can be found on page X.

We also extensively reviewed literature from researchers and colleges around the country about experiments made in their respective institutions. These papers provide a broader context for understanding the phishing environment, the issues that need to be addressed in phishing education, and possible strategies for improving phishing awareness. A list of these resources can be found on page X.

Adopting a policy of improved security education offers many potential benefits, while also risking several pitfalls:

1. Better informing students about these issues makes the community safer
2. Teaching students about phishing gives them more practical knowledge as they leave St. Olaf
3. Convincing students that learning and applying safety practices may be challenging
4. Poor implementation could decrease student trust in IT

In order to address these issues, we developed five potential solutions:

1. An email campaign to raise awareness in a non-intrusive way
2. A poster campaign to give security education a persistent physical presence on campus
3. A technical-literacy week to draw great attention to the issue and the resolution of the trust issue
4. A phishing education training program for incoming freshmen to systematically educate students
5. A phishing campaign in make a lasting impacting on the most vulnerable students, at the possible risk of decreasing their trust

As a final recommendation, we would encourage you to pursue solution 4 as the primary solution complemented with solution 2. Introducing software training appears to us to be the most effective way to reach all students and educate them appropriately. Supplementing this detailed education with posters will help students keep the issues in mind throughout the year.

## Table des matières

# Ethical Issues and Tradeoffs

A major issue in the topic of security education, and phishing education in particular, is finding the balance between the value of students knowing the relevant information and the difficulty of getting them to learn this information.

One the one hand, phishing is a significant issue, being able to cause significant damage to both an individual and an organization. Fraud and identity theft resulting from a successful phishing attack can cause lasting problems for an individual, and if the information gleaned from a phishing attack is used to breach security, these headaches can be multiplied across thousands or millions of people. Although the damage might not so dramatic on a small campus, it can nevertheless but both the phished student or professor and the rest of St. Olaf at greater risk.

On the other hand, knowing how to avoid phishing, much like safety measures in general, can seem unimportant until it is too late to make a difference. As a consequence, convincing students to have a vested interest in learning about phishing (or other online security measures) is difficult, and teaching students effectively without their willing participation is challenging. The fundamental nature of phishing exacerbates this issue -- unlike many safety protocols, which only apply in rare or specialized situations, knowledge about phishing can be relevant at any of the innumerable times when someone reads an email. This magnifies not only the importance of phishing education but also the consequences for doing it poorly. Since phishing emails depend on convincing users that sender's request for their information is legitimate, avoiding phishing usually requires trained skepticism, and overselling the risk of phishing or strategies to avoid phishing (as might be necessary to overcome student apathy) could make students paranoid.

Our solutions attempt to balance these conflicting interests by exploring various points on the spectrum between inviting students to learn and compelling students to learn.

Based on our research, both from literature and from interviews with students, our recommendations favor compelling students to learn. The St. Olaf students we interviewed were all vulnerable to some form of phishing email, and their general email reading habits suggest that inviting students to learn may be insufficient. Although this may risk alienating students, we think the value of ensuring that students know this information is worth it.

# Possible Solutions

According to our research and the literature out there, phishing can expose any organizations to major security breaches. At St. Olaf, there is certainly not as many risks associated with stolen data than a major corporation would yet the college faces financial problems as well as the security of its students through not offering an education to phishing and social engineering in general.

In order to educate the student body, the college needs to introduce some form of education based on the scale and scope the Information Technology department wants to address. There will considerations about the balance between the need for additional security and the social, temporal and financial costs of such solutions.

We identified five major solutions to educate the student body and we detail them later:

- An email campaign
- A poster campaign
- A technical-literacy week
- An assessment test for incoming students
- A phishing campaign

Here is a brief summary of each method:

| | students reached | amount of information | effectiveness | ease of repetition | resources required | overall quality |
|---|---|---|---|---|---|---|
| Email | low to high | medium | low | high | low | low |
| Poster | medium | low | low to medium | high | low | low to medium |
| Literacy Week | medium | high | medium | low to medium | medium to high | medium |
| Training for Freshmen | high | high | high | high | medium to high | high |
| IT Phish | medium | medium | high | medium | medium to high | medium to high |

# Email Campaign

The email campaign would be an informative email sent to all students. It is an easy and non-intrusive way to reach all students and it can contain a lot of information and links to other resources. However, as seen from our research, students skim through email and need to feel a connection in order to read an email.

An email campaign about phishing would face the same issues any marketing firm face. It is hard to ensure people read the email and it would therefore need to carefully designed and written to ensure that the students feel a need to read the email. There is no interest and immediacy for the student to click on links.

One solution we envision could be to force students to sign an online pledge stating that they read the resources and are aware of phishing but this would be most likely to fail just as no one reads the “Terms of conditions” when the order online.

It might be possible to increase student interest in the email by adding incentives. For instance, include a quiz about phishing, and students who pass the quiz would be entered into a drawing for money or some other prize.

The cost associated with such a solution ranges from extremely low for a basic email since the infrastructure and software are already part of the college system, to moderately high if a prize drawing is included depending on the quantity and quality of the prize. An additional cost would be time as students could come up with questions that would require more time from helpdesk.

We identified the following advantages for the email campaign:

- It is easy to implement
- It is cheap
- It reaches a large audience
- It makes it easier for students to communicate their doubts and questions

On the other side, there are inconvenient with such campaign:

- There is no guarantee that students will read it
- It is unlikely to make lasting impact

We believe that it could be useful as part of a more global and comprehensive strategy, but would not generally recommend it since students could easily ignore or forget it. In any case, it would not be sufficient on its own.

# Poster Campaign

A poster campaign would be a campus-wide physical diffusion of facts about phishing. We envision posters that would share a danger about phishing and how to avoid it. It would need to be a catchy poster for which students relate, perhaps around social networks. It could be similar to the “It’s on us” poster campaign.
A couple lines could be

- IT will never ask for passwords in email
- Gmail is not always Gmail: Always check link destination before clicking along with a screenshot of a Gmail login and the fake URL highlighted.
- Check whether sender is familiar/has legitimate email address

We identified a couple key locations for the posters:

- Major bulletin boards with high concentration of students
    - Buntrock Commons
    - Rolvaag Library Entrance
    - Outdoor in front of the Library
    - Cage
- TVs: part of the campus wide slideshow
- Computer Labs: each computer lab should have poster signs about it.

The cost of such a campaign is relatively cheap:

- 36 color 11”x17” posters cost $19.80
- 48 color 11”x17” posters cost $26.40

In addition to the printing cost, a designer will be needed.

The advantages of a poster campaign are:

- Information is presented in easily digestible packages
- Students would be exposed to posters many times throughout the day, months and different pieces of information making memorization easier.

However, there are also inconvenient with posters:

- The paper format does not relate to Internet, thus a dissociation of poster information from its context.
- Students are overwhelmed with posters and thus it is a competition to be seen.
- Implementation requires following a protocol.

This solution would be insufficient on its own, in particular because it is distant from reading emails, but it long term exposure could make it a useful complement to a more concentrated solution.

# Technological Literacy Week

Our third solution is the organization of a thematic week around technological literacy. There are constantly weeks dedicated to a specific topic such as the Financial Literacy Week. Our solution would be the implementation of a similar format with games, seminars and tutorials throughout the week to educate people about technology. The underlying goal here would be to make more aware of technology without planning on talking about obscure terms such as phishing.

Rather, we would for example share with people tricks about Gmail and mention phishing as a security threat. We could also for example talk about privacy on social networks.

This week could be used to teach people to become better with technology and introducing basic security concepts. The goal of the program would be to make students relate to the topics in order to have them feel interested by the discussion.

We believe that this could be a great tool to reach students concerned about their security online as well as people that believe they lack technological knowledge. It could qualify as a Wellness event and/or fulfill other classes' requirements, and classifying it in this way could help boost attendance.

This solution is more costly as it requires a lot of planning and organization in order to develop these events. There would be a need to promote the events as well as fund them.

However the cost come with great advantages:

- It provides context for thorough discussion of email safety
- It creates a platform for discussing whatever other ideas IT would like to publicize
- It brings a listening audience that wants to learn more about technology.

There are inconveniences associated with such solution though:

- It requires significant effort to implement
- Students who would most benefit from the sessions may not attend the sessions because of the fear of lack of knowledge or because they believe that they know enough already.
- Mixing phishing with so many other topics would dilute the security mention.

We believe that this would be worthwhile if topics brought up by IT relate enough to students that they feel concerned and join the audience. We also believe that it would need to be heavily publicized. Another suggestion to better publicize and enforce security education through this kind of events would be to distribute cool goodies with phishing warning so that students unconsciously remember the security tips.

# Assessment Test for Incoming Students

Prior to joining the St. Olaf student body, incoming freshmen are required to take an Alcohol and Drug Education test.
We believe that adding a Security Education component would be beneficial to the St. Olaf Community as a whole and also give more value to the St. Olaf degree as it would certify that students coming out of the school have an understand of security concerns associated with computing. It is a valuable skill as students enter the workforce and become part of highly competitive businesses.

Such a requirement would ensure that all incoming students are reached through before they even make their first steps on campus. It is highly beneficial, as they would then enter their 4-year undergraduate cycle. We also would like to evoke the possibility to retro activate this requirement for all current students in order to ensure that all students are on page with new security education.

We believe that it would be IT role to introduce this requirement to the Dean

As for the cost, the only one we see is the cost of the software. We have been in contact with a startup in San Francisco called Apozy that develops education software through a game-like web platform. The product manager Samantha Manke is a St. Olaf alumnus. She has mentioned that St. Olaf could benefit and test the software on scale for free.

There are a lot of advantages with this method:

- The school ensures that all students are reached.
- The school has the control of what information is shared and can customize it.
- It reaches students before they start their time at St. Olaf, thus it maximizes effectiveness with respect to St. Olaf

However, we see a couple disadvantages:

- From our personal experience with the Alcohol and Drug assessments, it is likely to annoy students
- The impatience of getting it done may decrease the impact of material
- It may require a little bit of extra bureaucracy to ensure that all students complete the training
- It could be costly depending on the software

We believe that this would be the most effective solution. St. Olaf would put itself in the sphere of very innovative institutions that have proceeded to insert Online Security Education as part of their curriculum.

# Phish Students

The last solution we propose is perhaps the least ethical and most controversial one. It consists of sending students a phishing email, and if a student succumbs to the bait, lecture them.
Despite the difficulties, various schools have successfully implemented a comparable strategy. One example is the United State Military Academy at WestPoint, where researchers phished the student body through sending carefully prepared emails to students. Dodge compiles details about their process and results in the paper “Phishing for user security awareness”.

There are two non-financial costs with such an implementation. First, it will require time to respond to students. Second, it could harm the trust that the student body has into IT.

We see a couple advantages to that solution:

- It targets only students who actually give in to a phish
- It teaches through example, which generally more effective than abstract training
- It provides useful data about phishing awareness

However, advantages are outplayed by disadvantages:

- It may decrease trust in IT (by betraying the faith that IT wouldn’t trick students)
- It requires a lot of finesse to write a suitable email
- It would be difficult to account for which kind of phishing emails students are vulnerable.
- It might not be a reproducible way to raise phishing awareness (a careful strategy is necessary in order to incorporate this year to year)
- it would require large time investment from IT (would likely receive a large amount of emails both from people would catch the phish and are caught by the phish)

It certainly would be the most effective way to increase phishing awareness where most necessary, and it would also provide lot of information about student practices and knowledge that would otherwise be difficult to obtain. At the same time, this strategy is the most vulnerable to backlash and consequently would require the most care in implementation.
Resources

# Methodology: Think-Aloud Protocol

The primary method used to determine the threat of phishing emails to St. Olaf students was a think-aloud protocol in which we asked participants to go through a provided inbox of emails and describe how and why they would react to each email. We were particularly interested in how well students could recognize phishing emails, and we had a secondary interest in email habits in general in order, for instance, to predict the effectiveness of an educational email campaign.

In order to provide a consistent testing environment, we created a new email account, and sent approximately 40 emails of various types to this account using the Linux sendmail command. The emails, reproduced in full below, represent a combination of real emails at St. Olaf, fake emails similar to what might be received at St. Olaf, real phishes either received by St. Olaf or classic, and fake phishes modeled off of research articles.

Participants were initially self-selected through an email to extra@stolaf.edu and were supplemented by friends of the researchers for a total of participants.

In general, the results showed that St. Olaf students would benefit from additional knowledge about phishing safety, as the participants generally missed at least one phish, and often more.

The secondary data about email reading practices in general reveal and emphasize some of the difficulties of communicating information about phishing. Most participants tended to read the entirety of an email only if the email is short or of direct personal interest, and it was not uncommon to delete an email without opening it if it appears to contain unimportant or uninteresting information. Without more concrete benefits, such as a possible reward, emails about phishing or phishing-related events could go unnoticed.

The organization and implementation of these protocols may have introduced several possible confounding variables:

- Students may behave differently when being observed than under normal circumstances
- A subtle roleplaying aspect may have been less suspicious of strange emails; for instance, in the context of the experiment, there may have been ambiguity about whether it was more appropriate to pretend to know an unfamiliar sender or to treat them as a stranger
- Among the respondents from extra, there may be a predisposition to respond to strangers and unusual emails compared to the general St. Olaf population

# Protocol

The general protocol is copied below. This was applied with some modifications, in particular with regard to follow-up questions depending on a participant's responses.

Inquiry Email

> Hello!
>
> My name is Matthew Johnson. This semester I am taking a class called "Ethical Issues in Software Design," which involves a research project, and part of my project involves learning more about how people read emails in order to suggest ways to improve the email experience. In order to get better data, I am hoping to meet with four to eight students in person sometime during the next week or two in order to find out how they read their emails.
>
> The study would involve describing your thought process while reading some emails that I provide, and I don't expect that it would take more than 30-45 minutes. Although I cannot provide any monetary compensation, I could give thanks in the form of a snack from The Cage.
>
> If you would like to participate or would just like to hear more details, please let me know! I appreciate any help you can offer.
>
> Thank you,
>
> Matthew

## Introduction

Hello! Thank you again for being willing to participate in this study. Just as a reminder, this study is for part of a project a class I'm in called Ethical Issues in Software Design. The particular question I'm hoping to learn about through these interviews is how St. Olaf students read their emails.

## Informed Consent

Before we get to the details of the interview, I'd first like to talk about how I plan to use the data. The information from this interview will only be used to help make recommendations as a part of my project for the Ethical Issues class, and none of the information will be personally identified with you. If you ever decide that you would prefer that I don't use the information from this interview, you can just let me know, and I will get rid of it. Also, you are welcome to stop or skip any parts of the interview that you would like. Do you have any questions?

## Think-Aloud Details

This type of interview is usually called a "think aloud protocol," and the general idea is that I will ask you to look at a variety of emails and describe what you're looking

at and how you decide what to do with the email -- for instance, what parts of the email you read, skip, or skim, and whether you reply to the email, save it for later, or delete it. To give you a better idea, I'll look at a few emails as though I were doing the think aloud.

(Three examples -- one from the registrar, which I would skim and say that I would immediately follow up on the links; one about scheduling some event, which I would say I would not reply immediately, but star it and mark it as unread as a reminder; and one that is either obvious spam or an Extra email about something that doesn't affect me, and I would delete without opening.)

Do you have any questions?

Alright, then let's get started! To try to keep this session around 30 minutes, I will interrupt if it looks like we will run out of time. Keep in mind that there are no right or wrong answers -- it's just about the emails.

Prompts

- What are you looking at?
- What are you thinking about?
- What detail has caught your attention?

Follow-Up

Overall, what did you think of the emails?

Did you notice any strange patterns?

Although it is useful to learn about how St. Olaf students read emails in general, the type of email I was most interested in is phishing emails. My group is thinking of recommending that St. Olaf add a phishing-awareness program for students similar to the drug and alcohol programs, and we are trying to find out what aspects of phishing are most important to emphasize.

# Typical Emails

### Building the emails

The emails for this study were copied from or inspired by real emails received at St. Olaf, phishing emails received at St. Olaf, and phishing emails used in research papers.

We set up a dummy email account for the purpose of this study (esd.study@gmail.com), and sent the emails to this account using the Linux sendmail command. From a primary directory, the emails were placed in a directory called “emails”. The emails (with the exception of the first three, which were used for a demo) were ordered randomly, with the order being saved in a file called “email_order”. The emails were sent using this script:

```
#!/bin/bash
TO=esd.study@gmail.com
EMAIL_DIR=emails
EMAIL_ORDER=email_order
while read EMAIL; do
 echo sendmails $TO $EMAIL_DIR/$EMAIL
 sendmail $TO < $EMAIL_DIR/$EMAIL
 sleep 1
done <$EMAIL_ORDER
```

All emails, with the exception of two, were successfully received by the account. An Amazon confirmation email was marked as spam, and the PayPal phish was not received at all. This is most likely due to one of Google’s strategies at reducing spam in Gmail (see Taylor).

Due to the overall length, only a few sample emails are included in this report. The complete bodies of the emails are available at request.

## A real phish

From: "Help Desk" <info@helpdesk.com>
To:
Subject: Scheduled Maintenance & Upgrade

Help Desk

Attention Account User,

Scheduled Maintenance & Upgrade

Your account is in the process of being upgraded to a newest of Windows-based servers and an enhanced online email interface inline with Internet infrastructure Maintenance. The new servers will provide better anti-spam and anti-virus function, along with IMAP Support for mobile devices that Support IMAP to enhance your usage.

To ensure that your account is not intermittently disrupted but active during and after this upgrade, you are required to kindly confirm your account by stating the details below:

* User name:
* Password:

This will prompt the upgrade of your account.

Failure to acknowledge receipt of this notification, might result to a temporal deactivation of your account from our database.

Your account shall remain active upon your confirmation of your login details.

We do apologize for any inconvenience caused.

Help Desk

### A fake phish

```
From: "Jason Roth" <jroth@stolaf.edu>
To:
Subject: Student Drive Problem
Content-Type: text/html
</p><p>
<!-- Based on the phishing email that appeared in the paper
"Where did they go right? Understanding the deception in phishing
communications" by Wright, Chakraborty, Basoglu, Marett --">
</p><p>
This email is to inform you of a problem we are having with the
information technology database. Due to a data collision we have
lost some information and are unable to recover. In order to get
the database back up and working we need you to forward us your
student ID number (the number found on your ID card.)
</p><p>
Please respond to this email with your code by the end of the
day.
</p><p>
Sorry for the inconvenience.
</p><p>
Jason Roth
Network Administrator
```

### A real email

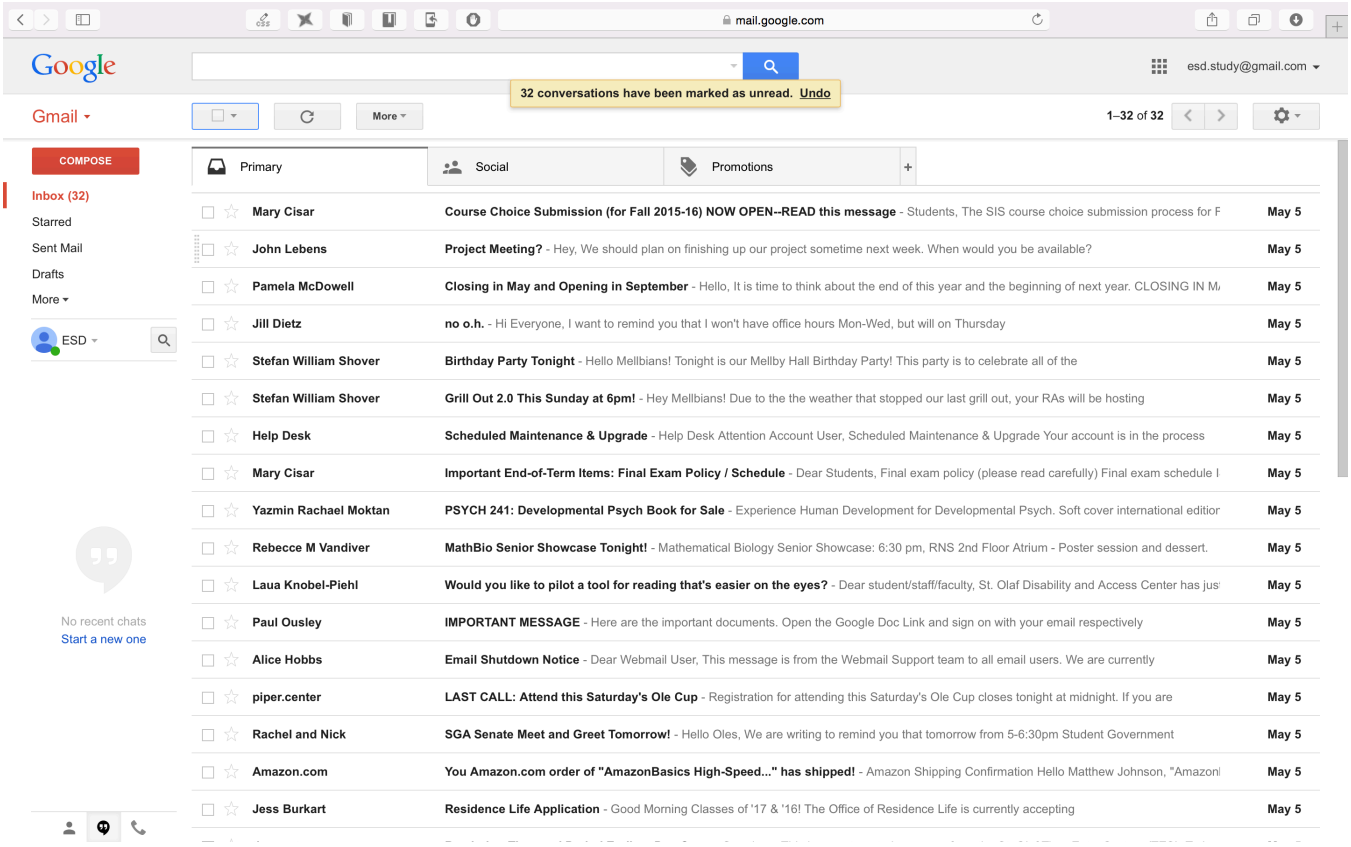
```
From: "Abdi Musse" <mussea@stolaf.edu>
To:
Subject: Buy, sell, and exchange with oles.
Content-Type: text/html
</p><p>
Dear Oles,
</p><p>
I am emailing to inform you about a new website for oles to buy,
sell, and exchange CHEAP textbooks, furniture, clothes, and
everything else in the St. Olaf community. This website is an
organized St. Olaf extra. Best of all, it is exclusive to the
Olaf community!
</p><p>
Before purchasing any expensive college materials or books from
the bookstore, take 30 seconds to see if you can find what YOU
want at a cheap cost on the website.
</p><p>
This website is built by Olaf students FOR Olaf students in order
to help you find what you want at a DISCOUNT price.
</p><p>
Have a great rest of the spring!
</p><p>
Site: <a href="http://www.bookdem.com">www.bookdem.com</a>
</p><p>
St. Olaf: <a
href="http://www.bookdem.com=stolaf">www.bookdem.com/stolaf</a>
</p><p>
Have any questions? Contact us at <a
mailto="info@bookdem.com">info@bookdem.com</a>
</p><p>
Enjoy,
</p><p>
The Bookdem Team
</p><p>
```

### A real email with more complicated formatting

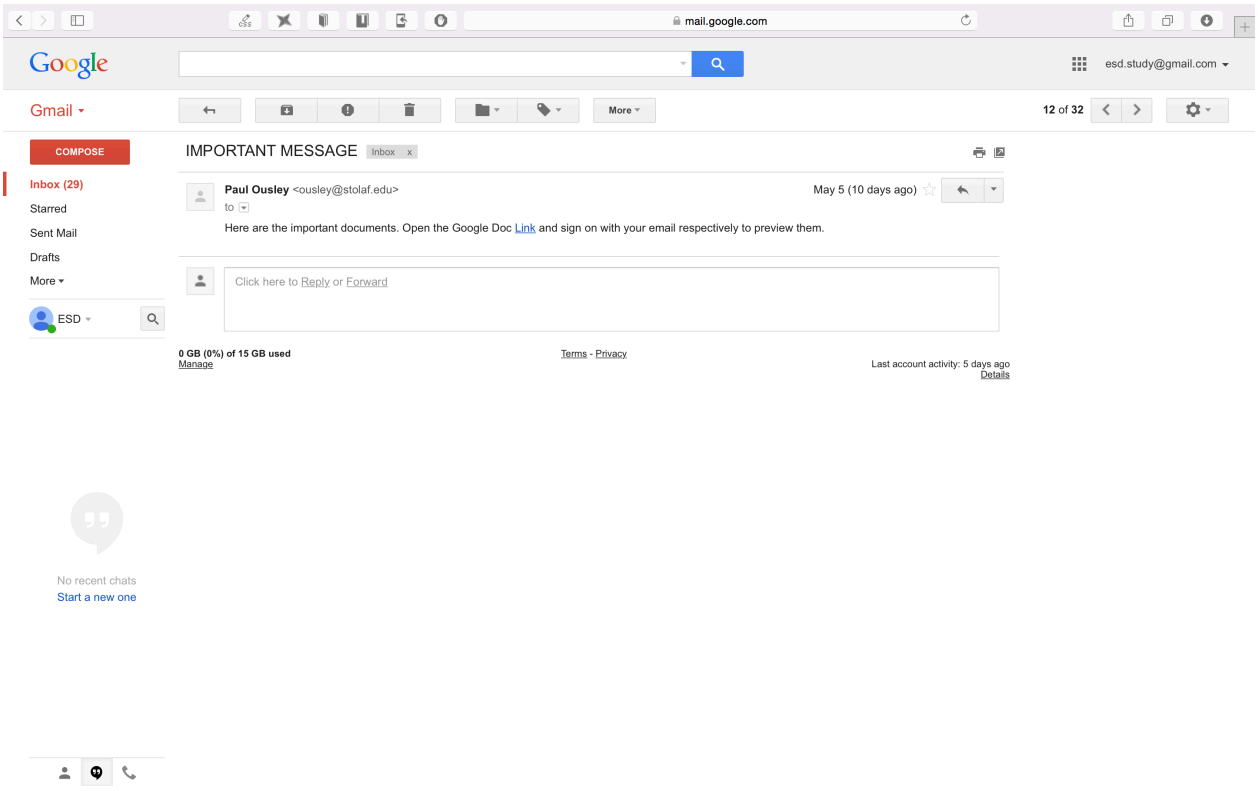
```
From: "Stefan William Shover" <shover@stolaf.edu>
To:
Subject: Grill Out 2.0 This Sunday at 6pm!
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr"><font size=3D"6" color=3D"#073763">Hey
Mellbians!</font><d=
iv><font size=3D"6"><br></font></div><div><font size=3D"6"><font
style=3D"b=
ackground-color:rgb(102,102,102)" color=3D"#6fa8dc">Due to the
weather =
that stopped our last grill out</font><font color=3D"#0b5394"
style=3D"back=
ground-color:rgb(102,102,102)">,</font> your RAs will be hosting
another! C=
ome join us this <u><b style=3D"background-
color:rgb(255,255,0)">Sunday at =
6PM in the Mellby Lawn</b></u>=C2=A0and enjoy=C2=A0<u><b
style=3D"backgroun=
d-color:rgb(255,255,0)">FRE</b><b style=3D"background-
color:rgb(255,255,0)"=
>E FOOD,</b></u><font color=3D"#6fa8dc" style=3D"background-
color:rgb(39,78=
,19)">=C2=A0nice weather </font><font color=3D"#ffff00"><font
style=3D"back=
ground-color:rgb(111,168,220)">(63 and sunny!=C2=A0</font><font
style=3D"ba=
ckground-color:rgb(111,168,220)">)</font><font
style=3D"background-color:rg=
b(111,168,220)">,</font></font><font color=3D"#6fa8dc"
style=3D"background-=
color:rgb(39,78,19)"> and fellowship with other
Mellbians!=C2=A0</font></fo=
nt></div><div><font size=3D"6"><br></font></div><div><font
size=3D"6">We ho=
pe to see <i><b><u>you</u></b></i> there!</font></div><div><font
size=3D"6"=
>Your RAs</font></div></div>
```

## Screenshots

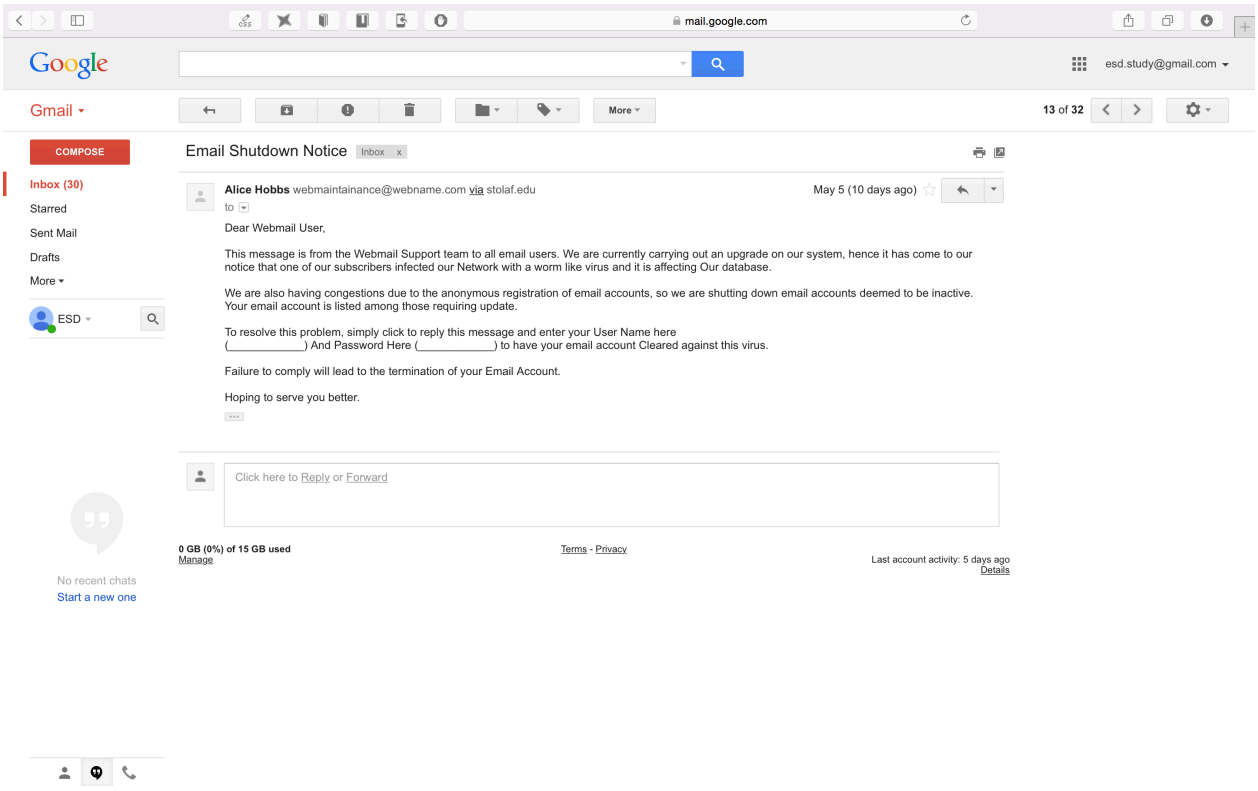
### *Gmail Inbox*



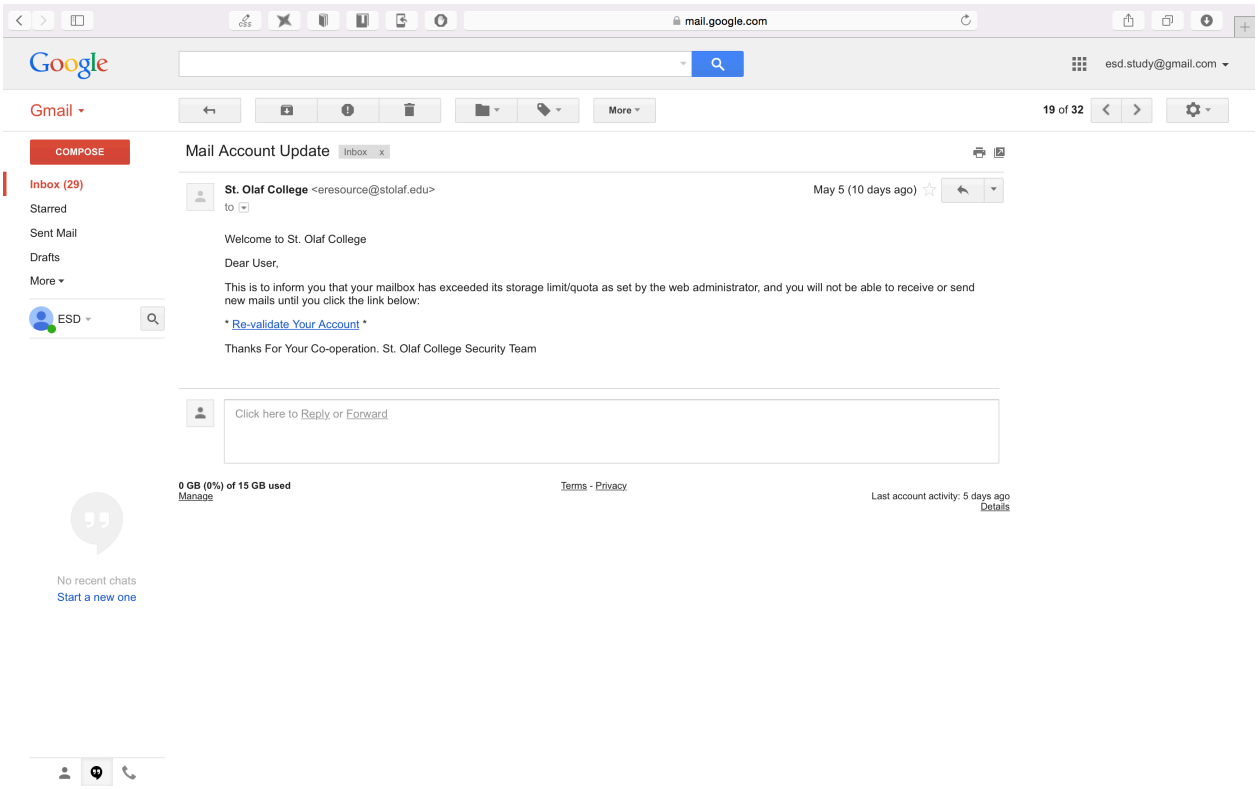
## *A real phishing email that got subjects suspicious*



## *A real phishing email that got 75% of the subjects responding*



## *A real phishing email that got some of the subjects to click the link*



# Talk-Aloud Results

## Analysis

From the results, we have seen that all the subjects fell in one of the trap and clicked on a scam link and/or responded to an email with their credentials.

We have noticed that most of the subjects look at the subject of the email first and then the sender. This for example would be the reason why an alerting subject would get victim's attention. Nevertheless, the sender of the email is also important for building and maintaining the victim's trust. Participants were more likely to trust the emails signed by an individual with credentials rather than by a team or complete stranger.

Even when the participants noticed or suspected a phish, none of them actually took action to report the scam. This might be due to not knowing the correct person to contact in such as situation, not realizing the benefit of marking a message as spam, or simple apathy.

An additional important observation is how students read long, administrative emails in general. Often, if a message came from the Piper Center, registrar's office, or the like, they would skim the email rather than carefully reading it, usually because they did not expect the message to be particularly interesting, helpful, or relevant. This behavior should inform the solution to phishing education since it highlights the need to present the information that either encourages or requires students to pay attention.

You can see in the next pages the actions of each subject per email.

## Subject 1

Class: 2017
Major(s): Economics, Asian Studies
Gender: Male

Notes: Subject would first read subjects then names. He identified phishing emails but did not bother report them. He did not know that name of the URL would be different than the actual URL.

Answer to questions post-test:

| File Name | Description | Response | Notes |
|---|---|---|---|
| demo_0.txt | Registration | mark unread, star | sees sender, which sets expectations for contents; skip header; skip through familiar content; all caps annoying, pays more attention to links; ignore bullets |
| demo_1.txt | Project Meeting | | |
| demo_2.txt | Extra: Skirt | delete | no value or relevance |
| misc_1.txt | Pause Delivery | | |
| housing_0.txt | Housing Closing | | |
| misc_5.txt | Summer Session | leave read | unfamiliar name, read before opening; read bullets (though uninterested) |
| real_possibility_1.txt | St. Peter District | would follow through (if knew person) | confusing formatting; typo; read all of it (not shouting, and the email didn't make enough sense to be able to skim) |
| misc_2.txt | Office Hours | delete | read email from home page, not the email itself; useless subject |
| survey_2.txt | SGA Survey | do survey immediately, mark unread | offer of money caught attention; enjoys doing surveys; ignored names |
| real_phish_2.txt | Antivirus | investigate; talk to someone in person, not over email | instruction to click on link, lack of personalization are red flags; threat |
| misc_9.txt | Mellby Birthday | | |
| misc_0.t | Mellb | delete | no date; annoying formatting (though liked the yellow on |

| | | | |
|---|---|---|---|
| xt | y Grill Out | | blue for sunny weather) |
| real_phish_1.txt | Upgrade | follow up in person, not email | suspicious; read email to get more info to know how to respond |
| registrar_0.txt | Final Exams | leave read | skip links, and most or all of email |
| extra_0.txt | Extra: Book | delete | not relevant |
| survey_1.txt | Social Media | do survey, delete | annoying subject, but likes surveys, so read it |
| fake_phish_0.txt | Summer Housing | ignore (mark as read) | not relevant (but read ahead on main page) |
| misc_4.txt | Math Bio Posters | delete | not relevant (because it is today, read ahead to find justification to not go) |
| extra_2.txt | Reading Tool | delete | long sentences, but interesting; unfamiliar person; read to end, and gave credibility to contact/identifying info; decided not part of target audience |
| real_phish_3.txt | Google Doc | delete | who is this guy? |
| real_phish_0.txt | Email Shutdown | delete | read subject before name; notes threats for personal info; noted strange address; no name/personalization |
| piper_1.txt | Ole Cup | leave read | piper.center, so probably not as interesting; doesn't initially know what Ole Cup is |
| sga_0.txt | Meet and Greet | unread if possible to go to event | smores! Unsure if time would work – if yes, would try to attend |
| amazon_html_0.txt | Amazon | | |
| misc_8.txt | | | (no subject) → what is this? |
| tes_0.txt | TES | follow up immediately | urgency; not suspicious about it even though does not have a name (less sensitive information, familiar/recurrent email, comes from trustworthy service, safe URL) |
| real_phish_possibility_1.txt | Quota | follow link? Check quota, ask roommate first | hesitance, but has enough trustworthy elements |
| piper_0.txt | Alumni | delete | not interesting; too long |
| fake_phish_3.txt | Financial Aid | forward to parent | familiar; formatting – better with bold? Skip most of email |
| extra_1.txt | Norway | delete | key information easy to read; seems to require registration, Norwegian antiques |
| fake_phi | PayP | | |

| | | | |
|---|---|---|---|
| sh_1.txt | al | | |
| misc_6.txt | Choir | delete | no interest – not musical |
| survey_0.txt | Stat Survey | do survey, delete | survey, but wall of text; when skimming, picks out details that is for stat students, posters; send is PhD is a plus |
| fake_phish_2.txt | Student Drive | check whether sender is legitimate (if not in directory, just delete); look up "data collision" | asks for personal info, but from St. Olaf; look up sender; notes seeming disconnect between the issue in the email and the usefulness of person info |
| misc_7.txt | Journal | | |
| misc_3.txt | Parking | follow link | email could be relevant; skim, skipping first link (unclear what it is) but open St. Olaf link; reread, then do first link |
| real_phish_possibility_0.txt | Quota | ask roommate | doesn't trust; suspects hacked account |
| real_phish_possibility_2.txt | Survey | | who is this? Survey! |
| extra_3.txt | Book Exchange | delete | signing "Bookdem team" is suspicious; okay with using extra instead |
| real_possibility_0.txt | Medicine | | |
| extra_4.txt | Sublease | forward to cousin (near Dinkytown) | |

## Subject 2

Class: 2016
Major(s): Biology
Gender: Female

Notes:

Answer to questions post-test:

| File Name | Description | Response | Notes |
|---|---|---|---|
| demo_0.txt | Registration | | |
| demo_1.txt | Project Meeting | | |
| demo_2.txt | Extra: Skirt | | |
| misc_1.txt | Pause Delivery | delete | organization already has funding |
| housing_0.txt | Housing Closing | delete | not relevant |
| misc_5.txt | Summer Session | delete | not interested in summer session |
| real_possibility_1.txt | St. Peter District | read; reply | skip to end; (email doesn't have enough context to make sense) |
| misc_2.txt | Office Hours | delete/ignore | not relevant |
| survey_2.txt | SGA Survey | open, take survey (if on computer, not phone) | open; money and survey caught interest; didn't read most of email |
| real_phish_2.txt | Antivirus | delete | not interested in upgrade |
| misc_9.txt | Mellby Birthday | delete or save | open to see what food; delete or save accordingly |
| misc_0.txt | Mellby Grill Out | delete or save | open to see what food; delete or save accordingly |
| real_phish_1.txt | Upgrade | respond with username/password | open/skim |
| registrar_0.txt | Final Exams | delete | |
| extra_0.txt | Extra: Book | delete | |
| survey_1.txt | Social Media | delete | |
| fake_phish_0.txt | Summer Housing | delete | already has summer housing plans |
| misc_4.txt | MathBio Posters | probably delete | open; reads student names and first lines of the descriptions, skims rest; would go if friends involved or going |
| extra_2.txt | Reading | delete | |

| | | | |
|---|---|---|---|
| | Tool | | |
| real_phish_3.txt | Google Doc | delete | |
| real_phish_0.txt | Email Shutdown | reply with username/password | read; respond |
| piper_1.txt | Ole Cup | | read to find out what event – skims for around 3 seconds |
| sga_0.txt | Meet and Greet | leave unread | reminder to self to see if time works |
| amazon_html_0.txt | Amazon | mark as read | keep as reminder |
| misc_8.txt | ResLife Application | delete | |
| tes_0.txt | TES | delete | follow up on TES in another window manually |
| real_phish_possibility_1.txt | Quota | follow link | read to find out what event – skims for around 3 seconds |
| piper_0.txt | Alumni | mark as read | read now, check date later |
| fake_phish_3.txt | Financial Aid | delete | |
| extra_1.txt | Norway | delete | |
| fake_phish_1.txt | PayPal | delete | |
| misc_6.txt | Choir | delete | |
| survey_0.txt | Stat Survey | do survey, delete | skim, then do survey |
| fake_phish_2.txt | Student Drive | respond with username/password | |
| misc_7.txt | Journal | reply, asking whether a paper qualifies | |
| misc_3.txt | Parking | delete | |
| real_phish_possibility_0.txt | Quota | delete | |
| real_phish_possibility_2.txt | Survey | delete | |
| extra_3.txt | Book Exchange | delete | |
| real_possibility_0.txt | Medicine | | open; read most; click on link, and forward to other leaders |
| extra_4.txt | Sublease | delete | |

## Subject 3

Class: 2016
Major(s): Music
Gender: Female

Notes: Subject goes through email very carefully and marked them read instead of deleting them

Answer to questions post-test:
The subject said these are normal, standard emails and that nothing seems suspicious beside maybe the quota one.

| File Name | Description | Response | Notes |
|---|---|---|---|
| demo_0.txt | Registration | Clicked on it | Noted important, would at least open it |
| demo_1.txt | Project Meeting | opened | |
| demo_2.txt | Extra: Skirt | deleted without reading | |
| misc_1.txt | Pause Delivery | deleted without reading | |
| housing_0.txt | Housing Closing | clicked and then realized not interested | |
| misc_5.txt | Summer Session | not interested in sciences | |
| real_possibility_1.txt | St. Peter District | started reading and then looked like spam | |
| misc_2.txt | Office Hours | opened because confused | possibly interested |
| survey_2.txt | SGA Survey | not interested | don't care about 30 |
| real_phish_2.txt | Antivirus | deleted without reading | |
| misc_9.txt | Mellby Birthday | marked as unread | |
| misc_0.txt | Mellby Grill Out | marked as unread | |
| real_phish_1.txt | Upgrade | interested in schedule | clicked and cried |
| registrar_0.txt | Final Exams | marked read | |
| extra_0.txt | Extra: Book | not interested into extra | |
| survey_1.txt | Social Media | delete anything from extra | |
| fake_phish_0.txt | Summer Housing | deleted because not related | |
| misc_4.txt | MathBio Posters | marked as read | |
| extra_2.txt | Reading Tool | read because concerned | |
| real_phish_3.txt | Google Doc | would not be open | |
| real_phish_0.txt | Email Shutdown | opened because seems like it would affect her | |
| piper_1.txt | Ole Cup | opened because know someone in ole cup | |
| sga_0.txt | Meet and | marked as read | |

| | | | |
|---|---|---|---|
| | Greet | | |
| amazon_html_0.txt | Amazon | would open if | would click |
| misc_8.txt | ResLife | marked as read | not interested in res life |
| tes_0.txt | TES | no idea what that is | |
| real_phish_possibility_1.txt | Quota | Clicked on link | |
| piper_0.txt | Alumni | opened and thought about reading | |
| fake_phish_3.txt | Financial Aid | opened and clicked link | |
| extra_1.txt | Norway | interested then realized have to pay money | |
| fake_phish_1.txt | PayPal | | |
| misc_6.txt | Choir | opened | |
| survey_0.txt | Stat Survey | will do it if bored | |
| fake_phish_2.txt | Student Drive | would reply it to fix problem | |
| misc_7.txt | Journal | seems superfluous | |
| misc_3.txt | Parking | felt affected | |
| real_phish_possibility_0.txt | Quota | opened and did not know about technical limitations | |
| real_phish_possibility_2.txt | Survey | ignored | |
| extra_3.txt | Book Exchange | opened | |
| real_possibility_0.txt | Medicine | know people in the club | |
| extra_4.txt | Sublease | opened and close | |

## Subject 4

Class: 2016
Major(s): Economics
Gender: Male

Notes: Subject goes through email pretty fast by just looking at subject and content. The subject does not bother looking at sender.

Answer to questions post-test:
The subject stated that these emails seemed like normal emails a St. Olaf student would get beside the upgrade one.
The subject also stated that these emails were no different than his regular emails.

| File Name | Description | Response |
|---|---|---|
| demo_0.txt | Registration | ignored |
| demo_1.txt | Project Meeting | opened |
| demo_2.txt | Extra: Skirt | deleted without reading |
| misc_1.txt | Pause Delivery | deleted without reading |
| housing_0.txt | Housing Closing | read |
| misc_5.txt | Summer Session | deleted without reading |
| real_possibility_1.txt | St. Peter District | opened and not interested |
| misc_2.txt | Office Hours | deleted without reading |
| survey_2.txt | SGA Survey | deleted without reading |
| real_phish_2.txt | Antivirus | deleted without reading |
| misc_9.txt | Mellby Birthday | deleted without reading |
| misc_0.txt | Mellby Grill Out | deleted without reading |
| real_phish_1.txt | Upgrade | responded |
| registrar_0.txt | Final Exams | deleted without reading |
| extra_0.txt | Extra: Book | deleted without reading |
| survey_1.txt | Social Media | deleted without reading |
| fake_phish_0.txt | Summer Housing | deleted without reading |
| misc_4.txt | MathBio Posters | deleted without reading |
| extra_2.txt | Reading Tool | deleted without reading |
| real_phish_3.txt | Google Doc | clicked on link |
| real_phish_0.txt | Email Shutdown | flagged as spam |
| piper_1.txt | Ole Cup | opened and read |
| sga_0.txt | Meet and Greet | deleted without reading |
| amazon_html_0.txt | Amazon | opened and read |
| misc_8.txt | ResLife | deleted without reading |
| tes_0.txt | TES | deleted without reading |
| real_phish_possibility_1.txt | Quota | opened |

| | | |
|---|---|---|
| piper_0.txt | Alumni | opened and thought about reading |
| fake_phish_3.txt | Financial Aid | opened and clicked link |
| extra_1.txt | Norway | deleted without reading |
| fake_phish_1.txt | PayPal | opened and clicked link |
| misc_6.txt | Choir | deleted without reading |
| survey_0.txt | Stat Survey | deleted without reading |
| fake_phish_2.txt | Student Drive | would reply it to fix problem |
| misc_7.txt | Journal | deleted without reading |
| misc_3.txt | Parking | deleted without reading |
| real_phish_possibility_0.txt | Quota | opened and click |
| real_phish_possibility_2.txt | Survey | deleted without reading |
| extra_3.txt | Book Exchange | deleted without reading |
| real_possibility_0.txt | Medicine | deleted without reading |
| extra_4.txt | Sublease | deleted without reading |

# Resources

## Annotated Bibliography


“Designing and Conducting Phishing Experiments”. Indiana University. Finn, Peter and Markus Jakobs. Web. April 20th, 2015.

In this article, the authors describe the risks associated with conducting phishing experiments. This involves respecting the Institutional Review Board(IRB) rules and analyzing user reactions to the experiments realized.

"Anti-Phishing Act of 2005." *Wikipedia*. Wikimedia Foundation, n.d. Web. 25 Mar. 2015.

In this Wikipedia article, the author describes the basics of a proposed bill to punish criminals harder. It was however unsuccessful and did not pass.

"Controlling the Assault of Non-Solicited Pornograph and Marketing (CAN-SPAM) Act of 2003.” 108th Congress, 1st session. Web. 22 Mar. 2015.

Although this bill does not relate to phishing by name and was apparently of limited effectiveness, it does establish some of the legal definitions and context surround phishing, and most phishing attacks would most likely violate some aspect of this bill. Consequently, it helps give more perspective on influences and responses to phishing or similar attacks.

Dodge, Ronald C. Jr., Curtis Carver, and Aaron J. Ferguson. “Phishing for user security awareness.” *Computers & Security* 26 (2007): 73-80. Web.

This paper details an experiment and training exercise held at WestPoint Military Academy to evaluate the effectiveness of the student awareness of and ability to recognize phishing emails. If St. Olaf decided to try to address phishing education by phishing its own

students, this would be a valuable resource for seeing the details of one possible implementation.

Florencio, Dinei. "Evaluating a Trial Deployment of Password Re-use for Phishing Prevention." *Proceedings of the Anti-phishing Working Groups 2Nd Annual ECrime Researchers Summit* ECRime '07 (2007): 26-36. *ACM Digitial Library*. ACM, 10 Apr. 2015. Web. 23 Mar. 2015.

In this journal article, Florencio describes a methodology to detect whether an account has been corrupted. The author states that it is nearly impossible to prevent a attacker to steal a password through phishing. However, he describes a simple way to detect misuse of accounts based on the login location.

Galaria v Nationwide Insurance Co. 998 F.Supp.2d 646. United States District Court, S.D. Ohio, Eastern Division.. Web. 22 Mar. 2015.

The plaintiffs in this case tried to sue their insurance company for the increased risk of fraud (including phishing) following the theft of personal identification information. The court, however, ruled that increased risk at “some indeterminate point in the future” was insufficient to prove that the plaintiffs would suffer damages. This ruling suggests a partial answer to the question of St. Olaf’s legal responsibility in respect to phishing in that, unless St. Olaf’s actively causes people to be phished, St. Olaf is probably not accountable for the risk.

*How Not to Get Hooked by a Phishing Scam*. Washington, D.C.: Federal Trade Commission, 2005. Print.

In this article, the federal trade commission shares policies to teach people how to avoid getting scammed by emails. It is intended for institution and corporation use but include elements that are applicable to anyone.

Kim, Daejoong, and Jang Hyun Kim. "Understanding Persuasive Elements in Phishing E-mails: A Categorical Content and Semantic Network Analysis." *Online Information Review* 37.6 (2013): 835-50. Web.

In this research article, the researchers establish the results of their research by laying out the elements that make a phishing email more persuasive and successful. It will be helpful for us as we develop our think-aloud protocol.

Kumaraguru, Ponnurangam, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. "School of Phish: A Real-world Evaluation of Anti-phishing Training." *Proceedings of the 5th Symposium on Usable Privacy and Security* SOUPS '09 3 (2009): 1-12. *ACM Digital Library*. Carnegie Mellon CyLab, Google, 15 July 2009. Web. 23 Mar. 2015.

In this journal article, the researchers describe the methodology and results of their security test. They tested a couple hundred students and studied their response to phishing training. It was unsuccessful.

Mensch, Scott, and LeAnn Wilkie. "Information Security Activities of College Students: An Exploratory Study." *Academy of Information and Management Sciences Journal* 14.2 (2011): 91-116. *ProQuest*. Web. 25 Mar. 2015.

In this paper, the researchers at University of Pennsylvania studied the online behaviors of college students. Through this study, they researched how students interact and use online

services such as social networks and emails. They also tested other protocols such as Wi-Fi and networks security, but this is not of our interest.

Taylor, Brad. “Fighting phishing with eBay and PayPal.” Web blog post. *Official Gmail Blog*. Blogspot.com, 8 July 2008. Web. 25 Mar. 2015.

This blog post describes one of the strategies implemented by Google to attempt to reduce spam and phishing in Gmail. It explains why one of the emails sent as part of the think-aloud was marked as spam and one was not received at all.

Wright, Ryan, Suranjan Chakraborty, Asli Basoglu, and Kent Marett. "Where Did They Go Right? Understanding the Deception in Phishing Communications."*Group Decision and Negotiation* 19.4 (2010): 391-416. Web.

In this research paper, the authors explore the feelings associated with phishing and how phishing can build emotions in target to enable actions desired. This helps both develop our think-aloud protocol