המידע שלכם חשוף!

5 הטעויות הנפוצות בשמירה על מידע

ארגונים ועסקים פועלים כל העת על מנת לשמור על המידע הארגוני ולהתנהל בצורה בטוחה ברשת. למרות זאת, מדי פעם מתפרסמות ידיעות על פריצות למידע רגיש של חברות שונות. בבחינה של הגורמים המרכזיים המאפשרים את דליפת המידע, ניתן למנות סיבות הקשורות בתוכנה, סיבות הקשורות בחומרה, אך בעיקר, סיבות הקשורות לגורם האנושי. **במאמר זה נתמקד בגורם האנושי.**

אין ספק שאף אחד לא מעוניין לגרום נזק למחשב שלו או למערכת המידע הארגונית. אולם רבים מאתנו מורגלים לפעול בצורה שלרובנו תיראה תקינה, אך בפועל, תחשוף את המחשב והטלפון הנייד שלנו לפריצות, תסכן את המידע הפרטי שלנו ותפתח פתח למידע השייך לארגונים בהם אנו עובדים. הבשורה המשמחת היא שעם מודעות לסכנות וביצוע פעולות פשוטות, ניתן להימנע מחשיפה שכזו. אז מהן הטעויות הנפוצות וכיצד ניתן להימנע מהן?

1

טעות ראשונה – **פתיחת אוטומטית של קישור מצורף למייל או סמס.**
מדוע זו טעות? אנו מקבלים כל יום אינספור מיילים וסמסים, שברבים מהם יש קישור המעביר לקובץ או לאתר אחר. העומס היומיומי שכולנו חווים, גורם לרבים מאיתנו להקליק על הקישור ללא שהקדשנו מחשבה לכך שפתיחת קישור לא מזוהה עשויה להעביר אותנו לאתר משוטה, להכניס וירוס למחשב שלנו ובמקרים חמורים אף לאפשר להאקרים לנעול את המחשב ולדרוש כופר תמורת שחרורו.

הפתרון - סגלו לעצמכם הרגל: לפני הקלקה על קישור, ודאו שאתם מזהים את השולח ושהקישור לאתר נראה תמים. כלומר כתובת אתר ברורה וידועה, במבנה של כתובת רשת לגיטימית (למשל – www.website.com/extension או website.co.il/page). חשוב לשים לב שאין טעות או שגיאה בשם האתר. זכרו, אם יש ספק אין ספק. כלומר, אם חבר או קולגה שלח לכם מייל או סמס עם קישור שנראה מוזר – צרו קשר עם השולח וודאו שאכן הוא שלח לכם לינק מרצונו.

2

טעות שנייה – **שימוש באותה הסיסמה לכל התוכנות, המייל הארגוני והאישי, חשבונות ועוד.**
מדוע זו טעות?
בעולם הפיזי, יש לכם המון דלתות ולכל אחד מנעול אחר. המטרה היא שאם מפתח אחד הולך לאיבוד או נגנב, רוב המנעולים האחרים שלכם נשארים בטוחים. העולם הווירטואלי זהה מבחינת הרציונל אך גניבת סיסמאות בו יותר קלה בצורה משמעותית.

הפתרון - קודם כל, חשוב לבחור סיסמאות חזקות. סיסמה חזקה מורכבת משילוב של אותיות גדולות, קטנות, מספרים וסמל מיוחד כלשהו. כמו כן, מומלץ לבחור מספר סיסמאות שונות לאתרים וחשבונות שונים והפרידו בין סיסמאות של חשבונות אישיים וארגוניים. כך תפחיתו את הסיכון.

3

טעות שלישית – **אישור אוטומטי להרשאות שונות בעת הורדת תוכנה או אפליקציה.**
מדוע זו טעות? בכל פעם שאתם מורידים תוכנה חדשה או אפליקציה חדשה למחשב או הנייד, אתם נדרשים לאשר הרשאות לשימוש במידע במחשב לצורך הפעלת האפליקציה החדשה. האקרים עשויים לנצל הרשאות שנתתם כדי להשיג גישה לקבצים ולמידע אישי ועסקי.

הפתרון: על מנת להימנע ממצב של פריצה לכלל החשבונות שלכם, יש לוודא שאתם מורידים אפליקציה בטוחה מחנות אפליקציות מוכרת. וכן שאתם מסירים הרשאות שאין בהן צורך אמיתי להפעלת האפליקציה.

4

טעות רביעית – **שימוש בדיסק און קי מהבית במחשב שבארגון.**
מדוע זו טעות? פעמים רבות אנו חושבים שהמחשב הפרטי שלנו נקי ושמור. עם זאת, רובנו לא נבחין אם הותקנו על המחשב הפרטי שלנו תוכנות רוגלה למיניהן, כאלה המנטרות את המידע שעובר במחשב. שימוש בדיסק און קי והעברתו מהמחשב הביתי למחשב הארגוני, עשויה לחשוף את המחשב הארגוני לסכנות כאלו.

הפתרון: לא מחברים דיסק און קיי פרטי למחשב בארגון. אך פעם. נקודה.

5

טעות חמישית – **גלישה ברשתות וויי-פיי ציבוריות**
מדוע זו טעות? גלישה ברשת ווי פיי ציבורית לא מאובטחת חושפת את המידע שלכם לכל מי שנמצא ברשת הזאת. המידע שעובר ברשת כולל את הסיסמאות שלכם לאתרים אליהם גלשתם (אימייל, פייסבוק, בנק ועוד)

הפתרון: לא גולשים במחשב הארגוני ברשתות ווי פיי ציבוריות. מומלץ מאד גם לא לגלוש עם הטלפון הנייד באותן רשתות בדיוק מאותן הסיבות. במקרים בהם אין ברירה אלא לגלוש במקומות ציבוריים, עדיף להשתמש במכשיר הסלולרי כ"נקודה חמה" שתאפשר גישה לרשת סלולרית פרטית ומאובטחת עבורכם.

לסיכום, סקרנו מספר טעויות התנהלות נפוצות מאוד בקרב אנשים רבים. למעשה, קל מאוד לפעול בצורה בטוחה ומוגנת יותר ברשת, אך הדבר דורש מודעות ונכונות לשנות הרגלים. בצעדים יחסית פשוטים כולנו יכולים לסייע בהגנה על מידע רגיש, הן בסביבת מערכות המידע הארגונית והן במחשבים הפרטיים.

בהצלחה ושנה אזרחית חדשה ומוגנת!

המרכז לחינוך סייבר
CYBER EDUCATION CENTER