

# עולם הדיגיטאלי

הסכנות הדיגיטאליות במכשירי הבנק האוטומטיים

## זהירות: מצלמים לנו את הקוד הסודי

האיומים הדיגיטאליים מופיעים מכל הכיוונים. עוד לפני פסח קיבלנו פניה דחופה מקורא שביקש לבדוק: האם זה נכון ששימוש תמים במכשיר בנק אוטומטי להוצאת כסף יכול לחשוף את החשבון שלו לגניבה מצד האקרים? וזו לשון ההודעה שהגיעה אליו:

**זהירות - הם פועלים רבות כעת בערב פסח !!**

כנופיה חדשה הגיעה לארץ. הם מדביקים מדבקות בכספומטים שאוספות את נתוני האשראי - וגונבים כסף מאנשים. בכני ברק הגיעו עשרות תלונות למשטרה. יש לעקוב ולהזהר!

הסיפור מפחיד. הסבר מלא לא סופק. היו שמועות על מדבקה דקה ושקופה שמכילה את אבזר הצילום. אולי אם מכסים את הלחצנים עם יד אחת בשעה שמקלידים את המספר הסודי זה יעזור, ואולי גם זה לא. התלונות הגיעו, לפי השמועה, מבני ברק אבל גם מערים אחרות: בת ים, אשדוד. האחרים, בשעת משלוח המכתב, לא אותרו למרות מאמצי המשטרה.

מה עושים?

"בגדול אמרו שאין לזה פתרון ועדיף בימים הקרובים לפחות לא להוציא כסף. אם כבר, אז רק דרך הבנק עצמו". עדיף גם לקנות באשראי מאשר להוציא מזומן לאותה מטרה ולהסתכן.

מה נכון ומה לא נכון? - מ. ה. ב"ב

**בירור**

חיפוש הראה שדיון בזה קיים רק בפורום חרדי שכבר הזכרנו בעבר, פרוג. אחד החברים, PINATI אפילו הביא צילומים לדוגמא של ציוד ההעתקה.



לפי מה שמתואר שם אין הרבה מה לעשות. אלו ההמלצות:

להשתמש בכספומט בתוך בנק ולא מבחוץ. לגנבים יהיה יותר קשה להתקין את אמצעי המעקב שלהם בתוך הבנק.

כאשר מקלידים קוד סודי, יש לכסות את ההקלדה ביד השנייה וכדאי להעביר את האצבעות גם על מקשים אחרים כדי לבלבל.

לשמור מרחק מאנשים אחרים. אם מישו מתקרב מדי לבקש ממנו להתרחק. לא ברור לנו עד היום אם יש ממש בהתראות אלו, אבל למה לא להזהר. אלו ההמלצות הקבועות לכל שימוש במכשיר בנק אוטומטי.

בהצלחה!

## למכשירים אוטומטיים...



כך גישה נוחה לאשנב בלי לעורר תשומת לב. לפי הדיווח, תוך רבע שעה יכול האקר להתחבר למכשיר האוטומטי המסויים שמושך את תשומת לבו. בשעה שלוש בבוקר, מציין Tomsguide, סביר שלא יהיו רבים שיפריעו לו. (דווקא בני ברק, שבה יוצאים ללמוד ותוזרים מלימוד בכל השעות זה אחרת...).

אפשר אפילו לחבר מקלדת בתנאים מסוימים למכשיר האוטומטי. יש "מקשים חמים" מהסוג שמוגדרים במקלדות שלנו וגם כאן אלט + טב מאפשר לעבור תפריטים.

עוד התברר כי רבים מן המכשירים האלו מסתמכים עדיין על חלונות XP, ומערכת ההפעלה הזו, עם כל יתרונותיה ויציבותה (עבור מי שזוכר), אינה ממוגנת היטב. זו אחת הסיבות שהחליפו אותה במתקדמות יותר.

לעתים במכשיר האוטומטי עצמו יש הסרטות של פעילות הקלדות. רק לחשוב שהבנק עצמו אוסף מידע שיכול לשרת את הפורצים...

כאן צריך לציין שכמה תוכנות אבטחה של הבנק, גם של חברות ידועות כמו מקאפי או קספרסקי, עדיין הכילו "פרצות" לטענת חברת פוזיטיב.

בתוכנה אחרת הסיסמה שמאפשרת לגשת למכשיר בתור "מנהל על" עם כל הסמכויות היתה רשומה באנגלית, זמינה לכל האקר מתחיל.

ההאקרים יכלו להוסיף נוזקות למנגנון ההפעלה של המכשיר ולאסוף מידע. אפשר לקנות נוזקות כאלו ברשת האפלה, תמורת 1500 דולרים לאחת. ההשקעה הזו תחזיר את עצמה לנוכלים...

אפשר גם לחבר דיסק און קי ליציאת יו.אס.בי שקיימת גם היא במכשיר. אפשר לשחק שם עם הביט...

הדבר הטוב שאפשר לציין שם הוא שבארה"ב החוק מגן על הקלדות כמעט בכל המקרים בהם נגנב כסף מחשבונם. רק מה? צריך לעקוב אחרי החשבון, לזהות פעילות חשודה, ולדווח מייד אבל מייד לבנק.

העצה האחרונה הזו חשובה גם בארץ. לא ברור אם בישראל פועלים האקרים ברמה של ארה"ב. אפשר רק לקוות שלא. אולם מה שכולנו צריכים לעשות הוא לעקוב אחרי המתרחש בחשבון, לזהות כל פעולה חריגה, ולדווח מייד לבנק.

זה ענין של פה האופיינית גנין דיגיטאלי,

תכת כדי לבצע מיטרד קטן אמצע נובמבר נות כמעט בכל

ראה המכשיר יוב של כספת אצל רובנו, על נות. אבל אפשר ישיר או לפתוח ולכל לקוח של מודעים לה עם התקשורת הזו

ש עם המרכז, לתקשורת של והיתרון היחיד די ומעתיקים או

למחשב של היא שצריך לשם

## מושג במחשבים: חתימה דיגיטאלית

אמנם התופעה המוזרה התרחשה בתוכנה שאינה משמשת בדרך כלל את ציבור קוראינו, אולם היא ממחישה כיצד יכולות להיות תקלות פתאומיות בתוכנה וכיצד מחפשים פתרון ומתמודדים.

מת שכחה לעדכן פרוטוקול תקשורת וגרמה מבוכה ובהלה אצל משתמשים (הבעיה כבר נפתרה... אבל המוניטין נפגע)

מאשר להתעלם ולהסתכן.

יש כאן גם נקודה לזכות תוכנת ESET, ששומרת ומזהה הליכים בעייתיים וחוסמת אותם,

האישורים שלהם.

הבעיה נועדה להיפתר באיחור של כמה שעות ולאחר עידכון של התוכנה הבעיה נעלמה.

פעולתה, התוכנה נזקקת

לשירותים שונים, ושירותים אלו זקוקים לאישור שמעיד שהם

באישור רב

ניסיתי להיכנס יעה של תוכנת ESET. לפיה

בנוע /

ורה ומפחידה