

למד מיומנות הישרדות חדשה: איתור דיפ-פייק (זיוף עמוק)

מה הם דיפ-פייק?

המילה " דיפ-פייק " היא שילוב של "למידה עמוקה" ו"זיוף". דיפ-פייק הם תמונות, סרטונים או הקלטות אודיו מזויפות. לפעמים האנשים שבהם נוצרו על ידי מחשב, דמויות מזויפות שנראות ונשמעות כאילו הן אנשים אמיתיים. לפעמים האנשים הם אמיתיים, אבל התמונות והקולות שלהם עוברים מניפולציות לגרום להם לומר דברים שהם לא עשו או אמרו. לדוגמה, סרטון דיפ-פייק יכול לשמש כדי ליצר סלבריטאי או פוליטיקאי שאומרים משהו שהם מעולם לא אמרו. באמצעות הזיופים המאוד אמיתיים האלה, התוקפים יכולים ליצור מציאות חלופית שבה אתה לא תמיד יכול לסמוך על העיניים והאוזניים שלך.

חלק מהדיפ-פייק יש מטרות לגיטימיות, כמו סרטים המחזירים שחקנים שנפטרו לחיים כדי לשחזר דמות מפורסמת. אבל תוקפי סייבר מתחילים למנף את הפוטנציאל של דיפ-פייק. הם משתמשים בהם כדי להטעות את החושים שלך, כדי שהם יוכלו לגנוב את הכסף שלך, להטריד אנשים, לתמרן בוחרים או דעות פוליטיות, או ליצור חדשות מזויפות. במקרים מסוימים, הם אפילו יצרו חברות מדומות המורכבות מעובדים מזויפים. אתה חייב להיות זהיר עוד יותר ממה שאתה מאמין בעת קריאת חדשות או מדיה חברתית לאור ההתקפות הללו.

ה-FBI מזהיר שבעתיד לדיפ-פייק תהיה "השפעה חמורה ונרחבת יותר בשל רמת התחכום של המדיה הסינתטית שבה נעשה שימוש". למד לזהות את הסימנים של דיפ-פייק כדי להגן על עצמך מהדמיות האמינות ביותר הללו. לכל צורה של דיפ-פייק - תמונת סטילס, וידאו ואודיו - יש קבוצת פגמים משלה שיכולים להסגיר אותה.

תמונות סטילס

דיפ-פייק שאתה עשוי לראות לרוב הוא תמונת הפרופיל המזויפת במדיה החברתית. התמונה למטה היא דוגמה לדיפ-פייק מהאתר thispersondoesnotexist.com (האדם הזה לא קיים). מתחת לתמונה יש חמישה רמזים שונים לכך שזה יכול להיות דיפ-פייק. תבחין שלא קל לזהות את הרמזים האלה וקשה לזהות אותם:



1. רקע: הרקע לרוב מטושטש או עקום, וייתכן שיש לו תאורה לא עקבית כמו צללים בולטים המצביעים לכיוונים שונים.
2. משקפיים: הסתכלו היטב על החיבור בין המסגרות לזרועות ליד הרקה. לדיפ-פייק יש לעתים קרובות חיבורים לא תואמים עם גדלים או צורות מעט שונות.
3. עיניים: נראה שעניינה נמצאות באותו מיקום בתמונה המשמש כיום לתמונות פרופיל מזויפות, ובתוצאה מכך יש המכנים "מבט דיפ-פייק".
4. תכשיטים: עגילים עשויים להיות חסרי צורה או מחוברים בצורה מוזרה. שרשראות עשויות להיות מוטבעות בעור.
5. צווארונים וכתפיים: הכתפיים עשויות להיות מעוותות או לא תואמות. צווארונים עשויים להיות שונים בכל צד.

וידאו

- חוקרים מהמכון הטכנולוגי של מסצ'וסטס, MIT, פיתחו רשימת שאלות כדי לעזור לכם להבין אם סרטון וידאו אמיתי, וצינו שלעתים קרובות דיפ-פייק אינם יכולים "לייצג באופן מלא את הפיזיקה הטבעית" של סצנה או תאורה.
1. לחיים ומצח: האם העור נראה חלק מדי או מקומט מדי? האם גיל העור דומה לגיל השיער והעיניים?
 2. עיניים וגבות: האם צללים מופיעים במקומות שהייתם מצפים להם?
 3. משקפיים: האם יש בוהק? יותר מדי בוהק? האם זווית הבוהק משתנה כאשר האדם זז?
 4. שיער פנים: האם שיער הפנים נראה אמיתי? דיפ-פייק עשויים להוסיף או להסיר שפם, פאות או זקן.
 5. שומות בפנים: האם השומה נראית אמיתית?
 6. מצמוץ: האם האדם ממצמץ מספיק או יותר מדי?
 7. גודל שפתיים וצבע: האם הגודל והצבע תואמים לשאר הפנים של האדם?

חוקרים אומרים שטכנולוגיות כמו ספקטרוגרמות יכולות להראות מתי הקלטות קול מזויפות. אבל לרובנו אין את המותרות של מנתח קול כאשר תוקף מתקשר. הקשב להגשה מונוטונית, גובה הצליל או רגש מוזר וחוסר רעשי רקע. זיוף קול יכול להיות קשה לזיהוי. אם אתה מקבל שיחה מוזרה מארגון לגיטימי, אתה יכול לוודא אם השיחה אמיתית על ידי ניתוק ואז התקשר לארגון בחזרה. הקפד להשתמש במספר טלפון מהימן, כגון מספר טלפון שכבר יש לך ברשימת אנשי הקשר שלך, מספר טלפון המודפס על חשבון או הצהרת הארגון, או מספר הטלפון באתר הרשמי של הארגון.

סיכום

שים לב שתוקפים משתמשים באופן פעיל בדיפ-פייק. הם יכולים ליצור חשבונות מזויפים במדיה החברתית כדי להתחבר אליהם או ליצור סרטונים מזויפים כדי להשפיע על דעת הקהל. חלקם אפילו מוכרים את השירותים שלהם ברשת האפלה כדי שתוקפים אחרים יוכלו לעשות את אותו הדבר. אנחנו לא מצפים ממך להפוך למומחה לדיפ-פייק, אבל אם אתה מתחמש ביסודות של זיהוי הזיופים, אתה תהיה הרבה יותר טוב בהגנה על עצמך. אם אתה חושד שזיהית דיפ-פייק, דווח על כך לאתר או למקור המארח את התוכן.



עורכת אורחת

Kerry Tomlinson (@KerryTNews) הוא כתב חדשות סייבר ב-Ampere News ומקצוען מוסמך ל-SANS Security Awareness. המשימה שלה היא לתרגם את מה שקורה בעולם הדיגיטלי עבור אנשים מכל רמות הידע עם ידיעות חדשותיות מרתקות ומלאות תובנות ומצגות מושבות.

משאבים

הנדסה חברתית: <https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering>
האם אתה יכול לזהות את הזיוף? (Ampere News): <https://www.amperesec.com/news/can-you-spot-the-fake>
מבחן הדיפ-פייק של MIT (MITI): <https://detectfakes.media.mit.edu/>
זהה את הדיפ-פייק: <https://www.spotdeepfakes.org/en-US>

תורגם לקהילה על ידי: גדי מרגלית ודרור ענבר

OUCH! פורסם על ידי SANS Security Awareness ומופץ תחת רישיון [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) אתם חופשיים לשתף או להפיץ ניוזלטר זה כל עוד אתה לא מוכר או משנה אותו. ועדת מערכת: וולטר סקריינס, פיל הופמן, אלן וואגנר, לסלי רידאוט, הנסיכה יאנג