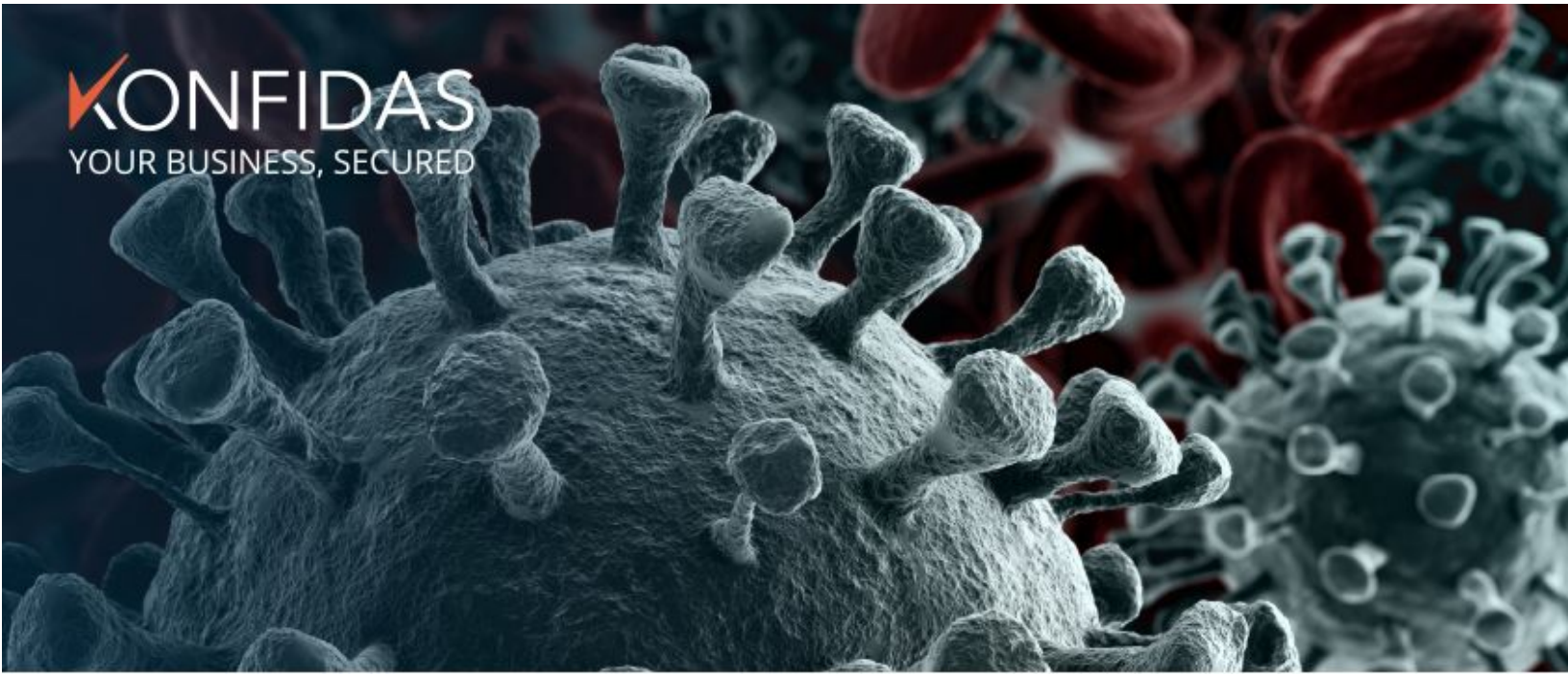


היבטי סייבר ונגיף הקורונה (COVID-19)

עדכון יומי ליום א', 22.03.2020

הדוח היומי מתפרסם גם במדור "קפטן אינטרנט" של עיתון הארץ

https://www.haaretz.co.il/captain

איומים, התקפות והתראות

#1

משרד הבריאות הישראלי מתריע על הודעת פייק ניוז נוספת.

משרד הבריאות מדווח על הודעת פייק ניוז נוספת, הפעם בשם הרב יצחק יוסף, בנושא קיום יחסי אישות בזמן בידוד.[1] יש לשים לב ולהיזהר מהודעות כוזבות רבות אשר מופצות במדיה החברתית ובערוצים אחרים ולהקפיד להתעדכן באמצעות ערוצים אמינים, כגון אתר משרד הבריאות וערוץ הטלגרם שלו, פורטל החירום הלאומי של פיקוד העורף והאתר של מערך הסייבר הלאומי.

[1] https://t.me/MOHreport/3309

#2

משטרת ישראל מפרסמת אזהרה לציבור על ניסיונות הונאה על רקע מגפת הקורונה.

מתווה ההונאה מתבצע באמצעות מספר דפוסים: יצירת קשר עם הקורבנות באמצעות: (1) שימוש במייל ואתרים מתחזים לחברות מוכרות בעולם, (2) יצירת קשר טלפוני עם אוכלוסיות הגיל השלישי והתחזות לרופא שמוסר הודעה לפיה קרוב משפחה מאושפז בבית חולים בעקבות נגיף הקורונה, ויש צורך בהול בהעברת תשלום על מנת לממש טיפול מציל חיים, (3) הפצת מיילים המכילים קישורים מתחזים לאתרי אינטרנט המספקים ייעוץ רפואי לציבור. מיילים אלה מפיצים עדכונים נוספים, כמו המלצות על דרכי התגוננות ומפת התפשטות עולמית של הנגיף. בנוגע להונאות מסוג זה, על פי משטרת ישראל "ההונאות טרם הגיעו לישראל, ובשלב הזה לא ידוע על אזרחים שנפלו קורבן למעשים, אך נבקש להזהיר את הציבור באפשרות הקיימת ולנהוג במשנה זהירות."[2]

#3

קמפיין פישינג נוסף המתחזה לארגון הבריאות העולמי.

חברת MalwareBytes Labs מדווחת שקמפיין פישינג נוסף מתחזה לארגון הבריאות העולמי (World Health Organization). קמפיין זה מופץ באמצעות מיילים המכילים קובץ בשם :"MyHealth-Ebook.zip", הכולל בתוכו נוזקה שגונבת מידע מהמחשב אליו הורד הקובץ ונשמר בצורה מוצפנת ב-Google Drive.

אינדיקטורים רלוונטיים:

HASH:

de1b53282ea75d2d3ec517da813e70bb56362ffb27e4862379903c38a346384d

FormBoo URL:

[3]drive.google[.]com/uc?export=download&id=1vljQdfYJV76IqjLYwk74NUvaJpYBamtE

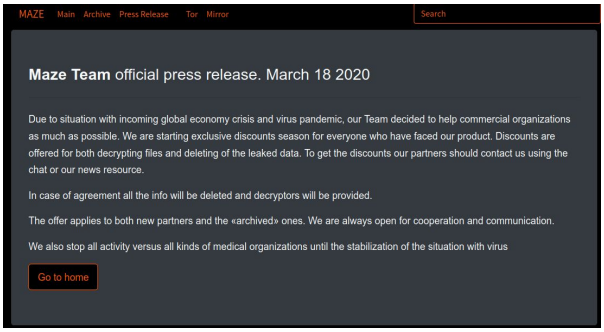
[2] https://www.gov.il/he/departments/news/police_covid-19_17032020_phishing

[3] https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

#4

האקרים ממשיכים לנצל את בהלת הקורונה לצרכי תקיפה ומפרסמים הודעות שיימינג.

לאחרונה מתחיל מתווה התקיפה של ההאקרים לקבל צורה של אתרים המוכרים מוצרים רפואיים להתמודדות עם הקורונה, הודעות פייק ניוז וקמפיינים של פישינג והנדסה חברתית. ניתן לראות כי גם בפורומים פנימיים, האקרים מתעניינים בחולשות ותקיפות העושות שימוש במגיפה לצורך טיוב התקיפה.[4] כל זאת נעשה חרף ההתחייבויות הפומביות של חלק מההאקרים להימנע מטירגוט בתי חולים ומרכזי בריאות נוספים.



מעניין לגלות שקבוצת תקיפה השתמשה באתר האינטרנט של אחד מקורבנותיה כדי לפרסם "הודעה לעיתונות", מזוייפת כמובן, לפיה "בגלל המשבר הגלובלי ומגיפת הקורונה היא תציע הנחות לקורבנות הכופר שלהם.[5]

#5

עליה עולמית במתקפות הספאם ופוגענים הקשורים לנגיף הקורונה ב-Q1 של 2020.

דוח של Trend Micro מציג את הכמות העצומה של מתקפות ספאם ופוגענים הקשורים בנגיף הקורונה. ניתן לראות בתרשים כי ברבעון הראשון של 2020, בצל הקורונה, היו בבריטניה יותר מ-80,000 פוגענים ומתקפות ספאם ובצרפת יותר מ-45,000. אירופה מובילה בכמות המתקפות, ואחריה אסיה, צפון אמריקה ואמריקה הלטינית.[6]

[4] https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

[5] https://krebsonsecurity.com/2020/03/security-breach-disrupts-fintech-firm-finastra/#more-50960

[6] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

#6

פרצות אבטחה באפליקציות לניהול סיסמאות.

מחקר שנערך באוניברסיטה ביורק בחן חמש אפליקציות מוכרות בעולם לניהול סיסמאות (LastPass, Dashlane, Keeper, 1Password, and RoboForm). בחקירה נמצאו בהן 4 חולשות חדשות. אחת מהן, המשותפת ל-1Password וב-LastPass, נגרמת ממנגנון לקוי של השלמה אוטומטית של הסיסמאות באתרים השונים, ובכך יוצרת חשיפה מיותרת של סיסמאות נוספות הרלוונטיות לאותו אתר - לדוגמה, סיסמאות לחשבונות גוגל.[7]

סייבר וקורונה בישראל

#7

הממשלה אישרה את תקנות המשק לשעת חירום, הכוללות את מערך הסייבר הלאומי ואת חברות הסייבר.

ב-22.03.2020 בשעה 08:00 נכנסו לתוקף של 7 ימים תקנות שעת חירום המתייחסות, בין השאר, לכוח אדם חיוני במשק. במסגרת התקנות הללו, מערך הסייבר הלאומי מורשה להעסיק 70% אחוזים ממצבת העובדים[8]. חברות הסייבר והמחשוב במשק הישראלי אף קיבלו הרשאה להעסיק כוח אדם באופן חריג, לרבות שירותי טכנאות, שירותי תקשורת, השירותים והמוצרים של הגנת הסייבר ואבטחת מידע ושירותי מחשוב, שירותי תמיכה, תחזוקה ואחזקת בסיסי נתונים ופיתוח הכרחיים, כל עוד לא ניתן לבצעם באמצעות גישה מרחוק,[9] "ובלבד שהגופים צמצמו ככל האפשר את מספר העובדים למספר הדרוש לצורך הבטחת פעילותם החיונית..." (תקנה 2(ב)).[10] גם חברות התקשורת הוחרגו לצורך אספקת השירותים או המוצרים הנדרשים לשם המשך פעילותם התקינה של תחומים כגון: שירותי בזק פנים-ארציים נייחים, שירותי בזק בינלאומיים, שירותי רדיו טלפון נייד ("מובייל"), לרבות ברשת אחרת, שירותי גישה לאינטרנט, שירותי תקשורת נתונים, שירותי תקשורת לווויינית, שירותי אירוח שרתים, שירות מיתוג אינטרנט ואיגוד האינטרנט הישראלי[11]. בהקשרי שרשרת האספקה של המערכת הבנקאית ושוק ההון, הוחרגו, בין היתר, ספקי שירות של מערכת ליבה בנקאית וספקים העוסקים במתן ייעוץ לגוף מוסדי בנושאי ממשל תאגידי, ניהול סיכונים וכו'[12].

[7] http://eprints.whiterose.ac.uk/158056/8/Revisiting_Security_Vulnerabilities_in_Commercial_Password_Managers_2.pdf

[8] https://www.gov.il/BlobFolder/guide/new_action_level/he/new_action_level_files_guidelines_full.pdf

[9] https://www.gov.il/BlobFolder/guide/new_action_level/he/new_action_level_files_guidelines_industry.pdf

[10] https://www.gov.il/he/departments/faq/corona-regulations

[11] https://www.gov.il/BlobFolder/guide/new_action_level/he/new_action_level_files_guidelines_communication.pdf

[12] https://www.gov.il/BlobFolder/news/spoke_takanot210320/he/Gov_Dec_Takanot210320.pdf
https://www.gov.il/he/Departments/Guides/new_action_level?chapterIndex=2

#8

משרד הבריאות מפרסם את אפליקציית "המגן" - אפליקציה למלחמה בקורונה.

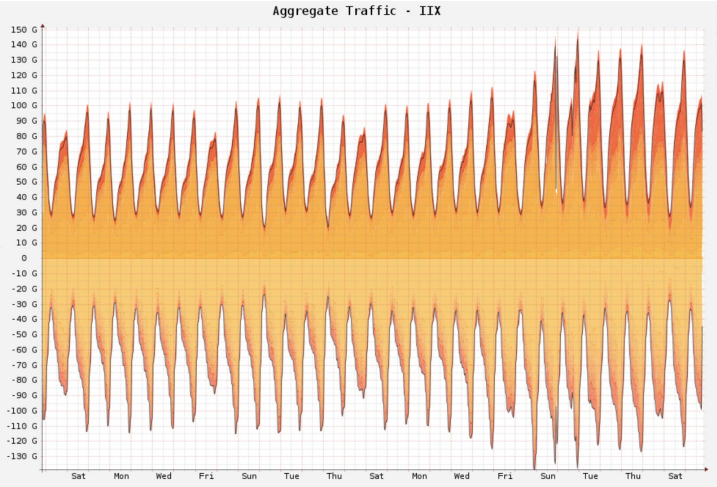
אפליקציית "המגן" מצליבה את מיקום המשתמש עם מפות המסלולים של חולי הקורונה המאומתים ומעדכנת במקרה של חפיפה. האפליקציה פועלת ברקע והמידע נשאר על המכשיר של המשתמש בלבד. ניתן להוריד את "המגן" ללא תשלום גם ב-App Store וב-Google Play.[13]

פרופ' מיכאל בירנהק התייחס להביטי הפרטיות של האפליקציה וציין: "הייתי בקשר עם צוות משרד הבריאות בשבוע החולף, בדקתי את תנאי השימוש של "המגן" בהיבטי הפרטיות (אך לא בהיבטי אבטחת מידע, שאינם בתחום המומחיות שלי [...] ואני מבקש לומר בצורה ברורה: *** בהיבטי הפרטיות, זו אפליקציה מצוינת ***"[14].

#9

עלייה בעומסים בחברות תקשורת בישראל - משק התקשורת הוגדר כמשק חיוני.

העומסים בתעבורת האינטרנט עלו באופן צפוי בהיקף שבין 20% ל-30%[15]. ניתן לראות על פי נתוני התעבורה הכוללים של ה-IIX מאיגוד האינטרנט הישראלי את העליה בעומסים החל מיום ראשון ה-15.3.2020. יש לקחת בחשבון שהנתונים הם רק של תעבורה פנים-ישראלית (מכתובת ip ישראלית לכתובת ip ישראלית) ושלא כל התעבורה הפנים ישראלית עוברת דרך המחלף (בזק בינלאומי, סלקום ופרטנר מקושרים גם ישירות ביניהם)[16]. מבדיקה שנעשתה על ידי משרד התקשורת עם חברות התקשורת, עולה כי הן ערוכות למתן מענה גם במקרה של עומסים משמעותיים יותר.[17] כחלק מהערכות חברות התקשורת למשבר הנחה שר התקשורת שחברות התקשורת יפעלו על פי ההגדרות הבאות: המערך ההנדסי יפעל ב-100% כח אדם על מנת לוודא פעילות תקינה של כלל המערכות, מערך השירותים הכללי ירד ל-50%, מטה והנהלה ל-30%.[18]



[13] https://itunes.apple.com/us/app/id1503224314?ls=1&mt=8
https://play.google.com/store/apps/details?id=com.hamagen
[14] https://twitter.com/Birnhack/status/1241799050292350976
[15] https://www.gov.il/he/departments/news/18032020_1
[16] https://www.isoc.org.il/technologies-and-infrastructure-services/iix/iix-statistical-traffic-data
[17] https://www.isoc.org.il/technologies-and-infrastructure-services/iix/iix-statistical-traffic-data
[18] https://www.gov.il/he/departments/news/16032020

#10

הפסקת ניוד מספרים.

שר התקשורת הנחה להקפיא את יכולת הלקוחות לבצע מעבר בין חברות הסלולר החל מיום ראשון ה-22.3.2020 למשך שבועיים. המהלך מאפשר לחברות לרכז מאמץ בתחום הכשירות הטכנית, לצמצם כח אדם שבשגרה מופנה לגיוס ושימור לקוחות, וליצור בטווח הנראה לעין ודאות פיננסית גבוהה יותר לחברות[19]. על פי השימוע שהתקיים ב-23.3.2020 במשרד התקשורת, "בתקופה זו נדרש כי בעלי רישיונות הרט"ן ("מובייל") יפנו את כל משאביהם ליציבות טכנולוגית של הרשתות, ושמירה על רציפות תפקודית במתן שירות למנוייהם. ביצוע פעולות שיווקיות לצורך קליטת מנויים עלול לגרוע ממשאבי בעלי הרישיונות הנדרשים בעת הזו למיקוד פעילותם באספקת שירות תקשורת באופן רציף הכולל, בין היתר, תפעול של הרשת, טיפול באירועים מתפתחים ומתן שירות ללקוח."[20]

#11

רשות החדשנות מפרסמת קולות קוראים לפיתוחים ומוצרים תעשייתיים שיסייעו בהתמודדות עם נגיף הקורונה.

ביום ראשון ה-22.3.2020 פרסמה הרשות שני קולות קוראים כדי לאפשר ליזמים לתרום למאמץ נגד התפשטות נגיף הקורונה. הם מיועדים לתמיכה בפיתוחים במגוון תחומים, ביניהם הרחבת השירותים הניתנים ברפואה מרחוק.[21]

#12

הרשות להגנת הפרטיות ממשיכה לעמוד לשירות הציבור גם בימים אלה.

עקב ההשלכות הרבות של התפשטות נגיף הקורונה, בין היתר בתחום הגנת הפרטיות, **הרשות להגנת הפרטיות הקימה "קו חם"** לסיוע במתן פתרונות פרקטיים ומהירים בתחום זה. השירות זמין דרך עמוד הפייסבוק או במייל: ppa@justice.gov.il.[22]

#13

כרטיסי הרב-קו יסייעו לאבחן אם אדם נסע עם חולה קורונה.

שירות חדש של משרד התחבורה והרשות הארצית לתחבורה ציבורית **מאפשר לנוסעי התחבורה הציבורית שביצעו נסיעות בכרטיס הרב-קו לקבל מידע על היסטוריית הנסיעות.** שירות זה מאפשר לעשות חיתוך מדויק של קווי אוטובוס

[19] https://www.gov.il/he/departments/news/18032020_1

[20] https://www.gov.il/BlobFolder/rfp/22032020_4/he/Hearing_Teaching_by_virtue_of_provision_under_section_11b_of_the_Communications_Law.pdf

[21] https://innovationisrael.org.il/events/4893

[22] http://uclicks.inforumail.com/?page=webview&message=%2CEzN0lT02YzM&token=6671870087-9bf3bbc0ff98ce528f31e807af00608d

בהם נסעו לצורך השוואה עם מסלולי נסיעה של חולי קורונה מאובחנים. לצורך בדיקה יש להתקשר למוקד המידע של משרד התחבורה *8787 או למפעיל התחבורה ולמסור את מספר כרטיס הרב-קו האישי.[23]

סייבר וקורונה בעולם

#14

ה-FBI מפרסם אזהרה כנגד הונאות הקשורות בנגיף הקורונה.

באזהרה של ה-FBI מוצגות ההונאות הנפוצות ביותר: מיילים כוזבים מטעם ה-CDC (Centers for Disease Control and Prevention), מיילים מסוג פישינג לצורך גניבת פרטים אישיים (סיסמאות, פרטי אשראי, פרטי התחברות) ואתרים כוזבים למכירת ציוד רפואי ייעודי להתמודדות עם הנגיף.[24]

#15

NIST מפרסמים המלצות לאבטחת עבודה מרחוק (teleworking).

המכון הלאומי לתקנים וטכנולוגיה (NIST) פרסם מקבץ הנחיות לצורך התנהלות בטוחה בעת עבודה מרחוק. ההנחיות כוללות טיפים וקווים מנחים לעבודה מרחוק, למניעת האזנות, להקשחת שיחות ועידה ועוד.[25]

#16

הנחיות לזיהוי כוח אדם חיוני להגנה על תשתיות קריטיות בארה"ב.

הסוכנות האמריקאית להגנת הסייבר ותשתיות קריטיות (CISA) פרסמה הנחיות בהן הגדירה כיצד לזהות אילו עובדים חיוניים להגנה על תשתיות קריטיות. ההנחיה נועדה לתמוך בזיהוי מגזרי התשתית הקריטיים והעובדים החיוניים לשמירה על השירותים החיוניים לארה"ב ונדרשים לפעול באופן תקין בזמן מגפת הקורונה. CISA מגדיר 16 סקטורים כתשתיות קריטיות, וביניהן בריאות, גופים פיננסיים, תחבורה, אנרגיה, מזון, וטכנולוגיית המידע.[26]

[23] https://www.gov.il/he/departments/news/multi_line_cards_will_help_diagnose_if_you_traveled_with_a_corona_patient
[24] https://www.ic3.gov/media/2020/200320.aspx
[25] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf
[26] https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19

#17

אפליקציה לאיתור חולי קורונה בסינגפור.

לצורך האטת קצב התפשטות נגיף הקורונה בסינגפור, ממשלת סינגפור פיתחה אפליקציה בשם "TraceTogether". האפליקציה מבוססת על מעקב אחר אותות Bluetooth של מכשיר הטלפון לצורך זיהוי המסלול של חולי קורונה והאם יש נדבקים נוספים בקרבת מקום. לאפליקציה יכולת לזהות מרחק בין שני מכשירים אשר היא מותקנת בהם וכך לאמת מקרי הדבקה. ניתן להשתמש במידע זה כדי לזהות אנשי קשר קרובים על סמך קרבת ומשך המפגש בין שני משתמשים. לאחר אישור שאדם נושא את הנגיף, הוא יכול לבחור לאפשר למשרד הבריאות לגשת לנתונים באפליקציה כדי לעזור בזיהוי אנשי קשר שהיו בקרבה פיזית אליו.[27]

#18

Cert-EU, Enisa, Europol והאיחוד האירופי הוציאו הצהרה משותפת

בהצהרה שניתנה, הכריזו הגופים כי יש ביניהם שיתוף פעולה וקשר מתמיד לצורך מעקב אחר פעילויות חשודות במרחב הסייבר והגברת מודעות האזרחים.[28]

#19

צפויה עלייה משמעותית בעלות נזקי הסייבר בשנת 2021

דו"ח של Cybersecurity Ventures מציג נתון חדש, לפיו בשנת 2021 צפוי העולם לשלם כ-6 טריליון דולר בשנה בגין נזקי סייבר. גורם מהותי בנתון הזה הוא המעבר החד לעבודה מרוחקת כתוצאה מנגיף הקורונה ובהתאם לכך גידול בהתקפות הסייבר על נתח גדול יותר מהאוכלוסייה.[29]

[27] https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether
[28] https://www.enisa.europa.eu/news/enisa-news/joint-fight-against-covid-19-related-threats
[29] https://finance.yahoo.com/news/cybercrime-damage-costs-may-double-172000803.html

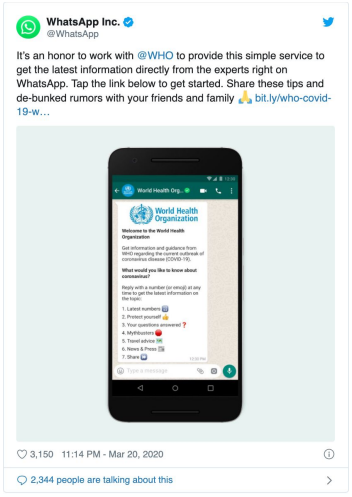
פתרונות

#20

Proofpoint מציעה סט חינמי של חוקי IDS לזיהוי תקיפות הקשורות בנגיף הקורונה

יחידת המחקר של החברה זיהתה 42 חתימות של איומי סייבר הקשורים בנגיף הקורונה. חתימות המכילות מיילים, קבצי Word, דפי אינטרנט, חשבונות משתמשים ועוד.[30]

#21



וואטסאפ בוחנת פיצ'ר שיעזור להתמודד עם פייק ניוז.

וואטסאפ משיקה, בשיתוף פעולה עם ארגון הבריאות העולמי (WHO), שירות המספק מענה אמין ומהיר בכל הנוגע לדרכי התמודדות עם נגיף הקורונה. בכך עוזרת וואטסאפ לצמצם את הסתמכות המשתמשים על גורמים כוזבים ברחבי הרשת ומפיצי פייק ניוז.[31]

#22

מיקרוסופט מפסיקה את עדכוני Microsoft Edge בגלל הקורונה.

כתוצאה מההתפתחויות האחרונות בתחום הסייבר, חברת מיקרוסופט החליטה כי היא מפסיקה להוציא עדכוני תוכנה ל-Microsoft Edge. גם ב-Google Chrome הכריזו כי יתמקדו בהגברת האבטחה עקב התגברות האיומים, על פני שחרור גרסאות חדשות.[32]

[30] https://www.proofpoint.com/us/threat-insight/post/practitioners-update-free-covid-19-related-ids-rules
[31] https://twitter.com/WhatsApp?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1241110782235930624&ref_url=https%3A%2F%2Fabout.fb.com%2Fnews%2F2020%2F03%2Fcoronavirus%2F
[32] https://blogs.windows.com/msedgedev/2020/03/20/update-stable-channel-releases/
https://twitter.com/MSEdgeDev/status/1241055996379664384

העשרה

#23

450 קורסים אינטרנטיים חינמיים מוצעים על ידי האוניברסיטאות המובילות בעולם.

העובדה כי מרבית המשק מושבת ולא מועסק גורמת למוסדות אקדמיים רבים לפתוח קורסים דיגיטליים לאוכלוסייה הרחבה, כדי לתמוך בניצול יעיל יותר של הזמן בבית. כתוצאה מכך, שמונה האוניברסיטאות בליגת הקיסוס (Ivy League) מנגישות קורסים במגוון תחומים : מדעי המחשב, אומנות ועיצוב, עסקים, תכנות ועוד.[33]

#24

איך לנצח במלחמת העולם נגד נגיף הקורונה? מאמר המשך.

אל"מ (מיל.) שי שבתאי, יועץ אסטרטגי בחברת קונפידס, מנתח במאמר את הצורך ב"אסטרטגיית סיום" למשבר הבריאותי של הקורונה, על מנת שהיעדים לניהולו יהיו ברורים, וכדי לסמן את שלב המעבר ל"יום שאחרי", בו המיקוד יהיה טיפול באתגרים הכלכליים הגלובאליים שנוצרו. שבתאי מציע חמש אסטרטגיות אפשריות, ובנוגע לכל אחת מהן הוא מתאר את המאמץ הנדרש בעדיפות הגבוהה ביותר. הניתוח נותן בידי מקבלי ההחלטות כלים לחשיבה על כל אסטרטגיית התמודדות ותיעדוף המאמצים במסגרתה. בנוסף, במאמר ממליץ שבתאי על הגדרת השלבים לניהול המשבר, שהם מקבילים למתודולוגיה של ניהול אירוע סייבר חמור[34].

הציטוט היומי

"ישראל מפעילה סמכויות מעקב חירום, כדי לעקוב אחר אנשים שעלולים להיות חולים ב-COVID-19, ובכך היא מצטרפת לסין ואיראן בשימוש במעקב המוני בדרך זו. אני מאמין שהלחץ יגדל למנף תשתיות מעקב ארגוניות קיימות למטרות אלה בארצות הברית ובמדינות אחרות." [35]

ברוס שנייר, מהבלוג

Schneier on Security (20.3.2020)

[33] https://www.freecodecamp.org/news/here-are-380-ivy-league-courses-you-can-take-online-right-now-for-free-9b3ffcbd7b8c/

[34] https://medium.com/konfidas/how-to-win-the-covid-19-insurgency-world-war-follow-up-263651001bb8

[35] https://www.schneier.com/blog/archives/2020/03/emergency_surve.html

לעדכונים נוספים

ערוץ הטלגרם: https://t.me/corona_cyber_news

טוויטר: https://twitter.com/konfidas

פייסבוק: https://www.facebook.com/konfidas

אתר האינטרנט של קונפידס: https://www.konfidas.com/

הבלוג של קונפידס: https://medium.com/konfidas

*** סוף המסמך ***

31 Rothschild Blvd.Tel Aviv, 6578414

Office: +972-3-6444417 | info@konfidas.com | www.konfidas.com