

OUCH!

עלון מודעות אבטחת מידע למשתמשי מחשב

קניות באופן מאובטח

סקירה כללית

עונת החגים מתקרבת לרבים מאתנו ובקרוב מיליוני אנשים יחפשו לקנות את המתנות המושלמות. רבים מאתנו יבצעו קניות באינטרנט בחיפוש אחר דילים נהדרים ובנוסף כדי להימנע מהמונים רועשים בחנויות. לרוע המזל, פושעי הסייבר יהיו פעילים גם כן, הם ייצרו אתרי קניות מזויפים וישתמשו בטקטיקות אחרות להונאת אנשים. בעלון זה אנו מסבירים כיצד תוכלו לבצע קניות מקוונות בבטחה ולהימנע מלהפוך לקורבן.

חנויות מקוונות מזויפות

פושעי רשת מייצרים חנויות מקוונות מזויפות המחקות את המראה של אתרים אמיתיים או שמתמשים בשמות של חנויות או מותגים ידועים. כשאתה מחפש את המבצעים הטובים ביותר ברשת, אתה עלול למצוא את עצמך באחד האתרים המזויפים האלה. על ידי רכישה מאתרים כאלה אתה יכול לסיים את קנייתך עם פריטים מזויפים או גנבים, ובמקרים מסוימים, הרכישות שלך לעולם לא יועברו. הגן על עצמך מחנויות מקוונות מזויפות:

במידת האפשר, קנה מהחנויות המקוונות שאתה כבר מכיר, בוטח בהן ועשית איתן עסקים בעבר. הוסף סימניות לחנויות מקוונות בהן ביקרת בעבר ובטוח בהן.



שימו לב למחירים טובים יותר משמעותית מאלו שאתם רואים בחנויות המקוונות שהוקמו. אם העסקה נשמעת טוב מכדי להיות אמיתית, היא עשויה להיות מזויפת.



תפעילו שיקול דעת אם האתר דומה לזה בו השתמשתם בעבר, אך שם התחום של האתר, או שם החנות שונה במקצת. לדוגמה, אתה רגיל לקניות באמזון, שכתובת האתר שלה היא www.amazon.com, אך בסופו של דבר אתה קונה באתר מזויף שיש לו כתובת אתר דומה, אך האות 'ס' מוחלפת במספר '0'.



הקלד את שם החנות המקוונת או כתובת האינטרנט שלה במנוע חיפוש כדי לראות מה אחרים אמרו עליה. חפש מונחים כמו "הונאה", "תרמית", "לעולם לא שוב" או "זיוף".





רמאים באתרים לגיטימיים

שים לב גם כשאתה קונה באתרים מהימנים. חנויות מקוונות גדולות מציעות לרוב מוצרים שנמכרים על ידי אנשים או חברות שונות שעלולים להיות בעלי כוונות הונאה. יעדים מקוונים כאלה דומים לשווקים בעולם האמתי, בהם מוכרים מסוימים אמיתיים יותר מאחרים. בדוק את המוניטין של כל מוכר לפני ביצוע ההזמנה. היזהר ממוכרים שהם חדשים בחנות המקוונת או שמוכרים פריטים במחירים נמוכים במיוחד. עיין במדיניות החנות המקוונת לגבי רכישות מצדדים שלישיים כאלה. כאשר יש ספק, רכוש פריטים שנמכרו ישירות על ידי החנות המקוונת, ולא על ידי מוכרי הצד השלישי המשתתפים בשוק המקוון שלה.

תשלומים מקוונים עבור רכישות

בדוק באופן קבוע את דפי כרטיס האשראי שלך כדי לזהות חיובים חשודים. במידת האפשר, אפשר את האפשרות להודיע לך באמצעות דואר אלקטרוני, טקסט או אפליקציה בכל פעם שמתבצע חיוב בכרטיס האשראי שלך. אם אתה מוצא פעילות חשודה, התקשר מיד לחברת האשראי שלך ודווח עליה. הימנע משימוש בכרטיסי חיוב במידת האפשר. כרטיסי חיוב לוקחים כסף ישירות מחשבון הבנק שלך, אם בוצעה הונאה יהיה לך הרבה יותר קשה להחזיר את הכסף שלך. אפשרות נוספת היא שימוש בשירותי תשלום ידועים, כמו PayPal, לרכישות מקוונות, שאינן חושפות את מספר כרטיס האשראי שלך לספק. לב-סוף, שקלו להשתמש בכרטיס מתנה לרכישות מקוונות.

רק מכיוון שחנות מקוונת בעלת מראה מעוצב ומקצועי, אין פירושה שהיא לגיטימית. אם האתר גורם לך לאי נוחות, אל תשתמש בו. במקום זאת, פנו לאתר ידוע שאפשר לסמוך עליו או שהשתמשתם בו בבטחה בעבר. יתכן שלא תמצא את העסקה המדהימה הזו, אך יש סיכוי גדול יותר שתגיע למוצר לגיטימי ותימנע מהונאות.



עורך אורח

לני זלצר הוא מנהל אבטחת המידע הראשי באקסוניוס, מנכ"ל וסופר בכיר במכון SANS. תוכלו לעקוב אחריו בטוויטר כ- lennyzeltser@zeltser.com ולקרוא את הבלוג שלו ב- zeltser.com.

מקורות

<http://www.sans.org/u/X7k>

<http://www.sans.org/u/X7p>

<http://www.sans.org/u/Xu9>

הנדסה חברתית:

הונאה באמצעות מדיה חברתית:

הפיכת סיסמאות לפשוטות:

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Security Awareness, הפצתו ברישיון [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/), הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה www.sans.org/security-awareness/ouch-newsletter. עורכי המערכת: וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי | תורגם על ידי: גדי מרגלית ודרור ענבר

