EDUCAUSE Webinar
Campus-Wide Two-Factor Authentication (2FA) Saturation Campaign

Daniel Stein, Branch Chief
Department of Homeland Security (DHS)
National Cybersecurity Education & Awareness Branch (CE&A)

October 2018

Cybersecurity Education & Awareness (CE&A)

DHS CE&A leads national cybersecurity public awareness, education, training, and workforce development efforts to support the protection against and response to cyber threats and hazards to the Homeland’s economic and national security.

CE&A focuses on the following programs and activities:
- Cybersecurity Awareness Programs
- Formal Cybersecurity Education (K-12 and Collegiate)
- Training and Education Programs
- Cybersecurity Workforce Development Programs
- State, Local, Tribal, and Territorial Cybersecurity Engagement
- Strategic Partnerships
It’s all on NICCS™

CE&A resources are easy to access through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Interactive and searchable NICE Cybersecurity Workforce Framework
- Training catalog with thousands of cyber-related courses
- Tools for cybersecurity managers
- List of upcoming cybersecurity events
- Hundreds of links to cybersecurity resources

NICCS averages 150,000+ page views each month: Visit niccs.us-cert.gov

Foundation for the Cybersecurity Workforce

NICE Cybersecurity Workforce Framework

- Describes cybersecurity work
- Supports strategic workforce development
- Includes 7 Categories, 30+ Specialty Areas, 50+ Work Roles
Federal Virtual Training Environment (FedVTE)

DHS offers free cybersecurity training for U.S. government employees and veterans!

✓ Available to Federal, State, Local, Tribal, and Territorial government employees and U.S. military veterans
✓ Courses range from beginner to advanced levels
✓ 245,000+ active users
✓ 31,000+ veteran users (through our non-profit partner Hire Our Heroes™)
✓ Over 60 courses - and growing!

Fedvte.usalearning.gov

National Cybersecurity Awareness Month

• Cybersecurity is our shared responsibility and we all must work together to improve our Nation’s cybersecurity

- Strengthen the Nation’s Cybersecurity Ecosystem
  Contribute and commit to strengthening the Nation’s cyber ecosystem

- Tackle it Together
  Cybersecurity is a cross-cutting, cross-sector problem, so we all have to work together

- Build the Cybersecurity Workforce
  Increase and strengthen the cybersecurity workforce across all sectors

- Protect Critical Infrastructure
  Heighten resilience and understand how to best protect critical infrastructure from cyber threats
CYBERSECURITY SATURATION CAMPAIGN
UTAH VALLEY UNIVERSITY

EDUCAUSE WEBINAR
11 OCTOBER 2018
UVU OVERVIEW

Utah Valley University
• 39,931 students
• 65+ baccalaureate programs, 85+ associate/certificate/diploma programs, and 12 graduate programs

UVU’S 2FA (DUO) IMPLEMENTATION
• Mandatory for Faculty and Staff on 1 October 2017
• Optional for students
PROBLEM

- How we influence students to do something completely optional?
- Barriers include: awareness, perceived inconvenience, lack of technical knowledge, privacy concerns, apathy.

SOLUTION

- Multipronged campus saturation campaign during October 2017
- Planning started Spring 2017
SATURATION CAMPAIGN PARTICIPANTS

- Administration
- University Marketing/PR
- External PR (Thatcher + Co.)
- National Cyber Security Alliance
- Department of Homeland Security
- Office of Information Technology
- Information Systems & Technology Department
- Institutional Research
- Students

SATURATION CAMPAIGN GOALS

- Raise awareness of National Cybersecurity Awareness Month.
- Increase student usage of 2FA authentication.
- Gather additional information about general cybersecurity awareness and attitudes.
- Promote NCSA #lockdownyourlogin messaging.
PRE-CAMPAIGN SURVEY

• Sent to 5,185 students; 499 completed the survey for a response rate of 9.62 percent.
• 22 Questions; mix of open-ended, yes/no, multiple-choice.
• Required IRB approval.

EXAMPLE SURVEY QUESTIONS

• In your opinion, how concerned do you think UVU is about your online safety as a student?
• What are some ways you as an individual can make your online accounts (e.g., online banking accounts, social media accounts, etc.) more secure?
• In the last year, have you been notified that your personal information may have been compromised, due to a data breach?
MULTIPRONGED CAMPAIGN

- Email/Video Messaging from University Administration.
- Digital Signage.
- Posters.
- Social Media Campaign.
- Cybersecurity Club Tables.
- Feature on main uvu.edu page.

ADMINISTRATION

- President Holland video.
- President’s email blast.
DIGITAL SIGNAGE

- 28 Horizontal (landscape)
- 56 Portrait
- 4 Banner (three horizontal in a row)

POSTERS

- Department bulletin boards.
- Classrooms.
- Student study areas.
SOCIAL MEDIA

• Facebook messages posted by UVU, UVUSA, and President Holland, including videos.

• Tweets by UVU, UVUSA, UVUCSC, and President Holland, including videos.
UVUCSC TABLES

- UVU Cybersecurity Club ran sign-up tables with laptops for enrollments in high-traffic areas throughout October.

HOME PAGE FEATURE / LANDING PAGE

- During October 2017, the UVU home page had messaging in rotation with dedicated landing page.

Cybersecurity at UVU

UVU has made strong authentication available to all UVU account holders. By installing a simple smartphone app, you can prevent access to your account, even if someone learns your password. Discover more about why this is a great idea at lockdownyourlogin.org.

When you are ready to Lock Down Your Login, click here to enable this protection on your UVU account through the myUVU portal.
POST-CAMPAIGN SURVEY

- Sent to 5,500 students; 288 completed the survey for a response rate of 5.20 percent

RESULTS

How Concerned UVU is about Online Safety

<table>
<thead>
<tr>
<th></th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very</td>
<td>46%</td>
<td>53%</td>
</tr>
<tr>
<td>Somewhat</td>
<td>42%</td>
<td>38%</td>
</tr>
<tr>
<td>A little</td>
<td>8%</td>
<td>6%</td>
</tr>
<tr>
<td>Not at all</td>
<td>3%</td>
<td>3%</td>
</tr>
</tbody>
</table>
RESULTS

Use Different Password for Each Account

<table>
<thead>
<tr>
<th></th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>71%</td>
<td>62%</td>
</tr>
<tr>
<td>No</td>
<td>29%</td>
<td>38%</td>
</tr>
</tbody>
</table>

RESULTS

How Respondent Rates Security of Combination of Login and Password

<table>
<thead>
<tr>
<th></th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-Extremely</td>
<td>13%</td>
<td>19%</td>
</tr>
<tr>
<td>4-Very</td>
<td>49%</td>
<td>49%</td>
</tr>
<tr>
<td>3-Somewhat</td>
<td>35%</td>
<td>26%</td>
</tr>
<tr>
<td>2-A Little</td>
<td>3%</td>
<td>5%</td>
</tr>
<tr>
<td>1-Not at all</td>
<td>5%</td>
<td>1%</td>
</tr>
</tbody>
</table>
RESULTS

Respondent Definition of Multi-factor Authentication

<table>
<thead>
<tr>
<th>Description</th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of personal questions</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Using more than one method to authenticate identity*</td>
<td>0%</td>
<td>3%</td>
</tr>
<tr>
<td>Using login and password</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>Using tools and technologies to add layer of protection</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>All the above</td>
<td>33%</td>
<td>40%</td>
</tr>
<tr>
<td>Not sure</td>
<td>7%</td>
<td>6%</td>
</tr>
</tbody>
</table>

*Response option not included in follow-up survey

RESULTS

Awareness of Cybersecurity Campaigns

<table>
<thead>
<tr>
<th>Campaign</th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Campaign</td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>On-campus Campaign</td>
<td>34%</td>
<td></td>
</tr>
</tbody>
</table>
RESULTS

Awareness of Campaign Messages*

- Own your online presence: 30% in Post-Survey vs. 12% in Pre-Survey
- Safer for me, more secure for all: 33% in Post-Survey vs. 22% in Pre-Survey
- When it doubt, throw it out: 15% in Post-Survey vs. 6% in Pre-Survey
- Share with care: 44% in Post-Survey vs. 11% in Pre-Survey
- Keep a clean machine: 28% in Post-Survey vs. 17% in Pre-Survey
- Lock down your log-in: 35% in Post-Survey vs. 20% in Pre-Survey
- Privacy is like money: value it protect it**: 0% in Post-Survey vs. 0% in Pre-Survey
- Stay safe online**: 33% in Post-Survey vs. 27% in Pre-Survey
- I'm not sure**: 40% in Post-Survey vs. 27% in Pre-Survey

*The pre-campaign survey question asked about whether respondents had heard any of the following cybersecurity advice phrases. The post-campaign survey asked which messages were used in the campaign.

**Response option was not used in either the pre-campaign survey or post-campaign survey.

RESULTS

Interest in Cybersecurity Courses*

- Yes: 21% in Pre-Survey vs. 29% in Post-Survey
- Maybe: 45% in Pre-Survey vs. 35% in Post-Survey
- No: 35% in Pre-Survey vs. 64% in Post-Survey

*The pre-campaign survey question asked about interest in cybersecurity courses. The post-campaign survey asked about interest in cybersecurity courses post-campaign.
**RESULTS**

Respondent Interest in Cybersecurity Career

<table>
<thead>
<tr>
<th></th>
<th>Pre-Survey</th>
<th>Post-Survey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Maybe</td>
<td>19%</td>
<td>23%</td>
</tr>
<tr>
<td>No</td>
<td>72%</td>
<td>69%</td>
</tr>
</tbody>
</table>

**RESULTS**

Cybersecurity Top Topics of Interest

In each survey, respondents were asked to pick their top three areas of interest pertaining to cybersecurity.
### RESULTS

**How Respondents Learned About Campaign**

<table>
<thead>
<tr>
<th>Source</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friend, professor, or other staff</td>
<td>20%</td>
</tr>
<tr>
<td>Text alerts or UVAnounce</td>
<td>24%</td>
</tr>
<tr>
<td>Digital signage</td>
<td>25%</td>
</tr>
<tr>
<td>Booths/help desks</td>
<td>6%</td>
</tr>
<tr>
<td>Email from President Holland or UVU faculty</td>
<td>62%</td>
</tr>
<tr>
<td>UVU Social Media</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>11%</td>
</tr>
</tbody>
</table>

**Percent of Sample that Installed Two-factor Authentication because of Campaign**

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shopping (Amazon)</td>
<td>16%</td>
</tr>
<tr>
<td>Video Streaming services</td>
<td>11%</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>3%</td>
</tr>
<tr>
<td>Music</td>
<td>19%</td>
</tr>
<tr>
<td>Social Media</td>
<td>5%</td>
</tr>
<tr>
<td>Other financial</td>
<td>10%</td>
</tr>
<tr>
<td>Banking</td>
<td>11%</td>
</tr>
<tr>
<td>Email</td>
<td>27%</td>
</tr>
<tr>
<td>Other*</td>
<td>27%</td>
</tr>
</tbody>
</table>
RESULTS

Likelihood of Using Multi-Factor Authentication Moving Forward

- Very Likely: 20%
- Likely: 50%
- Not Very Likely: 24%
- Not Likely at All: 6%

RESULTS

Respondent Would Recommend Multi-factor Authentication to Others

- Yes: 41%
- Maybe: 49%
- No: 10%
RESULTS

Respondent Aware of October as National Cybersecurity Awareness Month

- Yes: 18%
- No: 82%

RESULTS

Respondent Aware of Where on Campus to Find Info about Staying Safe Online

- Yes: 14%
- No: 63%
- Not Sure: 23%
RESULTS

Downloaded DUO offered through UVU

- Yes: 24%
- No: 34%
- Haven't heard about it: 42%

RESULTS

How Respondents Learned about DUO

- Friend, professor, or other staff: 16%
- Text alerts or UVAnnounce: 7%
- Digital signage: 5%
- Booths/help desks: 2%
- Email from President Holland or UVU faculty: 57%
- UVU Social Media: 16%
- Other: 27%
RESULTS

Respondents Thought Worthwhile to Download DUO

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
<th>Not Sure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>63%</td>
<td>15%</td>
<td>22%</td>
</tr>
</tbody>
</table>

RESULTS

How Respondents Learned about DUO

- Friend, professor, or other staff: 16%
- Text alerts or UVAnnounce: 7%
- Digital signage: 5%
- Booths/help desks: 2%
- Email from President Holland or UVU faculty: 57%
- UVU Social Media: 16%
- Other: 27%
RESULTS

How Respondent Would Encourage Others to Download DUO

- 60% Tell them it's easy
- 50% Tell them it's free
- 62% Tell them it's for their protection
- 48% Tell them it will make them safer online
- 2% Other

KEY FINDINGS

- Awareness/knowledge of “Lock Down Your Login” messaging (29 percent pre-campaign vs. 49 percent post-campaign.
- Seventy percent in the post-survey said they would ‘likely’ or ‘very likely’ use multifactor authentication moving forward.
- Correct definition of multi-factor authentication was 20 percent pre-campaign vs. 57 percent post-campaign.
KEY FINDINGS

- Fifty-seven percent of students who downloaded multi-factor authentication said they did so after receiving an email from the university president urging them to opt in via Duo. The email led to more than 800 immediate views of the Duo site.
- 16 percent of students said they were influenced by a friend, professor, or other staff member to download the app.
- Another 16 percent said they learned of it via UVU’s social media platforms.

KEY FINDINGS

- Sixty-three percent of those who downloaded the multi-factor authentication app said it was worthwhile to do so; 41 percent said they would recommend others do so, while 49 percent said they ‘maybe’ would recommend it to others.