

מגזין עצות מודעות



TEL AVIV אוניברסיטת
UNIVERSITY תל אביב

עובדים יקרים,

ריכזנו עבורכם מספר עצות מודעות חשובות שיסייעו לכם להגן עליכם, על משפחתכם ועלינו מפני גורמים זדוניים ברשת.

אנו מזמינים אתכם לקרוא ולהעשיר את עצמכם בידע חשוב זה על מנת שנוכל כולנו יחד, וכל אחד לחוד, להגן על עצמינו מפני הסכנות ברשת.

תוכן עניינים

- 4 טיפ 1 פישיונג
- 6 טיפ 2 כל מה שרציתם לדעת על סיסמאות ולא העזתם לשאול
- 8 טיפ 3 רכישה בטוחה באתרי אינטרנט
- 10 טיפ 4 התנהלות נכונה ברשתות חברתיות
- 12 טיפ 5 איך נגן על ילדינו ברשת?
- 13 טיפ 6 כך תתמודדו עם הונאות טלפוניות
- 15 טיפ 7 ההונאות הרווחות ברשת וכיצד להתמודד עמן



טיפ מודעות

מס' 1

פישנינג

מקורית להודעה פיקטיבית. כתובת המוסר זהה לכתובת המקורית, המייל מעוצב כדי לדמות את מבנה המייל המקורי של החברה השולחת ואפילו הלינק יכול להיות זהה.

ההודעות לרוב מסוגנות בנוסח זכייה או איום - דברים שמושכים אנשים ללחוץ על הקישור או לפתוח את הקובץ המצורף.

לדוגמא | הודעות מהבנק שדורשות שינוי פרטים, איום על סגירת החשבון או בקשה להזנת סיסמא על מנת להיכנס לחשבון, קבלות להזמנות אינטרנטיות למיניהן והודעות רנדומאליות מאנשים שאנחנו כביכול מכירים.

חשוב לשים לב, כאשר אנחנו מקבלים הודעה מהבנק או מכל אתר אחר, כדאי תמיד להיכנס לאתר המדובר דרך הדפדפן.

בכתבה זו, נדון בבעיה שיכולה לתקוף אותנו גם בבית וגם בסביבת העבודה- **פישנינג**.

פישנינג או בשמו העברי 'דיוג' הינו ניסיון לגניבת מידע רגיש ע"י התחזות ברשת האינטרנט או ניסיון להדביק את המחשב שלנו בוירוסים על ידי לחיצה על קישורים או פתיחת קבצים זדוניים. אנו נתקלים בתופעה זו במקרים רבים בערוץ הדואר האלקטרוני או דרך הרשתות החברתיות.

ככלל, המדובר בעברייני סייבר המנסים לגנוב מאיתנו פרטים אישיים כגון סיסמאות ופרטים בנוגע לכרטיסי האשראי וחשבון הבנק שלנו על מנת שיוכלו לנצל אותם בעתיד.

הונאות הפישנינג היום הן מאוד מתוחכמות, עד שכמעט ואי אפשר להבחין בין בהודעה



כדי לבדוק את אמינות התוכן במקרה של מייל המכיל קבלה על קניה למשל - היכנסו לאתר המקורי לו שילמתם ובדקו האם התבצעה רכישה בסגנון לפני שאתם פותחים את הקובץ.

המלצות



- **הימנעו מלחיצה על קישורים** או מפתחת קבצים בהודעות אשר נראות לכם חשודות אפילו במעט.
- במידה ואנחנו מתלבטים האם המייל אמין או לא - כדאי **תמיד לפנות לאתר המקורי** לא דרך הקישור שמופיע במייל ולא לפתוח ישירות את הקובץ המצורף לפני שמוודאים את מקור המייל לאשורו.
- אם אתם נרשמים לאתרים מסוימים, עדיף **תמיד לתת את המייל הפרטי ולא את המייל של עבודתכם.**

כיום, **עם ההתפתחות עולם המובייל**, ייתכן שגם בערוץ זה ינסו התוקפים לדוג אותנו. על כן, כאשר אנו מקבלים הודעת SMS מגורם לא מוכר הכוללת קישור-דלגו על הלחיצה, זו עלולה להיות מלכודת. פריצות לטלפון הנייד הן דבר נפוץ מאוד המאפשרות לתוקף לגנוב מכם מידע אישי כמו הודעות טקסט, מידע על אנשי קשר, מידע ארגוני ואפילו תמונות.



אם קיבלתם הודעה עם תוכן מוזר, לא מוכר או המכילה מלל שנראה מתורגם לתיבת המייל או ההודעות ברשת חברתית - קיים סיכוי סביר, שגם אם ההודעה מגיעה מכתובת מוכרת, היא יכולה להיות זדונית. לכן חשוב לא ללחוץ על שום קישור ולמחוק את ההודעה.

בזמן העבודה, אנחנו עלולים לקבל את אותם מיילים חשודים, אך עם מטרה שונה. הפעם, המטרה לא תהיה לגנוב את פרטינו האישיים אלא להדביק אותנו בוירוסים או לחדור אל רשת הארגון.

לחיצה על הקישורים הנ"ל או פתיחת הקבצים המצורפים עלולים להוביל לנזקים גדולים לארגון ולנו כעובדים ולכן עלינו לפקוח עיניים.

כל מייל בסגנון שמתקבל לתיבה בעבודה צריך להישלח באופן מידי לאנשי אבטחת המידע בארגונכם לבדיקה מקיפה על מנת לשמור על ביטחונכם ובטחון לקוחותיכם.

וזה, לצערנו, עוד לא הסוף...

כל מה שרציתם לדעת על סיסמאות ולא העזתם לשאול

טיפ מודעות



מס' 2

תינעל האפשרות להזדהות כבר לאחר ניסיונות מעטים.

Password



Weak

Password



Medium

Password



Strong

על עותק של קובץ הסיסמאות של המערכת ומנסה להריץ סיסמאות ע"י שימוש במילון סיסמאות נפוצות. בשיטה זו לא מתמקדים במשתמש ספציפי, אלא תוקפים את קובץ הסיסמאות כולו.

הסיבה שמתקפה זו עובדת היא מפני שאנשים רבים בוחרים מילים פשוטות עבור הסיסמא שלהם - מה שמאפשר פריצה קלה עבור התוקפים.

Brute Force (מתקפת כוח גס) - מדובר בניסיונות חוזרים לפיצוחן של סיסמאות כניסה למחשב, אפליקציה או שירות מסוים באמצעות כל הסיסמאות האפשריות המורכבות מהמידע שאוסף התוקף על הקורבן באמצעות  **הנדסה חברתית** (רשתות חברתיות ועוד), עד להצלחה. במקרים רבים

אם אחת הסיסמאות שלכם היא תאריך הלידה שלכם או של הבן שלכם, מספר הטלפון הנייד, שם המשפחה שלכם, שם חיית המחמד האהובה עליכם או צירוף של כמה מאלו יחד- הטיפ הבא מיועד אליכם.

מהי סיסמה?

סיסמה הנה אות מוסכם המשמש כאמצעי זיהוי לשם בקרת גישה למשאב מסוים. היא יכולה להגיע כצירוף של אותיות, מספרים, וכן כצירוף של שני אלו יחד.

ישנן 2 מתקפות סייבר עיקריות שבהן משתמשים תוקפים על מנת לנסות לפצח את סיסמאות קורבנותיהם:

Dictionary Attack (מתקפת מילון) - במתקפת מילון, התוקף מצליח לשים ידו

Password

israel1805

Weak

אל תבחרו סיסמה
שכוללת את השם הפרטי
או שם המשפחה שלכם
וכן מספר טלפון או תאריך
לידה וכדומה.

Password

5Gra0&jp@!

Strong

שלבו אותיות (באנגלית-
גדולות וקטנות), **מספרים**
וסימני פיסוק בסיסמה.

Password

4fdv86!fg5

Strong

בחרו סיסמה באורך
מינימאלי של **8 תווים**.

*****אז איך בוחרים סיסמה?*****

זכרו לא לכתוב את
הסיסמאות בקרבת סביבת
העבודה (פתק על המסך),
בטלפון הנייד בצורה לא
מוגנת או על המחשב בקובץ
טקסט פשוט.

Password

Change Password

החליפו סיסמה
כל כמה חודשים.

Password

Facebook password

בחרו סיסמאות שונות
לאפליקציות בהן אתם
משתמשים (לדוגמה -
סיסמה שונה לפייסבוק,
לחשבון הבנק ולדוא"ל).

כללי אצבע לסיסמאות חזקות:

- הקפדה על אורך מינימאלי לסיסמה
- הקפדה על שימוש במגוון רחב יותר של תווים וסימנים כמו אותיות, מספרים וסימני פיסוק
- בדיקה שהסיסמה אינה חלק מהמידע המשפחתי/חברתי של המשתמש או בעלת יתירות גבוהה (כמו חזרה על תווים מסוימים מספר פעמים).
- יודגש כי מערכות רבות אף מגבילות את תוחלת החיים של הסיסמה (כלומר דורשות החלפת הסיסמה בתדירות גבוהה).



רכישה בטוחה באתרי אינטרנט

טיפ מודעות



מס' 3

תעודות אבטחה דיגיטליות

ברגע שתגיעו לעמוד הרכישה באתר בו אתם מבצעים את מסע השופינג שלכם, אמור להופיע מנעול נעול ליד כתובת העמוד. המנעול המפורסם הוא חלק מפרוטוקול האבטחה SSL. לחיצה על המנעול תציג בפניכם את שיטות האבטחה של האתר ולחיצה על "פרטי אישור" תפתח בפניכם חלון חדש המציג את תעודת האבטחה של האתר.

אבטחת שכבת התעבורה - Transport Layer Security (בקיצור TLS) וקודמו Secure Sockets Layer (בקיצור SSL), הם פרוטוקולי האבטחה הפופולריים והחשובים ביותר של רשת אינטרנט. כמעט כל אתרי האינטרנט המוגנים באמצעים קריפטוגרפיים מסתמכים על פרוטוקולים המהווים חלק מהחבילה

SSL/TLS. מסחר אלקטרוני, בנקאות מקוונת, דואר אלקטרוני, VoIP, מחשוב ענן ועוד. TLS נתמך על ידי מרבית הדפדפנים, בראשם גוגל כרום, אינטרנט אקספלורר, ספארי, פיירפוקס, אופרה ועוד. SSL/TLS הוא פרוטוקול ורסטילי שמטרתו אבטחת שיחת שרת/לקוח בשיטות קרפיטוגרפיות חזקות והוא אמור למנוע ציתות, זיוף, או חבלה (שינוי זדוני) של המידע העובר בין השרת והלקוח. מאפשר חיבור אנונימי, אימות שרת (חד-צדדי) או אימות דו-צדדי, תוך שמירה על דיסקרטיות ושלמות המסרים.

כשחלון תעודת האבטחה של האתר פתוח, בלשונית הראשונה ניתן לראות בשדה האחרון את תוקף האישור, וודאו שהאישור בתוקף. כמו כן, וודאו גם שכתובת ה-URL

שמופיעה בשורת הכתובות, מתחילה ב-Https ולא ב-Http כפי שאנו רגילים משאר כתובות הרשת. ה-S בסוף ה-Http מסמלת שהכתובת היא Secured, כלומר מאובטחת.

אף אחד מאיתנו לא רוצה שיגנבו את פרטי כרטיס האשראי שלו ברשת. זה לא יקרה לכם אם תקפידו על כמה כללים. אז הנה המדריך שאף אחד ממושעי הסייבר לא רוצה שתקראו:

השימוש בדפדפן

השלב הראשון בלהבטיח שפרטי חשבון הבנק וכרטיסי האשראי שלכם לא יהיו חשופים לכל הוא פשוט לדאוג שהדפדפן שלכם יהיה מעודכן בגרסתו האחרונה. בין אם אתם משתמשים בכרום, באקספלורר או בדפדפן אחר. העדכונים בדרך-כלל מותקנים באופן אוטומטי, אך דורשים את אישור המשתמש.

למה? כדי לוודא שהדפדפן שלכם מעודכן בכל אמצעי האבטחה האחרונים האפשריים.

מדיניות פרטיות

מסמך מדיניות הפרטיות, או באנגלית "Privacy Policy" הוא למעשה הכיסוי המשפטי של החנות ושל החברה שעומדת מאחוריה. אם לא מצאתם מסמך כזה - מומלץ מאוד להתרחק מהאתר.

במידה ומצאתם מסמך מדיניות פרטיות באתר, בדקו שהאתר מתחייב לא להעביר את פרטי כרטיס האשראי שלכם, חשבון הבנק שלכם ואת מספרי הזיהוי שלכם לידי גורם צד שלישי.

במידה והאתר אינו מהמוכרים שביניהם או לא מוכר לכם, ניתן ואף צריך לבצע את הפעולות הבאות:

- בדקו מי עומד מאחורי האתר
- בדקו האם באתר מופיעים פרטי העסק כגון: כתובת העסק, שם העסק המתפעל את האתר וכדומה.

בדרך כלל ניתן לקבל את הפרטים הנ"ל בדפים כמו: אודות האתר, יצירת קשר או תנאי השימוש.

לידיעתכם, בירור המידע אודות האדם/חברה המתפעל את האתר הינו קריטי להחלטתך לגבי ביצוע התשלום והאמון שהינך מתבקש לתת באתר.

וודאו שהאתר מפעיל שירות לקוחות זמין, חשוב מאוד לוודא כי באתר מופיע מספר טלפון (עדיפות לטלפון נייד, ולא סלולארי) של שירות לקוחות.

בחלק מהאתרים לא מופיע מספר טלפון, אלא אפשרות ליצור קשר בדוא"ל בלבד. במקרה כזה מומלץ לוודא כי תהיה לך אפשרות להשיג את בעל האתר בדרכים חלופיות, כגון: דואר גיל, שירות 144 של בזק וכדומה.

אם לא מופיעים שום פרטי התקשרות באתר לשירות לקוחות או לפחות טופס יצירת קשר/כתובת דוא"ל, הימנע מביצוע התשלום באתר.

מה מספר האינטרנט?

תתפלאו לדעת עד כמה ניתן לעיתים קרובות למצוא ברחבי האינטרנט תגובות של לקוחות קודמים שביצעו בעבר רכישות באתר שהינכם מבקרים בו.

אם לאתר מסוים יש פגמים עקביים ובעייתיות כלשהי באספקת שירותים תקינים ללקוחותיו, סביר מאוד להניח שתמצאו מידע מקדים על כך באחד הפורומים או אתרי הביקורות באינטרנט.

לחיפוש תגובות היכנס לאחד ממנועי החיפוש וחפשו את המילים:

פידבקים + שם האתר או תלונות + שם האתר.

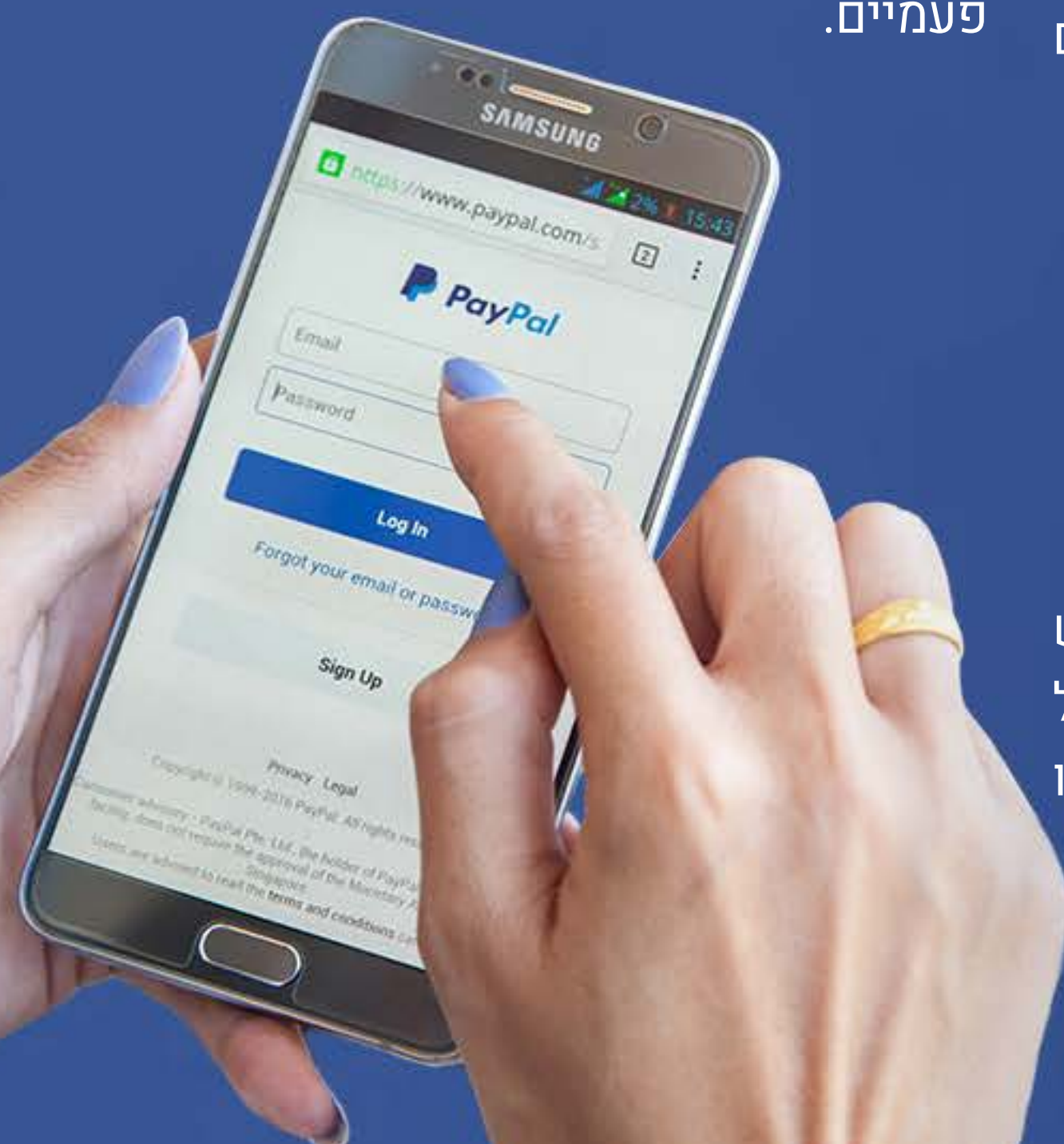
טוב, אז עכשיו הגעתם לשלב שאתם פותחים את הארנק...שלב התשלום. בשלב זה:

העדיפו להשתמש ב-PayPal

למה זה טוב? זה חוסך זמן בלהקליד מחדש את מספר הכרטיס, התוקף וה-CVV בכל רכישה, אך הדבר החשוב ביותר שלשמו

למעשה נוסדה PayPal הוא בכדי שלחנות המקוונת בה אתם מתכוונים לרכוש מוצר, לא תהיה גישה לפרטים האישיים שלכם, לרבות מספר חשבון הבנק, כרטיס האשראי וכל היוצא בזאת.

ועוד משהו קטן, באם המחיר של המוצר זול משמעותית ממקומות אחרים...תחשבו פעמיים.





התנהלות נכונה ברשתות חברתיות

טיפ מודעות



מס' 4

• **בדקו מיהם החברים המשותפים שלכם** – האם יש היגיון וקשר ביניהם.

• **בדקו את הפיד של הפרופיל** – האם עומד מאחוריו אדם אמיתי עם דעה ואמירות או שמע הפיד מורכב רק מתמונות (אותן כל אחד יכול להדביק).

לידיעתכם, ניתן גם לחפש את תמונת האדם דרך חיפוש התמונות של גוגל (לחיצה על אייקון המצלמה שמופיע בצד תיבת החיפוש יאפשר לכם לחפש את התמונה עצמה) ולבדוק האם אינה מועתקת מהאינטרנט.

אם עדיין אנכם בטוחים, פנו לאדם בתכתובת ושאלו אותו כיצד הגיע אליכם.

עולם, במילים אחרות, רוב הסיכויים שכל מה שתפרסמו יהפוך לציבורי ולנחלת הכלל. זכרו את משפט המפתח הזה בכל פעם שאתם מתכוונים לפרסם משהו, זה עלול להשפיע על העתיד שלכם, על חיפוש העבודה העתידי שלכם, על קבלת מועמדותכם לחוגים מסוימים וכיו"ב. בנוסף, היו ערניים למה שאחרים מפרסמים לגביכם, ייתכן כי זה מידע שאנכם רוצים בפרסומו.

אישור בקשות חברות

זכרו כי לא כל הנוצץ זהב הוא

• **בדקו מתי נוצר הפרופיל של מבקש החברות** – באם הוא נוצר לאחרונה, זה אומר דרשני.

אז כיצד נשמור על עצמנו בעת השימוש ברשתות חברתיות? ריכזנו עבורכם את הכללים והנה הם לפניכם:

פרטיות

שימו לב מה אתם מפרסמים, למי ומתי – לא כולם צריכים לדעת היכן אתם נמצאים, עם מי ומה אתם עושים בכל רגע.

ברוב הרשתות קיימות הגדרות פרטיות, היכנסו אליהן, בחרו את מידת והיקף הפרטיות שלכם – או במילים אחרות, קחו שליטה על הפרטיות שלכם.

פרסומים

כלל הברזל בנושא זה הנו שכל מה שפורסם, יישאר באינטרנט לדיראון

האם קיים מישהו מאתנו שאינו מחובר לרשת חברתית כלשהי? באם תשובתכם לשאלה הנה כן, אז כנראה שאתם שייכים למיעוט הולך ונעלם שמנותק מהעולם הרשתי... Facebook, Instagram, LinkedIn... אלו רק דוגמאות למבחר הרשתות החברתיות אשר רובנו משתמש ומנוי אליהן. רשתות אלו הפכו את העולם שלנו לכפר גלובלי קטן ומאפשרות לנו לפגוש ולתקשר עם אנשים בארצות מרוחקות, לשתף את חברינו במה שקורא אתנו, למצוא עבודה ועוד ועוד... אבל, אליה וקוץ בה, ברשתות אלו גם טמונים סיכונים רבים לכם, למשפחותיכם ולעבודתכם.

סיסמאות והזדהות חזקה

- אל תשתמשו באותן סיסמאות לחשבונות שונים – כי במקרה ומישהו גילה או גנב את הסיסמה, הוא יוכל לקבל גישה לכל חייכם הדיגיטליים.
- אל תשתמשו באותן סיסמאות בעבודה ובחייכם הפרטיים – אל תסכנו את עבודתכם על ידי שימוש באותה סיסמה בבית ובעבודה.
- השאירו את פרטיכם האישיים מחוץ לסיסמה – שימוש בתאריך הלידה שלכם, בשמכם וכו' הופך את סיסמתכם קלה לניחוש בידי גנבי זהויות.
- כאשר הדבר אפשרי השתמשו בהזדהות חזקה להתחבר לחשבונותיכם – הכוונה שתצטרכו להקליד קוד נוסף על מנת להתחבר לחשבונותיכם בנוסף לסיסמה. הזדהות חזקה תקשה על האקרים לפרוץ לחשבונותיכם.

- במקרה ואורך הסיסמה מוגבל ל 8 תווים – וודאו שסיסמתכם מורכבת מתמהיל של אותיות, ספרות וסימנים.
- במידה ואורך הסיסמה מאפשר זאת, שיקלו להשתמש ב- Passphrases כסיסמתכם- Passphrase הנה סיסמה המורכבת ממשפט או מחיבור של כמה מילים. הנה הדרך הנכונה ליצירת Passphrase ב- 2 צעדים פשוטים:
בחרו שלושה מילים מקריות – למשל: book, water, lightning (ספר, מים וברק). רק שימו לב שמספר האותיות שלהן שווה או עולה על 12).
- ערבבו אותן – רוב האתרים ידרשו שסיסמתכם תכיל גם ספרות וסימנים על כן אתם יכולים להוסיף את המינימום ולהשתמש ב- **Book1waterlightning!** כסיסמתכם. אין צורך להשתולל עם הוספת הספרות והסימנים, ודאו כי התוספות למילים שבחרתם קלות לזכירה.

הונאות

- שימו לב, פושעי סייבר לא מגבילים את עצמם לערוץ הדוא"ל. ניתן להונות אותנו גם באמצעות הודעות במדיה החברתית ולנסות לפתות אותנו למסור להם את פרטינו האישיים או הפיננסים. זכרו:
- אין מתנות חינם!
- לא לוחצים על קישורים או פותחים צופות בהודעות המתקבלות ממקור לא ידוע.
- גם אם ההודעה מתקבלת ממישהו מוכר – בחנו את ההודעה עצמה, האם היא מוזרה? לא תואמת את הסגנון או לא "נשמעת" כמו המכר?

עבודה

- על מנת שלא לחשוף את מקום עבודתכם לסיכונים:
- זכרו כי אנכם מייצגים את עבודתכם ברשתות החברתיות – אם ברצונכם לכתוב משהו הקשור לעבודתכם, התייעצו עם

הממונים עליכם תחילה.

באותה מידה חשבו פעמיים לפני שאתם מעלים תמונות שצולמו בעבודה על מנת שלא לחשוף מידע רגיש. ב- LinkedIn, חשבו פעמיים לפני פרסום תפקידכם והמערכות אתן אתם עובדים. באם אנכם בטוחים, התייעצו עם הממונה עליכם.

תנאי שירות

השתדלו להכיר את תנאי השירות והמגבלות של הרשתות, שימו לב מכיוון שמה שתפרסמו עלול להפוך לנכס של הרשת (בהסכמתכם לתנאי השירות כמובן).

איך נגן על ילדינו ברשת?

טיפ מודעות



מס' 5

אז איך אנחנו עושים את זה? פשוט מאוד:

דאגו ליצור סביבה פתוחה ותומכת עם ילדיכם – הראו עניין אמיתי בפעילותם ברשת, התעניינו במשחקים שהם משחקים בהם, בתחומי העניין שלהם בכל הנוגע לפעילותם האינטרנטית.

הרבו בשיחות עם ילדיכם בנושא הבטיחות ברשת והסכנות האורבות בה.

הדגישו את מושג האמינות והזהות ברשת – לא כל הנוצץ זהב הוא - לא כל מה שהם רואים או כל מי שהם מכירים Online מופיעים בזהותם האמיתית.

היו ערניים לשינויי התנהגות אצל ילדיכם – למשל, אם ילדיכם מפסיק באופן פתאומי להשתמש במחשב, ייתכן שהם חווים בריונות ברשת, שימו לב לשינויים קיצוניים במצבי רוחם.

בדקו באופן קבוע את אבטחת המידע ומדיניות הפרטיות של האתרים בהם ילדיכם גולשים – וודאו כי המדיניות והתניות אבטחת המידע מגינות על זהותם של ילדיכם.

ודאו כי הטלפונים הסלולאריים שלהם מוגנים: שימוש בקוד נעילה ובסיסמאות, התקנת אפליקציות רק מחנויות רשמיות ובדקו את ההרשאות שניתנו לאפליקציות המותקנות על מכשיריהם.

במקרים רבים **קיימות תוכנות אשר יכולות לסייע לכם לנטר אחר פעילות חריגה באתרים** או במחשב של ילדיכם. בעניין זה, קיימות למשל הרבה תוכנות אשר מאפשרות בקרת הורים לגבי התכנים אשר ילדיכם ייחשפו אליהם.

פעולות בסיסיות ופשוטות אלו יסיעו רבות לשמירה על ביטחון ילדיכם ברשת.

ההורים של היום עומדים בפני צבר דאגות חדש לגמרי בכל הקשור להתנהלות ילדיהם והסכנות האורבות ברשת, שהרי הילדים של היום חשופים לרשת האינטרנט בגיל צעיר מאוד, לרובם יש אף טלפון חכם החל מגיל צעיר והם "מחוברים" לעולם האינטרנטי 24/7.

אך האמת היא שרוב הילדים אינם מודעים להיקף הסכנות שאורבות להם ברשת, סכנות כגון פשיעת סייבר, מתחזים ותוכן לא הולם.

בתור הוריהם, זוהי האחריות שלנו ללמד אותם כיצד להתמודד עם הסכנות האורבות להם ברחבי הרשת.





כך תתמודדו עם הונאות טלפוניות

טיפ מודעות



מס' 6

רווח כספי, אך ייתכן ובחלקן תתבקשו לעשות פעולות אחרות כמו שליחת דוא"ל, העברת מסמך למישהו וכו'. לעיתים, שיחות **ווישינג** יכולות להגיע לכאורה מאנשים מוכרים. קרוב משפחה רחוק, מישהו שמטפל באחד הילדים שנקלע לצרה פתאומית, מנכ"ל החברה שצריך עזרה בהולה, נציג רשות ממשלתית שרוצה לסגור חוב או סט של תצורות אחרות. זכרו שהתוקפים רוצים לנצל את האמון שאתם רוכשים למתקשר או להקשר הדברים הנאמרים. כמו גם, התקפות אלו כוללות מסגרת זמנים בהולה. המתקשר מבקש שתעשו פעולה מיידית כדי להציל את המצב.

באותה תקופה פנו אלמונים מארגון הפשיעה של סופר בדואר אלקטרוני לעובדי מחלקת הנהלת החשבונות של 18 חברות אוסטריות, התחזו למנכ"ל או לאנשים מטעמו והנחו את העובדים להעביר סכומי כסף גדולים לשם מימון עסקי. העובדים הונחו לשמור על מידור מפני גורמים אחרים בחברה. מהות ההתקפה היא שימוש בשיחה טלפונית לצורך התחזות לגורם בר סמכא עבור הקורבן והיא מתויגת תחת קבוצה התקפות העושות שימוש **בהנדסה חברתית**.

ההתמודדות עם התקפות מסוג זה אינה פשוטה, אך אפשרית. **הכלל הראשון הוא להטיל ספק** בכל גורם שמתקשר אליכם ומבקש שתבצעו פעולה כלשהי עבורו. לרוב, הונאות מטרת הונאות אלו הוא

מקרה שנחשף לאחרונה על ידי משטרת ישראל מדגיש את העלייה בשימוש רמאים בהונאות טלפוניות הנקראות גם **Vishing** בלעז. שילוב בין קול (Voice) **ודיוג** (Phishing). במסגרת פרסום המקרה, נכתב כי המחלקה הבינלאומית בפרקליטות המדינה הגישה עתירה לבית המשפט המחוזי להכריז על אזרח ישראלי כבר הסגרה לאוסטריה, לצורך העמדתו לדין בגין עבירות הונאה חמורות. על פי בקשת ההסגרה, במהלך השנים 2015-2017 נטל אותו אזרח חלק מרכזי בפעילותו של ארגון פשיעה שהונה חברות אוסטריות והוציא מהן במרמה סכומי עתק. על פי דפוס הפעולה, המכונה **"הונאת מנכ"ל"** או "הונאת נשיא".



לאמת את זהות הצד השני, הכלל המומלץ הוא לא לשתף פעולה. אם בכל זאת את חוששים מהתוצאה, בקשו מהצד השני שם ותפקיד, נתקו את השיחה ויזמו בעצמכם טלפון לאותו גורם. חפשו לבד את הפרטים ברשת ואל תסתמכו על פרטים שהוא נותן לכם, הם עלולים להיות פרטים מזויפים.

אין ספק כי מתקפות וישינג הן וקטור תקיפה מוצלח, בעיקר בשל האמון שבני אדם נוטים ליחס לקול אנושי בשונה מטקסט כתוב בהודעות דוא"ל. עם זאת, על מנת להימנע מליפול קורבן למתקפות כאלו, עלינו להיות יותר ספקניים - להפעיל 'תחושות בטן', לנסות להבין מי יכול להיות בצד השני ומדוע הוא מבקש מאתנו לבצע פעולות ולנסות כמה שניתן להימנע מלחץ ולפעול לאימות הדברים הנאמרים.

הטלת ספק תוביל אתכם לאמת את זהות המשתמש או הקשר הדברים. אם השיחה מתבצעת ממספר חסום או לא מוכר, בקשו אמצעי אימות נוסף. אם המתקשר טוען שהילד נמצא בצרה - בקשו לדבר אתו או נתקו ונסו להתקשר לילד בעצמכם. אם המנכ"ל מבקש פעולה פיננסית בהולה, צרו קשר ישיר עם המנכ"ל ושאלו האם הבקשה הגיעה ממנו ותמיד הקפידו לעבוד על פי הנהלים. לעיתים, התקפה כזו מתחילה בדוא"ל המבקשת מהקורבן להתקשר למספר טלפון מסוים כדי להסדיר חוב. בכל מקרה כזה, רצוי לוודא את נכונות הפרטים. אם ישנו חוב בבנק לחברה, בדקו מול הנהלת חשבונות.

צעד הגנתי נוסף הוא להפנים שלא נותנים פרטים אישיים בטלפון לאנשים שלא מכירים באופן אישי. חלק מהתקפות **8 הוישינג** נועדו בין היתר לאסוף פרטי גישה של הקורבן לשירותים פיננסיים או אחרים. במידה ואינכם יודעים או יכולים

ההונאות הרווחות ברשת וכיצד להתמודד עמן

טיפ מודעות

מס' 7



סחיטה מינית

הקורבן מפותה לקיים קשר מיני וירטואלי (סקס וירטואלי) באמצעות הרשתות החברתיות ואתרי היכרויות כשבשלב כלשהו מודיע הסוחט, או אדם אחר מטעמו, לקורבן כי הוא צולם בשעת מעשה. הקורבן נדרש לשלם סכום מסוים, אחרת הסרטון יופץ באינטרנט. מקרים נוספים כוללים מכתבי איום אנונימיים עם דרישת כופר בגין, לכאורה, חומר מיני בו מופיע הקורבן.

התמודדות

יש להימנע מתיעוד / צילום של ביצוע מעשים מיניים. יש להימנע משיחות וידאו עם אנשים שאינם מוכרים באופן אישי. מומלץ

לחסום את שיתוף רשימת החברים ואת הפרופיל לצפייה רחבה ביישום הוידאו צ'אט. בנוסף לידיעתכם, ברוב המקרים בהם נשלח מכתב סחיטה לקורבן מדובר בניסיון שאין מאחוריו ראיות ממשיות – המקרה זה מומלץ לגשת למשטרה ולדווח על כך.

הצעת עבודה

הקורבן מקבל פנייה ברשת חברתית, לרוב בלינקדאין, מאדם זר המתיימר להיות איש כוח אדם או מנהל בדרג מסוים בחברה מתחום עיסוק דומה או זהה. הגורם הפונה מחזיק בפרופיל עדכני וכזה הכולל היסטוריה ועוקבים על מנת לספק לקורבן מצג שווא אמין. לאחר קניית אמונו של הקורבן הכוללת בקשת חברות, תוצע לקורבן משרה נוצצת כתלות במילוי טופס. מילוי הטופס ושליחתו

תשאיר את הפרטים האישיים בידי התוקף. במקרים מסוימים נוצל ערוץ זה לצורך ריגול מדינתי או עסקי (גיזס בפועל).

התמודדות

יש להימנע מיצירת קשר עם אנשים זרים ברשת כולל הימנעות משליחת פרטים אישיים. מומלץ לעדכן את הפרופיל האישי ברשת במידה שלא תסגיר את הפוזיציה הארגונית וכן מומלץ לא לעדכן פרטים נרחבים אודות פרויקטים בפועל. בכל פניה חשודה יש לדווח לממונים.

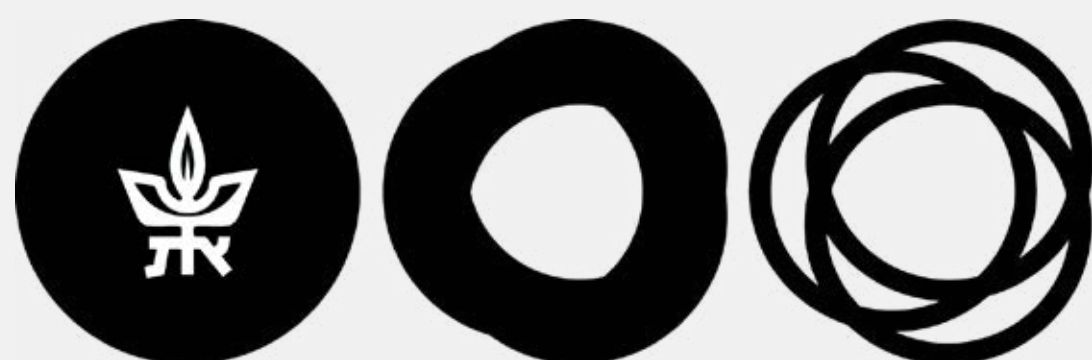
הונאות העברת כספים

(Compromise Email Business) - הדרך הנפוצה והמוכרת לביצוע הונאות העברת

כספים היא באמצעות דואר אלקטרוני או שיחת טלפון. מטרת התוקף היא לגרום לקורבן לתחושת לחץ תחת בקשה של גורם בכיר בחברה, בדרך כלל המנכ"ל. ייתכן כי הונאות אלו יבוצעו גם על ידי התחזות למס הכנסה או כל ארגון אחר. לרוב, התוקף יאסוף מודיעין על מנת ליצור אמינות בפניה (שמות, צורך ביטוי בכתב) ויבקש מהקורבן לבצע העברה בנקאית מחשבון הארגון או מחשבוננו הפרטי של הקורבן לחשבון בשליטתו.

התמודדות

רצוי לוודא בפניה ישירה לגורם הפונה שאכן הוא זה שביקש להעביר כסף. בעת קבלת החלטות תחת לחץ רצוי להתייעץ עם חבר לעבודה. בכל פניה חשודה יש לדווח לממונים.



TEL AVIV אוניברסיטת
UNIVERSITY תל אביב

