DCOYA - תאור פתרון

מבוא

חוזק השרשרת כחוזק החוליה החלשה....

ע"פ נתונים רשמיים של האנליסטים המרכזיים המסקרים את תחום אבטחת המידע, עולה כי בשנים האחרונות רובם המכריע של אירועי אבטחת המידע והסייבר (95%) נגזרים ישירות מטעויות/חוסר ידע של המשאב האנושי בארגון - משתמשי המחשב.

"Human error" is involved in more than 95 % of the security incidents investigated in 2014, the most prevalent form involves clicking on a malicious link found in a phishing message

"IBM Security Services 2014 Cyber Security Intelligence Index"

%95

רובם המכריע של הארגונים הינם בעלי מודעות אבטחת מידע גבוהה. מרבית הארגונים מרכזים את המאמצים והתקציבים בתשתיות אבטחת מידע מתקדמות, כגון מוצרי חומרה, תוכנה ושרותי אבטחה אחרים על מנת להקשיח את תשתיות המחשוב ולמקסם את רמת אבטחת המידע.

בהשוואה להיבט הטכנולוגי, הגורם האנושי אינו זוכה להתייחסות ולמשאבים מספקים, וכתוצאה מכך מהווה את החוליה החלשה בשרשרת אבטחת המידע. הצד התוקף, אשר לא מתעלם מעובדה זו, מנצל את המצב על מנת לעקוף ולבטל את מערך אבטחת המידע הקיים.

מתקפות פישינג (PHISHING)

מתקפת פישינג הינה המתקפה הנפוצה ביותר בשנים האחרונות בקרב מתקפות הסייבר. מתקפות הפישינג מתבססות כאמור על החוליה החלשה ביותר בארגון - הגורם האנושי. ההיסטוריה והניסיון מלמדים שלעולם, משתמשי הארגון יפלו קורבן למתקפת פישינג בדרך זו או אחרת. עובדה זו יוצרת פער ברמת אבטחת המידע הארגונית, אי לכך עולה הצורך בהגברת המודעות של הגורם האנושי בארגון למתקפות הפישינג השונות.(מתקפות איסוף/ נידוב מידע,מתקפות צד לקוח ומתקפות יעודיות)

הקושי הרב של ארגונים להתמודד עם סוג מתקפות אלו נובע בין השאר מהנתונים הסטטיסטיים של מתקפות אלו :

- 45% הצלחה בכלל המתקפות
- 80% מהמתקפות כוללות Malware
- 77% ממתקפות ה Phishing מתבצעות בערוץ המיילים

- 50% מהמיילים נפתחים ומדביקים את הארגון בשעה הראשונה משליחתם!

הדרך היעילה ביותר לצמצם משמעותית את חשיפת הארגון הינה הגברת המודעות של הגורם האנושי בארגון למתקפות ה Phishing השונות.(מתקפות איסוף/ נידוב מידע,מתקפות צד לקוח ומתקפות יעודיות.

תאור המוצר- שרות

כללי

חברת Dcoya פיתחה מערכת יעודית אשר נבנתה על מנת לספק מענה מלא לאיום מתקפות הפישינג , המערכת הינה מערכת גרנולארית אשר נבנתה באופן המאפשר ללקוח להנות משרות מנוהל מלא לצד נגישות לממשק ניהול אינטגרלי מלא מבוסס WEB, הממשק כולל סטטיסטיקות מלאות, היסטוריית סימולציות ארגונית, מגמות ארגוניות ונתונים עד רמת העובד הבודד, הנתונים מוצגים בצורה גרפית וברורה מאוד.

המערכת הינה מערכת עצמאית המוטמעת בענן גלובלי (Amazon) ,כמו כן ניתן ליישם את השרות דרך ענן מקומי בישראל.

מתודולוגיית האימון והלימוד

מתודולוגיית תוכנית המודעות מתבססת על מגוון תרחישי אימון הנובעים ומותאמים למגוון האיומים השונים אשר ממופים באופן תדיר ע"י צוות האנליסטים של חברת Dcoya

הסימולציות מתבצעות באופן סדיר ונפרסות בד"כ על פני מספר שבועות, מגוון הסימולציות מותאם לאופי הארגון, תחומי פעילות, פריסה גאוגרפית, מחלקות ובכלל לתמהיל הארגוני .כמו כן אופי ורמת הקושי של הסימולציות יקבעו בהתאמה לתוצאות הסימולציות הקודמות ולמגמות הארגוניות, כלומר, במידה וזוהה קושי החוזר על עצמו בזיהוי סוג סימולציה בעלת אופי מסוים ע"י משתמשים מסוימים, תבוצע סימולציה בעלת אופי / רמת קושי דומים בשנית, וכך עד לקבלת תוצאות המשקפות שיפור משמעותי ולהפך, משתמשים שיראו גרף לימוד חיובי או רמת מודעות גבוהה יעלו שלב במורכבות ורמת הקושי של הסימולציה.

מדי חודש נשלח קמפיין אחד המכיל מגוון של סימולציות הנשלחות לעובדים בצורה מבוקרת וחכמה המבטיחה פריסה נכונה אשר תמנע את הסגרת הפעילות בין העובדים ,כמו גם חשיפת העובדים למס

רב של תרחישי איום וזאת על מנת להבטיח שכל אחד מהעובדים יקבל הכשרה ואימון בהתאם לכלל התרחישים והאיומים הקיימים.

דוגמא לפריסת סימולציות מותאמות לאיומים השונים

דוגמא למגן סוגי הסימולציות

הסימולציות כוללות שימוש במדיה לימודית יעודית, משתמש שנלכד בסימולציה יחשף מיידית למדיה לימודית אשר תלמד ותמחיש הלכה למעשה מהן הטעויות שנעשו תוך פירוט הגורמים המחשידים במייל וממה עליו להזהר להבא, תהליך הלימוד מתבצע בגישה חיובית ומתודית, תוך ניטור מלא ואיסוף הנתונים של כל שלב בהליך הלימודי, שלב הלימוד מתבצע בהתאמה מלאה לסימולציה שנשלחה לעובד.

תוכנית לימוד מובנית – ATM- ADAPTIVE TRAINING MODULE

ATM- הינה יכולת אוטומטית מובנת של המערכת, המאפשרת להתאים את קצב חשיפת העובדים על פי רמת ביצועיהם בסימולציות קודמות וזאת על פי מתודולוגיית הלימוד. ע"י שימוש באלגוריתמים מתקדמים המערכת בונה קבוצות של עובדים לפי קריטריונים שהוגדרו מראש: עובד שנלכד במס מסוים של סימולציות, עובד שלא צלח את הלומדות באחוז שנקבע מראש, מחלקה המכילה מס רב של עובדים שנלכדו. כך למעשה מבטיחי הרכיב המתקדם הנ"ל התאמת התהליך לתוצאות הסימולציות הקודמות ורמת המודעות של כל עובד ועובד.

בנוסף אוכף רכיב ה- ATM את מתודולוגיית הלימוד על כל העובדים בארגון כך שעובד חדש אשר יתווסף לארגון בעיצומו של התהליך יקבל את אותו מערך לימוד הזהה לעובד אשר התחיל את התהליך מתחילתו. בנוסף לכל זאת מאפשר ה- ATM למקד את תהליך הלימוד באוכלוסיות בעלות מודעות ארגונית נמוכה (easy clickers) ומצד שני אימון מתקדם יותר לאוכלוסייה בעלת מודעות גבוהה באופן יחסי.

פן לימודי – תכני הדרכה

הסימולציות כוללות שימוש במדיה לימודית יעודית, משתמש שנלכד בסימולציה יועבר מיידית ללומדה אינטראקטיבית אשר תלמד את העובד הלכה למעשה מהן הטעויות שנעשו, תוך פירוט הגורמים המחשידים במייל וממה עליו להזהר להבא, תהליך הלימוד מתבצע בגישה חיובית ומתודית, תוך ניטור מלא ואיסוף הנתונים של כל שלב בהליך הלימודי, חומרי הלימוד אליהם יחשף העובד תואמים את גישת ה Micro Learning משמע הליך למודי קצר ענייני אשר במרבית המקרים אינו עולה על 30 שניות ,החומרים מוגשים בצורה מונפשת ובשפה המובנת לכלל העובדים, המערכת מאשפרת הטמעת הלוגו של הלקח על כל תוצריה.

לומדות להתרשמות

WhatsAppGold

FullEmailBox

PineApp

שרות מנוהל פרו -אקטיבי (SAAS)

אנו מאמינים שלכל לקוח מגוון צרכים משלו, רמת מודעות עובדים שונה,פריסה גאוגרפית שונה, תמהיל עובדים, ובעיקר מגוון איומים וחששות שונים, כמו כן אנו מבינים כי שגרת החיים הארגונית תקשה על הגורם המתפעל להעניק את כל רמת הקשב הדרושה לצורך התאמה מירבית של מכלול המתקפות, ניתוח התוצאות והמגמות.

חברת Dcoya מספקת שרות מנוהל אקטיבי אשר מאפשר ללקוחותיה להתאים את רמת ואופי המתקפות למכלול האיומים/ החששות הרלוונטיים ולבנות תוכנית מתקפות יעודית ויעילה, זאת תוך כדי שמירה על השקעה מינימלית ביותר בתהליכים התכניים והאופרטיביים של המתקפה מצד הלקוח.

סימולציות Phishing מוצלחות הינן מתקפות המותאמות לאקלים הארגוני, שפות, ולתמהיל העובדים ,מתקפות ג'נריות ולא מותאמות לארגון יניבו תהליך אימון ותוצאות פחות טובים משמעותית מאשר מתקפות שהותאמו לתמהיל הארגוני.

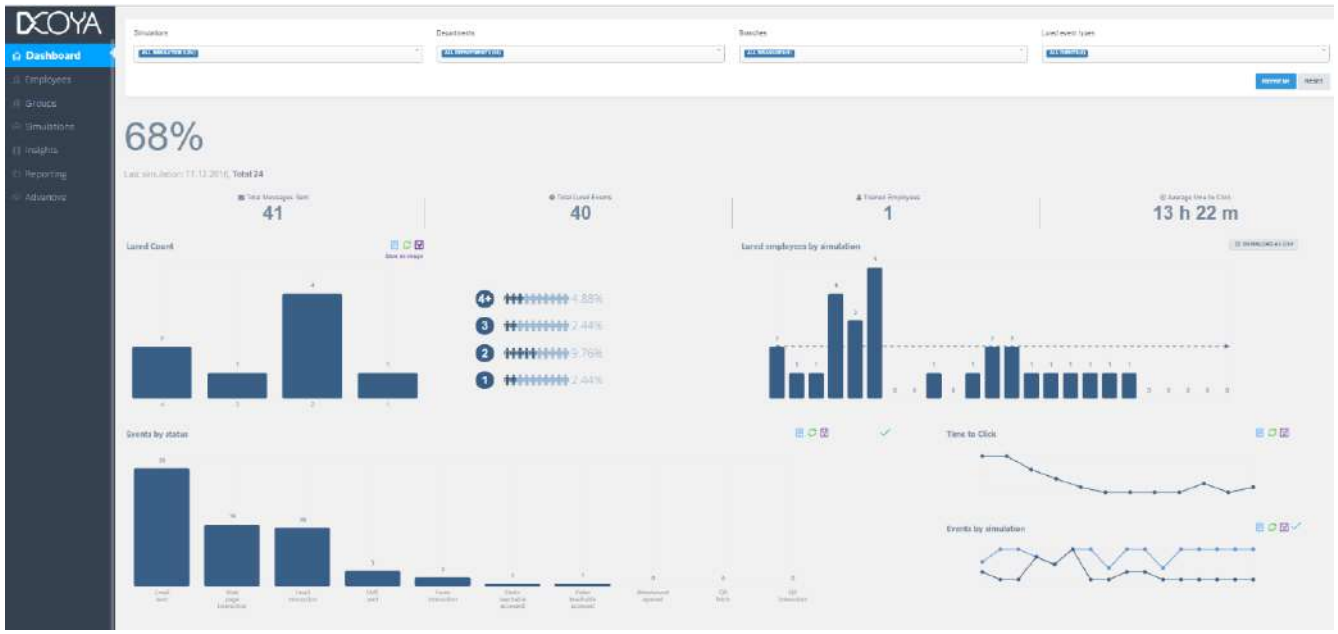
השרות המנוהל של חברת Dcoya כולל ניהול מלא של הקמפיינים בפועל, התאמת הסימולציות בהתאם לתמהיל הארגוני , פריסת הסימולציה על פני ציר החודש, עדכונים שותפים, הפקת דו"חות מנוהלים המותאמים לדרישות הלקוח וכל צורך שמועלה מצד הלקוח.

השרות המנוהל מאפשר ללקוחותינו להנות מגרנולריות מירבית, התאמה לאופי ולפריסה הגאו' של הארגון , קבלת תוצר מפורט יעודי ויעיל תוך כדי מינימום השקעה.

ממשק ניהול ודו"חות אינטגרלי מבוסס WEB

במקביל לשרות המנוהל האקטיבי , יועמד לרשות הלקוח ממשק ניהול ודו"חות מבוסס Web הממשק יכלול את כל היסטוריית הנתונים והסימולציות של אותו הלקוח (כגון מגמות על פני ציר זמן נבחר ברמת ארגון, מחלקה, מדינה, עובד וכו') כמו כן מידע Real Time לגבי סימולציות פעילות, מתן אפשרות ירידה לפרטים עד לרמת שמות העובדים , יכולת לעצור את שליחת הסימולציה באופן מיידי, ובנוסף יכולת לשלוח סימולציות נוספות באופן עצמאי – נקודתיות (מס עובדים ספציפי) או רוחביות, בנוסף לסימולציות המנוהלות על ידי הגורמים המוסמכים בחברת Dcoya.

ממשק הניהול כולל ספריית טמפלייטים עשירה ומגוונת ויכולת ומאפשר בנייה ושליחת סימולציה חדשה באופן מהיר יעיל ואינטואיטיבי.

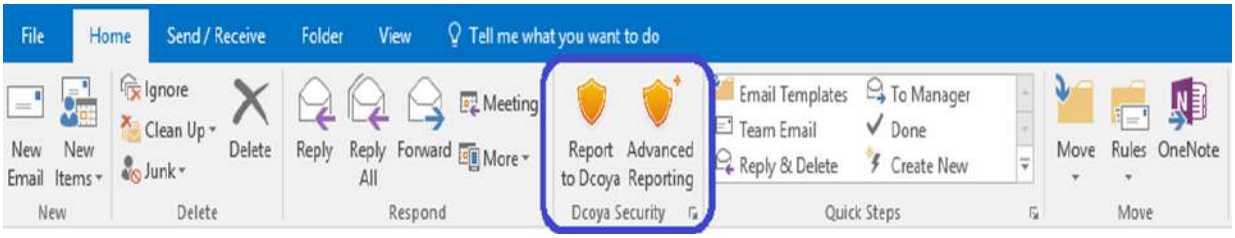


המרת תהליך המודעות למניעה פעילה

DCOYA ADVANTIVE™ - ADVANCED REPORTING – PLUG IN FOR EMAIL CLIENTS

הרעיון המרכזי הינו הפיכת העובדים מהחוליה החלשה בשרשרת אבטחת המידע לנכסי אבטחת מידע ארגוניים. ערנותו של עובד אחד עשויה לשמור על חוסנו של כלל הארגון ע"י חסימה בזמן אמת של מתקפות Phishing.

מתן יכולת דיווח על תוכן חשוד מייצרת מצב פרו אקטיבי ומעורר ערנות בו משתמשי הארגון יכולים להשתמש הלכה למעשה בערכים הלימודיים אשר נרכשו במהלך התוכנית לצורך דיווח מיידי על מייל החשוד כמתקפה. הדיווח מתאפשר ישירות מתיבת ה Inbox של העובד ע"י כפתור ייעודי ומותאם לארגון ברמת הנראות, בין אם מדובר במיילים במסגרת סימולציה מכוונת של חברת דיקויה ובין אם מדובר במתקפות אמיתיות המעלות חשד אצל המשתמש.

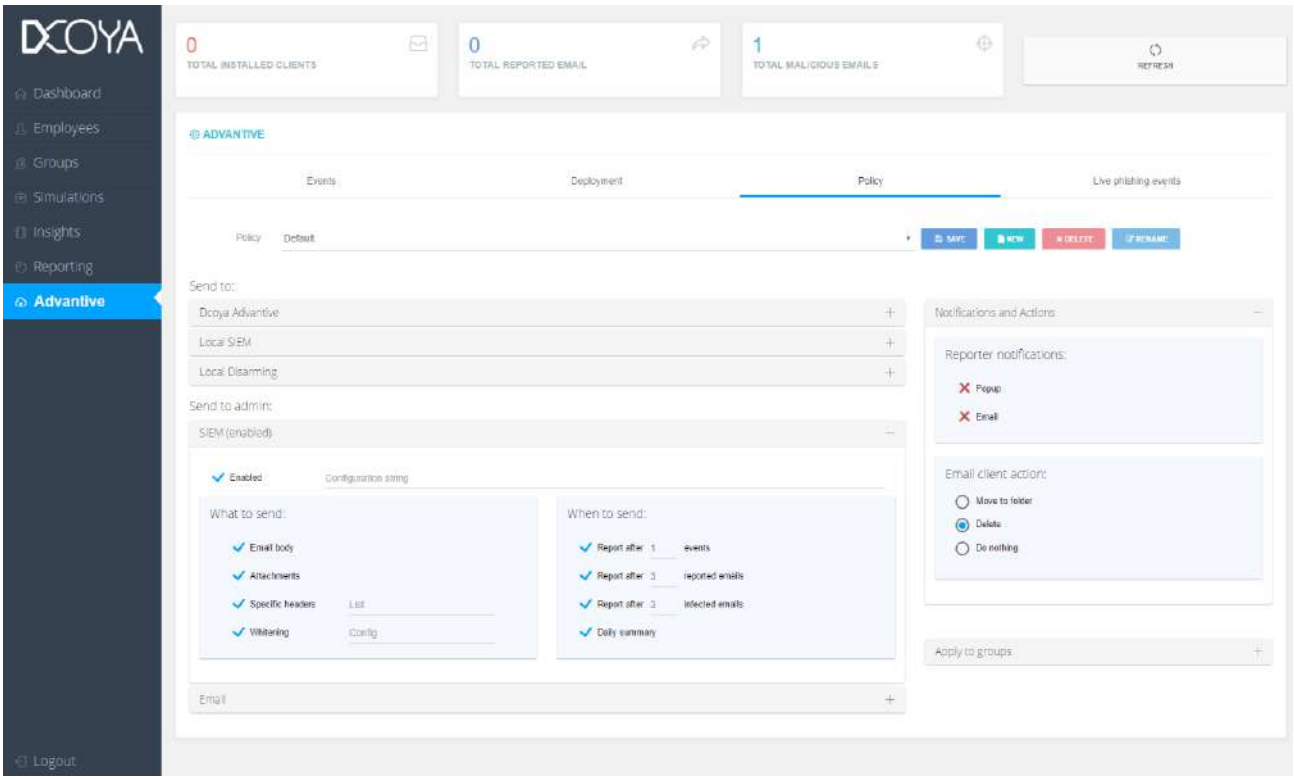


דיווח על תוכן חשוד ישלח את המייל למערכות פנימיות / Sand - Box ייעודי, SEIM/SOC ארגוני, או כל תשתית פנימית או חיצונית אחרת. המערכת מאפשרת דיווח מאובטח ללא פתיחת המייל וללא חשיפת הארגון למייל החשוד כפוגעני. לאחר שליחת הדיווח, המייל נמחק מהתיבה (או מועבר לתיקיה אחרת) בכדי למנוע הדבקה במידה ומדובר בנוזקה אמתית.

<u>ממשק הניהול</u>

כלל יכולות הדיווח ניתנות להגדרה דרך ממשק הניהול של המוצר. הממשק זמין באמצעות דפדפן Web סטנדרטי ולא דורש התקנות מיוחדות. ההזדהות מתבצעת באמצעות Two Factor Authentication מעל TLS.

ידע אודות הארגון ואודות עובדי הארגון שנצבר תוך כדי סימולציות הפישינג בא לידי ביטוי גם בעת ניהול יכולות הדיווח של Dcoya Advantive. כלל היכולות המפורטות בהמשך מסמך זה ניתנות להכלה על עובדים בארגון לפי השתייכות ארגונית כלשהי (כגון שייכות למחלקת מכירות) וכמו כן לפי תוצאות תרחישי הפישינג שנשלחו לארגון. לדוגמא, משתמש שנלכד בסימולציה (ז"א חלש בזיהוי סימולציות פישינג) יקבל מדיניות Advantive מחמירה יותר (למשל מחיקת ההודעה שדווחה), ואילו משתמש שלא נלכד ב x מתוך y הסימולציות האחרונות יקבל מדיניות Advantive מקלה יותר.



<u>פירוט היכולות</u>

בעת שליחת הודעה לדיווח, ניתן לבחור באפשרויות הבאות:

- יעד שליחת הדיווח: רכיב SOC \ SIEM מקומי של הלקוח, רכיב SOC \ SIEM מרכזי של דיקויה
- פרוטוקול הדיווח: אימייל, Syslog / CEF, API Call
- סוג מנוע סריקה: מנוע סריקה (אנטי-וירוס) מקומי המותקן אצל הלקוח
- תוכן המיועד לסריקה / לדיווח: כל ההודעה, רק התוכן, צרופות, מאפייני ההודעה (Headers)
- חיווי כלפי המשתמש: בחירת חווית השימוש של משתמש הקצה בעת שליחת ההודעה לסריקה / לדיווח – הצגת הודעה מותאמת אישית / שליחת אימייל.
- חיווי כלפי מנהל המערכת: בחירת חווית השימוש של מנהל המערכת בעת שליחת הודעה לדיווח על ידי משתמש הקצה – קבלת אימייל על כל דיווח / קבלת אימייל מסכם אחרי מספר דיווחים / קבלת אימייל מסכם אחרי מספר הודעות שדווחו וזוהו כנכונות (ז"א זיהוי של מתקפה אמתית על ידי אחד ממשתמשי הקצה / קבלת סיכום יומי.
- חווית השימוש של משתמש הקצה: מחיקת האימייל המדווח / העברה לתיקיה אחרת.
- החלה על קבוצה מסוימת: בחירת מקבץ העובדים שעליהם תחול המדיניות הנבחרת.

תצוגה בממשק הניהול

הודעות שדווחו על ידי משתמשי הקצה ניתנות לבחינה בממשק הניהול. בין השאר, ניתן לראות בצורה בטוחה (במקרה שמדובר בהודעה עוינת) את כל פרטי ההודעה השונים כגון שם השולח, כתובת השולח, נושא ההודעה, תאריך, שדות, צרופות וכ"ו.

רשימת המשתמשים שאצלם מותקן כפתור הדיווח גם כן מופיעים בממשק הניהול. בין השאר, ניתן לראות את כל ה-Agents המדווחים וגרסאותיהם, זמן רישום אחרון מול המערכת, ומספר פרטי זיהוי נוספים.

בנוסף, המערכת מציגה מספר נתונים כללים כגון כמות ההודעות שדווחו, כמות ההודעות העוינות שנמצאו ועוד.

כל פרטי התצוגה ניתנים להגדרה והתאמה אישית

סיכום

המערכת פותחה באופן ייעודי על מנת לספק מענה הוליסטי ומלא לאיום הפישינג על המשאב האנושי בארגון.

משתמשי הארגון חשופים למתקפות חוזרות ונשנות ולעיתים באופן יומיומי על ידי מיילים מתחזים וקבצים זדוניים אשר מועברים אליהם בדרכים שונות ובעיקרן תיבת המייל הארגונית. המערכת פותחה על בסיס ידע וניסיון של שנים בתחום ה – Hacking. תוך שימת דגש על התאמה לוקאלית ותרבותית של הסימולציות למדינת היעד בכלל זה, שפה, והבטים תרבותיים וגאוגרפיים אשר מותאמים למדינת היעד, כלל הסימולציות אותן מבצעת חברת Dcoya מדמות מתקפות אמיתיות אשר התקיימו בארגונים שונים בעולם.

המערכת מתוחזקת ומתעדכנת חדשות לבקרים על ידי צוות המחקר של חברת Dcoya. תפקידו של הצוות הוא לחפש באופן שוטף ברשתות האינטרנט וברשתות השחורות מתקפות עדכניות בעולם במטרה להזין את הארגון בדרכי התמודדות אל מול איומים מתחדשים באופן יומיומי.

תפיסת השרות המנוהל הפרו אקטיבי הינה אבן יסוד מרכזית בחברת Dcoya, העקרון בבסיס התפיסה הוא לאפשר ללקוחותינו להמשיך ולהתרכז בליבת העשיה שלהם מבלי להשקיע תשומות זמן בנושא העלאת המודעות והחינוך בקרב המשאב האנושי והפיכתם לכדי מניעה אקטיבית למתקפות Phishing .