שלום חברים,

זהו תיאור מערכת אבטחת המידע של תוכנת הארכיון. אני יוצא למילואים ועל כן מפרסם זאת עכשיו למרות שלא השלמתי את כל הבדיקות...

בקצרה, מנגנון אבטחת המידע של המערכת מתבסס על 2 הנחות יסוד:
1. לכל משתמש יש תיבת דואר פרטית וכתובת הדוא"ל היא שם המשתמש במערכת הארכיון שלנו
2. לכל משתמש יש טלפון נייד, חכם אשר מסוגל להריץ את תוכנת Google Authenticator.

תוכנת Google Authenticator היא תוכנה אשר מקבלת מחרוזת תווים אשר מהווה סוד-פרטי (בעולם ההצפנה: Secret) המוכר רק לאדם, למערכת בר-כוכבא ול- Google Authenticator, ומאפשרת לחולל ממנו פעם ב- 30 שניות קוד זיהוי בן 6 ספרות אשר יהיה אוטומטית מוכר (במהלך 30 השניות הללו) גם לשרת התוכנה של בר כוכבא.

סוד זה הוא אוסף תווים מאוד ארוך שאין שום סיכוי לבן תמותה רגיל לזכור אותו. הוא מופק ע"י מערכת בר-כובכא (מכאן שהיא כבר מכירה אותו), ונשלח במייל בצורת QRCode אל כתובת המייל הרשומה של המשתמש.

גם סוד זה הוא בן-חלוף. אם המשתמש לא ינצל אותו במהלך 10 דקות מאז שהוא נוצר, הוא יימחק מהמערכת, ובפעם הבאה יחולל מחדש קוד חדש.

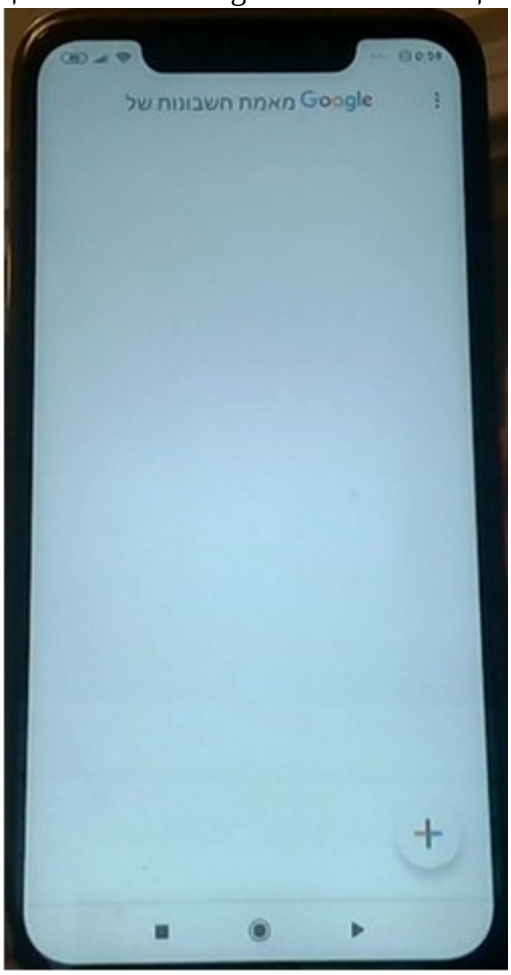
כאשר המשתמש מקבל במייל את ה- QRCode הוא סורק אותו באמצעות תוכנת Google Authenticator ובכך מושלם המעגל: הן שרת בר-כוכבא והן תוכנת ה- Google Authenticator מכירים את הסוד המשוייך לכתובת המייל של המשתמש.

מעתה והלאה – המשתמש יכול להזדהות למערכת בצורה קלה, ע"י הזנת כתובת הדוא"ל והקוד-המתחלף בן 6 הספרות שמוסרת לו תוכנת Google Authenticator. אם יזין קוד ישן מדי – המערכת לא תקבל את ההזדהות, ויהיה עליו להקיש קוד חדש בן 6 ספרות...

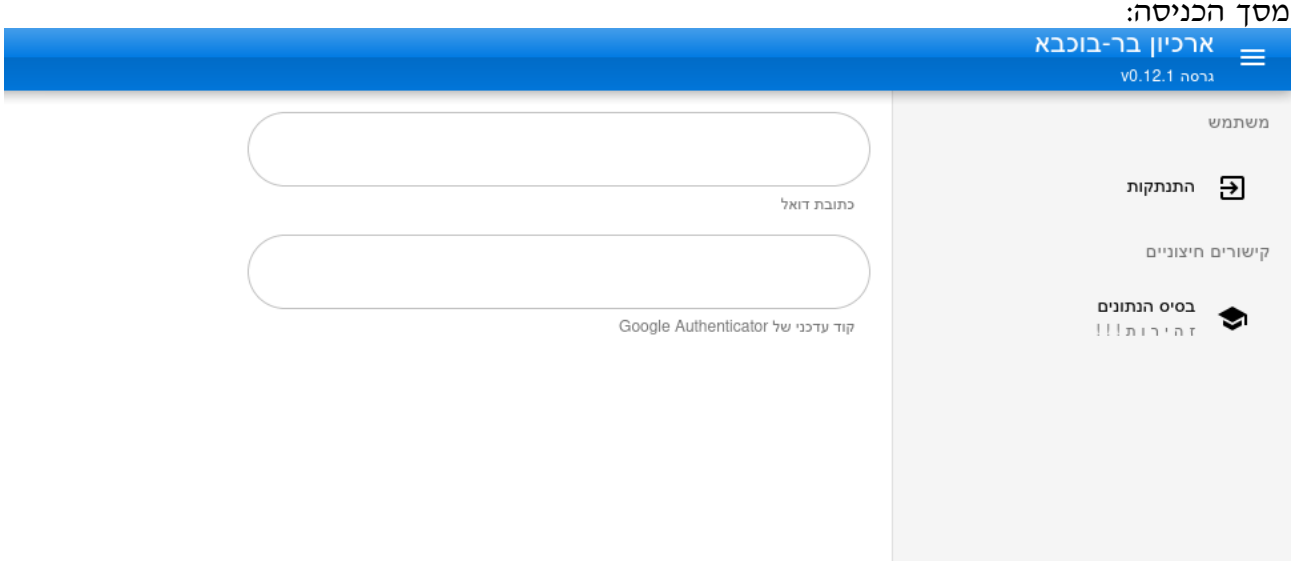
מעתה, המחשב של האדם מזוהה במערכת למשך 6 שעות, והמערכת לא תטריד אותו בהזדהות מחודשת..

מצ"ב מספר צילומי מסך אשר מדגימים את העבודה עם המערכת. מכיוון שתוכנת Google Authenticator לא מאפשרת צילומי מסך מתוך הטלפון הנייד – איכות צילום המסכים שלה תהיה לא ממש טובה... מצטער...

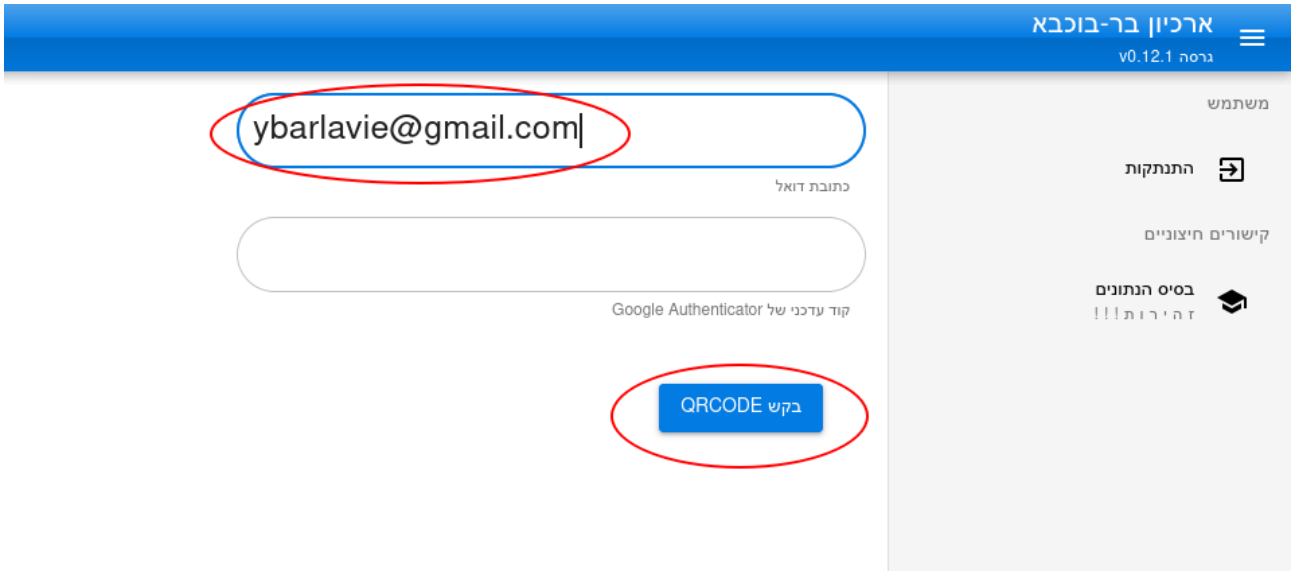
מסך Google Authenticator לאחר ההתקנה ולפני ייבוא קוד מערכת בר כוכבא:



מסך הכניסה:

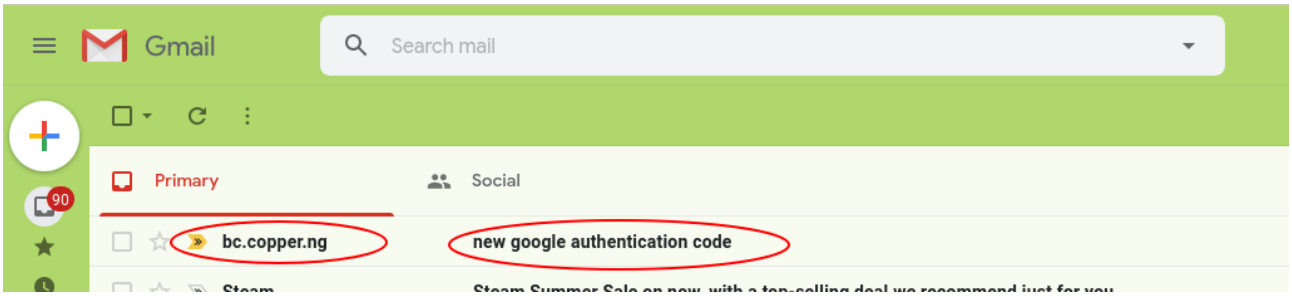


לקבלת Qrcode

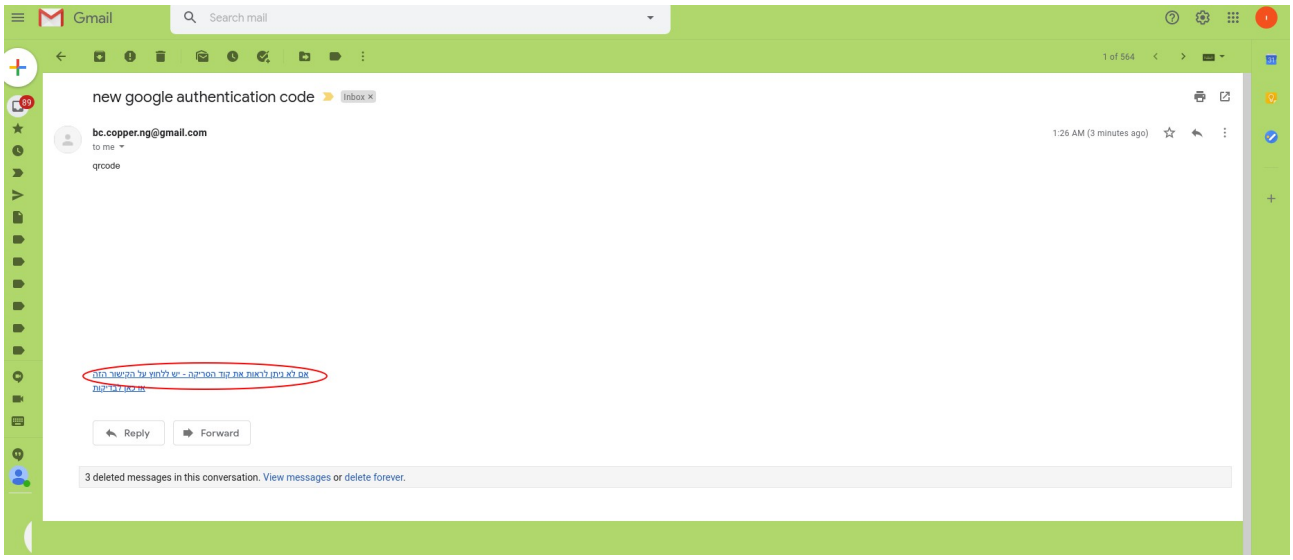


אם המשתמש (כתובת הדוא"ל) מוכר למערכת תתקבל הודעה בתחתית המסך:

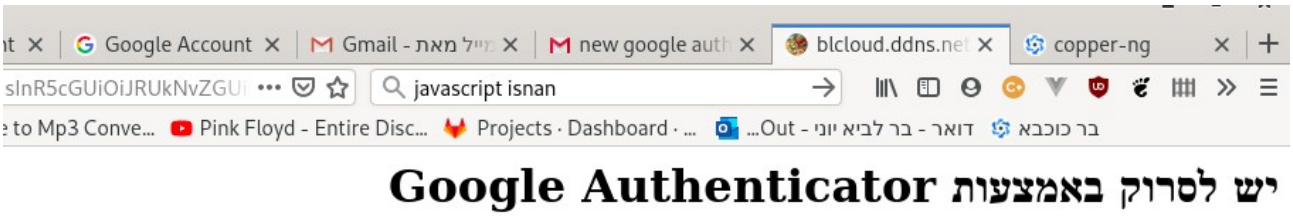
עכשיו יש 10 דקות לקבל את הקוד. הולכים לתיבת הדואר ובודקים:



לעיתים gmail לא מסכים להציג את הקוד, ולכן יש קישור להצגתו:

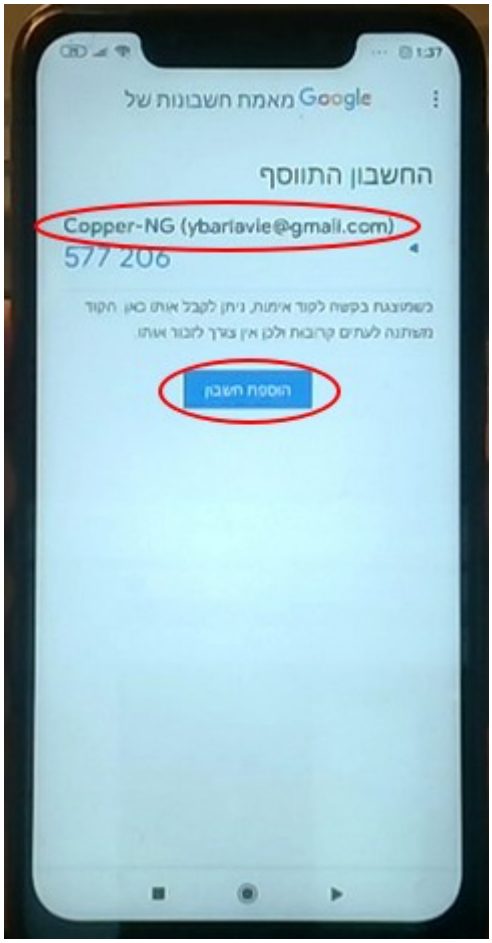


לוחצים על הקישור ו... (כמובן שטשטשתי כדי לא להסגיר את הקוד שלי...)

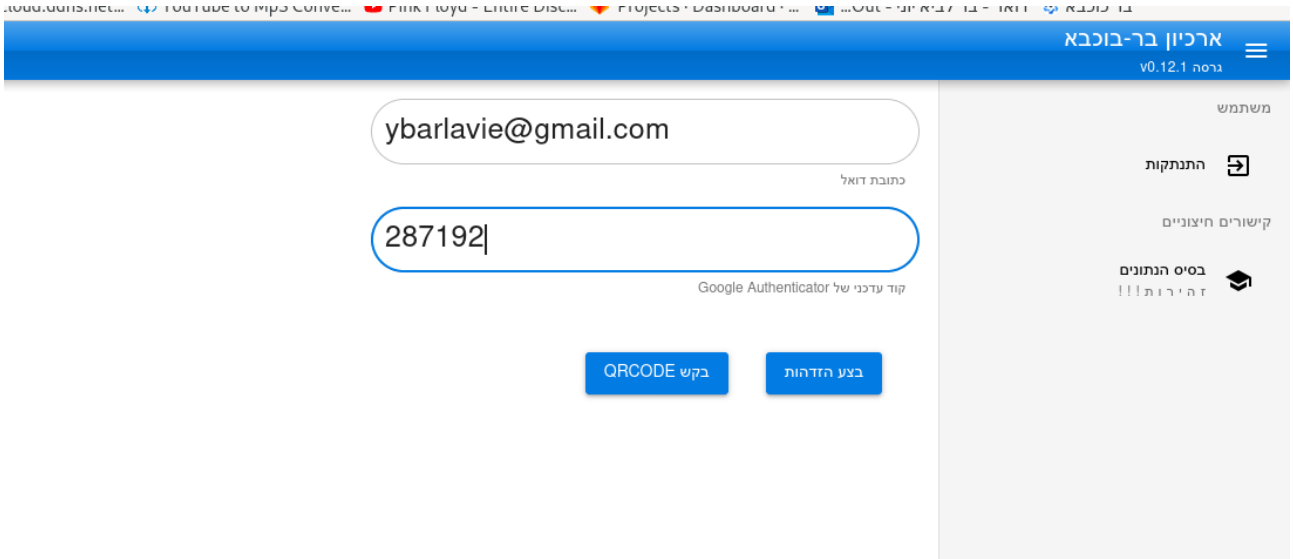


יש לסרוק באמצעות Google Authenticator

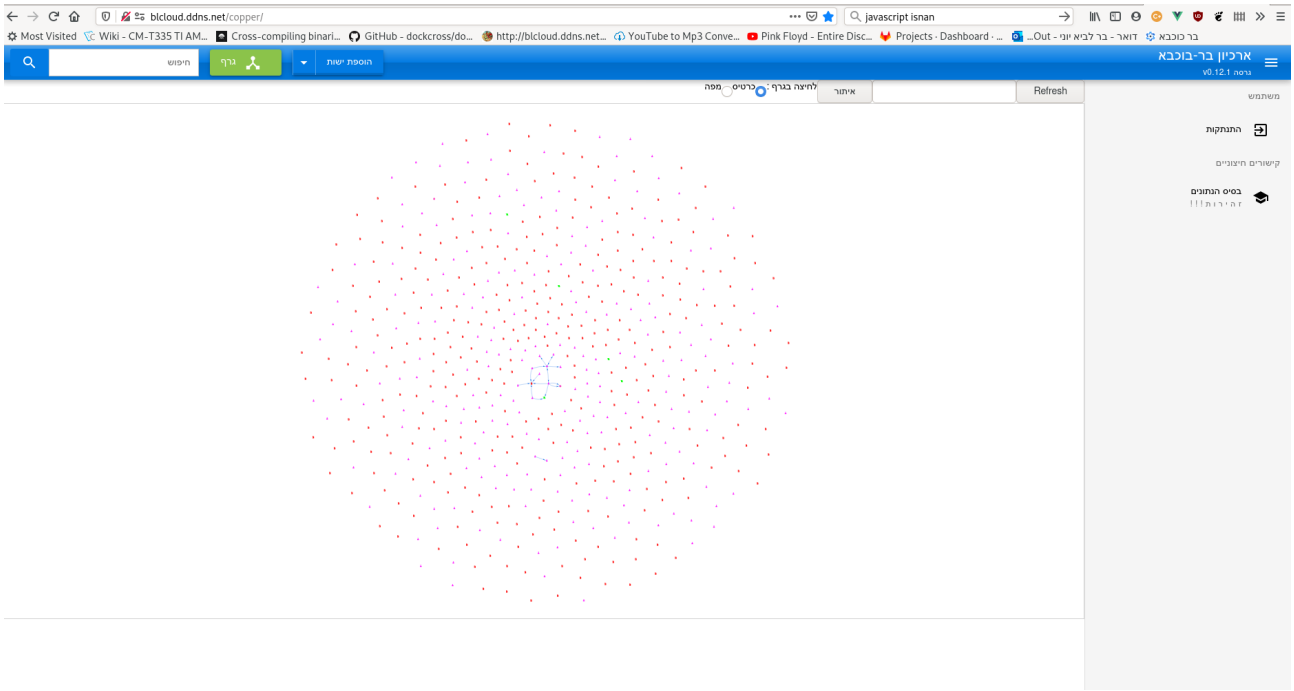
עכשיו סורקים את זה עם Google Authenticator בטלפון הנייד:



...לא שוכחים ללחוץ על "הוספת חשבון", ו... זהו. ה- Google Authenticator מוכן לעבודה. כל 30 שניות הוא מייצר קוד מספרי חדש אשר אורך חייו הוא 30 שניות, ויש להקיש אותו (בזמן) בחלון ההזדהות וללחוץ על "בצע הזדהות":



הצלחה!:



ועכשיו הכי חשוב !!! למחוק את הדוא"ל שהגיע מהמערכת. הוא מכיל קוד רגיש שלא כדאי שייפול לידיים הלא נכונות. למרות שאורך חייו הוא רק 10 דקות, עדיין, אנשי הצפנה טובים יכולים לפרוץ את שם המשתמש בעבודה קשה תוך שבוע-שבועיים...