For English version click here

שלום לבית הטכניון

האבטחה תמיד מוגזמת עד שאינה מספיקה " - רובי סינקלייר

זה אכן מה שרוב האנשים מרגישים. האבטחה מטילה מגבלות ומקשה על ההתנהלות ביומיום, כך שרבים לא אוהבים את זה. עם זאת, כאשר מתרחש אירוע סייבר, כולם שואלים מדוע לא היתה אבטחה חזקה יותר.

1. מחשבים ניידים

לאחרונה נגנב מחשב נייד של עובד הטכניון. המחשב נגנב יחד עם הרכב בו הושאר. אני מבקש להדגיש שחל איסור מוחלט להשאיר מחשבים ניידים, כמו גם כל חומר רגיש אחר ברכב או בכל מקום ללא השגחה. האיסור הוא מוחלט בלי קשר למשך הזמן בו המחשב מושאר ברכב. בכל מחשב ובמיוחד במחשב נייד חייבת להיות סיסמת גישה למחשב. מעבר לנזק הכספי של ערך המחשב, קיים ערך רב וסיכון רב הקשור לנתונים הקיימים על המחשב או ניתנים לגישה מהמחשב. במידה ומחשב נגנב או נאבד, חייבים **<u>בדחיפות:</u>**

א. להחליף סיסמאות
ב. להודיע לממונים, לצוות המחשוב ולקצין הבטחון.

צוות המחשוב יבצע את הפעולות הנדרשות ברמה הטכנולוגית והממונים בשיתוף עם ממונה אבטחת המידע יעריכו את הנזק הפוטנציאלי וינקטו בפעולות הנדרשות על פי תקנות הפרטיות והשלכות אחרות.

2. התקפה על בית החולים הלל יפה

אני מניח שרובנו קראנו בחדשות על פריצה זו. הנסתר עדיין רב על הגלוי. יחד עם זאת התמונה הזו ממחישה עד כמה, טעות אנוש עלולה להביא לחורבן של מערכות מחשוב' בלי קשר למערכות ההגנה המופעלות בארגון. אתם רואים בתמונה כי שם המשתמש והסיסמא הוצגו לא רק לכל העובד בפרוזדור אלא לכל מי שצפה במהדורת החדשות באותו יום. כל משתמש וכל מנהל יחידה

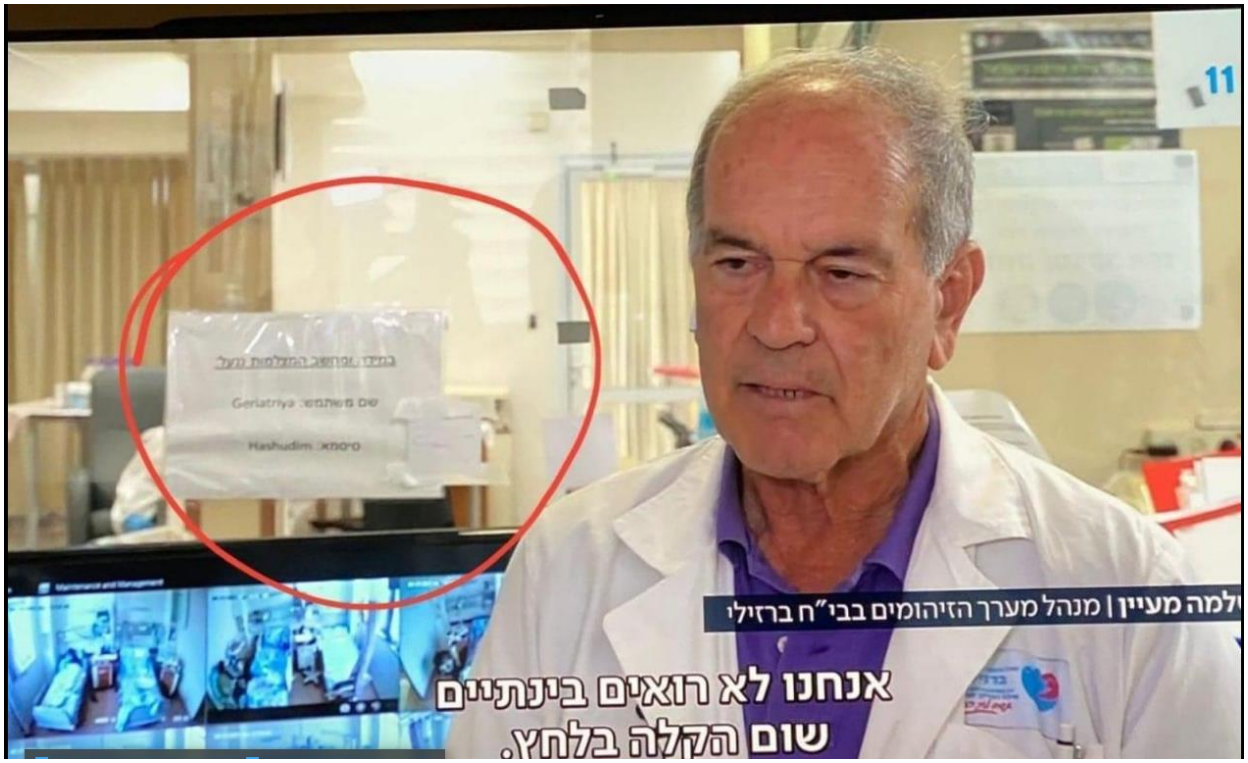
Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192

glickstein.m@technion.ac.il \ cis.technion.ac.il

חייב לשאול את עצמו אם גם הסיסמאות אצלו חשופות בצורה דומה!!



3. סוגי מתקפות פישינג

ברצוני להסביר מספר מונחים החוזרים על עצמם בחדשות.

המונח פישינג כולל מגוון קטגוריות משנה שונות. הכרות עם הסוגים השונים תסייע לזהות את האיום ולהתגונן מפניו.

Phishing, spear phishing, whaling, vishing, smishing, angler phishing, catfishing and pharming.

התרגום המילולי משעשע: דיוג, דיוג חנית, צייד לווייתנים, נעצור כאן בניסיונות לתרגם 😊.

• **דיוג phishing** : התקפת פישינג כוללת הודעה דונית שנשלחת על ידי פושעי סייבר, בדרך כלל להרבה אנשים. הודעה אחת יכולה להגיע ל 250 ועד -250,000 תיבות דואר. המטרה היא לתמרן אנשים, בדי להוריד תוכנות זדוניות למחשב, להעביר נתונים שלא במתכוון, לגנוב שמות משתמשים וסיסמאות ולבצע

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

פעילויות הונאה. תשעים ושישה אחוזים מהתקפות הדיוג מתבצעות באמצעות דוא"ל.

• **<u>דיוג חנית spear phishing ו ציד לווייתנים whaling</u>**: במקום להגיע למאות יעדים פוטנציאליים, תוכניות פישינג אלה מתמקדות לרוב במנהלים וביעדים בעלי ערך גבוה בארגון. עבריין סייבר עשוי לחקור פרופילי מדיה חברתית של מנהל או מידע מקוון אחר לפני פריסת הפיתיון של דיוג חנית. דליפות נתונים ופגיעה בפרטיות יצרו פוטנציאל עבור האקרים ליצור תיקי מידע מפורטים המעניקים אמינות לפתיון שלהם ברשת. דייגי חנית מכירים לעתים קרובות את שם הפרט, מקום עבודתו, שם התפקיד, כתובת הדוא"ל, מידע ספציפי על תפקידו המקצועי וכן מידע אישי על עמיתים, בני משפחה או אנשי קשר. זה מאפשר לפושעים ליצור פיתיונות דיוג חנית ברמה גבוהה ומשכנעים.

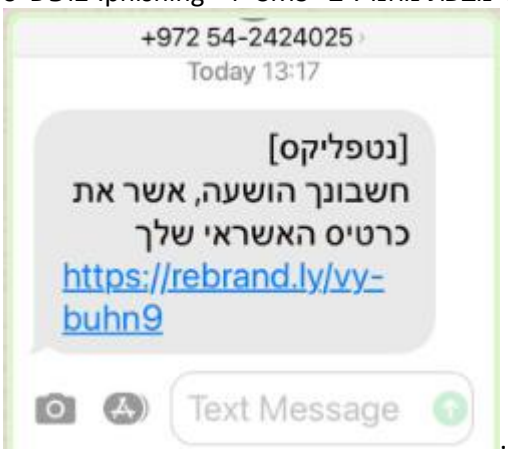
• **<u>Vishing(Voice phishing):</u>** זהו פישינג באמצעות טלפון. באמצעות מניפולציות רגשיות פושעי סייבר ממציאים מצבים שמשכנעים את המותקפים לחשוף מידע שהם בדרך כלל לא היו משתפים בטלפון. תוקף, יכול להתחזות למנכ"ל או למנהל אחר, ולגרום לאדם לציית ולסייע וכך למסור את המידע המבוקש.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

• **Smishing**: המילה 'smishing' נובעת מהמילים "SMS" ו- "phishing". פושעי סייבר שולחים הודעות טקסט הונאה לקורבנות תמימים.



• **Angler דיוג טרף**: סוג זה של דיוג כרוך בשימוש בחשבונות מזויפים של מדיה חברתית תוך התחזות לארגונים אמיתיים. שמות וזהויות מזויפים עשויים להיות בהבדל של כמה אותיות בלבד מהאותיות האותנטיות. באמצעות חשבונות מזויפים, פושעי סייבר יכולים לנצל את הנטיות של משתמשים להגיש תלונות לקוח באמצעות מדיה חברתית. תוך התחזות לתגובה לתלונה, פושעי סייבר יכולים לבקש מאנשים לספק מידע אישי. לחלופין, דייגי טרף עשויים להפנות אנשים לדפי תמיכה זדוניים מתחזים.

• **Cat Phishing דיוג חתולים**: שיטה זו כוללת שימוש בפרופיל אישי שהוקם במרמה באתר רשת חברתית, שנועד לסייע להאקרים להשיג רווחים פליליים.

• **Pharm Phishing התקפות חווה**: בהתקפת חווה, אתר מזויף מתחזה לאתר לגיטימי. באתר זה משתמשים מתבקשים להזין פרטים אישיים בטפסים או בחלונות קופצים. האתר עשוי לאלץ משתמש להוריד קוד זדוני. ישנם סוגים שונים של התקפות מסוג זה. השורה התחתונה היא שימוש באתר מזויף.

כל אחד מאיתנו עלול להיות מותקף בשיטות הדיוג השונות. היזהרו.

4. הזדהות חזקה MFA

רובנו מזדהים היום אל מול רוב מערכות הטכניון בהזדהות חזקה, קרי MFA. חלקנו משתמשים בתוכנה המותקנת על הטלפון החכם וחלקנו מקבלים SMS לטלפון החכם. אני רוצה להסביר את החולשות של שיטת ה SMS. לפני ההסבר אני מבקש להרגיע. שימוש ב SMS עדיף על סיסמא בלבד. בנקים , חברות ביטוח ואשראי משתמשים בשיטת ה SMS. הם עושים זאת לא בגלל שהיא עדיפה על יישומון בטלפון החכם אלא בגלל הפשטות ומניעת הצורך בתמיכת משתמשים רבים. במקרה שלהם מדובר בעשרות ומאות אלפי משתמשים. לשימוש ב SMS יש מספר חסרונות בפן אבטחת המידע.

א. ספק הסלולר שלך יכול לראות את תוכן ההודעות שאתה שולח ומקבל.
ב. האקרים יכולים ליירט הודעות SMS עקב חולשות בפרוטוקול הישן והרעוע עליו מבוסס ה SMS. הדבר מסכן חשבונות פיננסיים ואחרים.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology
Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

ג. קיימת אפשרות "לחטט" בתוכן של הודעות SMS.
ד. תוקפים יכולים לנסות לגנוב את מספר הטלפון הסלולרי שלך על ידי הטעיית צוות שירות הלקוחות של ספק הסלולר שלך ולקבל גישה להודעות ה SMS שלך.

ה. SMS היא טכנולוגיה מיושנת, אשר בבירור לא נבנתה מתוך מחשבה על פרטיות ואבטחה, אך משמשת אותנו עד היום.
ו. נכון להיום, עדיף להימנע מהשענות על SMS אם אתה מודאג מהפרטיות או מהאבטחה של החשבונות שלך.

המסקנה החד משמעית היא שהשימוש ביישומון עדיף על SMS. יחד עם זאת, השימוש ב SMS עדיף על שימוש בסיסמא בלבד ללא MFA.

השאלה מהגיליון הקודם

בסיום יום העבודה נתקלת בהתקן זיכרון מסוג USB זרוק על הרצפה. מה עושים?

א. מחברים אותו למחשב כדי לנסות למצוא אינדיקציה למי הוא שייך ולהחזירו לבעלים.
ב. השאר את זה איפה שהוא. זו לא הבעיה שלך.
ג. העבר אותו לאחראי על המחשוב ביחידה.
ד. הרווחת, קח את זה הביתה והשתמש בו.

התשובה הנכונה היא "ג" כך גם לא תגרום נזק לעצמך וגם תציל אחרים מלפעול באופן שגוי.

שאלה חדשה :

המחשב שלך נדבק זה עתה בתוכנת כופר וההאקר דורש כסף כדי לשחרר אותו. מה אתה עושה?

א - שולח דוא"ל לאיש ה- IT במשרד.

ב - מנסה כמיטב יכולתך להיפטר מהבעיה לפני שמישהו יגלה זאת

ג - משלם את הכופר. אתה צריך את הקבצים שלך בחזרה!

ד - מנתק את המחשב מהרשת.

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192
glickstein.m@technion.ac.il \ cis.technion.ac.il

Dear Technion Family

"Security is always excessive until it's not enough" - Robbie Sinclair
This is indeed what most people feel. Security imposes constrains and makes things more difficult, so everybody dislike it. However, when a Cyber event occurs, everybody asks why there was no more Security.

1. Laptops

A Technion employee's laptop was recently stolen. The computer was stolen along with the vehicle in which it was left. I would like to emphasize that it is strictly forbidden to leave laptops as well as any other sensitive material in the vehicle or anywhere unattended. The prohibition is absolute regardless of the length of time the computer is left in the vehicle. Every computer and especially a laptop must have a computer access password. Beyond the monetary damage derived from the cost of the computer, there is a great deal of value and risk associated with the data existing on the computer or accessible by it. If a computer is stolen or lost, you must **immediately**:

a. change the passwords
b. inform your management, the IT team and the security officer.

The IT team will perform the necessary actions at the technological level and the management together with the information security officer will assess the potential damage and take the necessary actions according to the privacy regulations and other possible consequences.

2. Attack on Hillel Yaffe Hospital

I assume most of us have read in the news about this hack. The hidden still prevails over the known. At the same time the picture below illustrates how much human error can lead to the destruction of computer systems, regardless of the protection systems implemented in the organization. You can see in the picture that the username and password were displayed not only to everyone in the corridor but to everyone who watched the news on TV that day. Every user and every unit manager must ask himself if his

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192

glickstein.m@technion.ac.il \ cis.technion.ac.il

passwords are exposed in a similar way!!

3. Phishing flavors

The term phishing has come to broadly encompass a variety of different sub-categories of this general operational schematic:
Phishing, spear phishing, whaling, vishing, smishing, angler phishing, catfishing and pharming. Understanding the differences can help you ¡identify the threat and defend accordingly.

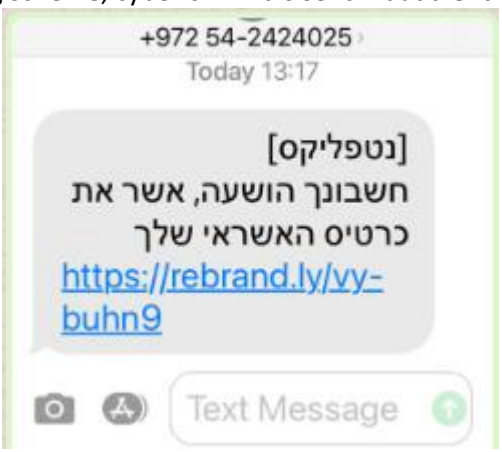
• **Phishing:** A phishing attack involves a malicious message sent by cyber criminals, usually to a large swath of people. Historically, a single message could hit anywhere from 250 to 250,000 inboxes. The aim is to manipulate persons, usually employees, to download malware onto systems, unwittingly exfiltrated data, share credentials and follow-through on wire fraud activities. Ninety-six percent of phishing attacks

are conducted via email.

• **Spear phishing and Whaling**: Rather than reaching hundreds of potential targets, these phishing schemes often focus on executives and other high-value targets. A cybercriminal may explore executive's social media profiles or other online information ahead of deploying the spear phishing bait. Data leaks and privacy abuses have created the potential for hackers to create detailed dossiers that lend credibility to their online trickery. Spear phishers often known an individual's name, place of employment, job title, email address, specific information about their professional role, and personal information about colleagues, family members or other contacts. This enables criminals to create high quality and convincing spear phishing lures.

• **Vishing**: Think phishing, but via phone. Using emotional appeals, cyber criminals fabricate situations that convince callers to divulge information that they ordinarily would not share over the phone. A scammer, for example, could pose as a CEO or another executive, making the person on the receiving end feel as though it is his/her obligation to hand over the requested information.

• **Smishing**: The word 'smishing' derives from the words "SMS" and "Phishing." In a smishing scheme, cyber criminals send fraudulent text messages to unsuspecting victims.



• **Angler phishing**: This type of phishing involves the using fake social media accounts to impersonate the accounts belonging to real organizations. Fake account names and handles may be just a few letters off from authentic ones. Using fake accounts, cyber criminals can capitalize on users' tendencies to make customer complaints via social media. In pretending to respond to a complaint, cyber criminals can ask individuals to provide personal information. Alternatively, angler phishers may point people to malicious customer support pages.

• **Catfishing**: This involves the use of a fraudulently established personal profile on a social networking site, designed to help hackers achieve criminal gains.

• **Pharming attacks**: In a pharming attack, a fake website masquerades as a legitimate one. Users are then asked to enter personal details into forms or pop-ups on the fake website, or a URL may force a user to download malicious code. There are assorted variations on these types of attacks. The bottom line is that all are duplicitous.

Each one of us may be a subject to any of these attacks. Be Careful.

4. Strong Authentication MFA

Today, most of us are authenticated with most of the Technion's systems with strong authentication, i.e., MFA. Some of us use the software installed on the smartphone and some of us receive SMS to the smartphone. I want to explain the weaknesses of the SMS method. Before the explanation I would like to reassure. Using SMS is better than using only textual password. Banks, insurance and credit companies use the SMS method. However, they do it not because it is preferable to a widget on the smartphone but because of the simplicity

and prevention of the need for wide user support. In their case there are tens and hundreds of thousands of users. The use of SMS has several disadvantages in terms of information security.

a. Your cellular carrier can see the contents of the messages you're sending and receiving.
b. SMS messages can be intercepted by hackers due to weaknesses in the rickety old protocol that powers them. This puts financial and other accounts at risk.
c. It is possible to snoop on the contents of text messages.
d. Scammers can try to steal your cell phone number by tricking your cellular provider's customer service staff and get access to your SMS messages.
e. SMS is just outdated technology. It clearly was not built with privacy and security in mind, and those design decisions are still with it today.
f. For now, it's best to avoid text messages if you're concerned about your privacy or the security of your accounts.

The conclusion is that using an APP is better than SMS. Nevertheless, using SMS is better than using a static password without MFA.

The question from previous newsletter

1. **You're just leaving your office for the day when you stumble upon a USB stick on the floor. What do you do?**
    a. Pick it up and plug it in to try and find an indication of whom it belongs to, so you can return it.
    b. Leave it where it is. It's not your problem.
    c. Hand it to IT team for them to deal with.
    d. Your lucky day. Take it home and use it.

The correct answer is "c" – this way you will not harm yourself and save others from mistakes

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION Israel Institute of Technology

Tel: +972 48294192

glickstein.m@technion.ac.il \ cis.technion.ac.il

New question:

Your computer has just been infected with Ransomware and the hacker is demanding money before releasing it. What do you do?

A - Send an email to the IT guy in the office.
B - Try your best to get rid of it before anyone finds out
C - Pay the ransom. You need your files back!
D - Disconnect your computer from the network

Moshe Glickstein - CISO
Division of Computing & Information Systems
Isaca: CISM, CISA, CDPSE
They want what you've got – Don't give it to them

TECHNION
Israel Institute
of Technology

Tel: +972 48294192

glickstein.m@technion.ac.il \ cis.technion.ac.il