



10 טיפים למניעת גניבת זהות במקום העבודה

גניבת זהות זוהי בעיה עולמית ומומחים בתחום מעריכים כי מכול 50 צרכנים (בעיקר כאלו המשתמשים ברכישות באמצעות כרטיסי אשראי) 1 נופל קרבן לגניבת זהות.

למי שחדש לו נושא זה של גניבת זהות: גניבת זהות מתרחשת כאשר מישהו אחר משתמש באינפורמציה האישית שלכם למטרות הונאה ומרמה. גם איסוף כתובות דואר אלקטרוני באופן לא מורשה ושליחת ספאם, הינה סוג מסוים של גניבת זהות.

גניבת זהות זוהי עברה פלילית כאשר השימוש החמור ביותר שנעשה בה על ידי גנבי הזהות הינה להשתמש באינפורמציה שנגנבה, לצורך ביצוע רכישות שונות, לפתוח חשבונות בנקים ולקבל הלוואות בשמכם ועוד. ע"פ הסטטיסטיקה העולמית, ייקח לקרוב הממוצע פרק זמן של 175 שעות עד שיעלה על גניבת זהות ויתחיל לטפל מול הרשויות השונות בנושא, ולעיתים פרק הזמן הזה יכול לארוך גם ימים רבים ואף שבועות, ועשרות אלפי דולרים שאתם חייבים לפתע בגין פעולות אותן לא ביצעתם.

בנוסף להגנות הבסיסיות אשר פירטתי במאמרים הקודמים, למשל: לא לספק לעולם פרטים אישיים באמצעות דוא"ל, לא להגיב למכתבי ספאם – בייחוד כאלו שאינכם יודעים מהו מקורם, ולדאוג שיש לכם במחשב תוכנת אנטי וירוס וחומת אש מעודכנת – דרך אגב, כיום יש מבצע לרכישת תוכנת ההגנה מהטובות בעולם, קספרסקי, במחיר מוזל לשני עמדות מחשב, היום אתמקד ב 10 טיפים אשר יתמקדו בנושא של כיצד להגן על עצמך מגניבת זהות במקום עבודתך.

1. אל תשאירו אפשרות גישה חופשית למידע במחשב העבודה שלכם גישה חופשית הינה אחת הדרכים בהן גנבי זהות משתמשים על מנת לאסוף עליכם מידע.

שאלו את עצמכם את השאלה: לכמה אנשים במקום העבודה יש גישה למחשב שלכם?

אתם צריכים להיות מודעים לקלות בה לעובדים נוספים או ללקוחות לשבת מול עמדת המחשב שלכם בהיעדרותכם

תכנתו את שומר המסך שלכם לנעול את המחשב לאחר מספר דקות בו לא בוצעה במחשב פעולה כלשהי: ודאו כי הכניסה חזרה אל המערכת דורשת סיסמה הידועה רק לכם.

2. אם אין באפשרותכם להשתמש בסיסמה לנעילת המחשב, העבירו את כול המידע אשר מכיל פרטים אישיים כלשהם אל דיסק נייד ונעלו את הדיסק/דיסקטים במקום מוגן.

3. הצפינו את הקבצים שלכם. אם אין באפשרותכם לבצע זאת בעקבות אילוצי העבודה, הצפינו לפחות את המידע במחשב אשר מכיל את פרטיכם האישיים. תוכנה טובה ולא יקרה הקיימת כיום בשוק ומתמחה בתחום זה של הגנת מידע הינה:

==> <http://www.pgp.com>

4. שימו לב לעובדים אשר נהוגים באופן קבוע להסתובב סביב העמדה שלכם ולפטפט איתכם ע"פ רוב הם אינם מתכננים לגנוב את זהותכם. מצד שני ייתכן שהם מבליים סביב העמדה שלכם במטרה לראות את הסיסמא או מידע אישי אחר תוך כדי פטפוט "תמים".

5. במקום להשתמש בסיסמא קבועה אחת לאתרים שונים, בחרו סיסמאות שונות אשר אינן קשורות האחת לשנייה או אליכם, ואחסנו אותן במקום בטוח ללא נגישות לגורמים חיצוניים. כאשר מערכת ההפעלה או אתר מסוים מבקש מכם לשמור סיסמאות, אל תקליקו על אישור.

6. אם החברה בה אתם עובדים מכניסה לשימוש מחשבים חדשים, ודאו כי לאחר שהעברתם את החומר מהדיסק הישן אל המחשב בחדש, הדיסק נמחק בצורה יסודית אשר מקשה את שחזורו. מחיקה רגילה של קבצים הינה קלה ביותר לשחזור על ידי כול אדם בעל ידע בסיסי במחשבים יש תוכנות מסחריות רבות אשר מוחקות את המידע בדיסק הקשיח ללא אפשרות שחזורו. אחת מהתוכנות החינמיות הקיימות הינה:

AbsoluteShield File Shredder . חשוב לדאוג למחיקה יסודית של הקבצים במחשב הישן היות ואינכם יכולים לדעת לאיזה ידיים הוא יגיע בעתיד.

7. בדקו עם אחראי המחשב במקום עבודתכם האם הסביבה המחשובית מוגנת מפני פורצים מקוונים והאקרים במידה ואין הגנה מספקת העלו את הנושא בפני הממונים תוך הארת נושא גניבת הזהות

8. שאלו את עצמכם. האם באמת יש צורך לסחוב את כול כרטיסי האשראי בארנק לעבודה?

עדיף לקחת אתכם רק את המידע האישי שאתם זקוקים לו להתנהלות היומיומית אך גם אז שמרו על הארנק שלכם במקום בטוח ומוגן כאשר אתם בעבודה, עדיף תחת מנעול ומפתח.

9. שאלו שאלות הבהרה כאשר חברים לעבודה מבקשים אינפורמציה אישית שלכם. יכולה להיות לזאת סיבה לגיטימית אך אם עובד מבקש לדעת את מספר תז שלכם שנת הלידה וכד.. יש לכם את הזכות לדעת בדיוק מדוע בררו מדוע האינפורמציה דרושה, איך ישתמשו בה והאם היא תשמר בסודיות

10. שמרו על אבטחת גישה אל הדואר האלקטרוני שלכם כאשר אתם בעבודה. דוא"ל זוהי דרך נפוצה לגנבי זהות אשר פורצים אליו ואוספים אינפורמציה אישית

אם אתם נוהגים לשלם חשבונות שונים דרך המחשב האישי (ארנונה, מים, חשמל..) אל תבצעו זאת המחשב במקום העבודה. שלמו באמצעות בנק הדואר הקרוב במקום זאת