## CSE 469 – Spring 2020

Homework 2: Phishing Kit Analysis (to be done in project groups)

Due date: Apr. 28. 3:00 pm

Submission: Gradescope (only one person per group)
https://www.gradescope.com/courses/79694

For full credit, please provide **screenshots and/or clear explanations** which each answer.

Group ID:

All Names:

Q1. What brand is being impersonated by the phishing kit? (1pt)

Q2. Is there any cloaking?  If so, where, and what is being blocked? (2pt)

Q3 a. What information is being phished?  (1pt)

b. How is the information exfiltrated? (1pt)

Q4. What is the *attacker's* e-mail? (1pt)

Q5 a. How does the kit backdoor work? [hint: look for PHP code that exfiltrates data] (1pt)

b. What is the *kit author's* e-mail? (1pt)

c. What information gets leaked? (1pt)

Q6. Where is the attacker likely located (country or region)? (2pt)

Q7. What other interesting observations do you think would be useful for a threat intelligence team? (1pt)

Q8. Extra credit: where is the *kit author* located, and how did you find out? (+1pt)