

5 הצעדים לעבודה מהבית באופן מאובטח

אנחנו יודעים שהמעבר לעבודה מהבית יכול להיות חדש עבור חלקכם, ייתכן שאף יהווה סוג של גורם לחץ בזמן שתנסו להסתגל לסביבה החדשה שלכם. אחת המטרות שלנו היא לאפשר לכם לעבוד מהבית באופן המאובטח ביותר ככל שניתן. להלן חמישה צעדים פשוטים לעבודה באופן מאובטח. הדבר הטוב ביותר בצעדים אלה הוא שהם לא רק מאבטחים את העבודה שלכם, אלא בנוסף הם גם ישמרו עליכם ועל המשפחה שלכם בטוחים יותר בעודכם מייצרים בית מאובטח.

אתם: הדבר החשוב ביותר הוא שהטכנולוגיה לבדה אינה יכולה להגן עליכם - אתם ההגנה הטובה ביותר. התוקפים למדו שהדרך הפשוטה ביותר עבורם להשיג את מה שהם רוצים היא להתמקד בכם במקום במחשב או במכשיר אחר שברשותכם. אם הם רוצים את הסיסמה שלכם, נתוני עבודה או להשיג שליטה על המחשב שלכם, הם ינסו לרמות אתכם ולגרום לכם לתת להם זאת והם יעשו זאת לעיתים קרובות על ידי יצירת תחושת דחיפות. למשל, הם יכולים להתקשר אליכם ולהתחזות לנציג תמיכה טכנית של חברת מייקרוסופט בטענה שהמחשב שלכם מזוהם. או שהם עשויים לשלוח לכם אזהרה באמצעות הודעת דוא"ל בה נכתב שלא ניתן למסור חבילה מסוימת ולרמות אתכם כך שתלחצו על קישור זדוני. הסימנים הנפוצים ביותר להתקפת הנדסה חברתית כוללים:



- מישהו היוצר תחושת דחיפות גדולה, לרוב באמצעות פחד, איום, משבר או דדליין חשוב. תוקפי סייבר טובים ביצירת הודעות משכנעות שנדמה כי מגיעות מארגון מהימן, כגון בנקים, גורמים ממשלתיים או ארגונים בינלאומיים.
- יצירת לחץ לעקוף או להתעלם ממדיניות או נהלי אבטחה, או הצעה שטובה מכדי להיות אמיתית (לא, אתם לא זכיתם בהגרלת הלוטו!).
- הודעה מחבר או עמית לעבודה, שבה החתימה, הטון או ניסוח ההודעה אינם נשמעים כמו אותו אדם.

בסופו של דבר, אתם ההגנה הטובה ביותר מפני התקפות אלה.

רשת ביתית: כמעט כל רשת ביתית מתחילה ברשת אלחוטית (המכונה לעיתים Wi-Fi). זה מה שמאפשר לכל המכשירים שלכם להתחבר לאינטרנט. רוב הרשתות האלחוטיות הביתיות נשלטות על ידי נתב האינטרנט שלכם או על ידי נקודת גישה אלחוטית ייעודית נפרדת. שניהם פועלים באותה הדרך: על ידי שידור אותות אלחוטיים למכשירים הביתיים המחוברים. המשמעות היא שאבטחת הרשת האלחוטית שלכם היא מרכיב מרכזי בהגנה על הבית שלכם. אנו ממליצים לנקוט בצעדים הבאים על מנת לאבטח אותה:



- שנו את סיסמת המנהל המגיעה כברירת המחדל של המכשיר השולט ברשת האלחוטית שלכם. חשבון המנהל הוא זה שמאפשר לכם לשנות את ההגדרות של הרשת האלחוטית שלכם.
- וודאו שרק אנשים אשר אתם בוטחים בהם יכולים להתחבר לרשת האלחוטית שלכם. עשו זאת על ידי הפעלת אבטחה חזקה. על ידי הפעלת אפשרות זו, אנשים המבקשים להתחבר לרשת האלחוטית שלכם נדרשים לספק סיסמה ולאחר שהם מתחברים הפעילויות המקוונות שלהם מוצפנות.
- וודאו שהסיסמה בה האנשים משתמשים כדי להתחבר לרשת האלחוטית שלכם היא סיסמה חזקה וכי הסיסמה הזו שונה מסיסמת המנהל. זכרו כי עליכם להכניס את הסיסמה פעם אחת בלבד לכל אחד מהמכשירים שלכם משום שהם שומרים וזוכרים את הסיסמה.

לא בטוחים כיצד לבצע צעדים אלה? שאלו את ספק שירותי האינטרנט שלכם, בדקו באתר האינטרנט שלהם, בדקו את התיעוד המגיע עם נקודת הגישה האלחוטית שלכם, או פנו לאתר האינטרנט של הספק.

סיסמאות: כאשר אתר אינטרנט מבקש מכם ליצור סיסמה: צרו סיסמה חזקה, ככל שיש בה יותר תווים, כך היא חזקה יותר. שימוש בביטוי סיסמה הוא אחד מהדרכים הפשוטות ביותר להבטיח שהסיסמאות שלכם חזקות. ביטוי סיסמה הוא פשוט סיסמה המורכבת ממספר מילים, כגון "דבש דבורים טהור". המשמעות של שימוש בביטוי סיסמה הוא שימוש בסיסמה שונה בכל אחד מהמכשירים או החשבונות המקוונים שלכם. כך, אם ביטוי סיסמה אחד נחשף, כל יתר החשבונות והמכשירים שלכם עדיין יהיו מוגנים. לא מצליחים לזכור את כל ביטויי הסיסמה הללו?



השתמשו במנהל סיסמאות, שזו תוכנה מיוחדת המתמחה בשמירה מאובטחת של כל ביטויי הסיסמה שלכם בפורמט מוצפן (ויש לה גם תכונות נהדרות נוספות!). לבסוף, הפעילו אימות דו-שלבי (המכונה גם אימות דו-גורמי או אימות מרובה גורמים) כאשר ניתן. זה עושה שימוש בסיסמה שלכם, אבל גם מוסיף צעד נוסף, כגון קוד הנשלח לסמארטפון שלכם או יישום המפיק את הקוד עבורכם. אימות דו-שלבי הוא ככל הנראה הצעד החשוב ביותר שתוכלו לנקוט בו על מנת להגן על החשבונות המקוונים שלכם וזה הרבה יותר פשוט ממה שאתם חושבים.



עדכונים: וודאו כי כל אחד מהמחשבים, המכשירים הניידים, התכניות והיישומים שלכם פועלים על גרסת התוכנה העדכנית ביותר שלהם. תוקפי סייבר כל הזמן מחפשים פגיעויות חדשות בתוכנות שהמכשירים שלכם משתמשים בהן. כאשר הם חושפים פגיעויות, הם משתמשים בתכניות מיוחדות כדי לנצל פגיעויות אלה ולפרוץ למכשירים שבהם אתם משתמשים. במקביל, החברות שיצרו את התוכנות למכשירים אלה עובדות קשה לתקן את הפגיעויות הללו על ידי פרסום עדכונים. כאשר אתם מוודאים שהעדכונים מותקנים במהירות על גבי המחשבים והמכשירים הניידים שלכם, אתם מקשים על אחרים לפרוץ למכשירים שלכם. על מנת לשמור על עדכניות, פשוט הפעילו את אפשרות העדכון האוטומטי כאשר ניתן. כלל זה ישים לגבי כמעט כל טכנולוגיה המתחברת לרשת, כולל לא רק מכשירי העבודה שלכם, אלה גם טלוויזיות המחוברות לאינטרנט, מוניטורים של התינוק, מצלמות אבטחה, נתבים ביתיים, קונסולות משחק ואפילו הרכב שלכם.



ילדים / אורחים: אחד הדברים שבמשרד כנראה אינכם צריכים לדאוג לגביו הוא ילדים, אורחים או בני משפחה אחרים המשתמשים במחשב העבודה הנייד שלכם או מכשיר אחר שלכם הקשור לעבודה. וודאו שבני המשפחה והחברים מבינים שהם לא יכולים להשתמש במכשירי העבודה שלכם, משום שהם עלולים בטעות למחוק או לשנות מידע, או אפילו גרוע מכך, הם עלולים בטעות לזהם את המכשיר.