077-5006206
052-6885006

אל תיתפס ברשת - כיצד להיזהר מעבירות הונאה באינטרנט

גלישה באינטרנט טומנת בחובה סכנות רבות, שעולות ככל שמתרבות השיטות בהם נוקטים עבריינים הפועלים במרחב הרשת במטרה להונות את הגולש התם. אחת מהשיטות שנהייתה נפוצה בשנים האחרונות היא שיטת ה"פישיניג" באמצעותה ניתן להשיג סיסמאות לחשבונות הבנק ולכרטיסי האשראי של הקורבנות. עו"ד אסף דוק מסביר מהי הונאה באינטרנט, מהם העונשים הקבועים בחוק בגין עבירה זו, כיצד ניתן להתגונן כנגדה, ומאילו אתרים עלינו לדעת להיזהר.

לא אחת מסתמכים הגולשים על מגוון מערכות אבטחה שיגנו על המידע האישי שלהם במרחב האינטרנטי מפני גניבות והונאות. אמנם, עולם הפשע אשר הולך ומעתיק את עצמו מהעולם הפיזי לעולם האינטרנט מפתח טכניקות הולכות ומתקדמות לביצוע עבירות במרחב הרשת תוך עקיפת מערכות ההגנה השונות וללא סיכון של התגלות. אחת מהשיטות הנפוצות של שימוש באינטרנט לביצוע עבירות מכונה "פישינג", או "דיוג" בעברית.

מהי שיטת הפישינג ברשת?

פישינג הוא אמצעי המאפשר השגת מידע אישי מהגולש כגון קודים סודיים, סיסמאות, פרטי כרטיס אשראי, מספרי חשבונות בנק וכו', באמצעות הודעת מייל או הודעת מסנג'ר שבתוכה קישור לאתר מתחזה. לאחר לחיצה על הקישור, הגולש התמים מוצא עצמו בתוך אתר המבקש ממנו מידע חסוי לשם ביצוע פעולות שונות. אמנם, מה שהוא לא יודע זה שהמידע שהוא מוסר מגיע לידיהם של עבריינים אשר הקימו את האתר והקישורים אליו עבור המטרה הבלעדית של השגת מידע, כספים, או ביצוע פעולות בשמו של הגולש. מדובר בשיטה נפוצה ויעילה, עד כדי כך שעל פי אתר "אנטיפישינג" רק במחצית הראשונה של שנת 2014 היו קיימים למעלה ממאתיים שישים אלף אתרי פישינג ברחבי העולם.

כיצד השיטה עובדת?

הפישינג הינה שיטה פשוטה אך מתוחכמת. מקים אתר הפישינג שולח הודעה המכילה כתובת אינטרנט אשר דומה לאתר אמיתי ואמין, בתקוה שמקבל ההודעה לא יחשוד שמדובר באתר מתחזה. יש לבחון בחינה מדוקדקת את פרטי הכתובת בכדי להבין שמדובר בכתובת מזויפת, ושההודעה אינה הודעה אמתית מאתר אמין. לאחר מכן העבריין ישלח הודעת מייל, או הודעה במסנג'ר דרך הפייסבוק, או לחלופין הודעה דרך פלטפורמה אחרת לקורבן. בהודעה, יימצא קישור ואזהרה לפיה על הגולש ללחוץ על הקישור שבהודעה בדחיפות ולהיכנס לחשבון שלו ממגוון סיבות, כמו: מישהו לכאורה ניסה לפרוץ לחשבון הקורבן, ישנה הצעה משתלמת שלא כדאי לסרב לה, וכו'. לחיצה על הלינק תביא את הקורבן לאתר המתחזה לאתר אמין, בעל אותו לוגו, עיצוב ואפשרויות, אך זהו בעצם צל של אתר ולא האתר האמיתי. לרוב, אתרי הפישינג עושים שימוש בשמן של חברות מובילות כדוגמת: **PayPal**, **Gmail, ebay, facebook, skpe** ועוד.

לאחר שהקורבן יכנס לאתר המתחזה, האתר יבקש מהקורבן להזין שם משתמש או סיסמא, כאשר לאחר הניסיון להתחבר באמצעותם תתקבל הודעה שגיאה או שהמערכת פשוט תתנתק. בשלב זה, הפישינג בעצם הצליח בפעולתו, קרי, הצליח "לדוג" את פרטיו האישיים של המשתמש - שם משתמש וסיסמה, שבהם העבריין ישתמש בזמן הקרוב כדי להיכנס לחשבונו של הקורבן. בפעם הבאה שהקורבן ינסה להתחבר לחשבון המשתמש שלו באתר האמיתי, יגלה שבוצעו בשמו מגוון פעולות כגון משיכות כספים מחשבונות בנק, רכישות שבוצעו בכרטיסי אשראי, הפצת דברי שטנה בפייסבוק, וכדומה.

העונשים הקבועים בחוק בגין הונאה באינטרנט

עבירות הונאה הן עבירות חמורות שתכליתן השגת תועלת ורווח אישי למבצעים אותן. בתרמית ה"פישיניג",

העבריינים משתמשים בסיסמאות של הקורבנות במטרה לגשת לחשבונות הבנק ולכרטיסי האשראי שבבעלותם. הדבר מהווה עבירת התחזות לאדם אחר שנידונה בסעיף 441 בחוק העונשין. על פי סעיף זה, חל איסור להתחזות לאדם אחר, בין אם חי ובין אם מת במטרה להונות. הדין למפר הוראה זו הוא עד שלוש שנות מאסר בפועל.

כמו כן, סעיף 415 לחוק העונשין קובע כי העונש הצפוי לאדם שהורשע בעבירה של קבלת דבר במרמה הוא עד 3 שנות מאסר. במידה והעבירה בוצעה בנסיבות מחמירות הענישה יכולה להגיע לעד 5 שנות מאסר. הנסיבות המחמירות אינן מנויות בחוק אלא נקבעות על-פי מידה והיקף נסיבות ביצוע העבירה.

בנוסף לאמור, על פי הוראה בסעיף 440, אדם הקושר קשר עם זולתו במטרה להונות אחרים עובר עבירה שבגינה עונש מאסר של עד שלוש שנים מאחורי סורג ובריח. זאת ועוד, על פי סעיף 16 לחוק כרטיסי חיוב, חל איסור ליטול או להחזיק בכרטיס חיוב תוך כוונה להשתמש בו או לאפשר לאחר להשתמש בו, שלא בהסכמת הלקוח. המפר הוראה זו דינו שלוש שנות מאסר בפועל. על פי סעיף 17 לחוק כרטיסי חיוב חל איסור לגנוב זהות וכסף באמצעות כרטיסי אשראי במרחב האינטרנט. העובר על כך דינו שלוש שנות מאסר. העונש מזנק לחמש שנות מאסר במידה והעבירה בוצעה בנסיבות מחמירות.

כיצד תוכל להגן על עצמך מפני הונאה?

ישנם מספר כללי זהירות על פיהם יש לנהוג. במידה ותקפיד על כללים אלו, תוכל להמשיך לגלוש ברשת בבטחה:
א. המנע מלמסור את פרטיך האישיים לגורמים שונים, במיוחד פרטים לחשבונות רגישים או כאלו המכילים כסף.
ב. במידה וקיבלת דואר אלקטרוני המכיל לינק, התחבר לכתובת באמצעות דפדפן עצמאי ולא דרך הלינק.
ג. עליך לדעת שבנקים אף פעם לא יוצרים קשר עם לקוחות באמצעות הודעת דואר אלקטרוני.
ד. בדוק היטב כל כתובת של אתר אינטרנט אליה אתה מגיע דרך הודעה כלשהי. קל מאוד לזייף כתובות באמצעות הוספה או השמטה של אותיות.
ה. תמיד תזכור שאין מתנות חינם. כל הצעה שנראית טובה מידי מכדי להיות אמתית או מכילה בתוכה "הצעות חד פעמיות למיניהן" - פשוט המנע מהן. כנראה שמדובר בפישינג.
ו. כל הודעה בכל פלטפורמה המכילה בתוכה בקשה להשבה דחופה ומידית ואשר מכילה בתוכה את פרטי הקורבן, כנראה שהיא פישינג. יש להימנע ממנה.

נפלת ברשת?

קל מאוד ליפול בפח של הונאות ברשת, והנזק הפוטנציאלי מהם הינו רב ביותר. אמנם, כל עוד תדע להימנע להיכנס לאתרים דרך הודעות שאתה מקבל ממקורות לא ידועים, ולהימנע מלחיצה על לינקים שונים, תוכל להמשיך לגלוש באינטרנט בבטחה, כאשר המידע האישי והרגיש שלך מוגן בבטחה. בכל מקרה בו נלקח ממך מידע אישי מהאינטרנט ללא רצונך, יש להיוועץ עם עורך דין פלילי המתמחה בעבירות מחשב ואינטרנט שילווה אותך בהליך המשפטי. במידה ואתה זקוק לייעוץ מקצועי בנושא זה, ניתן ליצור עימנו קשר בטלפון **052-6885006** או להשאיר פרטים ונשמח לסייע ולהציע לך מענה ופתרונות מקצועיים בהתאמה אישית. הפניה אינה כרוכה בהתחייבות כל שהיא מצדך. סודיות מלאה מובטחת.

{*:fast_contact}