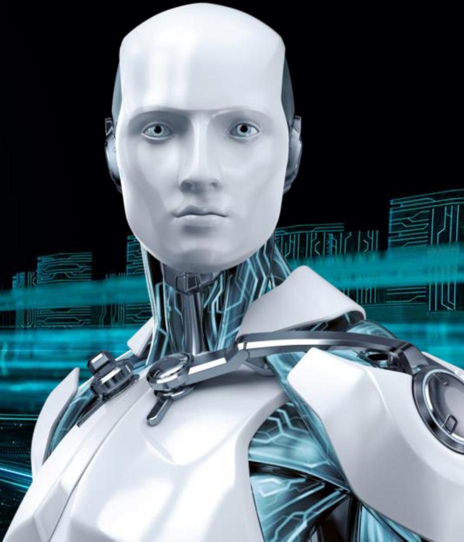
ESET ENJOY SAFER TECHNOLOGY™

Cybersecurity experts on your side

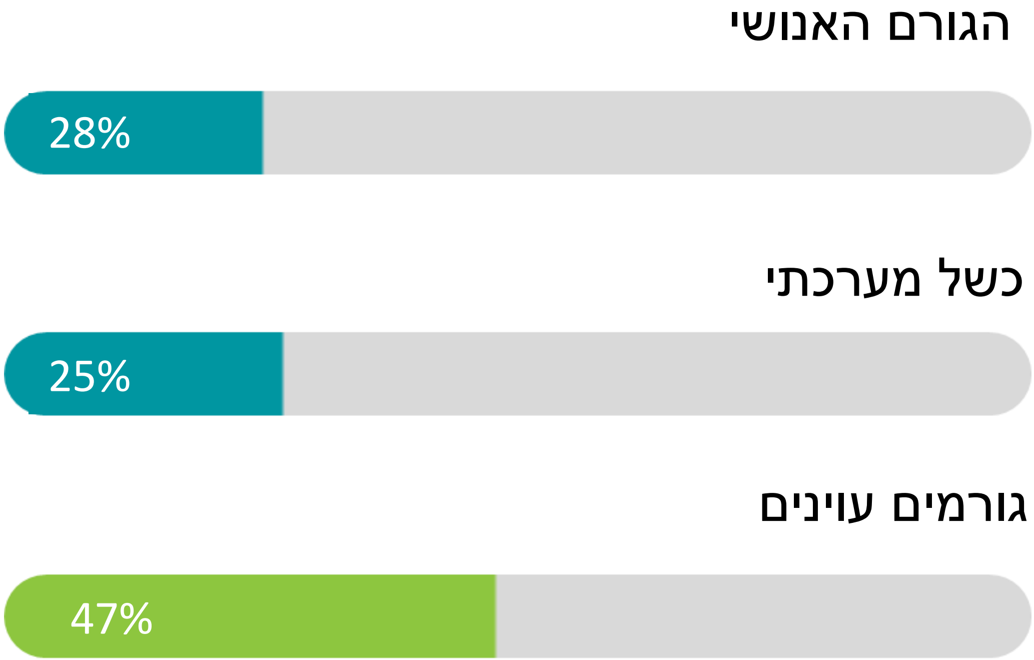
איך שומרים על אבטחת המידע בארגון



מה חשוב להכיר

- סקירת איומים
- סיסמאות בטוחות
- הגנה באינטרנט
- הגנה על תיבות הדוא"ל
- אמצעי הגנה נוספים

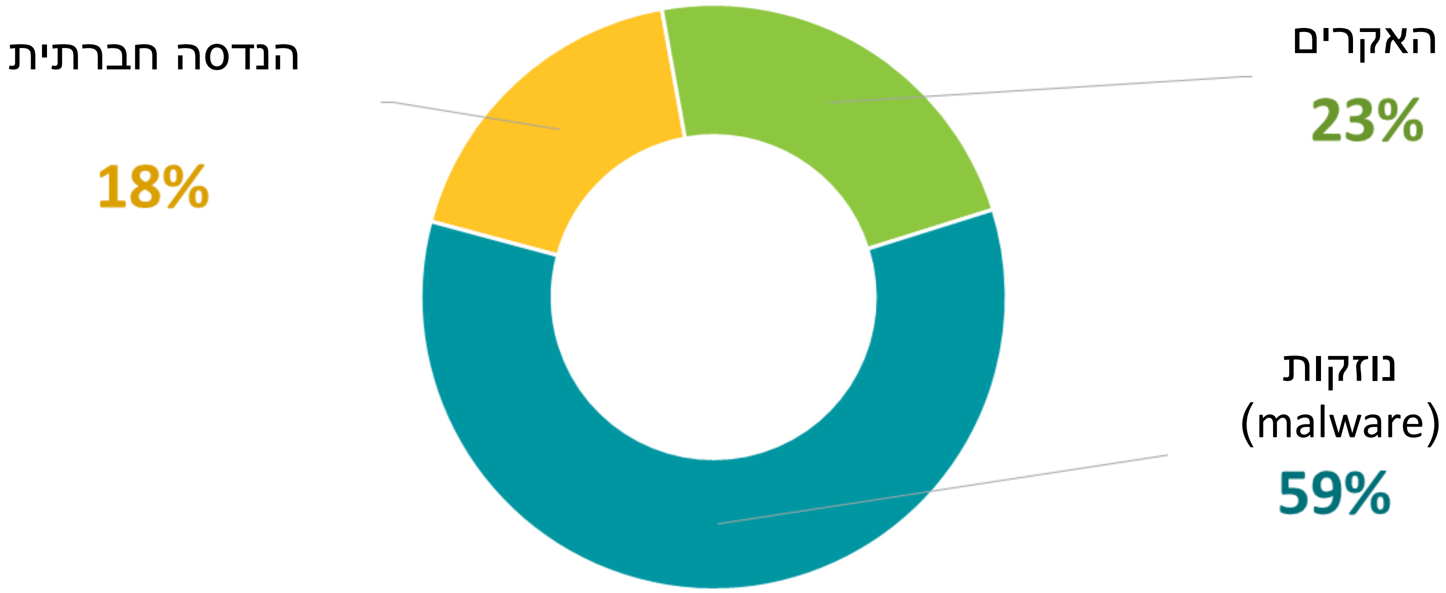
גורמים לדליפת מידע בארגונים



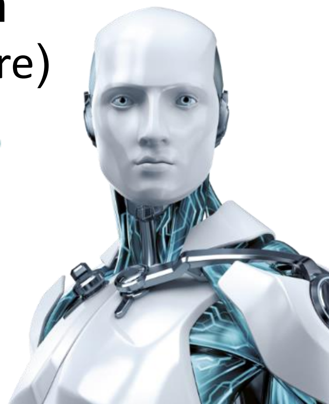
ENJOY SAFER TECHNOLOGY™

Ponemon Institute 2017 Cost of Data Breach Study: Global Analysis

גורמים עוינים



Verizon 2016 Data Breach Investigations Report – specifically: incidents involving credentials



סקירת איומים

ENJOY SAFER TECHNOLOGY™

סקירת איומים

הנדסה חברתית

פישינג

נוזקות (malware)

סקירת איומים

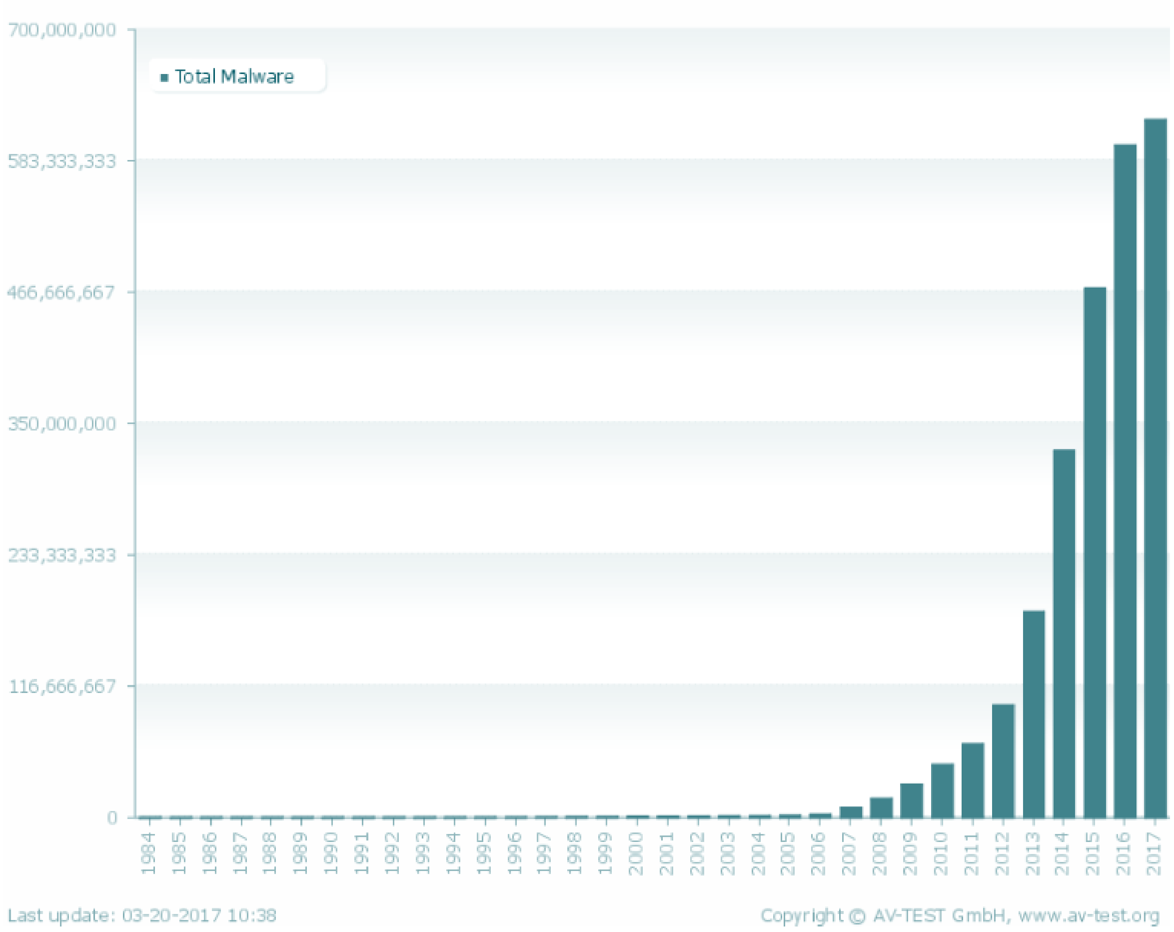
נוזקה (Malware)

לנוזקות (Malware) יש מגוון של סוגים ומשפחות

- Viruses
- worms
- Trojans
- Ransomware
- Rootkits
- Bootkits

ENJOY SAFER
TECHNOLOGY™

גידול בנוזקות (Malware) לאורך זמן



ENJOY SAFER TECHNOLOGY™

איך נדבקים בנוזקות?

דסקטופ

- לחיצה על קובץ, קישור זדוני במייל
- הורדת תוכנה זדונית שמסווה עצמה לתוכנה לגיטימית
- חיבור של התקן חיצוני לא מוכר למחשב

מובייל

- לחיצה על קישור זדוני שנשלח במייל
- הורדת תוכנה זדונית שמסווה עצמה לתוכנה לגיטימית
- התקנת אפליקציה ישירות מהאינטרנט ולא מהחנויות הרשמיות של גוגל ואפל

טיפים למניעת הידבקות בנוזקות

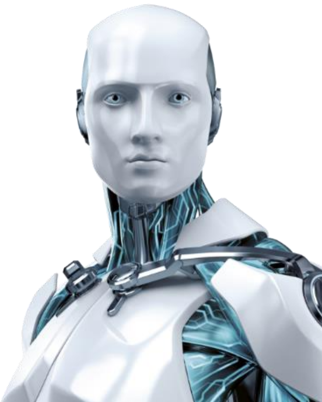
1. יש להתקין תוכנת אנטי וירוס בכל המכשירים
2. שימו לב לחיבור של התקנים חיצוניים לא מוכרים
3. לא ללחוץ על קישורים חשודים, לא מוכרים
4. הדרכת מודעות לעובדים

סקירת איומים

פישינג

מה זה פישינג?

- הונאה במסגרתה מתחזים לגוף מוכר ולגיטימי
- בדרך כלל ההונאה מופצת במייל המבקש לעדכן פרטי חשבון, פרטים אישיים וכו'
- לחיצה על הקישור ומילוי הפרטים שמועברת ישירות להאקרים



ENJOY SAFER TECHNOLOGY™

נתונים

12%

לוחצים על קבצים זדוניים
המצורפים למייל

30%

פותחים מיילים פישינג

Verizon 2016 Data Breach Investigations Report

דוגמאות

----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

כתובת חשודה

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

טעויות כתיב

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

בריחוף עם העכבר על הקישור רואים כתובת URL חשודה.
לא של PayPal

דוגמאות

טקסט שנראה מתורגם מאנגלית בצורה חובבנית

קישור חשוד

ENJOY SAFER TECHNOLOGY™

טיפים להימנעות מהונאות פישינג

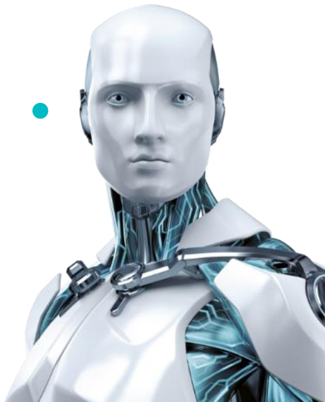
1. שימו לב אם השולח מוכר לכם
2. שימו לב לטעויות כתיב במייל
3. בדקו את ה- URL מבלי ללחוץ עליו (במעבר עם העכבר)
4. אל תלחצו על קישורים לא מוכרים

סקירת איומים

הנדסה חברתית

הנדסה חברתית

- מניפולציה של אנשים במטרה להשיג מהם מידע רגיש
- לרוב מתבצע באמצעות מיילים, אבל גם באמצעות רשתות חברתיות, אפליקציות מסרים ושיחות טלפון – vishing
- האקרים יכולים להתמקד בעובדים בדרגים בכירים, להתקשר ולבקש פרטי כתובת המייל שלהם/טלפון ולעשות בהם שימוש לרעה
- אותו גורם עוין יכול להתחזות לאיש מקצוע ולחדור לארגון בצורה פיזית ולגנוב מידע



ENJOY SAFER TECHNOLOGY™

טיפים למניעת הנדסה חברתית בארגון

1. יש להיזהר עם מידע שחושפים לגורמים מחוץ לארגון
2. חשוב לאמת זהות של ספקים ואנשי מקצוע
3. בכל מקרה של ספק לגבי זהות המתקשר, יש לנתק את השיחה ולהתקשר למשרד הרשמי ולוודא שאכן הם יצרו קשר

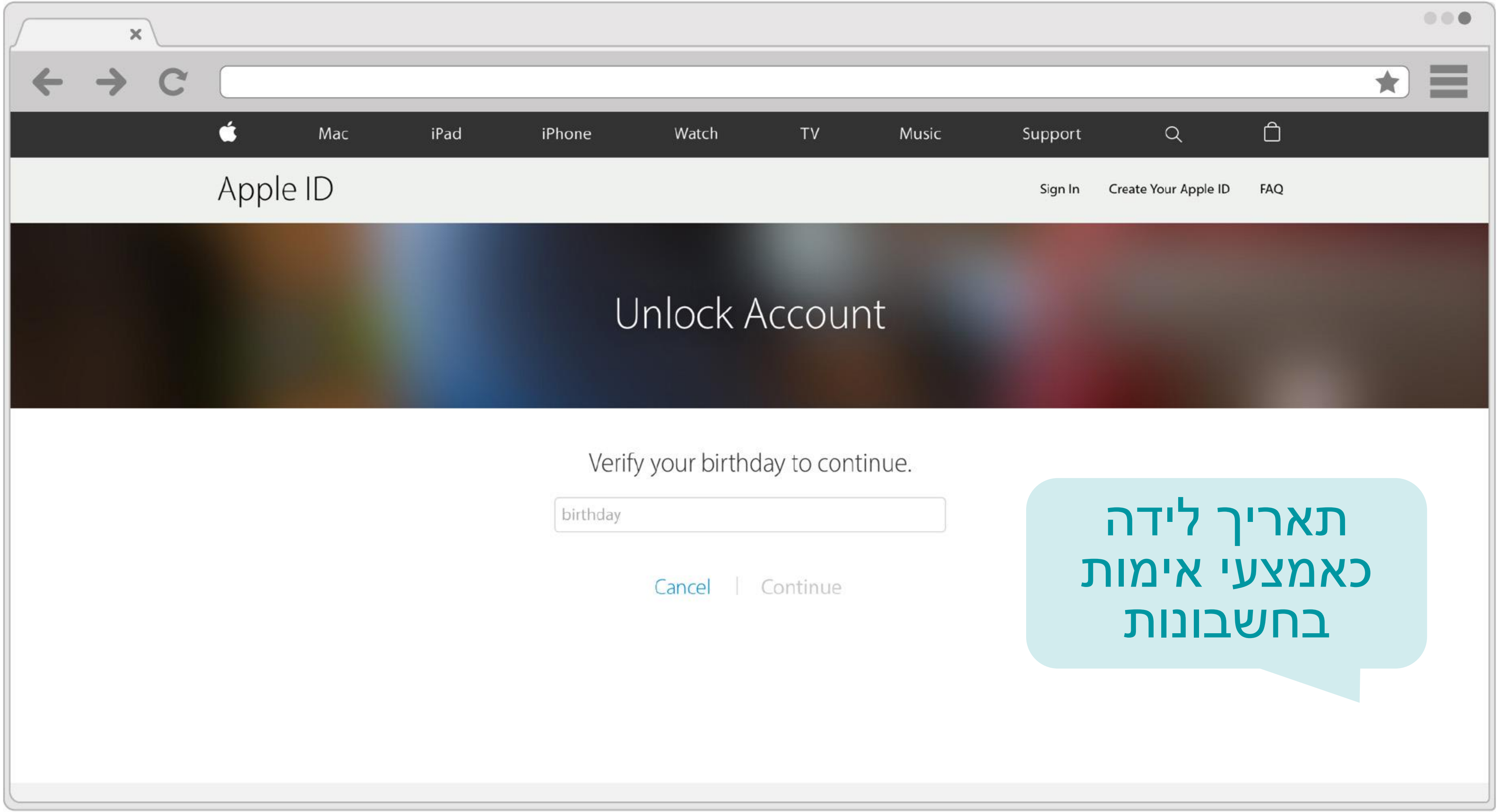
סיסמאות בטוחות

ENJOY SAFER TECHNOLOGY™

האם ניתן למצוא את התשובות לשאלות אלה בחשבון הפייסבוק שלך?

- באיזו עיר גדלת ובאיזו עיר את גר היום?
- מהו השם של חיית המחמד שלך?
- מהו שם התיכון שלמדת בו?
- מהו תאריך הלידה שלך?

ENJOY SAFER TECHNOLOGY™



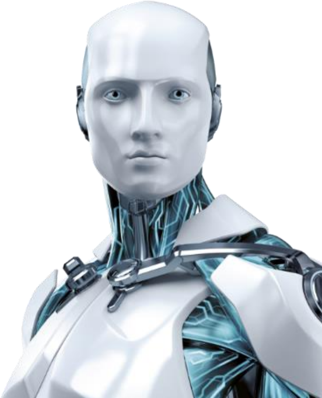
תאריך לידה
כאמצעי אימות
בחשבונות

שאלות אימות זהות

- בדרך כלל בשאלות של אימות זהות, נותנים פרטים נכונים
- גורמים עוינים יכולים לעשות שימוש במידע מחשבונות המדיה החברתיים כדי לחדור לחשבונות פרטיים
- מומלץ מאד להיזהר עם הפרטים שממלאים ולהתייחס אליהם כסיסמאות לכל דבר

חשיבות שמירה על סיסמאות גם במרחב הפיזי

- לא לשמור את הסיסמא בקרבת המחשב
- לא, גם לא בפתק מתחת למקלדת
- או בקובץ אקסל במחשב
- או כקובץ במחשב



חשיבות שמירה על סיסמאות גם במרחב הפיזי

- לא לשתף את הסיסמאות עם חברים, בני משפחה וקולגות
- לא לשתף ב-SMS, בוואטסאפ, בפייסבוק או בכל רשת חברתית את הסיסמא שלכם וגם לא במייל

ENJOY SAFER TECHNOLOGY™

10 הסיסמאות הנפוצות ביותר (שלוקח שנייה לפצח)

- 123456
- password
- 123456789
- 12345678
- 12345
- 111111
- 1234567
- sunshine
- qwetry
- iloveyou

האם אתם מזהים את הסיסמא שלכם ברשימה?

איך מגדירים סיסמא קשיחה?

- בחרו שלוש מילים אקראיות שאינן קשורות אחת לשנייה והקלידו ללא רווחים
- לפחות 12 תווים
- כוללת אותיות גדולות, קטנות, ספרות ותווים מיוחדים
- החלפה של תווים ברורים מאליו היא מיותרת (להחליף s ב $, להחליף o ב 0, להחליף A ב 4 וכו')

- השתמשו בסיסמאות שונות עבור שירותים שונים
- החליפו סיסמאות לעיתים תכופות, לפחות בשירותים שאתם מנדבים להם הכי הרבה מידע כמו גוגל ופייסבוק ולחשבונות חשובים כמו של הבנק.
- עבדו עם כלי ניהול סיסמאות המאפשרים יצירה ושמירת סיסמאות מורכבות ושונות ודורשים לזכור סיסמא אחת בלבד לצורך גישה.

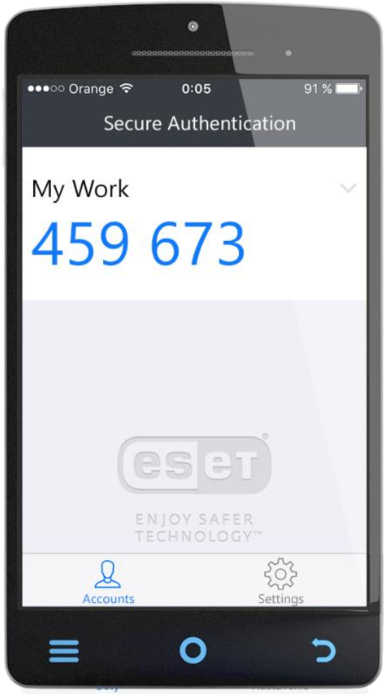
ESET ENJOY SAFER TECHNOLOGY™

מנהל הסיסמאות

אמצעי יעיל לשמירה על סיסמאות הוא שמירה בתוכנה מוכרת ומאובטחת לניהול סיסמאות. כך לא צריך לזכור עשרות סיסמאות, אלא סיסמא מורכבת אחת לכניסה לתוכנה

ENJOY SAFER
TECHNOLOGY™

אימות דו שלבי (2FA)



אימות דו שלבי הוא אמצעי יעיל להגנה על סיסמאות שמשתמשת בשני אלמנטים.

- שימוש במידע שיש למשתמש (סיסמא או קוד זיהוי)
- שימוש במכשיר פיסי – מכשיר נייד למשל

שילוב של השניים מחזק את ההגנה על המידע

טיפים להגנה על סיסמאות

1. שימוש בסיסמאות מורכבות וקשיחות בכל החשבונות
2. מומלץ לעשות שימוש באימות דו שלבי בכל החשבונות
3. יש להתייחס לשאלות אימות זהות כמו לסיסמאות

הגנה באינטרנט

ENJOY SAFER TECHNOLOGY™

איומים במרחב האינטרנטי

Internet of Things

רשתות Wi-Fi ציבוריות

HTTPS

HTTPS

- פרוטוקול לחיבור אינטרנט מאובטח
- חשוב לשים לב באתר שמבקש פרטי חשבון, כרטיסי אשראי וכו' מופיעה כתובת הURL בצבע ירוק עם מנעול והכיתוב HTTP

ENJOY SAFER TECHNOLOGY™

רשתות Wi-Fi ציבוריות

- בדרך כלל רשתות חינמיות ללא סיסמא להתחברות, קיימות בעיקר בבתי קפה, אוניברסיטאות, ספריות, מלונות ועוד.

- אל תניחו אף פעם שרשת WiFi בשם בית הקפה בו אתם יושבים היא אכן הרשת של בית הקפה. ייתכן וזוהי רשת שהקים האקר באותו השם..

- יש להיזהר בחיבור לרשת ציבורית ולהתייחס אליה כלא בטוחה

- אם אתם חייבים להתחבר לחשבון עם מידע רגיש (בנק, מדיה חברתית וכו') עדיף לעשות זאת מהמכשיר הנייד ברשת הסלולארית

ENJOY SAFER TECHNOLOGY™

Internet of things

- האינטרנט של הדברים המוכר כ-IoT מאפשר חיבור בין מכשירים, למשל בית חכם, רכב חכם וכו'.

- עם זאת, חשוב לזכור שבשימוש בIoT יש סיכון של פרצות אבטחה מאחר וכל אחד יכול להתחבר למכשיר החכם מרחוק באמצעות סיסמא (שלפעמים קל להשיג)

- ודאו שכל המכשירים החכמים מעודכנים בגרסאות האחרונות ביותר

ENJOY SAFER
TECHNOLOGY™

Internet of things

- נטרלו תכונות לא הכרחיות במכשירים החכמים (למשל מצלמה או רמקול בטלוויזיה חכמה)
- חשוב לוודא שהראוטר (נתב) אליו כל המכשירים החכמים מתחברים, מוגן בסיסמא קשיחה ומורכבת
- יש לדאוג שהראוטר מעודכן כל הזמן כדי להימנע מפריצות

טיפים להגנה באינטרנט

1. יש לבדוק שהאתר מאובטח לפני שמקלידים מידע רגיש
2. יש להתייחס לכל רשת ציבורית כאל רשת לא בטוחה
3. יש לוודא שהראוטר אליו מחוברים כל המכשירים החכמים מעודכן ומוצפן עם סיסמא מורכבת וקשיחה

הגנה על תיבות דוא"ל

ENJOY SAFER TECHNOLOGY™

הגנה על תיבות דוא"ל

קבצים מצורפים

הגנה מפני דואר זבל (ספאם)

שחזור סיסמא

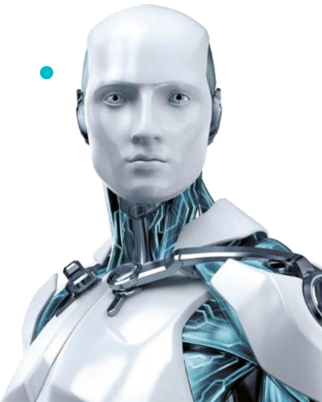
אימות דו-שלבי

הגנה על תיבות דוא"ל

אימות דו-שלבי

אימות דו-שלבי (2FA) ותיבת הדואר"ל

- דואר"ל הוא החשבון החשוב ביותר שזקוק להגנה, כי במידה ומישהו מקבל גישה לדואר"ל שלכם, הוא יכול לנצל את הפונקציה של איפוס הסיסמה כדי לקבל גישה לשירותים אחרים.
- אימות דו-שלבי הוא דרך מצוינת להגן על תיבת הדואר"ל מפני פריצות.
- רוב ספקי הדואר"ל הגדולים מאפשרים להגדיר אימות דו-שלבי על חשבון הדואר"ל.
- לאחר התקנה של אימות דו-שלבי, התוקף צריך גם את הסיסמה וגם את הטלפון הסלולרי שלכם כדי לפרוץ את חשבון הדואר"ל



ENJOY SAFER TECHNOLOGY™

הגנה על תיבות דוא"ל

שחזור סיסמאות

שחזור סיסמאות

- כאשר שוכחים סיסמא, האפשרות לשחזר אותה היא מאוד פשוטה. אם שחזור הסיסמא לא מוגדר נכון, בקלות ניתן להשתלט על חשבון הדוא"ל.
- אתרים מסוימים לא דורשים שאלת אבטחה או מידע נוסף פרט לכתובת המייל על מנת לשחזר את הסיסמא.
- בדרך כלל כאשר מבקשים לשחזר סיסמא שנשכחה, נשלח מייל לאישור שחזור הסיסמא.
- חשוב לעקוב אחר המיילים הללו וליצור קשר עם השירות ששלח את המייל במידה ואתם לא דרשתם לשחזר את הסיסמא באופן יזום (זכרו גם את המיילים המתחזים שהזכרנו קודם).

ENJOY SAFER TECHNOLOGY™

הגנה על תיבות דוא"ל

הגנה מפני דואר זבל (ספאם)

איך להתגונן מדואר זבל (ספאם)?

- כולם מקבלים דואר זבל. אפילו עם ההגנות הטובות ביותר, תמיד יהיו כמה שיעברו את כל הסינונים.
- יש ספקיות דוא"ל טובות יותר בסינון דואר זבל מאחרות.
- מוצר אנטי ספאם משלים יכול להוות סינון נוסף לזה של ספקית האימייל, ולהקטין את כמות דואר הזבל המתקבלת.

ENJOY SAFER TECHNOLOGY™

הגנה על תיבות דוא"ל

קבצים מצורפים

קבצים מצורפים

- קבצים מצורפים הם אחת מהדרכים הנפוצות ביותר להפצת נוזקות ווירוסים.
- גם קובץ מצורף שנראה כמו מסמך או קובץ אקסל או PDF, יכול להכיל נוזקה.
- לעולם אין לפתוח קבצים מצורפים ממקורות בלתי מוכרים.
- אם אתם רואים קובץ מצורף חשוד, אפילו קצת או למראית עין, שלחו אותו למנהל הרשת או אבטחת המידע שלכם כדי שיוודא שהוא תקין.

ESET ENJOY SAFER TECHNOLOGY™

טיפים להגנה על תיבות הדוא"ל

1. חשובה מדיניות ברורה לגבי פתיחת קבצים מצורפים בדוא"ל
2. לעולם אין לפתוח קבצים מצורפים ממקורות בלתי מוכרים.
3. לעולם אל תפתחו דואר זבל, גם אם התוכן שלו נראה לכם מצחיק או חובבני
4. השתמשו בסיסמאות מורכבות וקשיחות
5. אתרו ניסיונות לאיפוס סיסמא שלא נעשו על ידיכם כדי להימנע מהונאות וחטיפת חשבונות
6. אפשרו אימות דו-שלבי לא רק בחשבונות הדוא"ל אלא גם באתרים ואפליקציות אחרות שמאפשרות זאת (כמו ברשתות חברתיות)

אמצעי הגנה נוספים

ENJOY SAFER TECHNOLOGY™

טיפים נוספים להתגוננות

1. השתמשו בתוכנת אבטחת מידע (אתם יודעים איזו) בכל המכשירים שלכם, כן כן גם במובייל ולא רק במחשבים עם מערכת הפעלה Windows
2. הפרידו בין הסיסמאות של החשבונות הפרטיים שלכם לסיסמאות של החשבונות בעבודה.
3. עדכנו את כל התוכנות והחומרה בהם אתם משתמשים עם עדכוני האבטחה האחרונים.

ESET®

ENJOY SAFER TECHNOLOGY™