משרד ראש הממשלה
מערך הסייבר הלאומי
הרשות הלאומית
להגנת הסייבר

Black Friday

עצות לקנייה בטוחה באינטרנט

הערכים שלנו: מנהיגות, צניעות, שיתוף ומקצוענות

לקראת חג המולד, ראש השנה האזרחית, וה-Black Friday שיחול ביום שישי ה-24.11.17, עסקים ואתרי אינטרנט רבים ברחבי העולם ובישראל יוצאים בשלל מבצעים ומחירים אטרקטיביים. תקופה זו מאפשרת לנו ליהנות מהזדמנויות בכל רחבי הגלובוס, אך במקביל מהווה גם כר פורה לפשעי סייבר ומתאפיינת בריבוי הונאות ומלכודות רשת.

מה מומלץ לעשות כדי ליהנות מקנייה בטוחה?

1. הכינו את המחשב שלכם לחגיגת הקניות

- **מה זאת אומרת "להכין את המחשב"?**

מחשבים (לתשומת ליבך, גם מכשיר נייד הוא מחשב) מופעלים באמצעות תוכנת מערכת הפעלה. גם האפליקציות שלנו הן תוכנות, ומערכות האנטי-וירוס וחומת האש (Firewall) גם הן תוכנות. ספקי התוכנה השונים מוציאים לשוק אחת לתקופה עדכונים לתוכנות אלו. בין עדכונים אלו נמנים לרוב גם **עדכוני אבטחה**. עלינו לוודא שעדכונים אלו יותקנו על המכשירים שלנו.

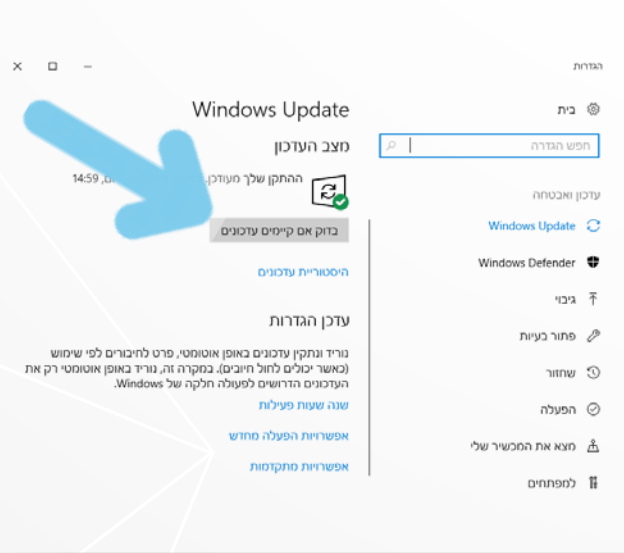
- **למה זה חשוב?**

עדכון אבטחה נועד לתקן כשל במערכת או פרצת אבטחה. עצם פרסומו של העדכון ברבים, חושף את הפרצה בפני גורמים בעלי כוונות זדון, אשר ימהרו לנצל את פרק הזמן העובר עד אשר כולנו נתקין את העדכון. לפיכך, **מערכת הפעלה** מעודכנת בכל העדכונים הנדרשים, עם **תוכנת אנטי-וירוס** ו**חומת אש** (Firewall) מעודכנים, תקשה על תוקפים פוטנציאלים ואולי אף תשכנע אותם לעבור הלאה ולחפש מחשב לא מעודכן שישמש טרף קל יותר. גם ה**דפדפן** מהווה קרקע פורה לתקיפות סייבר, ולכן יש לשמור על דפדפן מעודכן לגרסתו האחרונה. ולסיום, רצוי להקפיד כי יתר ה**אפליקציות** שלנו (כמו אפליקציות מדיה חברתית, אפליקציות מוזיקה וכו') מעודכנות באופן קבוע.

- **איך עושים את זה?**

ניתן להפעיל הגדרות של **הורדת עדכונים אוטומטית** או לחלופין **לבדוק באופן יזום** האם קיימים עדכונים חדשים.

בנוסף, אם טרם התקנתם על המכשיר שלכם תוכנת אבטחה, רצוי להתקין לפחות תוכנת אנטי וירוס וחומת אש אמינה. ניתן להתקין גם חבילת אבטחה מקיפה יותר, הכוללת מנגנון לזיהוי וירוסים, אנטי-פישינג נגד אתרים מתחזים ועוד.



2. ודאו שלא ניתן לנחש את הסיסמה שלכם בקלות

- **למה זה חשוב?**

להאקרים ולפושעי סייבר יש כלים המאפשרים להם לגלות מהי הסיסמה שלכם, אם הסיסמה "קלה לניחוש".

- **איך עושים את זה?**

יש להקפיד לבחור **סיסמה ארוכה בעלת 8-12 תווים לפחות**, אשר תקשה על ניחושה. סיסמה כזו, רצוי שתכלול **שילוב של אותיות קטנות, אותיות גדולות, מספרים ותווים מיוחדים נוספים**. חשוב מאוד **לא להשתמש באותה סיסמה** לשירותים וחשבונות שונים ברשת, כך שגם במידה ותיבת הדוא"ל נפרצה, חשבון הבנק, או חשבונות ברשתות חברתיות לא יהיו בסכנה.

בכדי להקשות באופן מיטבי על פריצת הסיסמאות שלכם, מומלץ להשתמש ב**אימות דו-שלבי** היכן שניתן. אימות דו שלבי מאפשר משלוח קוד חד פעמי אל המשתמש, באמצעות הודעת טקסט אל הנייד שלו או באמצעות אפליקציה ייעודית ליצירת קודים. את הקוד, נדרש המשתמש להזין בכניסה לשירות המבוקש (בד"כ רק בפעם הראשונה) כשלב שני לאחר הזנת הסיסמה הרגילה.

3. אל תסמכו על WiFi חינמי

- **מהו WiFi חינמי?**

במקומות רבים קיימות רשתות Wi-Fi פתוחות לציבור, שאליהן ניתן להתחבר ללא סיסמה.

- **למה זה חשוב?**

במקרים רבים מדובר ברשתות שקל מאוד להאזין לתעבורת התקשורת שלהן ובכך גם לאסוף מידע. לכן, מומלץ **לא להעביר פרטים רגישים ברשתות Wi-Fi ציבוריות** או **חינמיות** ולא לבצע קניות כאשר מחוברים לרשת מסוג זה.

- **מה מומלץ לעשות?**

אם הרכישה סובלת דיחוי, עדיף להמתין עם הקנייה או התשלום עד שתגיעו למחשב עם חיבור ל-WiFi מאובטח. אם אתם ממש חייבים לרכוש משהו באמצעות הסמארטפון, עדיף להשתמש בחיבור האינטרנט של הרשת הסלולרית שלכם, מאשר להשתמש ברשת חינמית כלשהי.

4. בדקו את אמינות המוכר

- **היכן מומלץ לקנות?**

העדיפו לחפש את המוצרים באתרי הקניות המוכרים ובעלי המוניטין.

- **למה זה חשוב?**

לעסקים המוכרים והידועים יש לרוב אבטחה מבוססת יחסית והם בטוחים יותר לשימוש.

- **איך עושים את זה?**

טרם הרכישה מומלץ לוודא כי האתר ממנו מבצעים את הרכישה **אמין**. אם האתר אינו מוכר, כדאי לערוך עליו בירור מוקדם. ממצאים שליליים אודותיו צריכים להדליק נורה אדומה ורצוי להתרחק ממנו. רצוי לבדוק כי לאתר יש גם **כתובת** פיזית ליצירת קשר ו**מספר טלפון** דרכו ניתן לקבל שירות לקוחות.

5. העדיפו להשתמש באפליקציות או באתרי החנויות הרשמיים

- **למה זה חשוב?**

פושעי הרשת עלולים ליצור אתרים מתחזים, שנראים בדיוק כמו אתרים פופולאריים כגון אמזון, eBay ועוד, באמצעותם הם יכולים "לגנוב" את פרטינו האישיים וגם את כספינו. גם בנייד עלולים ליצור אפליקציות זדוניות המנסות לנצל את הטעויות של הקונים בחיפוש אחר אפליקציות רשמיות. אפליקציות אלו בנויות כדי להטעות משתמשים להזין פרטי כרטיס אשראי או להוריד תוכנות זדוניות כדי לגנוב פרטים אישיים או לנעול את המכשיר עד שהמשתמש ישלם כופר.

- **איך עושים את זה?**

מומלץ **לגלוש אל אתרי החנויות ישירות מהדפדפן שלכם** - ולא באמצעות לחיצה על קישורים בפרסומות או מבצעים, שייתכן שנתקלתם בהם ברשתות החברתיות או בתיבת הדואר האלקטרוני שלכם. חיפוש בגוגל לרוב מביא את האתרים המקוריים ולא גרסאות פישינג מתוחכמות. במידה וכן הגעתם לאתר דרך פרסומת - חשוב **לוודא כי כתובת האתר היא הכתובת הנכונה והמדויקת**, משום שגורמים זדוניים ברשת משתמשים לעיתים באתרים בעלי כתובות דומות מאוד על מנת להטעות את הגולשים.

דרך נוספת היא להשתמש באפליקציות הרשמיות שלהם - **הורידו אפליקציות רק מחנויות אפליקציות רשמיות** כמו Google Play או Apple App Store. בדקו את הפרטים של האפליקציה לפני ההורדה. שימו לב למפתחים ולאיות של שם המותג.

6. רגע לפני הרכישה הגדולה, ודאו שהפרטים שרציתם למסור למוכר מגיעים רק אליו

HTTPS

- **כיצד עובר המידע שלנו אל בית העסק?**

המידע שעובר ביניכם לבין בית העסק (למשל, מספר כרטיס האשראי שהקלדתם מהנייד שלכם באתר האינטרנט שלו) יכול לעבור בשתי תצורות: מידע בתוך מוצפן ומידע בתוך גלוי.

- **למה זה חשוב?**

כאשר בית העסק עובד בתוך גלוי, אזי תוקף פוטנציאלי יהיה מסוגל ליירט את תעבורת הנתונים אותם הקלדנו ולהשתמש בפרטינו האישיים (לדוגמה, התוקף יכול "לגנוב" את מספר כרטיס האשראי שלנו) לצורך גניבת זהות, גניבת כספים ועוד.

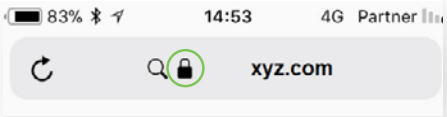
- **איך בודקים את זה?**

"שיטת העבודה" הנפוצה בתוך מוצפן נקראת SSL.

לפני שאתם ממלאים פרטים אישיים או מבצעים רכישה, **בדקו את שורת הכתובת של הדפדפן**. לצד כתובת האתר הרגילה (http), באתר מאובטח תופיע גם האות **S** באנגלית (**https**). באתרים חדשים אף יופיע הכיתוב בתחילת השורה **בצבע ירוק** (לעיתים הכיתוב ולעיתים הרקע, תלוי בסוג הדפדפן). סימן נוסף לכך יהיה בצורת **מנעול סגור** המופיע בשורת הכתובת או בתחתית הדף.

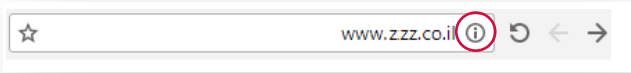
דוגמה בנייד:

- יופיע סימן של מנעול סגור



- לעיתים לחיצה על שורת הכתובת תציג את הכתובת המלאה:

- אם תחילתה של הכתובת צבועה ב**אדום** יחד עם קו אלכסוני המתוח על ה-https, או אם מופיע סימן קריאה (**!**) בתוך עיגול ליד הכתובת, סימן כי האתר אינו מאובטח ולא ניתן לסמוך עוד על הצפנת החיבור:



7. החלטתם לרכוש? ודאו שפרטי כרטיס האשראי שלכם מוגנים

- **כיצד בית העסק משתמש בפרטי כרטיס האשראי שלנו?**

חמש חברות האשראי (American Express, Discover, JCB, MasterCard, Visa) חברו יחדיו וקבעו תקן לאבטחת התשלום בכרטיסי אשראי. תקן זה נקרא תקן **PCI DSS**.

- **למה זה חשוב?**

התקן מבטיח הגנה על נתוני כרטיסי אשראי בכל סביבה בה הם מאוחסנים, מועברים או מעובדים, והוא אף כולל דרישות ליישום בקרות אבטחת מידע בארגונים המטפלים בפרטי כרטיסי אשראי. כך הסיכוי שפרטי כרטיס האשראי שלנו "יזלגו" מבית העסק לתוקף פוטנציאלי קטנים משמעותית.

- **איך בודקים את זה?**

אתר העומד בתקן, **יצהיר בדף התשלום** כי מנגנון אבטחת התשלום באתרו **עומד בתקן** PCI DSS.

8. לחלופין, במקום כרטיס אשראי, השתמשו באלטרנטיבות

- **למה זה חשוב?**

אפילו אם נקטנו בכל אמצעי הזהירות שפורטו לעיל, הסכנה שפרטי האשראי שלכם ייגנבו עדיין קיימת, ולא תמיד נדרש תחכום רב כדי "לגנוב" אותם.

- **איזה אלטרנטיבות קיימות?**

ישנן מספר אלטרנטיבות. אחת מהן היא שימוש ב**שירותי ארנק אלקטרוני מאובטחים**, המאפשרים ביצוע רכישה או קבלת תשלומים באינטרנט מבלי לחשוף כל מידע פיננסי הקשור לחשבון.

אלטרנטיבה נוספת היא **כרטיס אשראי טעון מראש** (Prepaid). הכרטיס מאפשר הטענה על פי תקציב מוגדר מראש ויכול לשמש לביצוע רכישות מקוונות ברשת תחת מסגרת ברורה. ניתן לרכוש כיום כרטיסים מסוג זה לקניות בישראל ובחו"ל, כאשר הכרטיס טעון מראש במטבע חוץ.

9. היזהרו מהודעות חשודות

- **מהן הודעות חשודות?**

הודעת דוא"ל או הודעת טקסט (מסרון/SMS) תמימה כביכול, המגיעה לתיבה ומציעה הצעה שיווקית קוסמת, מוצר נחשק במחיר מפתיע או זכייה בפרס כספי. פעמים רבות ההצעה נראית טובה מדי מכדי להיות אמיתית, כמו "אייפד חינם בכל קניה" או מוצרים נחשקים במחירים בלתי הגיוניים. הצעה כזו יכולה להופיע גם בפוסט פרסומת בפייסבוק.

הודעה חשודה נוספת הינה הודעה הקשורה לכאורה לחשבונית או קבלה (invoice, receipt) ממקור לא מוכר או בעלת סימנים מחשידים (נושא שאינו בהכרח קשור לשולח או לסוג ההתקשרות, שגיאות כתיב מוזרות).

- **למה זה חשוב?**

חלק ניכר מהתרמיות ומלכודות הרשת מתחילות בפתיחתה של הודעה כזו, בעקבותיה (לרוב ללא ידיעת הנתקף) התוקף מחדיר אלינו פוגען. פוגען כזה עלול "לגנוב" מידע פרטי ולהעבירו לתוקף ללא ידיעתנו, ועלול לפגוע בנו בדרכים שונות, למשל להצפין את המידע שלנו ולדרוש כופר תמורת פתיחתו.

בחודשים האחרונים פוגענים רבים מתפשטים באמצעות הודעות הקשורות לחשבונית או קבלה. במקרים רבים אחרים מתקבלת מאתר מתחזה הודעת דוא"ל המבקשת לאשר רכישה או להכניס פרטים אישיים, או נשלחים מסרונים לטלפונים ניידים בצירוף קישור ובקשה ל"עדכון פרטי התשלום".

שימו לב כי עסקים, חברות ואתרים לגיטימיים לא יבקשו מידע שכזה באמצעות הדוא"ל.

- **מה צריך לעשות?**

הימנעו מפתיחה של דוא"ל חשוד המגיע ממקור לא מוכר, או ממקור מוכר המציג סימנים מחשידים (נושא שאינו בהכרח קשור לשולח או לסוג ההתקשרות, שגיאות כתיב מוזרות).

אל תפתחו קבצים חשודים המצורפים להודעה, גם אם הם נראים תמימים לכאורה.

אל תקליקו על קישורים בגוף ההודעה או בפוסט חשוד - פתחו חלון דפדפן והיכנסו ישירות לכתובת הרצויה.

אל תספקו מידע אישי ופיננסי אם התבקשתם למסרו באמצעות הודעת דוא"ל או מסרון המגיעים אליכם "בהפתעה", ללא פעולה יזומה מקדימה שלכם למול האתר הלגיטימי, או דרך מדיה חברתית.

בעת שיטוט באתרים, **אל תגיבו לחלונות קופצים** (Pop-Up) חשודים המבקשים מכם את המידע הפרטי שלכם או המבטיחים לכם פרס אם תענו על שאלה או על סקר קצר, **סגרו אותם מיידית**.

הקשיבו לתחושת הבטן: אם זה נראה טוב מדי מכדי להיות אמיתי... כנראה שזה לא אמיתי!

10. בדקו את חשבון הבנק שלכם

- **למה זה חשוב?**

עיון בפירוט החיובים של כרטיס האשראי שלכם

עשוי לגלות לכם האם נפלתם קורבן למזימה או הונאה כלשהי.

- **מה צריך לעשות?**

מומלץ לשמור את קבלות הרכישה ו**לעבור באופן קבוע על פירוט חשבונות האשראי**, על מנת לוודא כי אין פעולות או חיובים חריגים. אם גיליתם בפירוט החיובים עסקאות שבוודאות לא ביצעתם, דווחו על כך מיד לחברת האשראי.

מומלץ להגדיר התראות באמצעות חברת האשראי או הבנק שלכם, כך שתקבלו מסרון או דוא"ל על כל רכישה המתבצעת בכרטיס האשראי. הגדירו התראות עבור סך רכישות מעל סכום מסוים כדי להגן על רכישות מרובות של סכומים נמוכים. ניתן גם להגדיר התראות רק על רכישות מחו"ל.

לסיכום, כדאי לזכור -

גם אם אתם קונים ותיקים באתרי אינטרנט פופולריים, אין משמעות הדבר שאתם חסינים מפני תקיפות, ניצול חולשות או ניצול חוסר תשומת לב.

אמצעי הזהירות והפעולות המוצעות במסמך זה עשויות, במידה רבה, להגן על המידע האישי והפיננסי שלכם.

קניות בטוחות ומוצלחות!

10 הדיברות **לקנייה בטוחה באינטרנט**