לומדה בנושא הגנת הסייבר

יש 3 מטרות עיקריות לאבטחת מידע

החשיבות והמחויבות לאבטחת מידע

חשאיות

מניעת גניבת / זליגת מידע

אמינות

מניעת שינוי המידע על ידי גורם לא מורשה או מידע שגוי

זמינות

זמינות המידע השמור במערכות בכל רגע נתון בכדי לספק שירות

למעבר בין העמודים
השתמש בחיצי המקלדת

חוק הגנת הפרטיות ותקנותיו

- עוסק בזכותו של כל אדם לפרטיות
- אוסר לפגוע בפרטיות של אדם ורשאי להטיל עונשים

התחייבות והסכמי סודות מול לקוחות

למעבר בין העמודים
השתמש בחיצי המקלדת

לומדה בנושא הגנת הסייבר

מה נחשב מידע רגיש?

כל מסמך המכיל מידע רגיש על החברה או לקוחותיה

- דוחות ביקורת
- סיכומי ישיבות דירקטוריון והנהלה
- סקרי סיכונים
- מידע אישי של עובדי החברה (משכורות)
- מידע על ספקי החברה
- נתונים על לקוחות החברה

מה נחשב מידע רגיש?

כל מסמך המכיל מידע רגיש על החברה או לקוחותיה

80% מאירועי אבטחת מידע בארגון נגרמים על ידי עובדים.
רובם בשוגג

החברה (משכורות)

- מידע על ספקי החברה
- נתונים על לקוחות החברה

לומדה בנושא הגנת הסייבר

כללים

אינטרנט

דואר אלקטרוני

מחשב אישי

סיסמה אישית

נעילת מערכת

מדיה ניידת

העברת מידע רגיש

שולחן נקי

דיווח

מבקרים

סיסמה

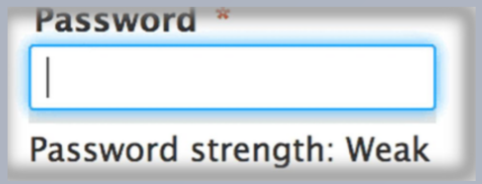
– אישית ולא ניתנת להעברה לאף גורם

– אין לשמור סיסמה באופן גלוי

– יש להחליף סיסמה כל שלושה חודשים או במקרה של חשיפה

– מכילה לפחות 8 תווים ומורכבת מאותיות גדולות, אותיות קטנות, מספרים וסימנים מיוחדים (אין להשתמש בסיסמאות כגון Aa123456)

– כל פעולה הנעשית תחת שימוש בסיסמתך האישית – באחריותך המלאה!



סיסמה

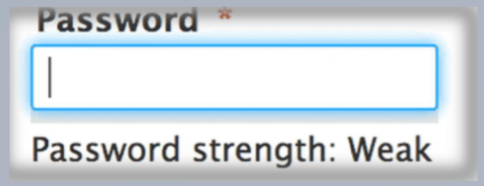
– אישית ולא ניתנת להעברה לאף גורם

– אין לשמור סיסמה באופן גלוי

– יש להה

– מכילה
קטנות, מ

– כל פעו



סיסמה

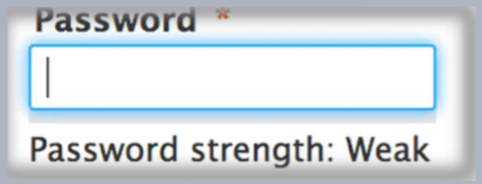
– אישית ולא ניתנת להעברה לאף גורם

– אין לשמור סיסמה באופן גלוי

– יש להחליף סיסמה כל שלושה חודשים או במקרה של חשיפה

– מכילה לפחות 8 תווים ומורכבת מאותיות גדולות, אותיות קטנות, מספרים וסימנים מיוחדים (אין להשתמש בסיסמאות כגון Aa123456)

– כל פעולה הנעשית תחת שימוש בסיסמתך האישית – באחריותך המלאה!



מחשב אישי ונייד

– נועד לצורכי עבודה בלבד
– אין להתקין תוכנות ו/או התקני חומרה ללא אישור
– אסור לבצע שינויים בהגדרות המחשב
– אסור להשאיר מחשב נייד ללא השגחה
– במקרה של תקלה יש לפנות לצוות התמיכה בלבד

מחשב אישי ונייד

– נועד לצורכי עבודה בלבד
– אין להתקין תוכנות ו/או התקני חומרה ללא אישור
– אסור לבצע שינויים בהגדרות המחשב
– אסור להשאיר מחשב נייד ללא השגחה
– במקרה של תקלה יש לפנות לצוות התמיכה בלבד

דואר אלקטרוני

בכל יום נשלחים כ 200,000 מיילים המכילים תוכן פוגעני או וירוסים (SPAM) העלולים להזיק למחשב או לחדור דרך המייל לרשת הפנימית של החברה

לכן יש להיות זהירים באופן השימוש במיילים ולשים לב לכללים הבאים:

אופן השימוש במיילים

– השימוש בדוא"ל הינו לצורכי התפקיד בלבד

- אין להירשם לשירות כלשהו עם דוא"ל של החברה שלא לצרכי תפקיד

– אין לפתוח הודעת דוא"ל ממקור לא מזוהה

- יש לשים לב לתוכן המייל, והאם הוא רלוונטי עבורי

-במידה והתקבל דוא"ל חשוד, יש לדווח על כך לצוות התמיכה הטכנית

- חל איסור להעביר בדוא"ל מידע רגיש / מסווג, לכתובת חיצונית,

ללא אישור וללא שימוש בהצפנה

שימוש באינטרנט

-לצורך התפקיד והעשרה מקצועית בלבד

-אין להוריד ו/או להתקין תוכנות מאתרי אינטרנט ללא אישור

-יש להימנע ממסירת מידע ברשתות חברתיות ובפורומים

-אין להיכנס לאתרים שיכולים לפגוע במחשב (כגון אתרי הימורים, הורדת קבצים וכדומה)

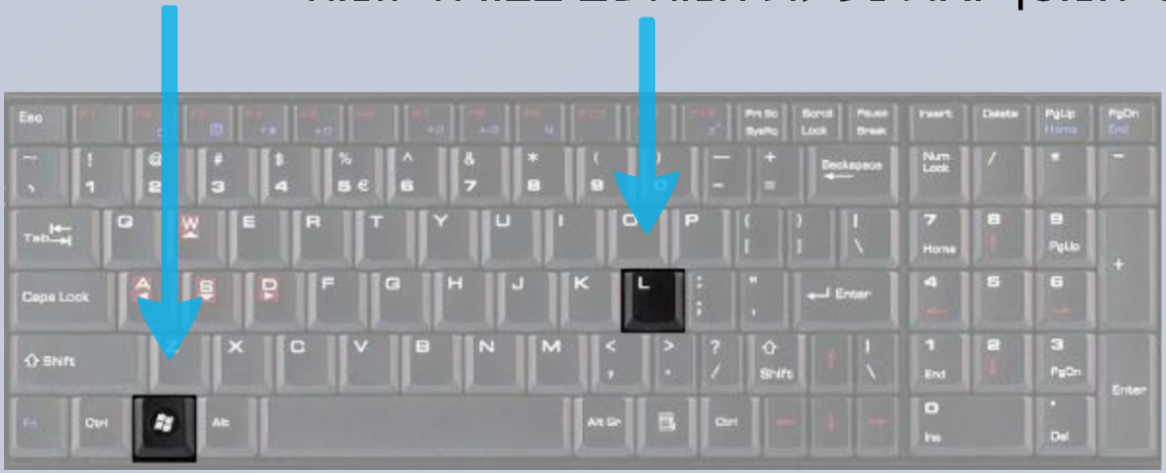
-מומלץ לא לשמור סיסמאות בדפדפן

נעילת מחשב

– תוכנת שומר המסך מופעלת אוטומטית לאחר 20 דקות רצופות של חוסר פעילות במחשב

– אין להשאיר עמדת מחשב חשופה

– אם הנך עוזב את עמדת המחשב לפרק הזמן העולה על 3 דקות, יש להפעיל את שומר המסך ואת נעילת המחשב בצורה יזומה



מדיה ניידת

-שימוש באמצעי אחסון ניידים, כגון: DOK או תקליטור CD/DVD מותרים רק לצורכי עבודה

-חל איסור להעתיק מידע רגיש ו/או מסווג לאמצעי אחסון נייד, ללא אישור

- אין להעביר בין לקוחות, קרובי משפחה וחברים אמצעי אחסון הנושאים מידע של המשרד

-חל איסור לחבר למחשב של המשרד אמצעי אחסון לא מזוהים או להשתמש בציוד אישי לפעילות עסקית

- יש להימנע מלהתקין אמצעי אחסון של המשרד ברשתות חיצוניות

- במקרה של אובדן, יש לדווח

העברת מידע

- אין להעביר מידע רגיש ו/או מסווג לגורמים בלתי מורשים
- מידע רגיש יש להעביר באופן מוצפן בלבד
- חומר פיזי רגיש, יש לשלוח בדואר רשום או על ידי שליח מורשה, במעטפה סגורה עליה כתוב "לנמען בלבד"
- יש להימנע משליחת מסמכים רגישים ו/או מסווגים באמצעות פקס;

במידה והכרחי, יש לנקוט בצעדים לווידוא קבלת המסמך אצל הנמען

טיפול במידע

- יש לשמור מסמכים רגישים ו/או מסווגים בכונני רשת

- אין להשליך מסמכים לפחי אשפה, אלא לפחים המיועדים לגריסה

- אין לתלות מסמכים רגישים ו/או מסווגים על לוחות מודעות

"שולחן נקי"

– אין להשאיר מסמכים רגישים או מסווגים ללא השגחה, כולל מסמכים השמורים על מדיה נתיקה

– בעת העדרות ממושכת יש להקפיד ולנעול את המסמכים והמדיה הנתיקה

– אין להשאיר חדרים לא נעולים בסיום העבודה או בעת היעדרות ממושכת

– יש להקפיד על נעילת המחשב בעת היעדרות

– יש להקפיד לא להשאיר מסמכים במדפסות / מכונות צילום / פקס

– יש להקפיד ששולחן העבודה יהיה נקי ממסמכים המכילים מידע רגיש

מבקרים

– אין למסור את תג העובד למבקרים או לעמית אחר

– אין לאפשר כניסה למבקרים אשר אינם אורחים מזוהים

– אורחים, לרבות ספקים, חייבים בליווי של המזמין עד ליציאה

– אין לאפשר למבקרים גישה למסמכים, למדיה, למחשב ולרשת

– אין לאפשר למבקרים להשתמש במשאבי המשרד (מחשב, מדפסת, מכונת צילום, פקס וכדו')

– אין לאפשר למבקרים לצלם בתוך המשרד, ללא השגחה ווידוא כי בצילום לא נכלל מידע רגיש או מסווג

דיווח

- דיווח הוא חובה מתוקף התקנות
- קיימת חובה לדווח על כל אירוע אבטחת מידע או חשד לאירוע

לדוגמא:
- סיסמא שהתגלתה
- מחשב נייד שאבד, או פלאפון נייד המחובר לחשבון המייל
- כרטיס עובד שאבד
- התנהגות המחשב חריגה
- התקנת תוכנה ללא אישור
- החדרת USB זר למחשב
- קבלת מייל חשוד או מתחזה

לומדה בנושא הגנת הסייבר

הנדסה חברתית

בהנדסה חברתית התוקפים
מנסים להתחזות לגורמים מזוהים
לארגון כדי לנצל את נכונות
הארגון לשתף איתם פעולה
התוקף יציג את עצמו כחלק
מהארגון או בעל ידע
פנימי, וכך עובדי הארגון
ייטו להאמין שהוא אכן
האדם הנכון

בהנדסה חברתית יש 3 טקטיקות שונות

פנים מול פנים

המקרים הנפוצים ביותר הם גורם זדוני שמזדהה בתור:

- טכנאי מחשבים/מדפסות
- שליח דואר/ספק

במטרה לבצע חדירה למערכות החברה

- עובד חדש מזויף/ריגול תעשייתי

במטרה לבצע ריגול תעשייתי

פנים מול פנים

המק

בטלפון

כיום בעולם הדיגיטלי, פרטים מזהים רבים נמצאים ברשת וניתן לגנוב זהויות בקלות.
לכן בהעברת מידע **בשיח טלפוני**, יש ולוודא בצורה חד משמעית מי הגורם שנמצא מעבר לקו (בין אם זה לקוח/ספק וכדומה).

במקרים של נסיון התחזות או פריצה למידע דרך שיחת טלפון, הפורץ ינסה להפעיל עלינו לחץ בכדי שנסייע לו.

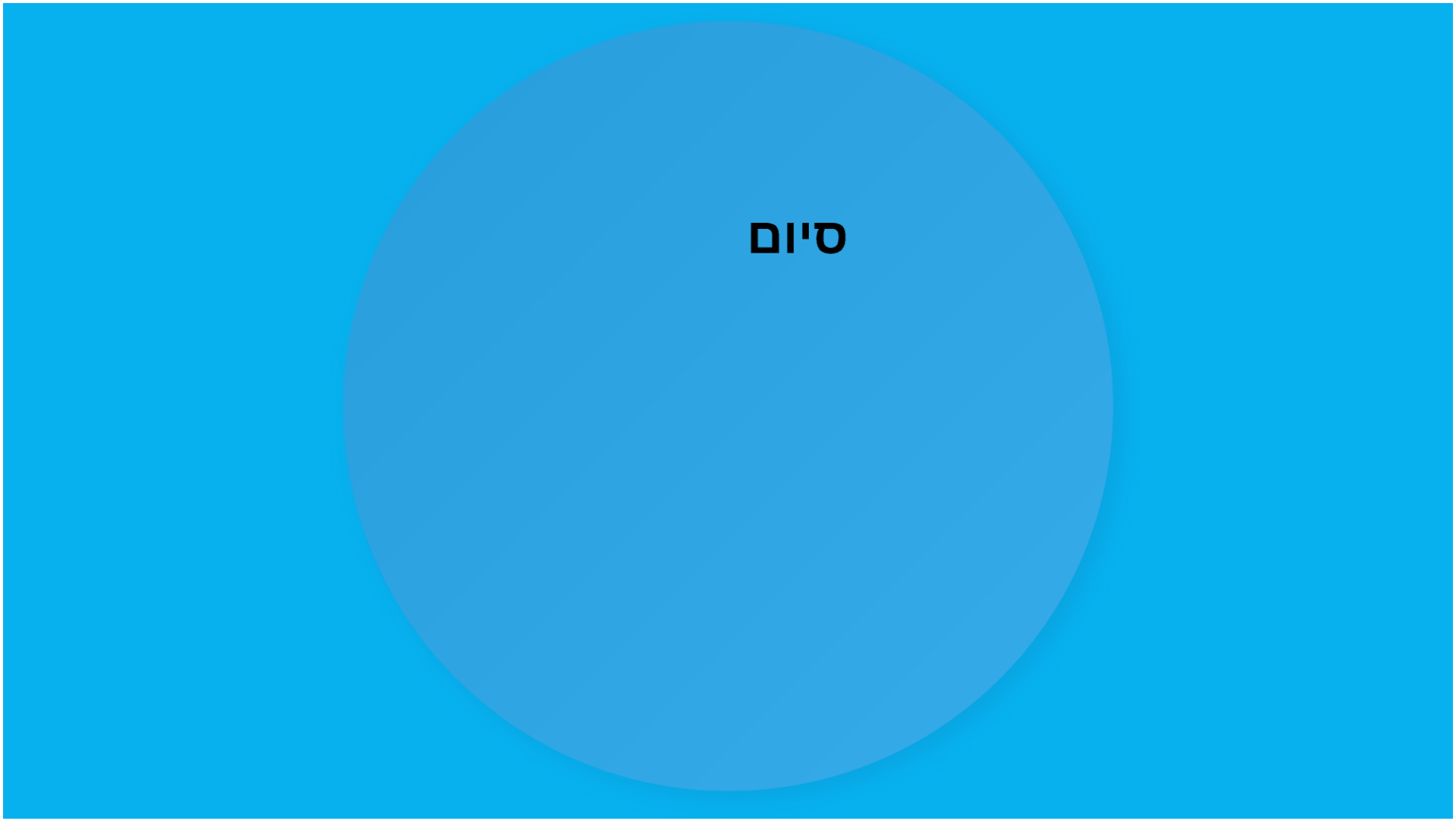
אנא צפו בסרטון הבא


And I can't remember what email address
we used to log on to the account,
and the baby's crying-
REAL FUTURE

במרחב הדיגיטלי

הנדסה חברתית דיוג ברשת(Phishing)

1. **כתובת הדואר האלקטרוני של השולח.**
כדי ליצור תחושת דחיפות שקרית, השורה 'מאת' עשויה להכיל כתובת דואר אלקטרוני שנראית רשמית.
2. **פנייה כללית בדואר אלקטרוני.**
פנייה כללית, כגון "משתמש יקר".
3. **מתן תחושת דחיפות שקרית.**
רוב הודעות הדואר האלקטרוני של דיוג (פישינג) מנסות להונות אותך באמצעות איום שחשבונך יהיה בסכנה אם לא תעדכן אותו מיד. הודעת דואר אלקטרוני שמבקשת ממך לספק בדחיפות פרטים אישיים מיועדת בדרך כלל למטרות הונאה.
4. **קישורים מזויפים.**
במקרים רבים, הודעת הדואר האלקטרוני של דיוג (פישינג) כוללת קישור שנראה חוקי, אך שולח אותך לאתר למטרות הונאה שכתובת ה-URL שלו זהה או שונה מזו של הקישור. בדוק תמיד את יעד הקישור לפני שתלחץ עליו. הזז את העכבר שלך מעל כתובת ה-URL בהודעת הדואר האלקטרוני ובחן את כתובת ה-URL בדפדפן. כמו תמיד, אם הקישור נראה חשוד, אל תלחץ עליו. פתח חלון דפדפן חדש והקלד
https://www.paypal.com/il.
5. **קבצים מצורפים.**
בדומה לקישורים מזויפים, ניתן להשתמש בקבצים מצורפים בהודעות דואר אלקטרוני של דיוג, והם עלולים להיות מסוכנים. לעולם אל תלחץ על מסמך מצורף. הדבר עלול לגרום לך להוריד תוכנת ריגול או וירוס. PayPal לעולם לא תשלח לך בדואר אלקטרוני קבצים מצורפים או עדכוני תוכנה להתקנה במחשב שלך.


סיום

לומדה בנושא הגנת הסייבר