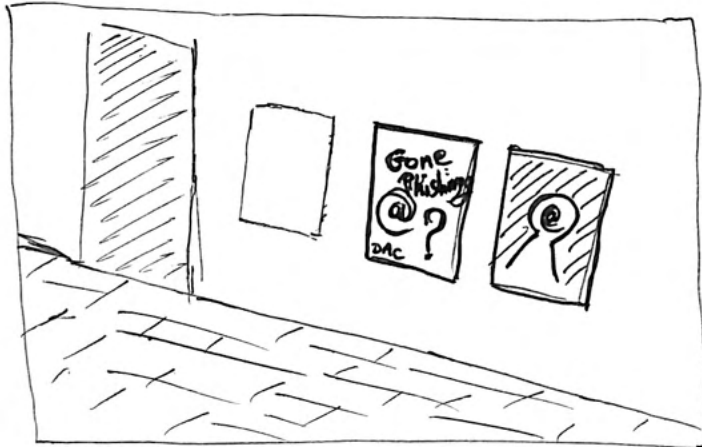


# PREVENT EXPLOITATION OF EMPLOYEE PRIVILEGES THROUGH PHISHING

LEVEL 1



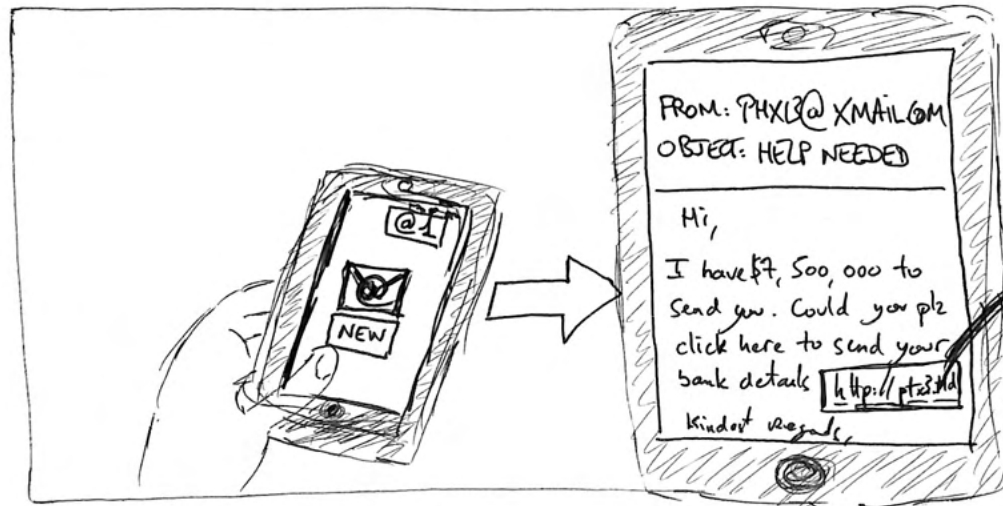
TEASING POSTERS



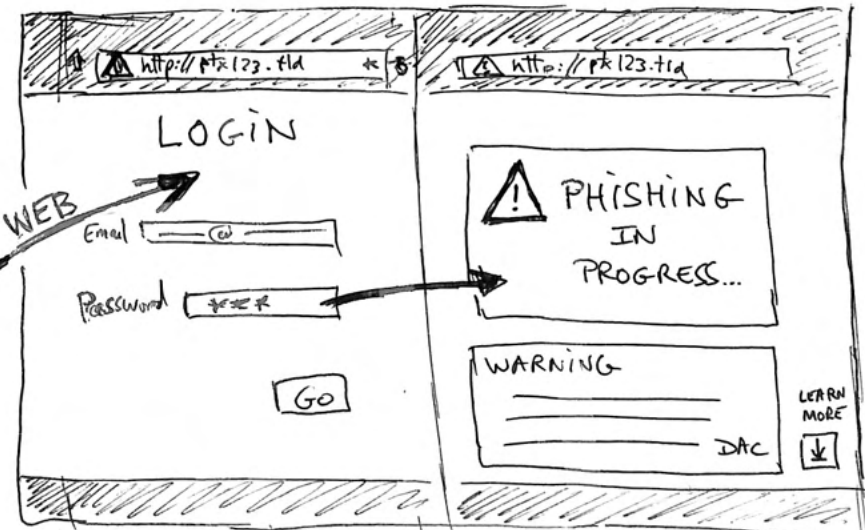
CHAMPIONS RECRUITMENT



BROWN-BAG MEETINGS



OBVIOUS PHISHING SCAM



ASSESSMENT: CREDENTIALS

FEEDBACK + OBJECTIVE

Storyboard 2.1.1

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



TEASING POSTERS

1. Attract Attention

Programming / Interactions

Performance Objectives

Storyboard 2.1.2

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



CHAMPIONS RECRUITMENT

1. Attract Attention
2. State the Objective

Programming / Interactions

Performance Objectives

Storyboard 2.1.3

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



BROWN-BAG MEETINGS

2. State the Objective
3. Stimulate recall of Prerequisites

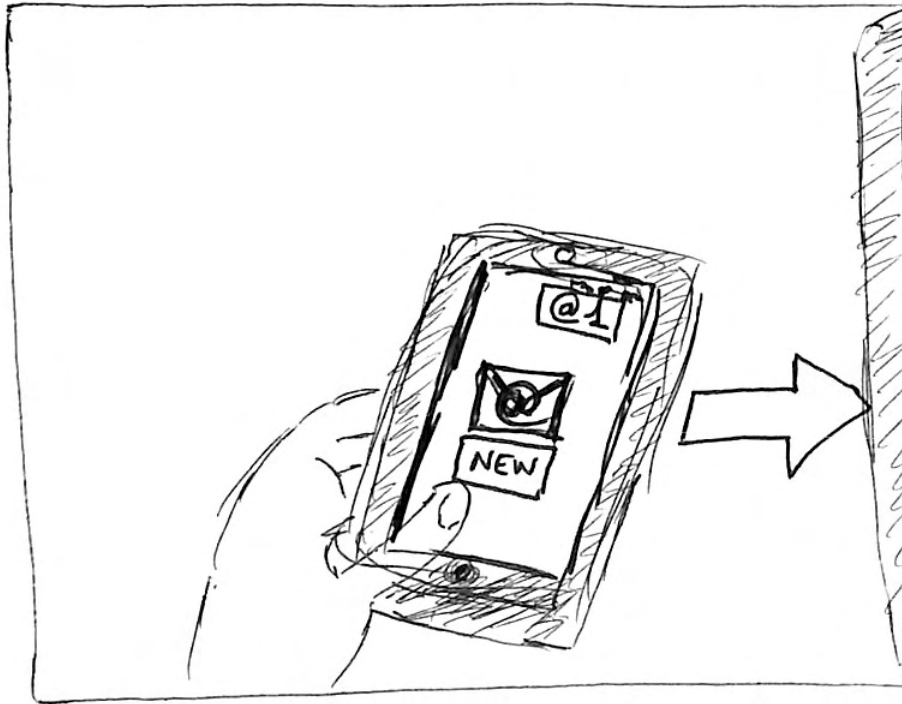
Programming / Interactions

Performance Objectives

Storyboard 2.1.4

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



4. Present Stimulus *Without Emphasis*  
9. Spaced Reviews and Generalization

Programming / Interactions

Send phishing test emails:

- at random intervals
- to targeted individuals
- progressively growing in numbers

Keep track of learners' level,  
with everyone starting at level 1.

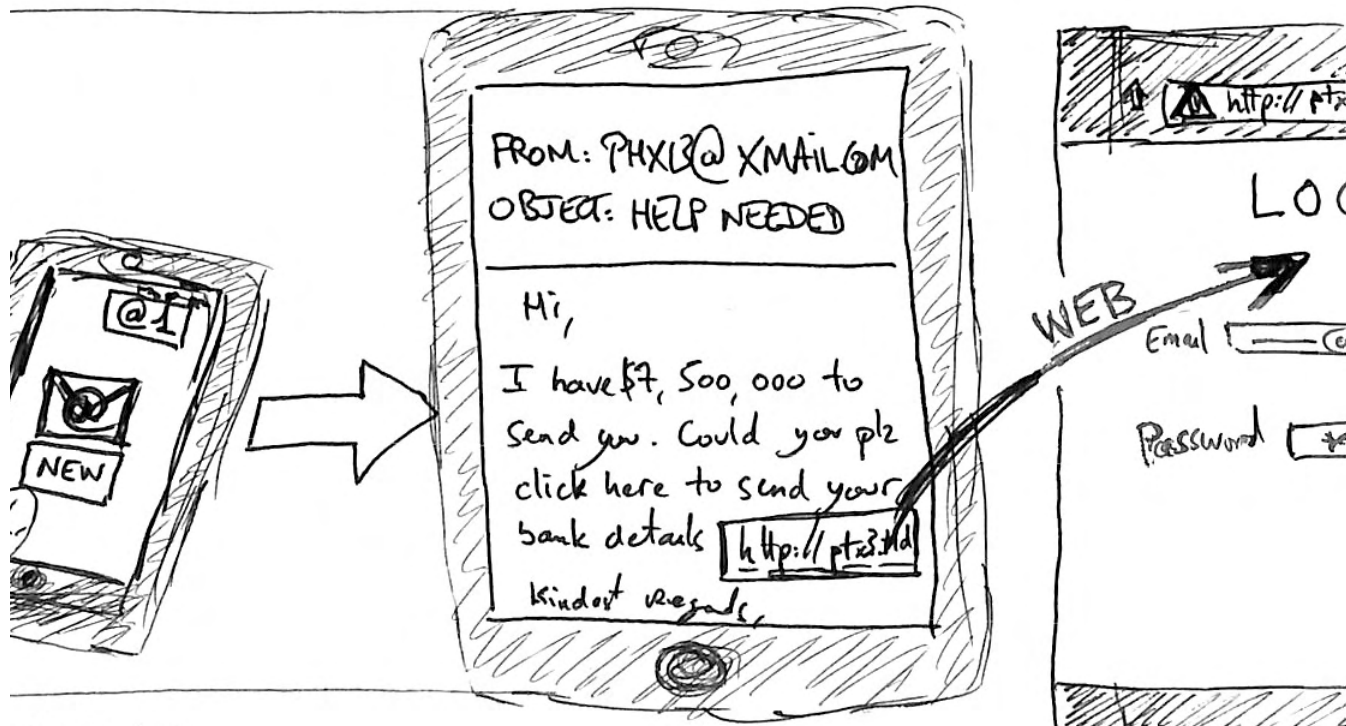
Performance Objectives

Storyboard 2.1.5

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events

4. Present Stimulus *Without Emphasis*  
8. Assessment



Programming / Interactions

Link to a fake login page.  
At level 1, the text of the link matches the URL.

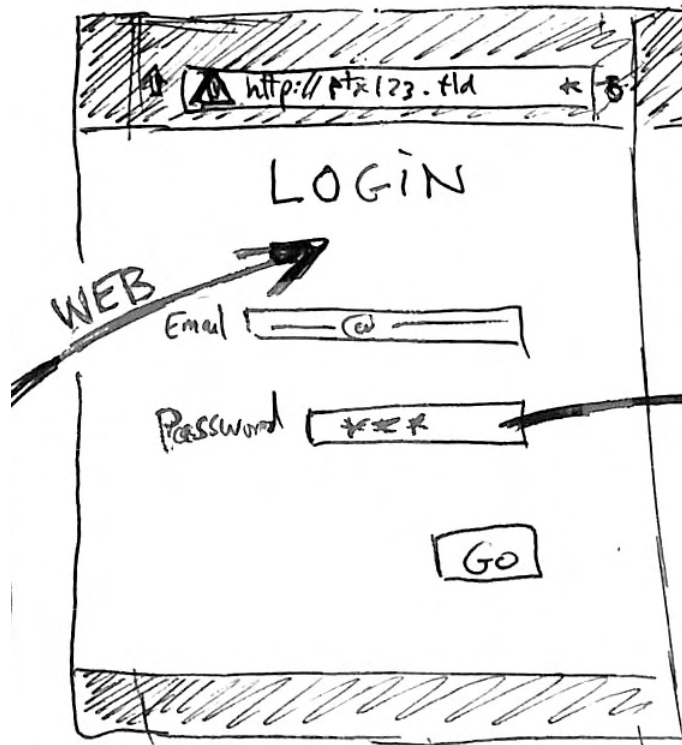
Performance Objectives

Given an email received from an unknown contact in the course of daily activities, with a URL which opens a login page similar to the one on Horizon extranet, the Horizon employee or volunteer IDENTIFIES (Intellectual Skill: Concrete Concept) the login form as unexpected and suspicious by not typing their password in the suspicious form at any point.

Storyboard 2.1.6

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



4. Present Stimulus *Without Emphasis*  
8. Assessment

Programming / Interactions

After typing 3 password characters,  
display Phishing in Progress feedback.

(continued)

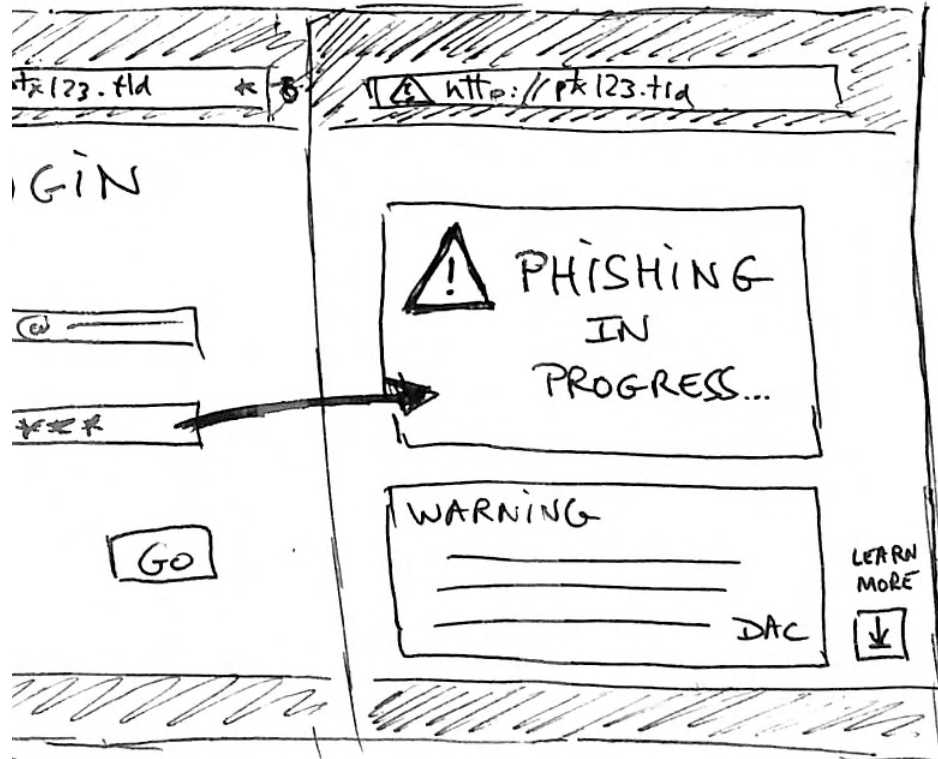
Given an email received from an unknown contact in the course of daily activities, with a URL which opens a login page similar to the one on Horizon extranet, the Horizon employee or volunteer IDENTIFIES (Intellectual Skill: Concrete Concept) the login form as unexpected and suspicious by not typing their password in the suspicious form at any point.

Performance Objectives

Storyboard 2.1.7

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



- 1. Attract Attention
- 7. Feedback
- 2. State the Objective
- 5. Learning Guidance

Programming / Interactions

Link to download a copy of the Learning Guidance in PDF format.  
Instructions on how to contact a human for more details.

Performance Objectives

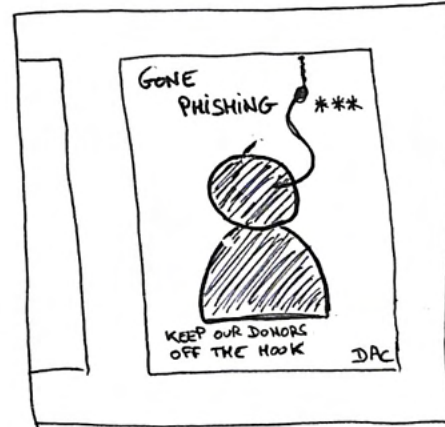
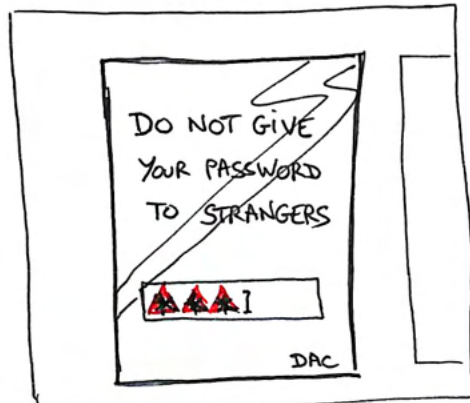


# PREVENT EXPLOITATION OF EMPLOYEE PRIVILEGES THROUGH PHISHING

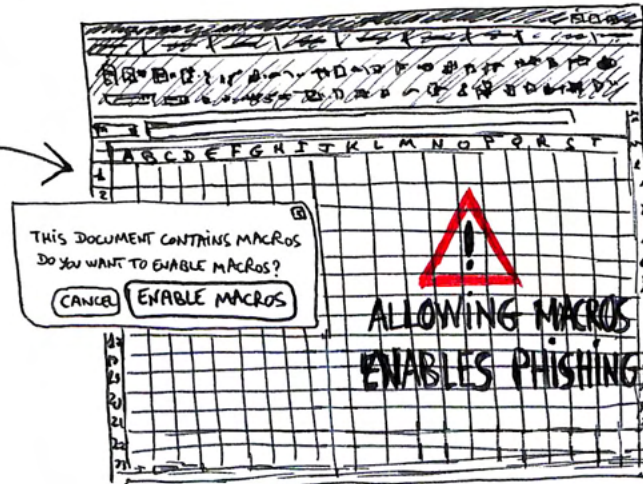
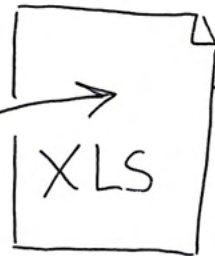
LEVEL 2



AT THE TRAINING-TASKFORCE OFFICE



INFORMATIVE POSTERS FROM THE DIGITAL AWARENESS COMMITTEE



Storyboard 2.2.1

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



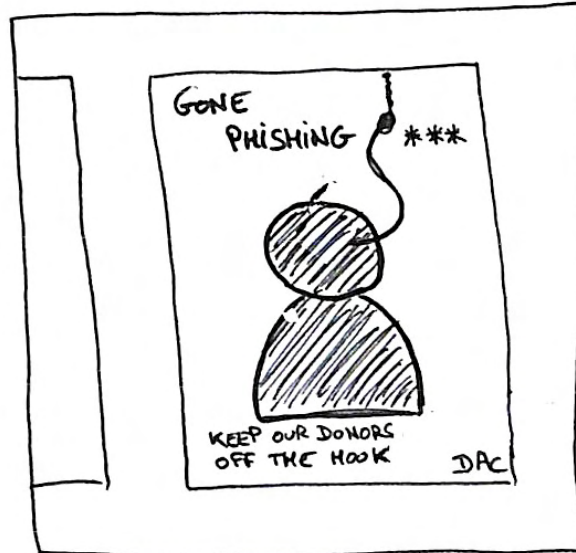
AT THE TRAINING TASKFORCE OFFICE

8. Assessment (by proxy)  
of the Change of Attitude

Programming / Interactions

Performance Objectives

- 1. Attract Attention
- 2. State the Objective
- 3. Stimulate Recall of Prior Learning



INFORMATIVE POSTERS FROM THE DIGITAL AWARENESS COMMITTEE

Programming / Interactions

Performance Objectives

Storyboard 2.2.3

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events

4. Present Stimulus *Without Emphasis*  
9. Spaced Reviews and Generalization

Programming / Interactions

Attached Spreadsheet with macros designed to assess the learner.



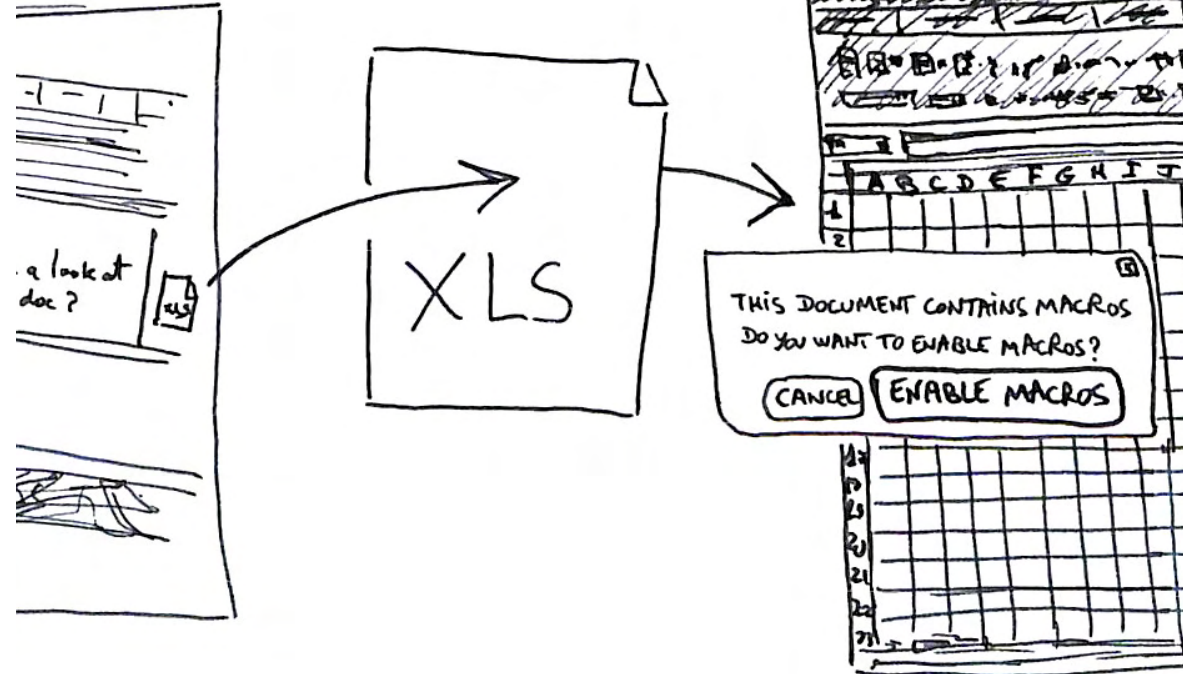
Performance Objectives

Given an email received from an unknown contact in the course of daily activities, with an attached file which is executable on the computer from which the email is read the Horizon employee or volunteer IDENTIFIES (Intellectual Skill: Concrete Concept) the attached file as executable and suspicious by not allowing it to run on the computer at any point.

Storyboard 2.2.4

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



4. Present Stimulus *Without Emphasis*  
8. Assessment

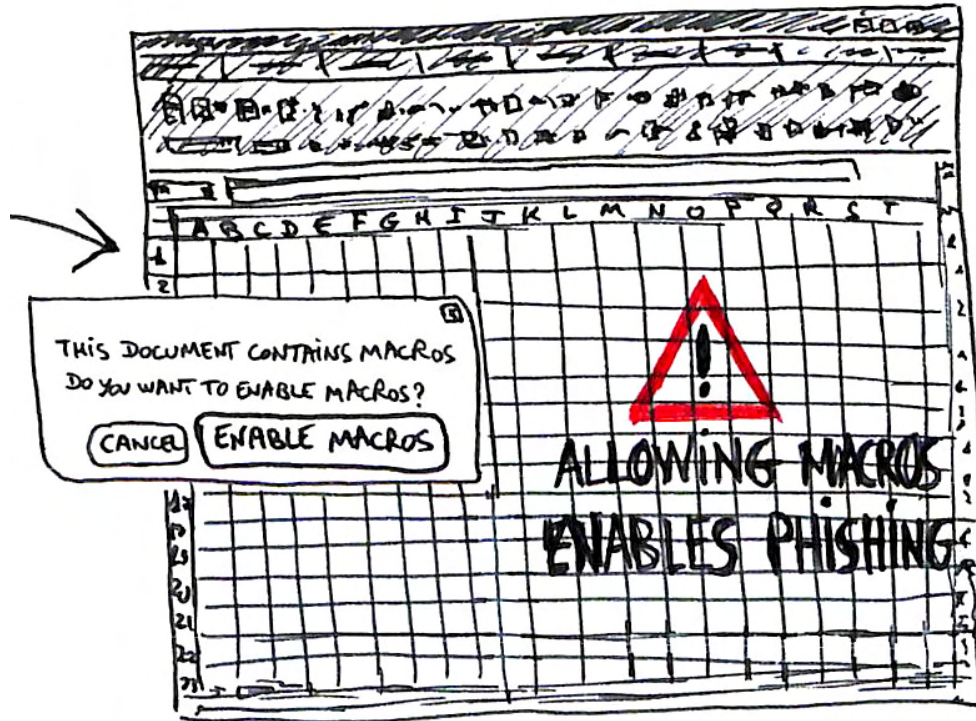
Programming / Interactions

Native notification about macros issued by spreadsheet software.

(continued)

Given an email received from an unknown contact in the course of daily activities, with an attached file which is executable on the computer from which the email is read the Horizon employee or volunteer IDENTIFIES (Intellectual Skill: Concrete Concept) the attached file as executable and suspicious by not allowing it to run on the computer at any point.

Performance Objectives



- 1. Attract Attention
- 7. Feedback
- 2. State the Objective
- 5. Learning Guidance

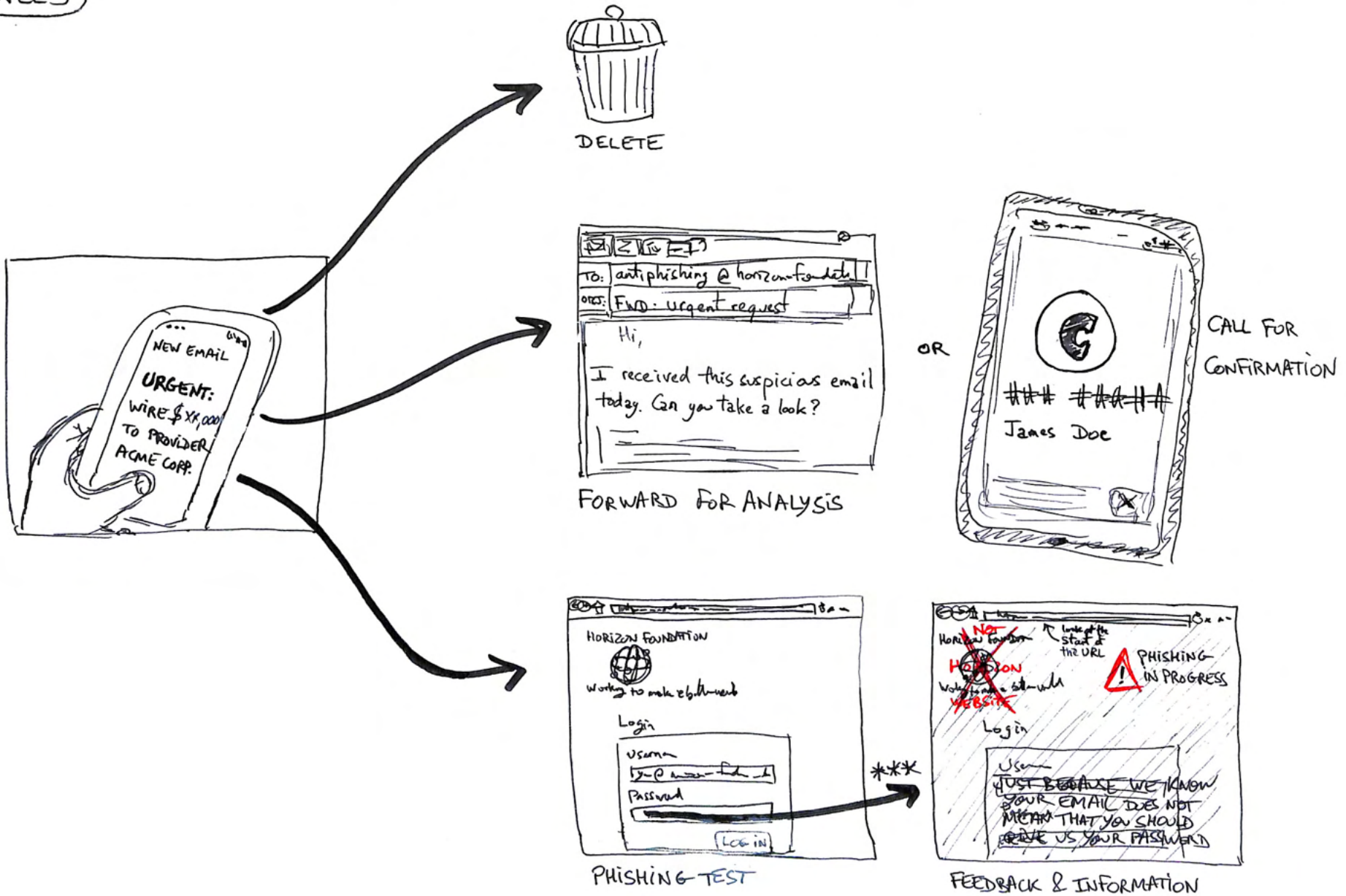
Programming / Interactions

Macros trigger the display of feedback about the Phishing in Progress, and instructional information which can be printed for reference.

Performance Objectives

# PREVENT EXPLOITATION OF EMPLOYEE PRIVILEGES THROUGH PHISHING

LEVEL 3



Storyboard 2.3.1

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events



4. Present Stimulus *Without Emphasis*  
9. Spaced Reviews and Generalization

Programming / Interactions

Link to fake login page with link text masking the real URL.

Performance Objectives



Storyboard 2.3.2

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events

8. (Implicit) Assessment



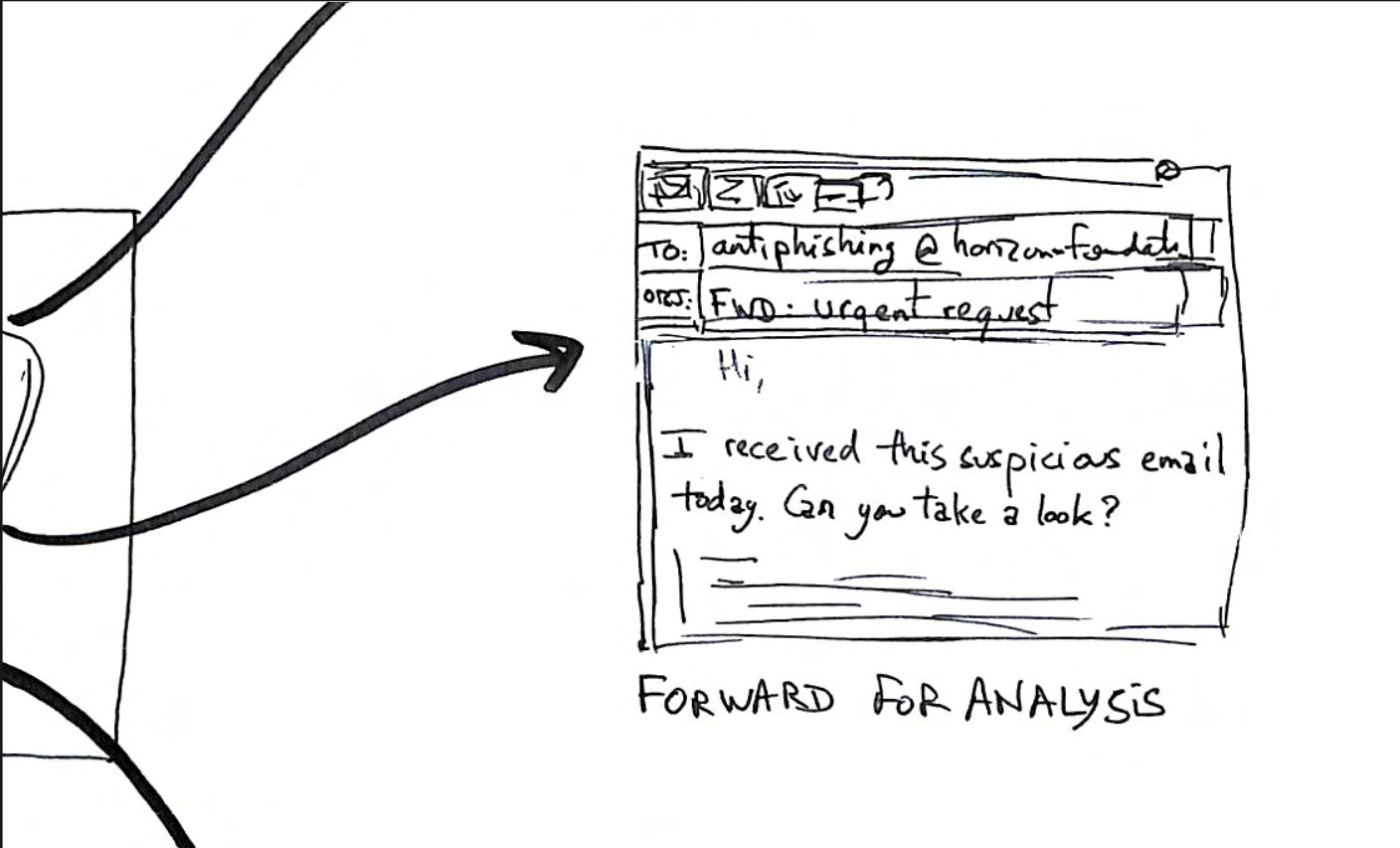
Programming / Interactions

This outcome is assumed when the learner does not take any of the other actions within two business days.


However, the assessment may still be changed from success to failure if the learner falls prey to the test scam after that initial delay.

Performance Objectives



| Storyboard 2.3.3  | Prevent Exploitation of Employee Privileges through Phishing | Instructional Events   |
|---|--|--|
|  |  | <p><b>8. (Explicit) Assessment</b></p> <p>And in email reply:</p> <p><b>7. Feedback (Thanks and Confirmation)</b></p> <p><b>2. State the Objective</b></p>                     |
|   |  | <p><b>Programming / Interactions</b></p>   |
|   |  | <p>Automated email reply with thanks, a confirmation and more details about the instructional phishing attempt.</p> <p>A reply to the automated email shall reach a human.</p> |

|  | Performance Objectives |
|--|------------------------|
| <p>Given an email received from an unknown contact in the course of daily activities with tell-tale signs that make it suspicious (an unusual tone or language or an unexpected request) the Horizon employee or volunteer<br/> <b>DEMONSTRATES</b> (Intellectual Skill: Rule)<br/> that they are aware of Horizon policy to report suspicious emails by forwarding it for analysis to the dedicated email address publicized on posters for that purpose, within 2 business days after receiving the email.</p> |                        |

| Storyboard 2.3.4   | Prevent Exploitation of Employee Privileges through Phishing | Instructional Events   |
|--|--|--|
|  <p>OR</p> |  | <p><b>8. (Explicit) Assessment</b></p> <p>And during the phone call:</p> <p><b>7. Feedback</b></p> <p><b>2. State the Objective</b></p> <hr/> <p><b>Programming / Interactions</b></p> <p>Automated phone answer with thanks, explanations and learning guidance.</p> <p>Option to talk to a human afterwards.</p> |

| <b>Performance Objectives</b>  |
|--|
| <p>Given an email received from a known contact in the course of daily activities with tell-tale signs that make it suspicious (an unusual tone or urgency or an unexpected request) the Horizon employee or volunteer DEMONSTRATES (Intellectual Skill: Rule) that they are aware of Horizon policy to double-check unexpected requests received by email by calling the contact to confirm the request using the phone number published for that contact in Horizon directory within 1 business day after receiving the email.</p> |

Storyboard 2.3.5

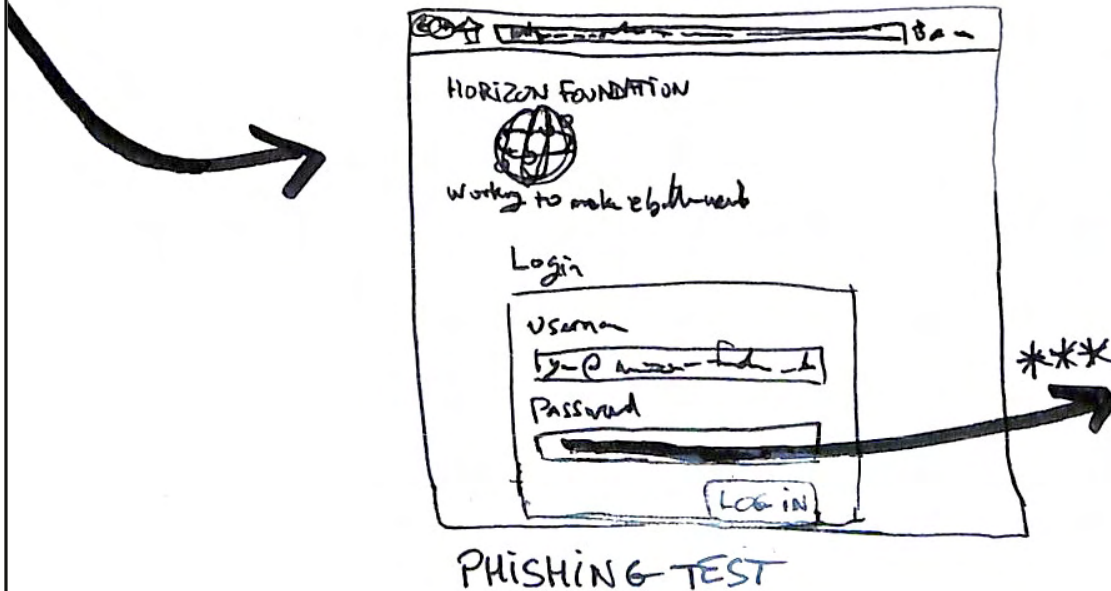
Prevent Exploitation of Employee Privileges through Phishing

Instructional Events

4. Present Stimulus *Without Emphasis*  
8. Assessment

Programming / Interactions

After typing 3 password characters,  
display Phishing in Progress feedback.



Performance Objectives

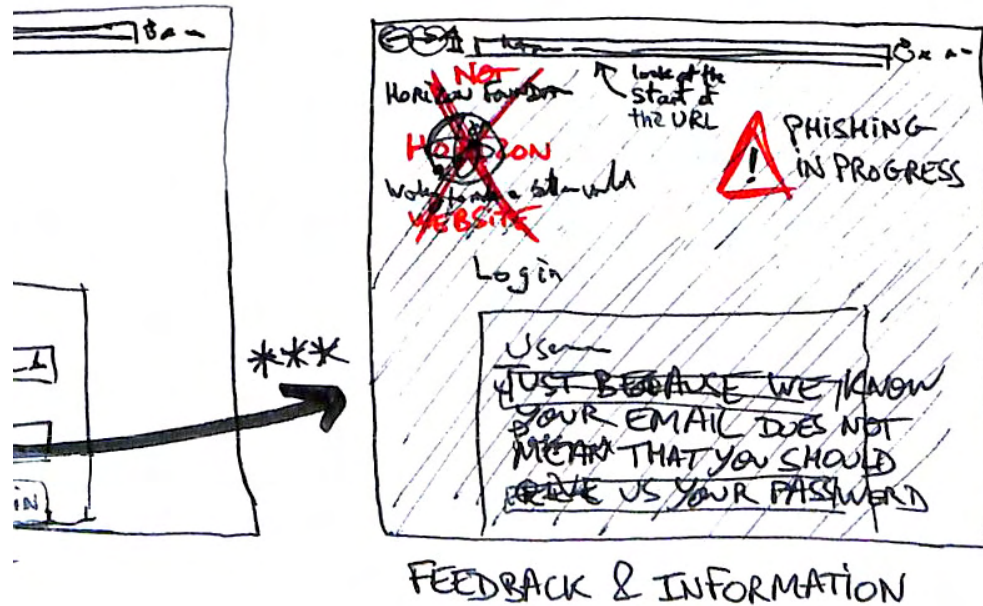
Given an email received from an unknown contact in the course of daily activities, with a URL which opens a login page similar to the one on Horizon extranet, the Horizon employee or volunteer IDENTIFIES (Intellectual Skill: Concrete Concept) the login form as unexpected and suspicious by not typing their password in the suspicious form at any point.

Storyboard 2.3.6

Prevent Exploitation of Employee Privileges through Phishing

Instructional Events

- 1. Attract Attention
- 7. Feedback
- 2. State the Objective
- 5. Learning Guidance



Programming / Interactions

Link to download a copy of the Learning Guidance in PDF format.  
Instructions on how to contact a human for more details.

Performance Objectives