שימו לב

המלחמה מתקיימת גם בגזרת הסייבר ויש נסיונות תקיפה מסוגים שונים, כולל משלוח מייל זדוני ופוגעני.

חשוב ביותר להעלות דריכות ולהיזהר בכל מייל מתקבל. מערכות ההגנה של הטכניון בכלל ובמייל בפרט פועלות אך אף מערכת אינה מספקת הגנה מוחלטת של 100%.

1. זהירות רבה נדרשת במיוחד במייל הכולל קבצים מצורפים או קישורים. מייל כזה עלול להתקבל גם ממישהו שאתם מכירים ( יתכן ומדובר בתיבה המאוד דומה בשמה או במקרה בו תיבת השולח נפרצה) וכמובן משולחים לא מוכרים.
2. יתכנו גם מיילים הכוללים תוכן פוגעני, כפי שהתקבל במהלך השבת אצל משתמים שונים בטכניון. מייל כזה שיש בו רק טקסט לא ייחסם על ידי מערכות ההגנה ברוב המקרים.
3. מערכות ההגנה על מייל מודיעות בחלק מהמקרים למשתמש על חסימה שבוצעה ואפשרות לשחרר את המייל. אנו ממליצים להימנע משחרור מלבד מקרים בהם המשתמש משוכנע ב 100% בחסימה שגויה. בכל מקרה של ספק אנא היוועצו במהנדסי המחשוב ביחידה.

כל מייל חשוד או דיווח בנושא מייל, חשוב להעביר במיידי לכתובת הבאה: [postmaster@technion.ac.il](mailto:postmaster@technion.ac.il)

המייל ייבדוק ע"י הצוות ובמידת הצורך יינקטו פעולות נדרשות

בברכה

אבטחת מידע

אגף המחשוב ומערכות מידע

הטכניון

Attention

The war is also taking place in the cyber front and there are various types of attack attempts, including malicious and offensive e-mails.

It is extremely important to raise vigilance and be careful with every email received. The Technion's protection systems in general and email protection in particular work well, but no system provides 100% absolute protection.

1. Great care is required especially with an email that includes attachments or links. Such an email may also be received from someone you know (it may be a mail box with a very similar name or in a case where the sender's box was hacked) and of course from unknown senders.

2. There may also be emails that include offensive content, as was received during the Shabbat for users at the Technion. Such an email that contains only text will not be blocked by the protection systems in most cases.

3. In some cases, email protection systems notify the user of a block that has been made and the option to release the email. We recommend avoiding release except in cases where the user is 100% convinced of a wrong blocking. In case of doubt, please consult the computer engineers in the unit.

In cases of suspicious email or reports about an email, it is important to forward it immediately to the following address: [postmaster@technion.ac.il](mailto:postmaster@technion.ac.il)

The email will be checked by the team and, if needed, necessary actions will be taken

Best regards

Cyber Security

Computing and Information Systems Division

Technion