Whatcom COMMUNITY COLLEGE

NCyTE CENTER

INFORMATION SECURITY AND THE CIA TRIAD

Nancy Stevens, First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

INFORMATION SECURITY AND THE CIA TRIAD

GONE PHISHING

Students explore the concept of trust in online interactions. The lesson begins with a warm-up activity. Students engage in a word association about information security risks and generate a word cloud. The PowerPoint slides provide background information on the scope of online information security problems. Students will then explore phishing emails. A Think-Pair-Share activity explores trust in our online interactions.

LAB ENVIRONMENT

Classroom or computer lab with Internet access and a projection device for the slides. Students contribute to a word cloud identifying words associated with information security risks. The instructor presentation introduces some statistics on online information security, so students understand the scope of the problem. The instructor leads students through a phishing and a social media scenario. Students will reflect on a prompt about trust through a Think-Pair-Share activity.

LAB FILES NEEDED

- CIATriad_Presentation.pptx
- CIATriad_GonePhishing_Activity_Solution.docx

GUIDING QUESTIONS

What is "trust" based upon in the online world?

How does the CIA Triad affect information security?

WARM UP

Students will contribute to a word cloud describing cybersecurity risks. An interactive online presentation tool, such as Mentimeter, can be used to display the prompt and to promote student interaction. Display this prompt for students: *What are 3 words that come to mind when you think about online security risks?*

Lead a brief discussion with students about the most popular responses (the larger the word appears in the word cloud, the more frequently it occurred as a response). Teaching Tip: You may want to assign the word cloud the day prior to this lesson, that will give you time to review the responses.

Establish that risks are inherent by engaging in online activities (email phishing, fake friend requests, social media bots, ransomware, data breach). Even if you do not participate in social media, your friends and family can post your photo and personal information. Current estimates indicate that phishing accounts for 90% of data breaches. If students are not familiar with email phishing, there are several websites with examples of phishing emails.

ONLINE PHISHING QUIZ/STEP 1

Select one of the phishing quiz websites provided in the slide presentation (and below) to give students an opportunity to explore phishing.

- Can you spot when you're being phished? (Google & Jigsaw)
- How is your Phishing IQ? (Sonicwall)
- Phising Quiz (OpenDNS.com)

PHISHING SCENARIO/STEP 2

Then guide students through the scenarios in the slide presentation. It's August and school will be starting soon. You have not checked your school email account since June. Your friends have told you that there are some important emails about senior photos that you should read. Your inbox has over one hundred unread emails. You scan the subject lines looking for the email about senior photos. There are lots of emails from colleges, reminders about summer reading, and then you see the subject line, "Urgent". You open the email, that reads as follows:

```
The attached document contains important information about your school
year. Kindly, click open file using supportive web browser. The
document is securely sent using PDF scanner. Feel free to contact me
if you have any questions.

Note: Open Attached PDF and preview with Existing ID
```

You click on the attachment, it opens in the browser, and you click on a link that says, "Sign in to view the document". You are redirected to a login page requesting your email address and password. You enter your credentials and some files start downloading to your computer. You now wonder whether you should have provided your email address and password. You feel a sense of panic as your computer is restarting.

FAKE SOCIAL MEDIA/STEP 3

The second scenario concerns social media requests. While checking your social media account on your phone, you see several new follower requests. You tap to confirm the requests as some of them look familiar, but others do not. You want to raise your follower count to boost your online presence, so more is better. Or is it? What harm can come from accepting fake follower requests?

TRUST/STEP 4

Think-Pair-Share Activity: What do phishing emails or fake social media accounts tell us about trust in the online world? (Think-Pair-Share is a collaborative strategy that students are required to first think about an answer to a question, then discuss with a partner, and to finally share out responses in some manner.)

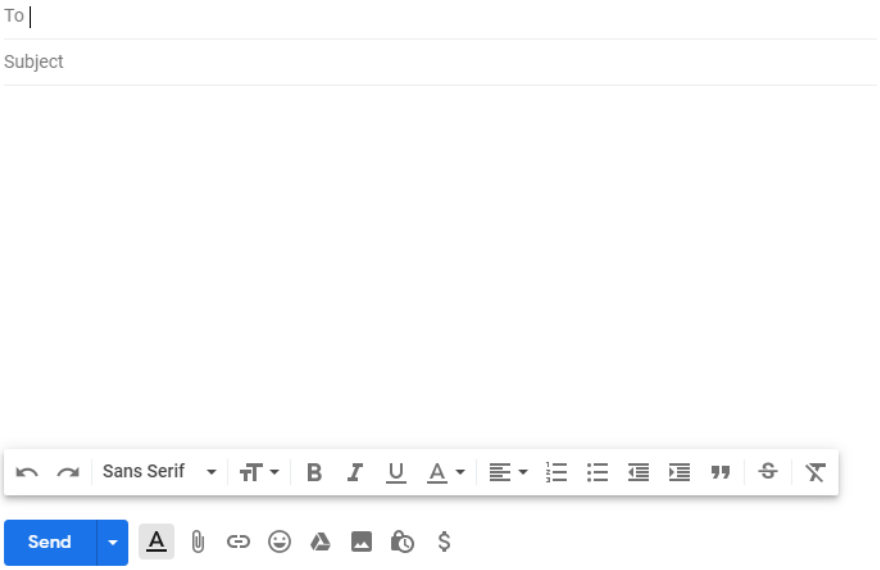
Possible responses:

- Easy to create and replicate
- Easy to amplify through the use of bots
- Followers can be purchased
- Lack of verification
- Accounts get hacked
- Illusions of safety
- Scams exploit human weakness
- Moderating content is difficult
- Financial incentives for fake accounts
- Disinformation campaigns by adversaries

CHALLENGE ACTIVITIES

The challenge activities are optional. In the first challenge, students compose a phishing email to demonstrate their understanding of how phishing works. In the second challenge, students research a privacy law.

 This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.



WHAT TO SUBMIT

Students independently complete a Phishing quiz in Step 1. Students share out responses in Steps 2 and 3 of the Lab. Step 4 is a Think-Pair-Share activity. Teachers may want to create an online discussion post to capture students' ideas in writing.