אאוץ! | בפברואר 2017

מרכז סליקה בנקאי בע"מ שירותי בנק אוטומטיים בע"מ

עלון מודעות אבטחת מידע חודשי לכולם

OUCH!

בגיליון זה...

- בדיקות קדם
- התקנים גנובים/אבודים
- גישה לרשת אלחוטית
- מחשבים ציבוריים

להישאר מאובטח בדרכים

סקירה כללית

אנחנו רוצים שתהיו מסוגלים להפיק את המרב מהטכנו־לוגיה בכל עת, גם כאשר אתם בנסיעות.

בעלון זה אנו ננסה להסביר איך אתם יכולים להתחבר לאינטרנט בדרכים ולהשתמש במכשירים שלכם באופן מאובטח.

עורך אורח

מארק ווילאמס הוא אדריכל האבטחה הארגונית BlueCross BlueShield טנסי. הוא גם מדריך SANS ונשיא ISSA בעיר Chattanooga עקב עבודתו הוא נוסע רבות ומבין את הבעיות שבהן אתה עלול להיתקל בעת נשיאת המכשירים הניידים שלך בדרך.

בדיקות קדם

כאשר אתם מחוברים לרשת בבית או בעבודה, הרשת עשויה להיות מאובטחת, בעת נסיעה אתם צריכים להניח כי כל רשת שאתם מתחברים אליה אינה מאובטחת ולא ניתן לסמוך עליה. אתם אף פעם לא יודעים מי עוד נמצא ברשת זו ומה ייתכן שהם עושים. הנה כמה צעדים פשוטים אשר יעזרו לכם להגן עליכם ועל הנתונים שלכם לפני שאתם נוסעים.

- המידע הבטוח ביותר הוא המידע שאתה לא מחזיק. זהה את המידע והנתונים שאתה לא צריך על כל המכשירים שאתה מביא אתך ולאחר מכן הסר את המידע מהמכשירים. זה יכול לצמצם משמעותית את הנזק במקרה והמכשירים שלך יאבדו, יגנבו או יוחרמו על ידי מכס או ביטחון גבולות. אם הטיול שלך הוא מטעם העבודה עלייך לשאול את הממונה עליך באם הארגון מספק מכשירים אשר ישמשו אותך במהלך נסיעת העבודה.
- נעל את המכשירים הניידים שלך ו / או המחשב הנייד באמצעות סיסמה או קוד גישה חזקה. בדרך זו אם הוא נגנב או אבד, אנשים לא יוכלו לגשת למידע שלך. בנוסף, מומלץ להפעיל או להתקין הצפנת דיסק מלאה בהתקנים ובמחשבים הניידים. עבור רוב הטלפונים הניידים, תכונה זו מופעלת באופן אוטומטי כאשר אתה משתמש במסך נעילה עם קוד שחרור.
- התקן או הפעל תוכנה על גבי המכשיר שלך כך שתוכל לעקוב אחריו מרחוק בעזרת מיקום המכשיר, ואפילו לבצע מחיקה מרחוק של המכשיר, במידה והוא אבד או נגנב.
- לפני שאתה עוזב עדכן את ההתקנים שלך, יישומים ותוכנות אנטי-וירוס, כך תוודא שאתה מפעיל את הגרסאות העדכניות ביותר. התקפות רבות מתמקדות במערכות הפעלה או תוכנה לא מעודכנות.

© SANS Institute 2017

להישאר מאובטח בדרכים

- בצע גיבוי מלא של כל המכשירים שלך. בדרך זו, אם משהו קורה להם תוך כדי נסיעה עדיין יש לך את כל הנתונים המקוריים במיקום מאובטח.
- עבור טיסות בינלאומיות, עלייך לבדוק עם ספק שירות הטלפון אם יש לך חבילת גלישה ושיחות. לעתים קרובות ספקי השירות גובים מחירים גבוהים עבור שימוש בנתוני גלישה, מומלץ לבטל את יכולת העברת נתונים סלולריות תוך כדי נסיעה בינלאומית, או לרכוש כרטיס SIM מקומי מראש על מנת לאפשר נסיעות בינלאומיות.

על מנת להישאר מאובטח בעת נסיעה, עלייך לאבטח את המכשירים לפני היציאה מהבית, לשמור עליהם בצורה פיסית ומאובטחת, ולהצפין את כל הפעילויות המקוונות.

התקנים גנובים/אבודים

ברגע שתתחיל את הנסיעה עלייך להבטיח את ביטחונם האישי של המכשירים שלך. לדוגמא, לא להשאיר את המכשירים במכונית משום שאנשים יכולים לראות אותם בקלות, פושעים עלולים לרסק את החלון של המכונית ולגנוב כל דבר בעל ערך שהם יכולים לקחת. בעוד שפשע הוא בהחלט סיכון, על פי מחקר של חברת Verizon לאנשים יש יותר סיכוי (פי 100) לאבד את המכשיר מאשר שייגנב. משמעות הדבר היא שתמיד לבדוק אם המכשירים שלך נמצאים עלייך כאשר אתה נוסע, למשל בעת בדיקה ביטחוניות בשדה התעופה, כאשר יוצאים ממונית או ממסעדה, חשוב לבדוק את חדר המלון או את הכיסא לפני שאתה יורד מהמטוס. זכרו לבדוק את כיס המושב האחורי במטוס!

גישה לרשת אלחוטית

גישה לאינטרנט בעת נסיעת לעתים קרובות מתבצעת באמצעות נקודות גישה ציבורית לאינטרנט, כגון אלה שתמצאו בכל בית מלון, בית קפה מקומי או בשדה התעופה. שתי בעיות עם אינטרנט ציבורי: אתה אף פעם לא בטוח מי הגדיר אותם ואתה לא יודע מי מחובר אליהם. עקב סיבות אלו הרשתות הציבוריות נחשבות כלא מהימנות. למעשה זו הסיבה שביצעת את כל הפעולות שיש לבצע על מנת לאבטח את המכשירים שלך לפני שעזבת. בנוסף, רשת אלחוטית מתב־ססת על גלי רדיו, כלומר, כל אחד אשר קרוב אלייך פיזית יכול באופן פוטנציאלי ליירט ולנטר את התקשורת. מסיבות אלה, במידה ואתה משתמש ברשת ציבורית, אתה צריך לוודא כי כל הפעילות המקוונת שלך מתבצעות באופן מוצפן. לדוגמה, בעת חיבור מקוון באמצעות הדפדפן שלך עלייך לוודא כי האתרים שבהם אתה מבקר הינם מוצפנים. אתה יכול לאשר זאת על ידי חיפוש https:// ו/או תמונה של מנעול סגור בכתובת או בשורת הכתובת של האתר שאתה

להישאר מאובטח בדרכים

גולש בו. בנוסף, ייתכן שאתה יכול להשתמש ב- VPN (רשת פרטית וירטואלית) אשר מצפינה את כל הפעילות המקוונת שלך כאשר היא מופעלת. ייתכן שחיבור מסוג זה יסופק לך על ידי מקום העבודה, או שאתה יכול לרכוש VPN לשימושך האישי. אם אתה חושש שאין רשת אלחוטית שאתה יכול לסמוך עליה, יש לשקול הפעלת נקודת גישה אלחוטית בטלפון החכם שלך. אזהרה: כמו שהזכרנו קודם, זה יכול להיות יקר בעת נסיעות לחו»ל, היוועץ עם ספק השירות שלך.

מחשבים ציבוריים

אין להשתמש במחשבים ציבוריים, כגון בלובי של בתי מלון או בבתי קפה אינטרנט, במיוחד בכדי להיכנס לחשבונות שלך או לגשת למידע רגיש. אין לך מושג מי השתמש במחשב לפניך, המחשבים עלולים להיות נגועים בנוזקות בשוגג או בכוונה. במידת האפשר, יש להשתמש רק במכשירים אשר אתה סומך עליהם. במחשבים ציבוריים אתה יכול לקבל מידע ציבורי כגון בדיקת מזג האוויר או התעדכנות בחדשות. כניסה אל כל החשבונות שלך כגון חשבון הדואר האלקטרוני שלך יכולה להיות הזמנה לפושעי סייבר אשר צופים מהצד.

למד עוד

הרשם לעלון OUCH! המפורסם אחת לחודש, עלון זה מתמקד במודעות אבטחת המידע, ניתן לקרוא עלונים קודמים וניתן ללמוד על מודעות אבטחת המידע של SANS באתר securingthehuman.sans.org/ouch/archives.

מקורות

ביטויי סיסמאות:	https://securingthehuman.sans.org/ouch/2015#april2015
גיבויים:	https://securingthehuman.sans.org/ouch/2015#august2015
נוזקות:	https://securingthehuman.sans.org/ouch/2016#march2016
הצפנה:	https://securingthehuman.sans.org/ouch/2016#june2016
ארכיון/תרגום עלון אאוץ':	https://securingthehuman.sans.org/ouch/archives

OUCH! יוצא לאור ומפורסם על ידי חברת SANS Securing The Human, הפצתו ברישיון Creative Commons BY-NC-ND 4.0 license, הנך רשאי להפיץ או להשתמש בעלון זה כעזר לתוכנית מודעות המשתמשים, כל עוד לא בצעת שינויים בעלון זה. לתרגומים או מידע נוסף, אנא פנה ouch@securingthehuman.org.

עורכי המערכת: ביל ויימן, וולט סקריוונס, פיל הופמן, בוב רודיס, שריל קונלי
תורגם על ידי: גדי מרגלית ודרור ענבר