OBJECTIVE: University students are attractive targets for identity thieves and hackers. According to the FTC’s Consumer Sentinel Network Data Book for 2012, they are among the highest percentage of identity theft victims. Many students do not realize the potential for fraud and do not guard their personal information as closely as they should. Student’s Social Security Numbers and birthdates are listed on everything from identification cards to social networking sites, making this information readily available to enterprising thieves. Universities and colleges are also attractive targets because they not only have valuable information, but their open environments make it easier for hackers to infiltrate systems undetected. Creating a student-focused awareness program will provide the following benefits to the UA Community:

1. Foster the security culture, and drive home the concept of “security as a habit.”
2. Increase students’ awareness of the resources available to them that are covered by their tech fee.
3. Create collaborative opportunities with UA academic departments that have marketing and audiovisual skill sets.
4. Provide the next generation with strong security habits that they can utilize as they graduate and join the fulltime workforce.

PROGRAM: The UA Student Security Awareness/Anti-Phishing Campaign has been entitled the “Think” Campaign. The main objective of this project is to provide education and awareness to members of the University of Arizona, from students to faculty and staff. Through future efforts by the University of Arizona Information Security team, various risks and threats directed at these key stakeholders can be minimized due to increased user awareness. Initially, the scope of this project is to create a program directed toward the student population. However, the materials developed can easily be adapted and used for other stakeholders, including faculty and staff. The primary goal of the “Think” Campaign will be to foster a culture committed to security that will minimize inherent risks associated with technology and the internet. Our project will be focused on the stakeholders, and less about the actual technology. In order for this project to have a significant impact on our stakeholders, the following deliverables are proposed:
• Relatable “skits/videos” that will touch on the various topics and issues outlined in the “Project Description” section above.
• Physical and digital posters, table toppers, free giveaways, newsletters, as well as other outreach materials.
• Security screensavers on departmental and OSCR computer lab desktop and laptop computers.
• Presentations to classes, organizations and forums
• Hands-on interactive activities, such as tent on the mall

Enhancement of services includes:
• Taking a strategic approach, rather than a scatter-gun approach, to educating our student population on securing their information, identities and systems. This is significant, as the student population is by far the largest portion of the UA community.
• Potential for partnerships with other University units, including Eller College of Management and the College of Fine Arts, with the intent to provide internship opportunities for Marketing and Visual Arts students. These students would be tasked with creating awareness materials that will appeal to their peers and optimize campus security awareness. Additionally, this will provide student interns with portfolio enhancing projects and real-world marketing and visual art experience.

Internal efficiencies are measured by a reduction in security incidents, including compromised accounts, compromised systems, and stolen laptops and mobile devices. Initially, the project is confined to work done primarily by three student workers, the Program Manager and the Senior Information Security Analyst. Increased security awareness for undergraduate and graduate students will help to mitigate risk to both University and personal information assets.

BUDGET:

<table>
<thead>
<tr>
<th>Expenditures</th>
<th>Year 1</th>
<th>Year 2</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td><strong>Personnel/Staffing</strong></td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td><strong>Supplies</strong></td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>Posters (11 x 17 – series of 10 posters, 250 copies each)*</td>
<td>$1,035</td>
<td>$1,035</td>
<td>$2,070</td>
</tr>
<tr>
<td>1/3 page flyers (3 per page, 1,000 copies, 2x per year)*</td>
<td>$430</td>
<td>$430</td>
<td>$860</td>
</tr>
<tr>
<td>Table Toppers (1 large + 1 small per mo during school year)*</td>
<td>$1,606</td>
<td>$1,606</td>
<td>$3,212</td>
</tr>
<tr>
<td>Bookmarks (distriute w/sales at UA Bookstores – 4,000 printed per semester)*</td>
<td>$993</td>
<td>$993</td>
<td>$1,986</td>
</tr>
<tr>
<td>8-1/2 x 11 flyers (series of 10 flyers, 500 copies each)*</td>
<td>$933</td>
<td>$933</td>
<td>$1,866</td>
</tr>
<tr>
<td>Marketing Materials** (e.g., branded pens, stress balls, hand sanitizers, foldable water bottles, mints)</td>
<td>$2,000</td>
<td>$2,000</td>
<td>$4,000</td>
</tr>
<tr>
<td>Advertising – UA Planner (Ad + 10 sidebars)</td>
<td>$500</td>
<td>$500</td>
<td>$1,000</td>
</tr>
<tr>
<td><strong>TOTAL PROJECT NEED</strong></td>
<td>$7,497</td>
<td>$7,497</td>
<td>$14,994</td>
</tr>
</tbody>
</table>
LAUNCH TIMELINE: UA Information Security has extremely limited funding. As a result, the project team will seek monies from the IT Student Advisory Board (ITSAB) for this project in the coming fiscal year. As well, the team will work to partner with campus organizations that may be able to augment the resources available, which will help with cost savings. Potential collaborations include working with Office of the CIO Marketing and Communications Team, Dean of Students Office, Residence Life, ASUA, Student Union, Student Affairs Marketing, ASUA Bookstores, Greek Life, and Academic Units.

The “Think” Campaign has been logically and functionally separated into 3 distinct sequential phases:

1. Create – design and creation of new outreach message/skit/video.
2. Deploy – newly created outreach mechanism will be spread throughout UITS, followed by the University at large.
3. After-Action – follow-up action item for participants with survey to increase end-user acceptance moving forward.

Objectives of the “Think” Campaign may include:

• Implement an awareness/outreach program consisting of at least 3 relatable videos and supporting documentation (via print media) pertaining to, but not limited to online reputation, social media, phishing, IT Security, and password protection by the beginning of the 2014/2015 academic year.
• Implement a sustainable process for conducting student/faculty/staff outreach events by July 2016.
• Staffing
• Collaboration with academic departments, e.g., Eller College of Management and College of Fine Arts
• Collaboration with administrative departments, such as Dean of Students Office, OSCR, 24/7 IT Support Center, Residence Life, Student Affairs Marketing, Greek Life, and ASUA
• Create internship positions in UAIS
• Create repeatable audience opportunities, such as MIS 111, MIS 415/416/417
• Procedures for continuing program

PROJECT MEMBERS:
Project Sponsor: Christian Schreiber - University Information Security Officer
Project Manager: Teresa Banks - Manager, Information Security and Compliance Programs
Barry Brummund - Deputy Chief Information Officer, Office of the CIO
ITSAB Executive Board Members – IT Student Advisory Board, UITS
APPENDIX: SAMPLES

Sample “Think” Campaign Topics and Scenarios

Online Reputation:
1. “Think before you post” - Disgruntled employee has a bad day, posts something inappropriate without thinking, later pulled into his supervisor's office and is reprimanded.
2. “Think before you post” - A hacker will do his homework prior to trying to hack or take over someone's account. If you have personal information that is also security question worthy like “secret question: where were you born?” on your profile you make it that much easier for intruders to gain access. (like leaving the key under the mat)
3. “Think before you act” - Student at a party takes unprofessional pictures and they get posted on social media. Next day for job interview employer tells them that they only employ professionals.
4. “Think before you act” - Disgruntled student goes on rant after finding out the results of his college entrance. Review committee comes across rant and decides not to give student a second chance.

Social Media:
1. “Think before you post” - A student posts their home address and phone number under profile information. They get in an argument with a stranger in class and threats are made. The stranger looks the student up and now knows where they live as well as their phone number.
2. “Think before you add” - Student trying to get to 10,000 friends on social media doesn’t think about who he is adding just how many friends he will have.
3. “Think before you share” - Student doesn’t set privacy settings on account and allows strangers to see personal information.
4. “Think before you Tweet” - Family household tweets that they will be out on vacation for a week. Come back to find out they were robbed.
5. “Think before you Instagram” - Student, over time, shares massive amounts of personal photos. Similar to a hacker “scoping” out a target with available online information, the pictures also allow for the hacker to steal his/her identity.
6. “Think before you Vine” - Student shares enough short vines of his/her house that a thief is able to scope out the location without ever getting within 100 yards.

Phishing:
1. “Think before you open” - Student sees “flashy” and “sexy” headlines in the subject line of numerous emails, once he or she opens the email, he has in-email HTML pictures set to automatically display, therefore leading to a computer virus.
2. “Think before you click” - Student receives dozens of emails every day, tired of verifying their senders and links, ends up getting computer virus that ruins his HDD.
3. “Think before you reply” - Student is prompted to win a new iPad by numerous emails claiming to be University studies, replies with credentials and personal information, identity theft occurs. (SSN).
4. “Think before you release” - Student gets offered a job via email. Student replies back with interest. Employer asks for personal information. Student releases sensitive information. (SSN).

Antivirus & Firewall:
1. “Think before you surf” - An unsuspecting student is casually browsing the internet without antivirus. As he moves from website to website, he is unprotected from a plethora of vulnerabilities, contract computer virus. In need of SOPHOS.
2. “Think before you download” - Another unsuspecting student is trying to download his favorite new music and movies from various unverified websites. In need of McAfee Siteadvisor. (verify Flash and video viewer.)

Passwords and Passphrases:
1. “Think before you share” - Student is in need of help for online quizzes and homework. Shares his password with multiple friends (maybe even through social media) and now his account becomes locked and/or his SSN/UA personal information/financial aid is compromised.
2. “Think before you create” - Student is prompted to create a new password as his or her previous password has expired. Because he or she is in a rush, a weak password is created.

SAMPLE ARTWORK

DO YOU HAVE A ROTTEN APPLE?

1 in 5 Macs are infected with Malware.
Protect yours with Sophos.*

*Sophos Rusted Security
THINK BEFORE YOU DOWNLOAD

• If you didn’t go looking for it, don’t install it
• If you installed it, update it
• If you no longer need it, delete it

Do you remember last night?
Your social network does.

THINK BEFORE YOU POST
First impressions happen before you walk in the door. 91% of employers check your social media accounts.*

**ONLINE REPUTATION**

Forbes Magazine, "What Prospective Employers Hope to See in Your Facebook Account"*

**THINK BEFORE YOU CLICK**

In one year the number of malicious web links grew by nearly 600%*