Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Work Plan**

**Goal:**Build a phishing tool that's purpose is to steal usernames, passwords and ids of students and university staff, it works by gathering phone numbers from WhatsApp groups, and sending a SMS to hundreds of students and university staff and ask them to change their annual password, the sender’s SMS messages is impersonating an official SMS message from the university.

**Challenges and how-to overcome them:**

Building a website that looks and feels as real as possible to the actual password changing website of the university. To encounter this matter, we retrieved the source file of the actual website and tweaked it to match the exact design of the real website.

**Strong points:**

1. The SMS message
2. The website can change its behavior according to the number of times that user has entered that website, thus reducing suspicion of the user by redirecting them to the original website and actually allowing the user to change his password.
3. We capture the user’s old and new passwords, and by doing so, we can look for a pattern in the user’s password (e.g. a single number that changes, capital letters turn into small letter, etc.)

**Milestones and timetable:**

|  |  |
| --- | --- |
| Milestone | Date |
| Defining the plan | 28/04/2020 |
| Front-end design | 05/05/2020 |
| Back-end design | 12/05/2020 |
| Database + VPS connection | 20/06/2020 |
| Python script for searching | 10/07/2020 |
| Finishing touches | 18/07/2020 |
| SMS integration | 14/09/2020 |

Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Overview**

**We saw an opportunity**

Every year, the university sends an e-mail asking students and staff members to change their password. At first, we thought the e-mail is a phishing mail, however, after thinking about it, we saw this as an opportunity to create our own phishing tool to get unauthorized access to the university staff’s account and change information accordingly.

We have also thought about the fact that new students don’t have much experience with the university’s system, and so we thought about joining Facebook groups, and posting “helpful” links such as Google Drive link, Student Management System, etc., and one of those links will be our phishing site. We would also join WhatsApp groups, extract phone numbers and send SMS asking the students to change their passwords.

**Why phishing website?**

Most students use the automated website to change their password and don’t change it manually through the Students Affairs Coordinator (מזכירות המחלקה).

**The front-end of the application**

The front-end is built to resemble the actual website as similarly as possible, this way we can fool the student/staff member without raising suspicion. The user gets logged in to our website (even if actual login details are incorrect), and gives the user the opportunity to change their password. After this, the user receives an error message saying passwords do not match and redirects them to the actual website to change the password. This way we reduce the user’s suspicion.

**The back-end of the application**

We used an SMTP server, and a CRON job to run a PHP script, which send mails every 24 hours.  
MariaDB for persistency, PHP to store data, connect to the database and define the logic of the application.­­

Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Extracting Data**

**Step zero:**

Gathering the phone numbers:

Taking the numbers from WhatsApp group.

A screenshot of a computer

Description automatically generated

Saving the element in txt file. By running the Python script, it parses it and takes out the numbers from it. You need to select the wanted groups, and it will send an SMS message automatically. User friendly graphical interface to help the SMSs.

To run the GUI script run this command:

> A screenshot of a cell phone

Description automatically generatedpython sendingSMS.py

SMS screenshot

**A close up of a logo

Description automatically generated**

“FREE SMS DEMO..”, because of trial account

GUI

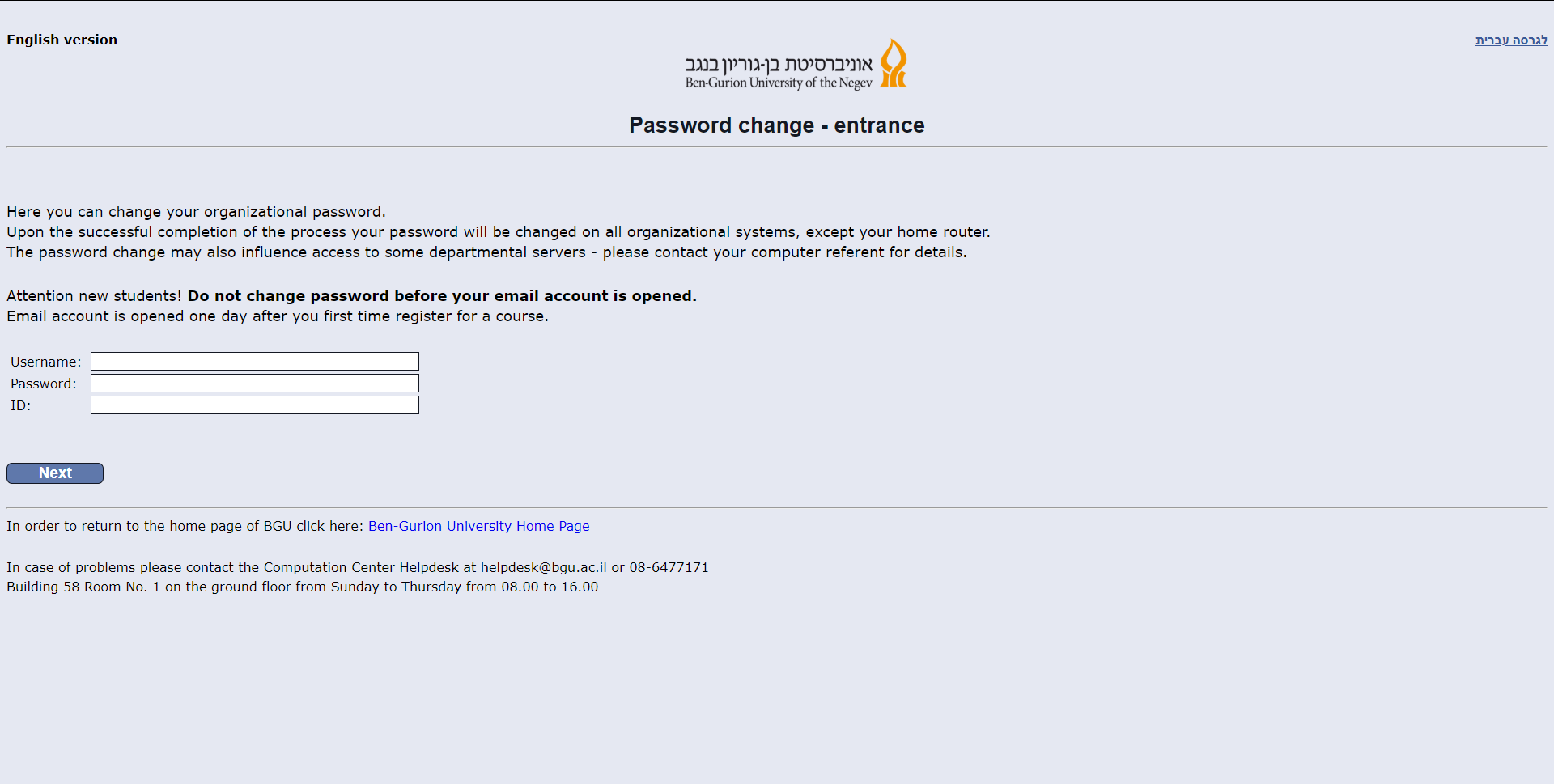
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

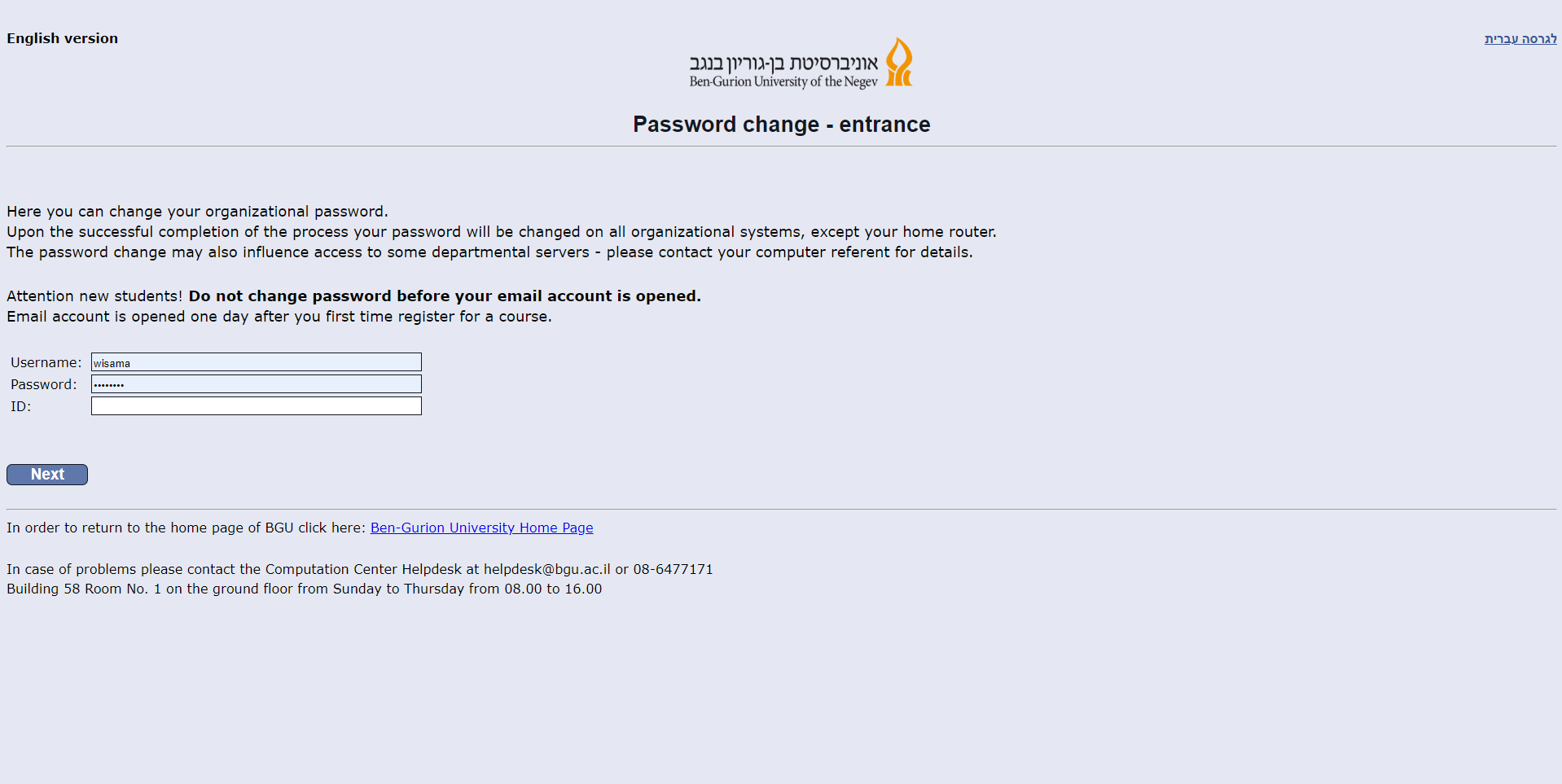
Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**English Phishing site vs English Original site**

**Step one:**

Phishing:



Original: 

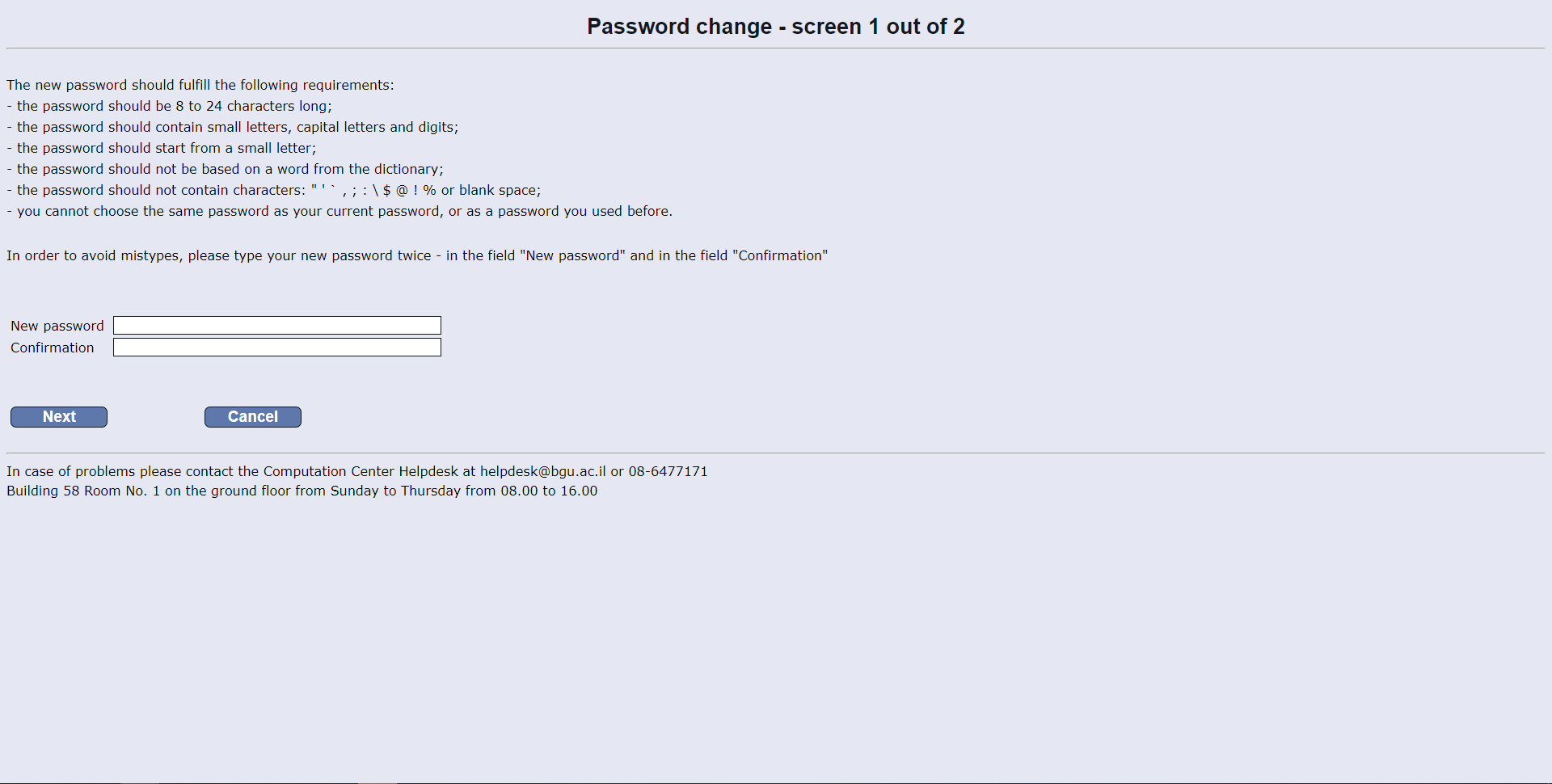
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

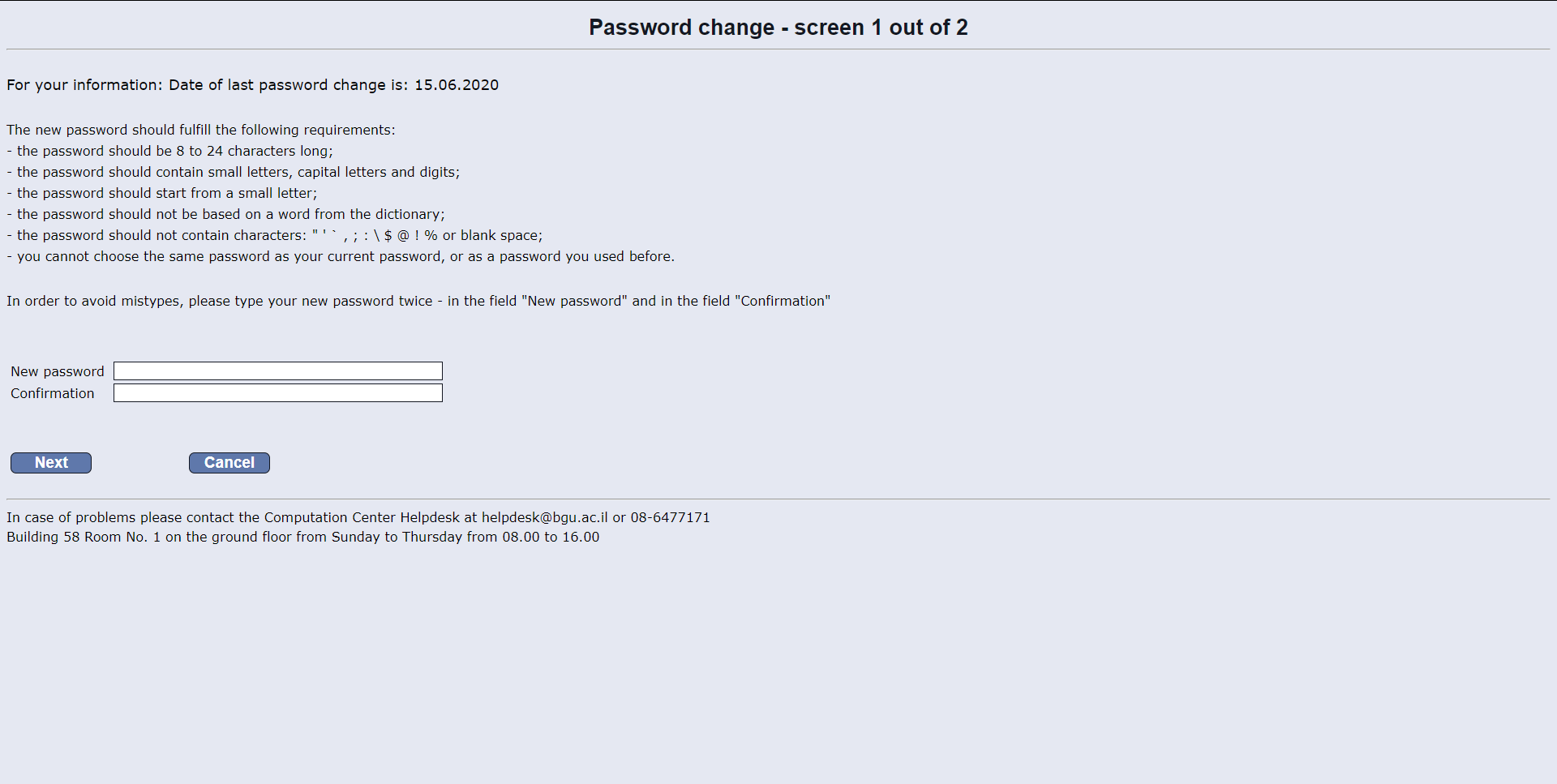
Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**English Phishing site vs English Original site**

**Step two:**

Phishing:



Original: 

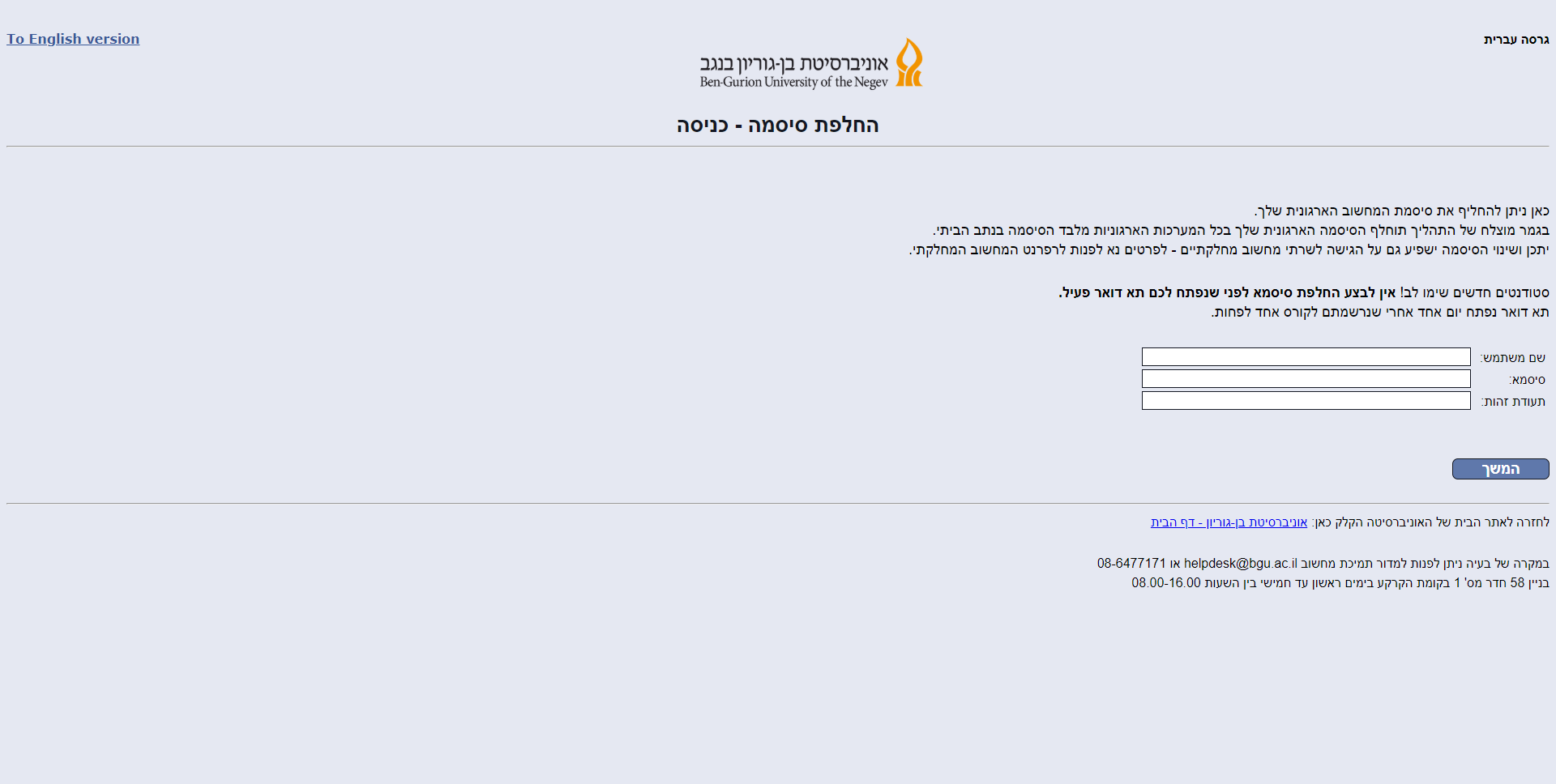
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

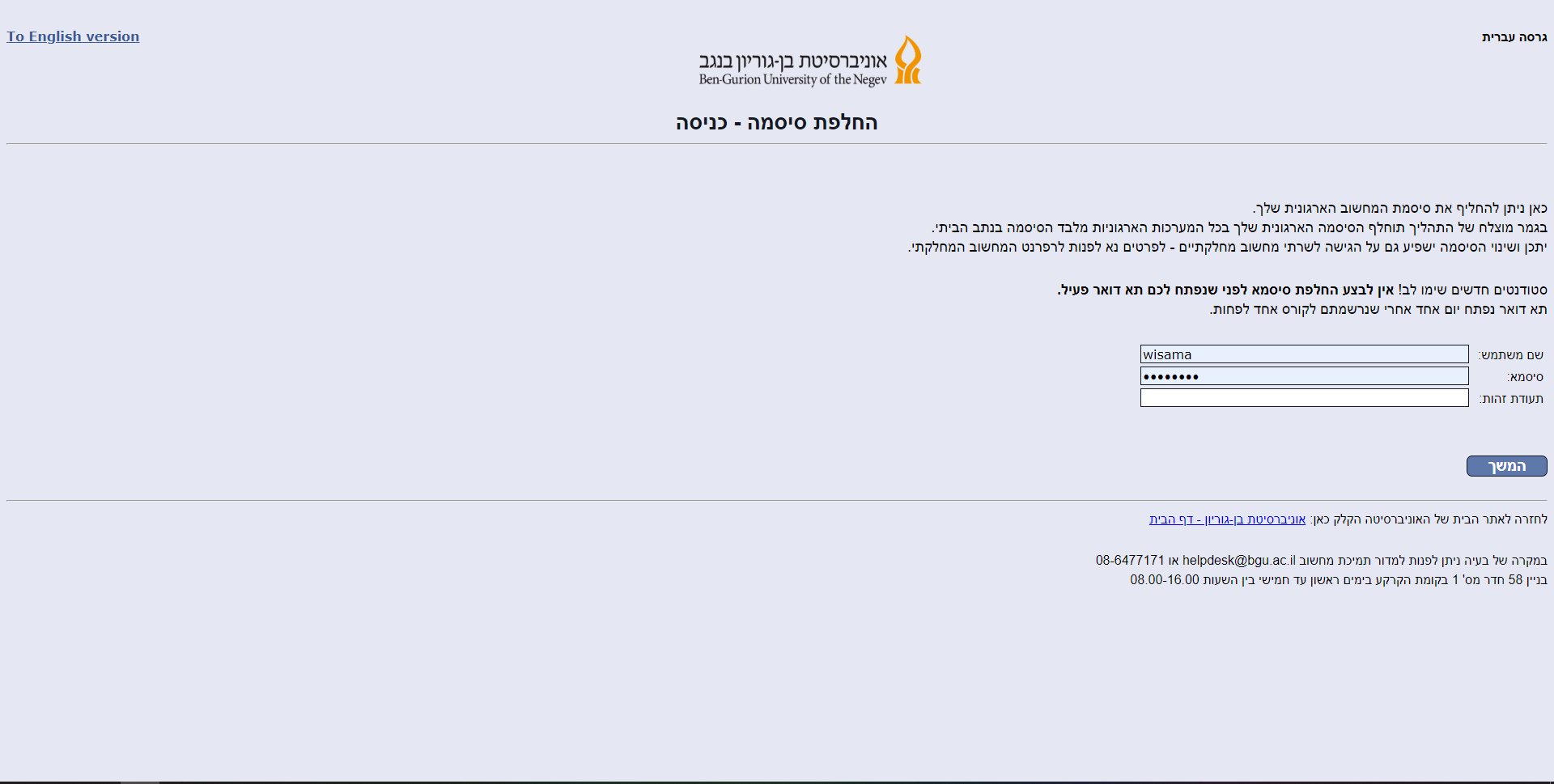
Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Hebrew Phishing site vs Hebrew Original site**

**Step one:**

Phishing:



Original: 

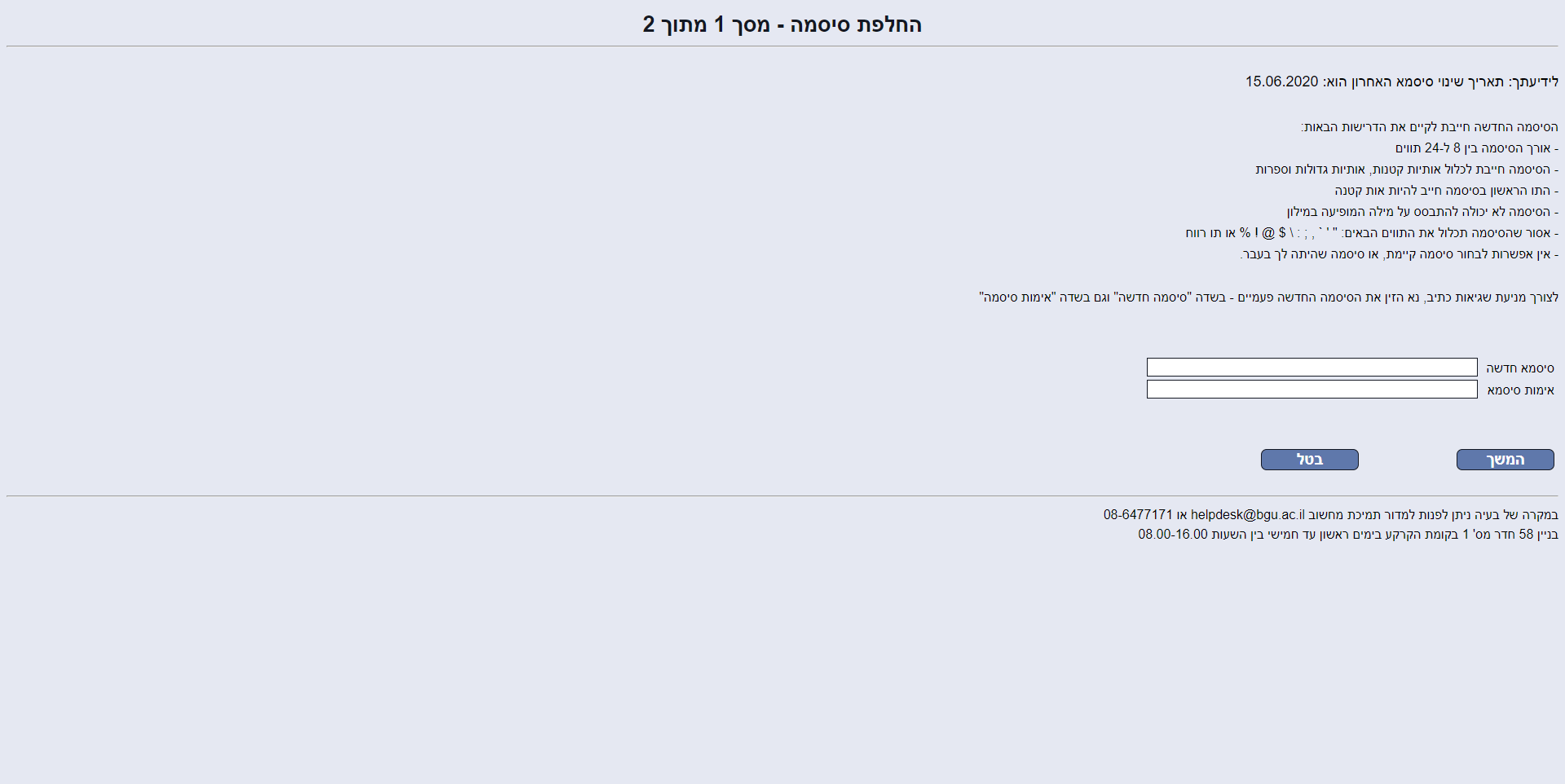
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

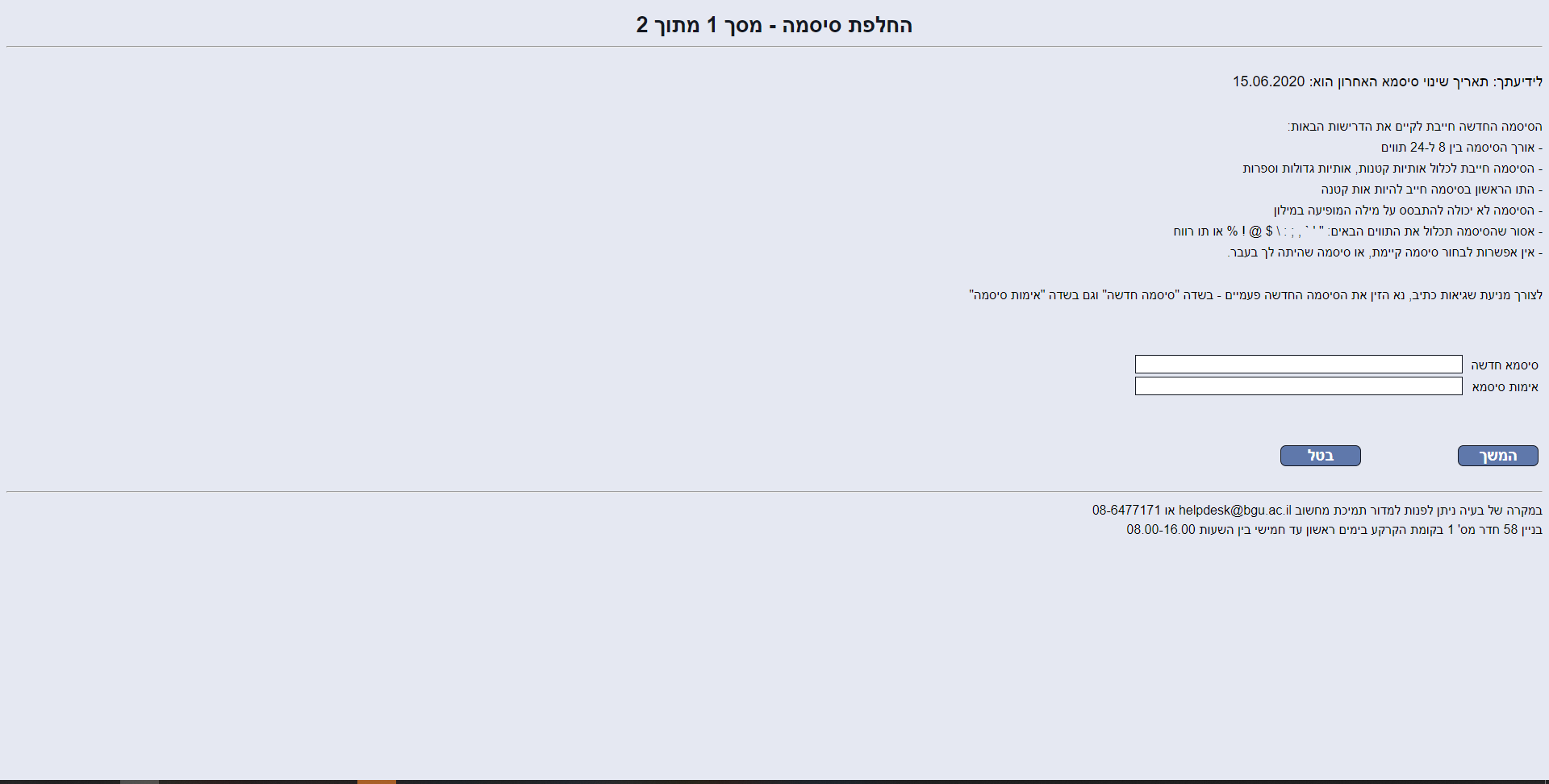
Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Hebrew Phishing site vs Hebrew Original site**

**Step two:**

Phishing:



Original: 

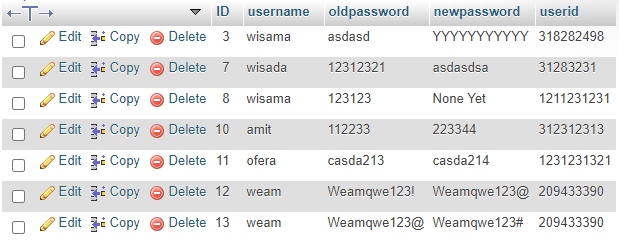
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

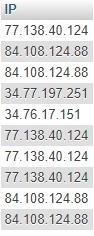
**Database**

**The data we store in the database:**

**The user’s password:**



**The user’s IP:**



Mini - Project on Network Security – 2020/Spring – Course number: 20214481

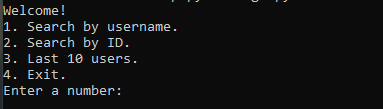
Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Database**

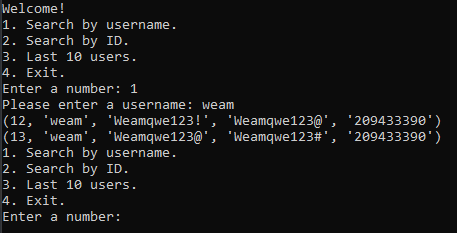
**Python script “bgu.py”:**

The script helps search the data inside the database in an easy manner:

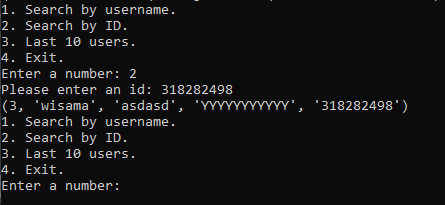
Main menu:



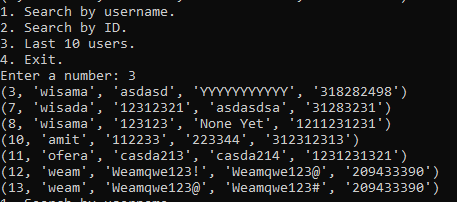
1. Search by username:



1. Search by ID:



1. Last 10 users:



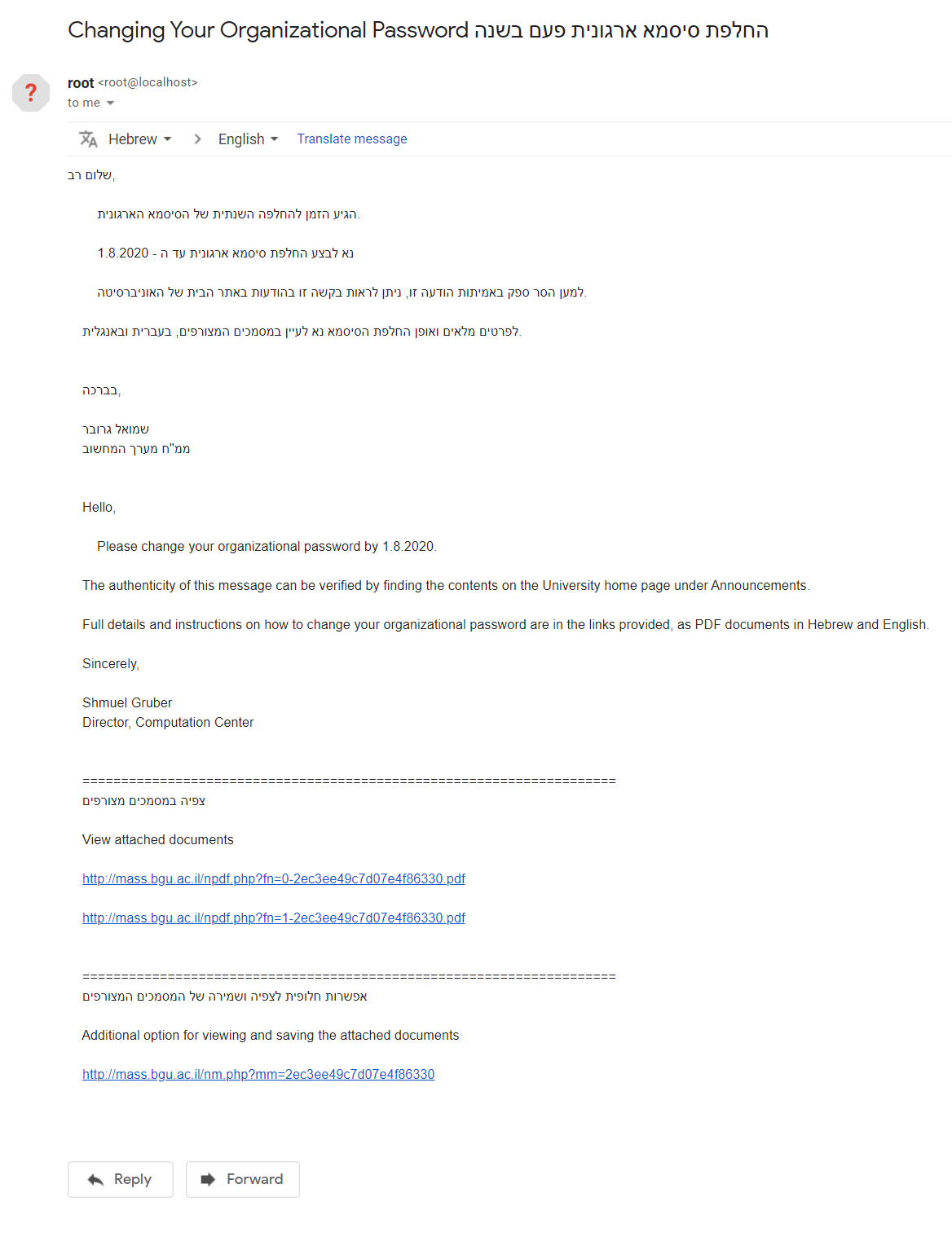
Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Installation and setup**

**Email received by the user:**





Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Installation and setup**

**Domain:**

We can purchase a domain which is very similar to that of the university’s actual domain, but we have opted not to do this, as this project is intended for educational purposes only, and we do not intend to use it in the future.

**Link to english site (phishing):**

The link to the first step:

<http://45.9.188.236/elogin.php>

**Link to hebrew site (phishing):**

The link to the first step:

<http://45.9.188.236/hlogin.php>

Mini - Project on Network Security – 2020/Spring – Course number: 20214481

Wisam Armaly – 318282498, Weam Hanosh – 209433390, Ibrahim Omari – 308451632

**Installation and setup**

**CRON JOB:**

Generate random username <user> and send the phishing email to <user>@post.bgu.ac.il.

The email is as follows:

Subject: החלפת סיסמא ארגונית פעם בשנה Changing Your Organizational Password

Body:

שלום רב,

הגיע הזמן להחלפה השנתית של הסיסמא הארגונית.

נא לבצע החלפת סיסמא ארגונית עד ה - 1.8.2020

למען הסר ספק באמיתות הודעה זו, ניתן לראות בקשה זו בהודעות באתר הבית של האוניברסיטה.

לפרטים מלאים ואופן החלפת הסיסמא נא לעיין במסמכים המצורפים, בעברית ובאנגלית.

בברכה,

שמואל גרובר

ממ"ח מערך המחשוב

Hello,

Please change your organizational password by 1.8.2020.

The authenticity of this message can be verified by finding the contents on the University  
 home page under Announcements.

Full details and instructions on how to change your organizational password are in the links  
 provided, as PDF documents in Hebrew and English.

Sincerely,

Shmuel Gruber

Director, Computation Center

=====================================================================

צפיה במסמכים מצורפים

View attached documents

http://mass.bgu.ac.il/npdf.php?fn=0-2ec3ee49c7d07e4f86330.pdf

http://mass.bgu.ac.il/npdf.php?fn=1-2ec3ee49c7d07e4f86330.pdf

=====================================================================

אפשרות חלופית לצפיה ושמירה של המסמכים המצורפים

Additional option for viewing and saving the attached documents

http://mass.bgu.ac.il/nm.php?mm=2ec3ee49c7d07e4f86330

 **אוניברסיטת בן-גוריון בנגב**

**טופס הצהרה על מקוריות עבודה**

**בקורס:**  נושאים באבטחת רשתות

הכנת עבודה נועדה לאפשר לסטודנט ליישם את הידע והמיומנות שרכש עד אז.

בעבודה צריכים לבוא לכדי ביטוי כישוריו האקדמיים, בין היתר: יכולת קריאה והבנה של טקסטים מדעיים, אינטגרציה של סוגי ידע שונים, חשיבה ביקורתית, כושר תכנון מחקר וביצועו ולבסוף, כתיבה מדעית רהוטה.

העבודה חייבת להיות ברובה המכריע **יצירה מקורית** של הסטודנט. כדי להבחין בין תרומתו לבין תרומותיהם של אחרים, וכדי למנוע פגיעה ב"קניין הרוחני" של כותבים שעליהם מסתמכת העבודה, חייב הכותב להקפיד על ציון המקורות שעליהם הסתמך. במילים אחרות, יש להצהיר מה המקור של כל אמירה או ידע שנלקח מאחרים. בכלל זה: ציטוטים ישירים של אמירות או ממצאים, רעיונות, דעות, ופרשנויות של אנשים אחרים. סטייה מכללי הציטוט, לא כל שכן נטילה ללא ציון ראוי של חלקי עבודה או עבודה שלמה של כותב אחר, מתפרשת לחומרה כניסיון להציג דברי אחרים כדברי הכותב עצמו והיא בבחינת עברה חמורה על כללי האתיקה המדעית.

**כדי למנוע אי הבנה בנדון אנו מבקשים ממך לחתום על ההצהרה הבאה:**

אני ויסאם ארמלי ת.ז. 318282498 מצהיר :

אני ויאם הנוש ת.ז. 209433390 מצהיר :

אני אברהים עומרי ת.ז. 308451632 מצהיר :

1. העבודה המצורפת בזאת היא פרי יצירתי המקורית ונכתבה על-פי \*כללי הציטוט המקובלים באקדמיה. כמו כן, אני מצהיר כי ידוע לי שהגשת עבודה אשר חלקים רבים ו/או משמעותיים ו/או מהותיים בה הועתקו מעבודה אחרת היא עבירה וכי אם יתגלה כי עברתי עברה זו, תוגש נגדי תלונה על כך לוועדת המשמעת של האוניברסיטה.
2. עבודה זו (או חלקים ממנה) לא הוגשה כמטלה בקורס אחר במסגרת לימודי.

תאריך: 18/07/2020 חתימה:

ויסאם ארמלי, ויאם הנוש, אברהים עומרי

**:כללי הציטוט נמצאים באתר המזכירות האקדמית בכתובת\* http://in.bgu.ac.il/acadsec/DocLib2/plagiarism\_heb**