

אגף מחשוב ומערכות מידע

מודעות לאבטחת מידע

7-6-2022

משה גליקשטיין
ממונה אבטחת המידע
CISO@Technion.ac.il



אחוז ניכר מהתקפות על ארגונים מתחיל בהתקפת פישניג

- גניבת שמות משתמש/סיסמאות (MFA בהחלט עוזר)
- הדבקת מחשבים (EDR יעיל בכ 90% בלבד)

יותר מדי משתמשים הקישו על הקישור = הדבקה!

כ 50% המשיכו והזינו את הסיסמא = גניבת סיסמא!

מעריב < מבזקי חדשות

חדשות מתפרצות

שלושה סטודנטים במוסד אקדמי מאיזור המרכז נעצרו בחשד לביצוע עבירות סייבר

שלושה סטודנטים בגילאי ה-20 הלומדים במכללה טכנולוגית באזור המרכז, נעצרו הבוקר בחשד לביצוע עבירות מחשב. על פי החשד, השלושה שלחו הודעת דיון ("פשינג") למרצים במכללה. לאחר שחלקם לחצו על הקישור שדרש מהם לאפס את סיסמתם, קיבלו החשודים גישה למערכת הדואר האלקטרוני ומערכת הלימוד הממוחשבת של המכללה. לאחר שנחקרו באזהרה במחלק לפשיעה מקוונת של משטרת מחוז תל אביב, שוחררו השלושה בתנאים מגבילים.

אלון חכמון 17:38 06/06/2022

שתפו:     

MAY 31, 2022 | STATESCOOP •

Officials in Portland, Oregon, said last week that the city recently lost \$1.4 million to fraudulent activity when a malicious actor gained access to a government email account. •

The city's Office of Management and Finance said Friday that the "fraudulent financial transaction" occurred in late April, but was only detected May 17 when the same account attempted another transfer of funds. While officials have said little else about the incident, they said it appears to stem from an email scam. •

"Preliminary evidence indicates that an unauthorized, outside entity gained access to a City of Portland email account to conduct this illegal activity," [a press release reads](#). •

The city said the incident is under investigation by the FBI, U.S. Secret Service and the Portland Police Bureau. •

MAY 27, 2022 | EDSCOOP •

• Network logins and VPN credentials from numerous U.S. colleges and universities are widely available for sale on cybercriminal forums operating out of Russia, according to an FBI alert issued Thursday. [The alert](#) warned that a “multitude” of U.S. schools were featured on these sites as of January, with malicious actors selling directories of stolen credentials for hundreds or thousands of dollars. Harvesting VPN credentials and other login information is often a byproduct of ransomware, spearphishing or another attacks, the FBI said, laying the groundwork for identity theft or future cyberattacks.

The FBI alert reminds colleges and universities to take several familiar protective steps, including ensuring that operating systems and other software is updated, implementing multi-factor authentication on as many services as possible, especially VPNs, and requiring strong passwords.

אבטחת מידע

תרגיל פישניג – סימני הזיהוי

האגף למחשוב
ולמערכות מידע



From: Technion <[redacted]>
Sent: Thursday, April 14, 2022 5:54 AM
To:
Subject: [redacted]

No-Reply@technion.co.il



המחשבים הישנים

במסגרת מדיניות הביטחון, עליך להחליף את סיסמאות הסיסמה.

המחשבים יישארו בלתי פתוחים עד אשר תחליף את סיסמתך.

המחשבים יישארו בלתי פתוחים 24 שעות לאחר מכן. כדי לפתוח את החשבון, עליך לפנות ל-CISO.

[Click here to change password](#)

Dear User,

As part of Technion Security policy, you're required to change your password periodically.

Since your password has not been updated in this period, please update your password as soon as possible.

Users that will not update their password will be locked in the next 24 hours, in order to unlock the account, the user will need to contact the CISO.

24 hours

Kind Regards, Security Team, Technion.



External e-mail, be judicious when opening attachments or links



היו זהירים במיוחד בטלפון חכם
כתובת השולח מוצגת באופן מקוצר
תירוצים:

- תזמון לפני חופשה
- קשה להבחין בדקויות כאשר קוראים
100 מיילים ביום
- מוזמנים לפנות לתוקפים בבקשת הקלות 😊

Technion

> גליקשטיין משה: To:
8:46

מדיניות החלפת
סיסמאות בארגון

הורריו

מה בתכנית

- מטרת ההדרכה
- סיכונים פוטנציאליים
- כללי התגוננות בעבודה
- כללי התגוננות בבית
- דיווח על פרצות

כללי

- אבטחת מידע – סודיות, שלמות וזמינות של הנתונים
- Confidentiality Integrity Availability – CIA
- להגן על הנתונים הקיימים במערכות המחשב בטכניון
 - נתונים אישיים
 - שכר
 - ציונים
 - מחקרים

- להגן על זמינות מערכות המחשוב
- להקפיד על שימוש חוקי במערכות המחשוב
 - התקפה מתוך הטכניון
 - הורדה ושימוש בחומרים המוגנים בזכויות יוצרים

אנחנו המשתמשים
חוליה קריטית
באבטחת המידע
המטרה היא להקטין
את הסיכונים

מה מטרת אבטחת המידע

- 1- לדאוג שהסיסמאות יהיו עם לפחות 10 תווים?
- 2 – לדאוג לזמינות, סודיות ושלמות הנתונים?
- 3 - להגן מפני כל הסכנות למערכות המידע?
- 4 – לודא שלכל חדר וארון יש מנעול?

מה מטרת אבטחת המידע

- 1- לדאוג שהסיסמאות יהיו עם לפחות 8 תווים
 - 2 – לדאוג לזמינות,סודיות ושלמות הנתונים
 - 3 - להגן מפני כל הסכנות למערכות המידע
 - 4 – לודא שלכל חדר וארון יש מנעול
- תשובה 2 כמובן (3 בלתי אפשרי)

מה מטרת אבטחת המידע

- הטכניון מחוייב על פי חוקי מדינת ישראל לשמירה על נתוני הפרט
- אבטחת מידע זה טכנולוגיה והתנהגות המשתמשים
 - לטכנולוגיה דואגים באגף המחשוב וכן ביחידות השונות (המנעול בכניסה לבית)
 - המשתמשים צריכים להיות מודעים לסכנות ולהתנהג בהתאם (לזכור לנעול את המנעול ולשמור על המפתח)
- אבטחת המידע חזקה - כחוזק החוליה החלשה ביותר
- מספיק משתמש אחד לא זהיר כדי לפגוע באבטחת המידע של הכלל

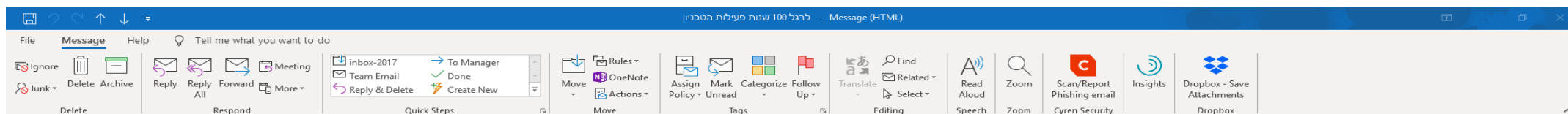
סיכונים פוטנציאליים במייל

- מייל טכניוני ואתרים טכניוניים תמיד מסתיימים ב – TECHNION.AC.IL
- לא COM לא NET לא CO.IL
- לא TEHNION ולא TECHNION
- קיבלת מייל מהטכניון- וודא כי הסיומת נכונה
- אזהרה בדבר קבלת מייל מבחוץ – WARNING: This email is from an external mail server, Please be careful when opening attachments or links.
- אם תוכן המייל חשוד (??) – נסה להתקשר, שתף נאמן אבטחת מידע/מהנדס מחשוב/CISO
- היזהרו מכל המאיצים בכם. דחוף! בהול! תוך 24 שעות!
- Better Safe Than Sorry
- בקשות להזדהות באתרים – שם משתמש וסיסמא, וודא את כתובת האתר, לוגו טכניון בלבד לא מספיק

סיכונים פוטנציאליים במייל

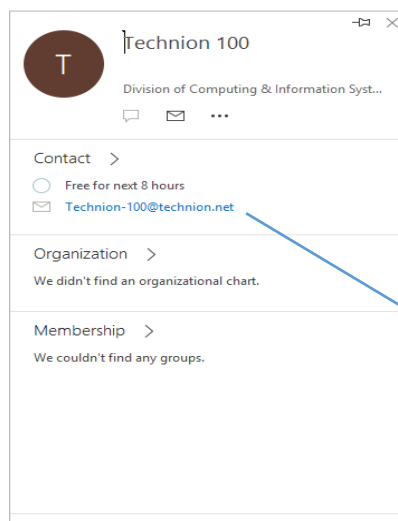
- דוגמא להתחזות לדיקן- מייל הדיקן מפורסם באתר הפקולטה
- המייל נשלח מ – Dean****@technion.ac.il
• במקרה זה התוקף למד פרטים חשובים דרך אתר הפקולטה
- דוגמא להתחזות לבעל תפקיד בכיר- USER@Technion-ac.com
• במקרה זה אחד המשתמשים נפל קרבן לפישינג וסיסמתו דלפה/נגנבה
- הדרך היעילה ביותר להקשות על התוקף היא שימוש בהזדהות חזקה 2F/MFA .
- בנוסף לסיסמא הסטאטית, המערכת תדרוש קוד חד פעמי נוסף שמיוצר בטלפון החכם. גם אם הסיסמא נגנבת התוקף לא יכול להיכנס למערכת ללא הטלפון החכם.
- ניתן לסמן למערכת לסמוך על מחשב ספציפי, למשל במשרד או בבית למשך 30 יום.

סיכונים פוטנציאליים במייל



לרגל 100 שנות פעילות הטכניון

Mail Campaign
To: בליקשטיין חשה
You replied to this message on 01/03/2020 15:19.



Technion-100@Technion.net

CIS-CYBER-DISTRIBUTION-L@LISTSERV.TECHNION.AC.IL

<On Behalf Of Technion-100@technion.net

Reply Reply All Forward
יום א 01/03/2020 15:17

שלום רב לעובדי הטכניון רבתי
לציון 100 שנות פעילות הטכניון מציע: משכורת נוספת ל-100 מעובדי
בצעד חסר תקדים לציון 100 שנות פעילות מציע הטכניון לעובדיו משכורת חודשית נוספת (משכורת שלוש עשרה).
חמישים עובדים מבין כלל הנרשמים יוגרלו לקבלת ההטבה, בעוד חמישים העובדים הראשונים שירשמו יקבלו אוטומטית את ההטבה ללא הגרלה.
הטכניון רואה בעובדיו נכס יקר ערך ומהותי לתפקודו של המוסד והוותיק והמוביל בארץ, שממנו יצאו מחקרים פורצי דרך רבים ואף שלושה פרסי נובל בעשרות האחרונים.
פרטים נוספים ורישום [בקישור זה](#)

ההשתתפות אסורה על חברי הנהלה וראשי יחידות

מנהלת חגיגות ה-100



שקר
15

<http://cis.technion.ac.il>

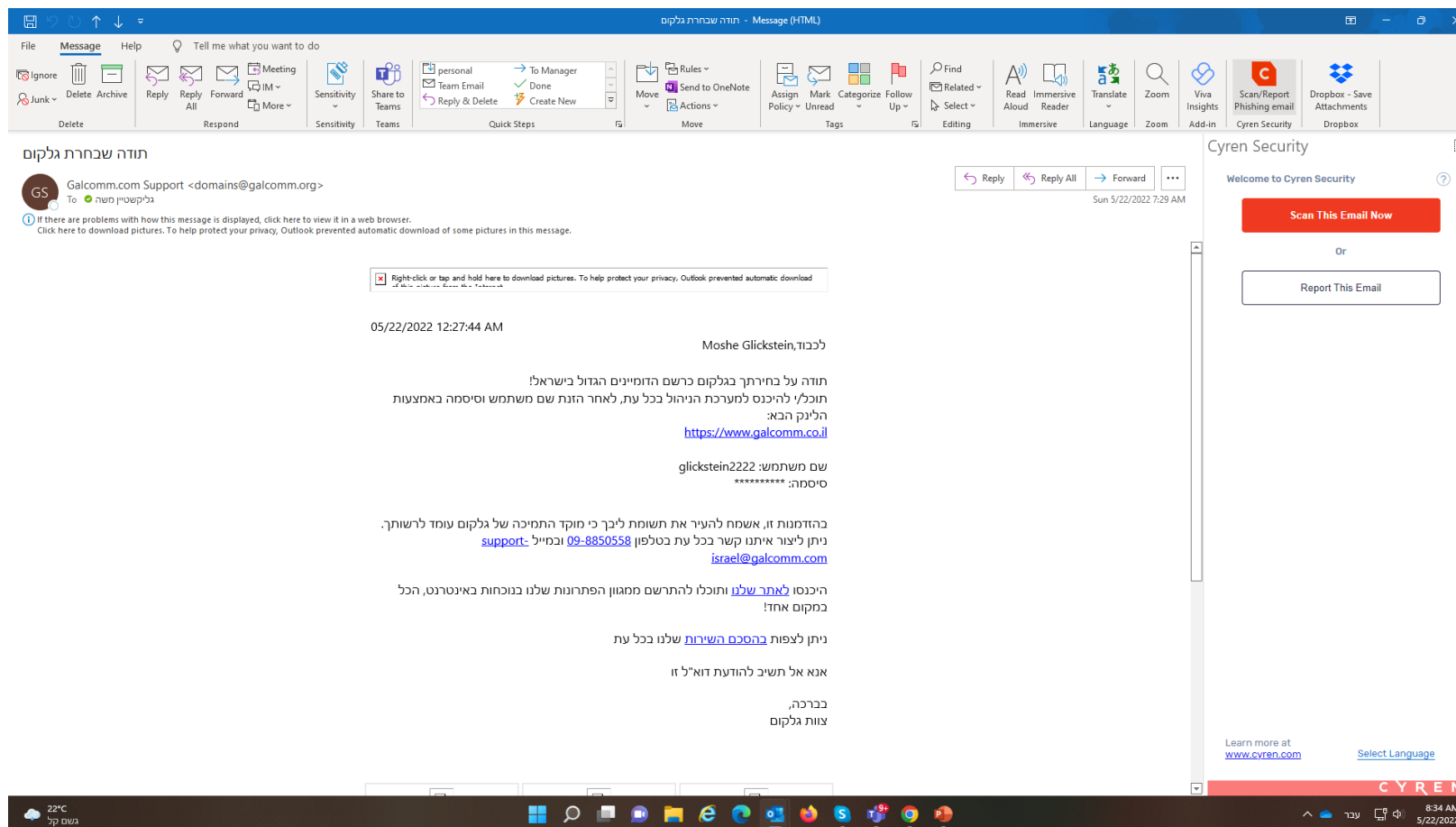
אגף מחשוב ומערכות מידע



מה עושים? ובעיקר מה לא עושים

- לעולם אל תמסור סיסמתך במייל
- אל תענה למייל שנראה חשוד
- אל תגיב ואל תלחץ על קישורים במייל או מסך חשודים
- אל תפתח צרופות במיילים חשודים
- השתמש בכפתור CYREN (בצבע אדום) לבדיקת חשד - Cyren
- תמחק את המייל החשוד או העבירו לנאמן אבטחת המידע ביחידה או לממונה אבטחת המידע הטכניוני.
- דווח על כל חשד, עדיפה אזעקת שוא מהתעלמות

CYREN



שקר
17

<http://cis.technion.ac.il>

אגף מחשוב ומערכות מידע



סיכונים פוטנציאליים

- דוגמא לשילוב של טכנולוגיה והתנהגות (צילומי מסך בהמשך)

- Social Engineering

- אמנות המניפולציה וההונאה של אנשים, כדי להשיג גישה למידע לצרכים לא חוקיים

- התקפות Social Engineering נפוצות ובעלות סיכוי הצלחה גבוה מהתקפות טכנולוגיות

- מתבסס על החולשות האנושיות של כולנו

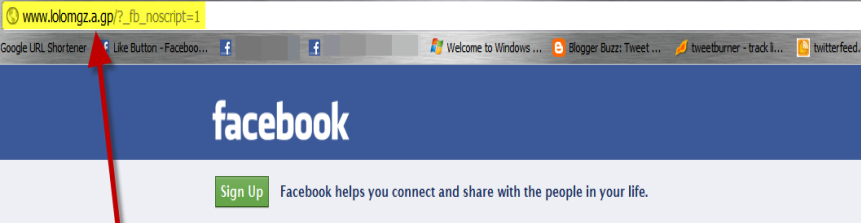
- Spear Phishing

- זה מייל המתקבל כביכול מאדם או חברה המוכרים לכם, אך נשלח ע"י גורם עוין.

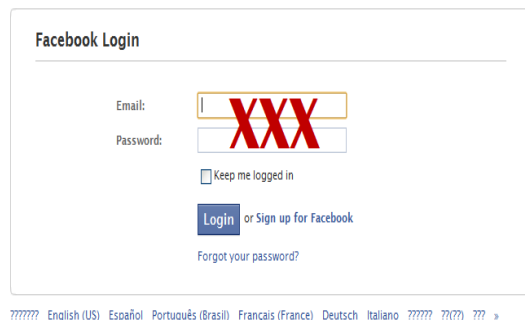
- מתבצע לאחר לימוד מעמיק של האדם המותקף, דרך רשתות חברתיות, פרסומים וכיו"ב

סיכונים פוטנציאליים

- איך לזהות סכנות?
 - הופעת דברים משונים על המסך
 - הודעות מוזרות
 - שגיאות מערכת
 - גרפיקה משונה
 - חוסר יכולת להשתמש במשאבים
 - תוכנות
 - קבצים
 - דיסקים
 - התנהגות לא רגילה של תוכנות
 - תוכנה שעובדת לאט מהרגיל, לא רצה כלל או לוקח לה הרבה זמן להתחיל לעבוד



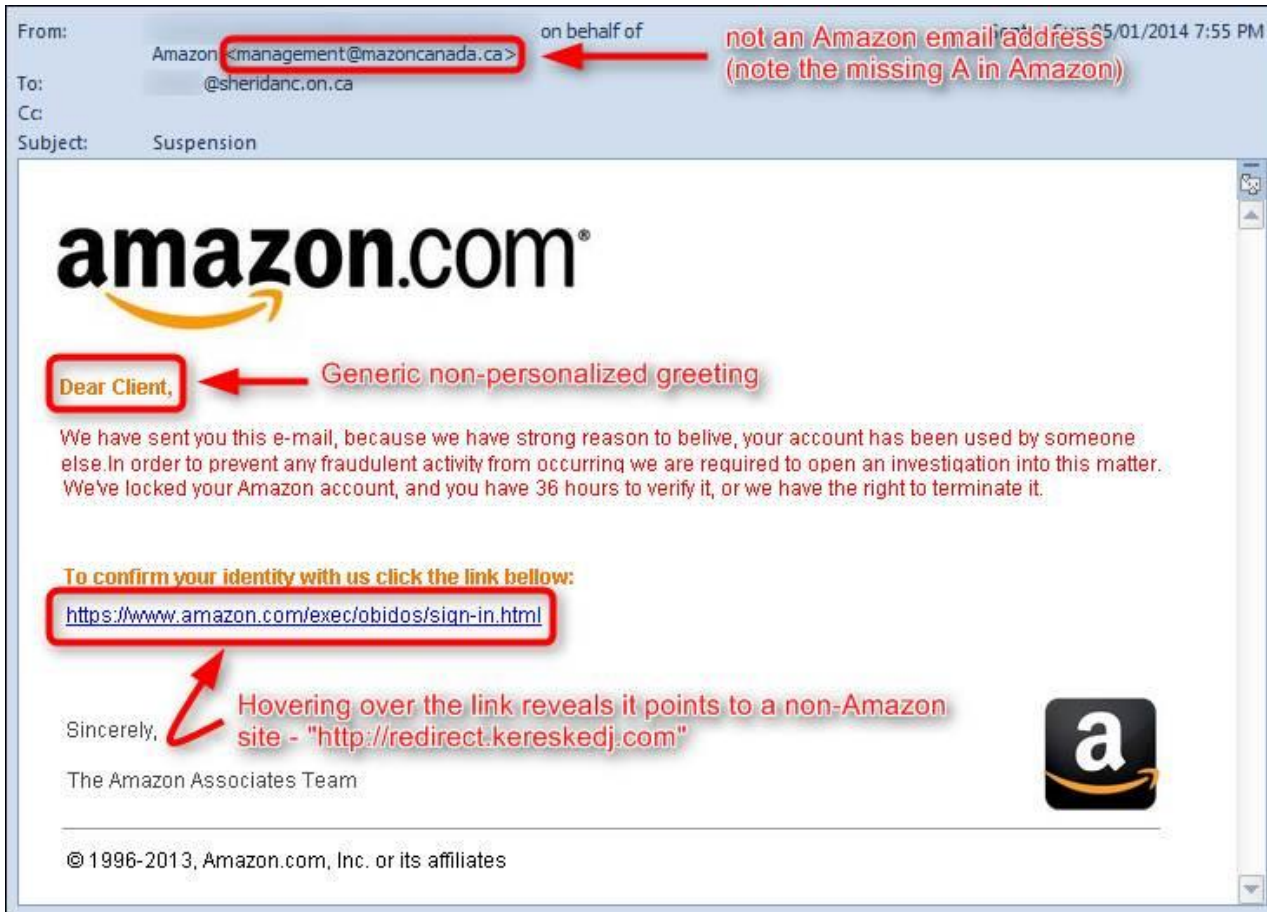
This is a Phishing Scam. This web site looks like Facebook.com, but if you note the web address in the the browsers address bar you can clearly see this is not Facebook.



סיכונים פוטנציאליים

- איך לזהות סכנות בגלישה (דפדפן) ?
- ריבוי חלונות קופצים Pop-up
- אתר מוכר- פועל אחרת או לא פועל
- התראות מרובות של האנטיוירוס או ה FIREWALL
- בקשה להוספת תוספים לדפדפן – רק אם מבינים מה עושים
- Phishing – נסיון להציג דף זדוני שנראה כמו דף אמיתי
- עוד דוגמאות בדף הבא
- המלצה מיידית: לסגור POPUP ע"י לחיצה על X ולא שום כפתור אחר

סיכונים פוטנציאליים





Dear valued PayPal® member:

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records on or before **August 30, 2006**.

Once you have updated your account records, you will be interrupted and will continue as normal.

To update your PayPal® records click on the following link:
<http://www.paypal.com/cgi-bin/webscr?cmd=p/upgrade>

Thank You.
PayPal® UPDATE TEAM

Accounts Management As outlined in our User Agreement we periodically send you information about site changes.

Visit our Privacy Policy and User Agreement if you need help:
<http://www.paypal.com/cgi-bin/webscr?cmd=p/privacy>

דוגמאות ל Phishing

From: Rahn-Lawler, Deana <Deana.Rahn-Lawler@henry.k> Sent: Thu 11/17/2011 8:30 AM
To: undisclosed-recipients
Cc:
Subject: Email Security

You have exceeded the storage limit on your mailbox.

please Copy/click the below link and fill the upgrade form.

<http://system-administratoroffice01.tk/> <<http://system-administratoroffice01.tk/>>

System Administrator
192.168.0.1

Disclaimer For Henry County Schools

"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you received this message in error, please contact the sender and delete the material from all computers."

This original email was sent to the internet for delivery at 17 Nov 2011 18:27:39 +0500

Phishing

source: Untitled

OmniWeb Help The Omni Group Apple Mac OS X Omni Products Yahoo! spamweb SpamCop DNS Stuff IronPort Threat Operations Center RFCs Wiki-SPF Times xword Telegraph xword Google Forced matrix BS

eBay eBay sent this message to buriliss pierce (lroc92). Your registered name is included to show this message originated from eBay. [Learn more.](#)

Question about Item -- Respond Now

eBay sent this message on behalf of an eBay member through My Messages. Responses sent using email will go to the eBay member directly and will include your email address.

Question from trlbch
[trlbch \(2377\)](#) ★
Positive feedback: 99.7%
Member since: Jun-14-09
Location: CT, United States
Registered on: www.ebay.com

Item: DELL Inspiron 9400 E1705 DUO 1.83 1GB 100GB GO 7800 256 (250001996470)
This message was sent while the listing was active.
trlbch is a **potential buyer**.

Hello, Did you sell the laptop or someone has put a fraudulent listing? If you are still seller tell me the buy it now price. Thank you

Respond to this question
Respond Now
Responses in My Messages will not include your email address.

Marketplace Safety Tip
Always remember to complete your transactions on eBay - it's the safer way to trade.
Is this message an offer to buy your item directly through email without winning the item on eBay? If so, please help make the eBay marketplace safer by reporting it to us. These "outside of eBay" transactions may be unsafe and are against eBay policy. [Learn more about trading safely.](#)

Is this email inappropriate? Does it violate eBay policy? Help protect the Community by [reporting it.](#)

Details for item number: 250001996470
Item title: DELL Inspiron 9400 E1705 DUO 1.83 1GB 100GB GO 7800 256
Item URL: http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=250001996470&sspage_name=ADME:B:AAQ:US:1
End date: Tuesday, Jun 27, 2006 06:57:14 PDT

Go to: <http://www.signin-ebay-com-very.land.ru/eBay.html>

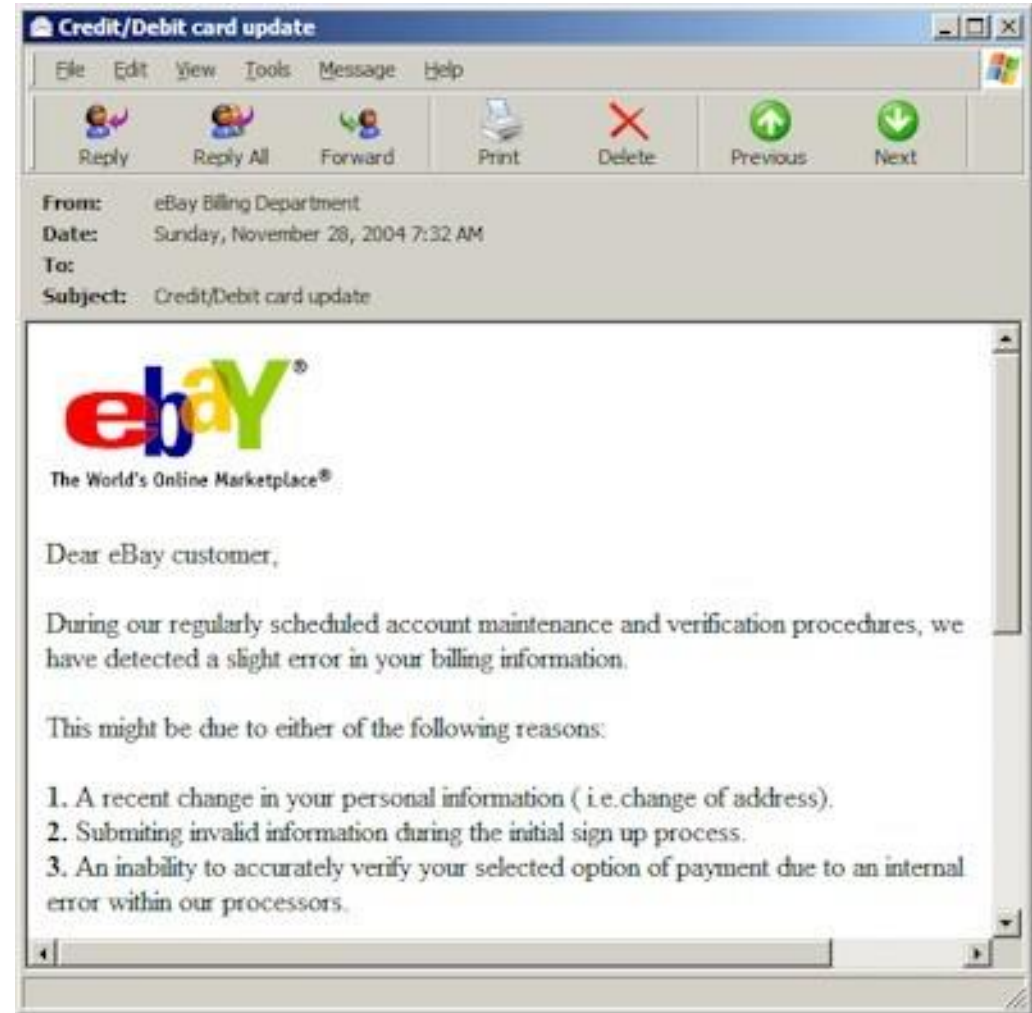
דוגמאות ל Phishing

חפשו את המנעול, את HTTPS ואת השם המדויק של האתר



שקר
23

<http://cis.technion.ac.il>



אגף מחשוב ומערכות מידע



סיכונים פוטנציאליים

- מה זה מייל PHISHING ?
 - 1. סוג של התקפה המשלבת social engineering
 - 2. עלול להיראות כמגיע מחברה או אדם מוכרים
 - 3. מכיל קישורים לאתר המבקש להזין פרטים אישיים
 - 4. כל התשובות נכונות

• RANSOMWARE כופר

- **תוכנה זדונית** המונעת שימוש בקבצים במחשב האישי ע"י הצפנה חזקה. נסיון לפרוץ את ההצפנה עלול להסתיים בשיבוש הקבצים. התוקף דורש תשלום ע"י ביטקוין הקשה למעקב.
- לא תמיד התשלום מבטיח פענוח הקבצים
- גובה התשלום תלוי בקורבן – התוקף לומד על הקורבן והקבצים טרם המתקפה
- היום ניתן לרכוש שירות התקפה של RANSOMWARE ברשת DARK WEB (יפורט)
- לעיתים יצרני ה AV מציעים פתרונות למתקפות מאוד ספציפיות
- **Ransomware** is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some **ransomware** encrypts files (called Cryptolocker).

מה עושים?

- לעולם אל תמסור סיסמתך במייל
- אל תענה למייל שנראה חשוד
- אל תגיב ואל תלחץ על קישורים במייל או מסך חשודים
- אל תפתח צרופות במיילים חשודים
- תמחק את המייל החשוד או העבירו לנאמן אבטחת המידע ביחידה או לממונה אבטחת המידע הטכניוני.
- דווח על כל חשד, עדיפה אזעקת שוא מהתעלמות
- CYREN

מה עושים - המשך?

- מה עושים כאשר יש חשד לבעיה
 - לסגור את כל הקבצים והיישומים
 - לא ללחוץ על שום בחירה על המסך, גם לא בחירה שאומרת "לא"
 - לנתק את המחשב מהרשת (עדיף מאשר לכבות)
 - לדווח למהנדס המחשוב היחידתי או ממונה אבטחת המידע
 - CISO@Technion.ac.il

סיכונים פוטנציאליים

- משתמשים עם זכויות גישה
- למשתמשים רבים יש זכויות גישה נרחבות ואף יכולת לשנות קונפיגורציה של שרתים והרשת
- אם התחנה של המשתמש לא מוגנת פיזית בהעדרו* – הפורץ מנצל את הזכויות שיש למשתמש האמיתי
- *גם אם מדובר בהעדרות לשירותים, להביא חומר מהמדפסת או לקפוץ לחמם אוכל במטבחון – ובאמצע מתפתחת שיחה או שקולגה מחדר אחר מעכב את המשתמש ללא כוונות זדון

סיכונים פוטנציאליים

• Social Engineering

- פנייה באמצעות הטלפון או המייל כדי להערים על המשתמש ולדלות ממנו מידע רגיש כמו סיסמאות, מספרי אשראי וכ"ד
- איך מזהים
 - הצד השני לא נותן פרטי התקשרות
 - זירוז בתואנות שונות
 - נסיון להפחדה – זה דחוף כי תאבד מידע, תאבד כסף וכיו"ב
 - שגיאות (כתיב, שמות, שאלות מוזרות)
 - בקשה למידע רגיש או חסוי
- מה עושים
 - נזהרים
 - מודאים זהות הצד השני
 - לא מגלים מידע רגיש או חסוי

איך מתגוננים

- איזו סיסמא יותר בטוחה?

- 1. linda12

- 2. 123Abc

- 3. Big_Apple!

- 4. B&H17Plu\$3428

- כמובן 4 - אותיות קטנות וגדולות, מספרים וסימנים מיוחדים

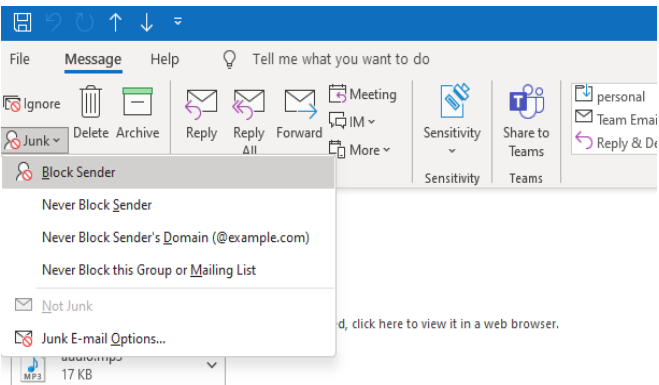
- מסוגלים לזכור? 😊

- &2023wecpvmI

איך מתגוננים

• על המשתמש

- לא לפתוח צרופות או להיכנס לקישורים במייל חשוד.
- בגלישה לודא באיזה אתר גולשים, במקום לינקים עדיף לכתוב את הכתובת או להשתמש בסימניות (Bookmarks)
- להסתכל היטב על הכתובת של האתר או שולח המייל
- לא תקבלו מייל מחברה המשתמשת בGOOGLE או YAHOO או WALLA
- שם האתר עלול להכיל שגיאות כתיב, החלפת אותיות וכ"ד
- לגרוס תדפיסים ולהשמיד דיסקים שאינם בשימוש
- לא להשאיר מחשב נייד, דיסק נייד, דיסק USB ללא השגחה
- להפעיל שומר מסך ביציאה מהחדר
- לא להעביר מכתבי שרשרת – רובם נגועים
- להיזהר בהשלמה אוטומטית של כתובות נמענים!!



איך מתגוננים

• מייל

- לא לפתוח SPAM ולא לענות ל SPAM ולא לבקש הסרה מרשימת תפוצה של SPAM*
- פתחת מייל ויש לך חשד – לא לפתוח צרופה, לא להיכנס לקישורים, למחוק או לקרוא למהנדס היחידה או ממונה אבטחת המידע
- אחוז גבוה של התעבורה באינטרנט זה SPAM שרובו נחסם בטכניון
- תמיד לודא את שם הנמען לפני משלוח – כבר קרו מיקרים לא נעימים ויותר מכך.
- למידע מסווג בקשו הפעלת הצפנה ממהנדס היחידה

• גלישה

- לא לגלוש באתרים מפוקפקים, בטח לא מהטכניון ולא ממחשב ביתי ממנו נכנסים למערכות הטכניון.
- לא להוריד קבצים ללא הבחנה
- לא לגלוש לאתרים אחרים במקביל לחיבור מול מערכות הטכניון מרחוק
- להפסיק הורדה של קובץ אם לא ביקשתם הורדה
- לא לבצע עדכונים מאתר המציע לעדכן או להתקין – לבקש ממהנדס היחידה אם יש צורך



איך מתגוננים

- עבודה מחוץ למשרד
- תמיד לשמור על המחשב הנייד או הטלפון החכם
- להתחבר רק דרך ה VPN הטכניוני, לא להתחבר דרך חיבורים פיראטיים
- הפעל גישה עם סיסמא לדיסק USB
- במקרה של אבדן/גניבת המחשב או ה USB לדווח מייד

איך מתגוננים

- גלישה המשך
- מתחנות ציבוריות (בתי קפה, מלון וכיו"ב) להקפיד
 - לא לשמור סיסמא בתחנה
 - להתנתק בסוף העבודה
 - לסגור את החלונות בסוף העבודה
 - לכבות המחשב בסוף העבודה
 - יתכן וצופים בכם
 - הניחו שכל מה שהוקש בתחנות ציבוריות מוקלט

איך מתגוננים

- גלישה המשך

- טלפון חכם זה מחשב לכל דבר

- להגן בסיסמא כי בד"כ לרוב היישומים הכניסה אוטומטית בלי צורך להקיש סיסמא
- להתקין AV רובם חנם
- לכבות BT כשאין בו צורך
- להגן על יישומים בסיסמא כאשר אפשר
- לא לשמור שמות משתמשים טריוויאליים כמו סיסמא, טכניון, ישראל כרט וכ"ד
- לא לטעון חשמלית דרך חיבורי USB אלא חיבורי חשמל בלבד (יש הגנה)
- להוריד תוכנות רק מחנויות רשמיות
- להתקין אופציית מחיקה מרחוק WherisMyiPhone



איך מתגוננים

- מחשב ביתי, ממנו נכנסים למערכות הטכניון
- כל מה שאמרנו על המחשב במשרד תקף
- להתייחס למסמכים מודפסים בהתאם לסודיות הנתונים בהם. גריסה או החזרה לטכניון
- בעיות נפוצות
 - אנטי וירוס לא מעודכן
 - מערכת הפעלה ישנה שכבר לא נתמכת או שלא בוצע לה עדכון
 - משתמשים נוספים בבית שלא עברו הדרכה זו
 - רשת WIFI ביתית ללא סיסמא
 - אם רוצים להוריד תוכנה, לא להוריד מלינק אלא מאתר מוכר download.cnet.com או אתרי יצרן
- היעזרות בגוף מקצועי לא רק תשמור על המחשב במצב אבטחה טוב יותר, אלא תאריך את אורך חייו ותשפר ביצועים, אבל לא לאפשר לטכנאי השכונתי השטלתות לא מבוקרת על המחשב

נהלים

• בטכניון קיימים נהלים המחייבים את כלל העובדים ללא יוצא מן הכלל

• נהלי עבודה בנושא תקשוב ומידע

• דוגמאות לנהלים לאו דוקא לאנשי מיחשוב:

- נוהל עבודה עם מיקור חוץ
- נוהל טיפול במאגרי מידע
- נוהל אבטחת מידע

• באתר אגף המיחשוב קיימות הנחיות והתראות

En

האגף למחשוב
ומערכות מידע

הטכניון
מכון טכנולוגי
לישראל

דף הבית » יחידות » אבטחת מידע » הנחיות אבטחת מידע

יחידות

אבטחת מידע

הנחיות להתנהלות נכונה

הדרכות והרצאות

הנחיות אבטחת מידע

חדשות אבטחת מידע

עשרת הדיברות באבטחת מידע (pdf)

התרעות אבטחת מידע

תקשוב

מערכות ליבה

חשבוניות מיקרוסופט

פיתוח אתרים

מערכות מידע מנהליות

26/03/2019	הנחיות מערך הסייבר ל OP-ISRAEL (pdf)
14/07/2019	שאלון עבור קבלן משנה באספקת שירותים (pdf)
07/08/2019	התמודדות עם כופרה - RANSOMWARE (pdf)
04/11/2019	חשיפת כתובות דוא"ל ושימוש ב CC לעומת BCC (pdf)
06/02/2020	הגנה על חיבת דואר וטיפול במקרה של פריצה (pdf)
01/07/2020	הגדרת הודעות חזקה לחשבון משותף (pdf)
05/11/2020	הטכניון עובר להודעות חזקה - Strong Authentication
10/01/2021	הפסקת שימוש ותמיכה בגרסאות TLS ישנות
24/06/2021	הגדרות שרתי Windows-DNS ברשת הטכניון (pdf)
24/06/2021	הגדרות DNS בכרטיסי הרשת של מחשבים ברשת הטכניון (pdf)
25/07/2021	הצעות הקשחה למגוון מערכות
25/08/2021	שירותי הפצת דואר אלקטרוני (pdf)
29/08/2021	מדריך הפעלת הודעות חזקה רב-שלבית (MFA) לשירותי מיקרוסופט בטכניון
10/10/2021	אבטחת מערכות מוליטימדיה

דיווח על פריצות

- אם המחשב שלך נדבק או שמידע נעלם או שובש
 - אם קיבלת מייל מעמית שאין סיכוי שהוא שלח
 - אם ניסו או הצליחו לגנוב לך מחשב, פלט, דיסק
 - בכל מקרה של חשד
-
- דווח מייד לקצין הבטחון או לנאמן אבטחת המידע ביחידתך או לממונה אבטחת המידע הטכניוני
 - אם אינך יודע מי נאמן אבטחת המידע ביחידתך שאל מייד

ברכות

- בזאת סיימתם את ההדרכה למודעות בנושאי אבטחת מידע
- הערנות והזהירות של כולנו, קריטיים לאבטחת המידע בטכניון
- תודה רבה