



בטיחות דיגיטלית בזמן מחאה

טיפים למוגנות ובטיחות
דיגיטליות למפגינים ות

המטרה של המדריך הזה היא לספק מידע וידע שיאפשרו
לך לקבל החלטות מושכלות לגבי הבטיחות הדיגיטלית שלך
בהתבסס על הנסיבות האישיות, על נטיות הלב, על המיומנות
הטכנית וגם על סתם נוחות.

אנו מקווים שהמדריך הזה ישמש משאב רב ערך גם
למוחים וחדשים וגם לפעילים. עם וותק - ושאמצעי
הזהירות שמוצגים בו יאפשרו לכולנו להפוך את המחאות
לפלטפורמות בטוחות ועילות יותר, ולמקום בו כל אחד.
יכול להיות חלק מתהליכים דמוקרטיים ולהשפיע.

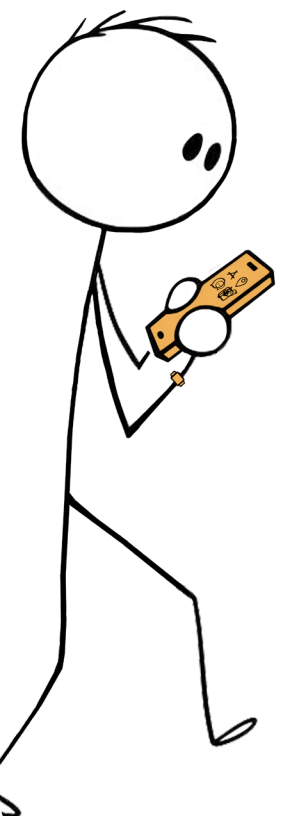
אנו שמחים להציג את המדריך לבטיחות דיגיטלית במחאות
והפגנות.

לפני הכול, חשוב להדגיש: המטרה שלנו היא לא להבהיל,
לא לעורר פרנויות ובטח שלא לערער את הרצון של אף
אחד. להשתתף בהפגנות ובמחאות. למעשה, אנו מאמינים
שמחאה היא דרך חיונית לאנשים להשמיע את קולם.
ולהביא לשינוי חיובי בחברה. עם זאת, אנו גם מכירים
בכך שהשתתפות במחאה יכולה לכלול סיכונים מסוימים,
ושואפים לסייע לך לצמצם את הסיכונים האלה.

המכון לטכנולוגיה חיובית



www.positive-tech.net



הימנעו משיתוף מידע רגיש באינטרנט



שימו לב מה אתם משתפים. במיוחד ברשתות חברתיות. בייחוד כדאי להיזהר כשמדובר במידע אישי שלכם ועל אחרים (שמות מלאים, כתובת או מספר טלפון, מקום עבודה). כל מידע עלול לחשוף פעילות ופעילים להטרדות ולאלימות מקוונת.

שימו לב שאתם לא משתפים. מידע אישי ו/או מיותר ו/או מפליל על עצמכם. ועל פעולות שלקחתם בהן חלק.

שימו לב שאתם לא מפיצים. קריאות לביצוע פעולות בלתי חוקיות, האשמות לא מבוססות, שפה מבזה או עלבונות כלפי עובדי ציבור.

שימו לב איזה מידע (מזהה ובכלל) מופיע בתמונות שאתם מפיצים ומפיצות (עוד על תמונות בהמשך).

בקיצור, תמיד חשוב להפעיל שיקול דעת.

לצד זה כדאי **לבדוק גם את הגדרות הפרטיות** – הן מאפשרות להחליט מי יראו את מה שתפרסמו. לדוגמה, בטוויטר הוסיפו לאחרונה אפשרות לשתף עם מעגל חברים קרוב בלבד, וגם בפייסבוק לא כל פוסט צריך להיות פתוח לגמרי. יש תכנים שעדיף לפרסם בקבוצות סגורות ולא בפיד הפתוח או בפיד לחברים (כדאי לזכור שהרבה מה"חברים" בפייסבוק הם אנשים שאנחנו לא באמת מכירים אישית).

חשוב גם לזכור שאפילו תכנים שתפרסמו לקהל מוגבל בלבד יכולים להגיע בקלות לעיניים אחרות באמצעות צילומי מסך וכדומה.

אם יש פרסום שחשיפה רחבה שלו עלולה להסב נזק ממשי לך או לאחרות, אסור לסמוך על הגדרות הפרטיות שיגבילו אותו.

* כל הנאמר כאן נכון להתנהגות ברשת גם בימים רגילים, אך בזמן מחאה נדרשת זהירות יתרה. לעוד מידע על התנהגות בטוחה בשוטף: "שנה את ההתנהגות שלך כדי למזער את המעקב הדיגיטלי" www.positive-tech.net/post/online-saftey-tips

מעקב שלטוני ברשתות חברתיות: סוכנויות שלטוניות מנהלות מעקב אחר פרסומים ברשתות חברתיות, ועושות זאת בכמה דרכים – משליחת סוכנים שמצטרפים לקבוצות פייסבוק פוליטיות, דרך שימוש בחשבונות מזויפים כדי להתגב לקבוצות סגורות ועד איסוף המוני וניטור של האשטאגים או פוסטים בסיוע בינה מלאכותית, על בסיס גאוגרפי או אחר. רק חוקים מעטים מסדירים את השימוש שגורמי האכיפה עושים באמצעים לניטור המדיה החברתית.

מעקב של מתנגדים: יחידים וקבוצות המתנגדים לפעילות שלכם. יכולים אמנם לעקוב אחרי מידע גלוי ברשתות חברתיות ולהצטרף למשל לקבוצות ואטסאפ גדולות, אבל בדרך כלל אין להם יכולת לנטר תקשורת – בניגוד לגורמים שלטוניים. חשוב שתחשבו איזה מידע על איזו פעילות חשוב לכם לשמור נסתר, ומפני מי. לפי זה תוכלו להחליט באילו כלים וערוצים להשתמש (ולא להשתמש).

ככלל אצבע, כדאי לזכור שאנחנו אף פעם לא יודעים בוודאות מי נחשף לתוכן שאנחנו מפרסמים, וגם לא מה האינטרס שלו (זה גם יכול להיות סוכנויות של מדינות זרות, עיתונאים ומוסדות כלכליים).

השתדלו להשתמש באפליקציות בטוחות למסרים מיידיים

כאשר מעבירים מסרים באפליקציות כמו סיגנל, וואטסאפ, טלגרם או מסנג'ר, המסרים האלה מוצפנים מקצה לקצה (כלומר, מוצפנים עם השליחה ואז מפוענחים אצל מקבלת ההודעה). זאת, בניגוד ל-SMS ולאפליקציות אחרות להעברת הודעות שאין להן הצפנה מקצה לקצה, ולכן צדדים שלישיים יכולים ליירט בקלות כל מה שתעבירו באמצעותן.

לשלוח הודעה בתוכנה מוצפנת זה כמו לשלוח מכתב במעטפה חתומה. לשלוח הודעה בתוכנה **לא** מוצפנת זה כמו לשלוח גלויה: כל אחד יכול לקרוא את התוכן שלה.

בשורה התחתונה, המומלץ ביותר לצרכי אבטחה הוא להשתמש באפליקציית **סיגנל** (מיד נפרט למה).

אבל לפני שנבחן את האפליקציות הספציפיות, חשוב לזכור:

1. כמו שנכתב קודם לכן, כל הודעה שנשלחת בקבוצה יכולה לדלוף למרות ההצפנה. הסיבה היא שבהרבה קבוצות יש פעילים פוליטיים מתנגדים או גורמים שנכנסו לשם מטעם המשטרה וגורמי אכיפה אחרים. במילים אחרות, כדאי להיחשש שכל מה שנשלח שם הוא פומבי.
2. הודעות יכולות לדלוף גם לאחר זמן (לדוגמה, אם המכשיר אבד והגיע לידיים הלא-נכונות). **בשיח רגיש כדאי להשתמש באופציות למחיקה אוטומטית של הודעות לאחר פרק זמן קבוע** (תכונה שזמינה בסיגנל ובוואטסאפ), ועדיין לזכור שגם זו לא ערובה לכך שההודעות לא יתועדו באמצעות צילום מסך, לדוגמה.

מה הצפנה מקצה לקצה עושה: הצפנה מקצה לקצה מגינה על תוכן ההודעה הספציפית ששלחת.

מה הצפנה מקצה לקצה לא עושה: הצפנה מקצה לקצה אינה מגינה על המטא-נתונים שלך: עם מי תיקשרת ומתי, באיזה מכשיר השתמשת, איפה היית פיזית בזמן השימוש באפליקציה. בפוטנציה, החברות שומרות את המידע הזה לנצח.

לא כל אפליקציות המסרים המוצפנות שוות זו לזו

יש כמה הבדלים חשובים בין אפליקציות המסרים החינמיות. אז על איזה שירות הודעות אפשר לסמוך?

הצפנה מקצה לקצה יכולה להגן עלינו מפני מעקב של השלטון, של האקרים ושל פלטפורמת ההודעות עצמה. אבל **האם האפליקציות שמבטיחות הצפנה כזו גם מקיימות?** לא בהכרח, ולא בכל המובנים. לדוגמה, וואטסאפ (של חברת מטא, והאפליקציה המועדפת על רוב המשתמשים בארץ) אמנם יישמה הצפנה מקצה לקצה בגרסאות העדכניות שלה, אבל מדיניות הפרטיות שלה מאפשרת לה לשותף המון נתונים: מספרי טלפון, שמות פרופילים, סטטוס, נתוני מכשיר, כתובת IP, נתוני מיקום ומידע על תדירות שליחת הודעות והנמענים שלהן. מסנג'ר (גם היא של חברת מטא) וטלגרם מציעות הצפנה מקצה לקצה, אבל לא כברירת מחדל. חוץ מזה, משום שמדובר בתוכנות קוד סגור, אי-אפשר לבדוק האם הן באמת עושות מה שהן מבטיחות (זה נכון במיוחד לגבי טלגרם, שמפעילה הצפנה ברמה נמוכה ולא כברירת מחדל, ויש גם חשש שהיא משתפת פעולה עם המשטר הרוסי).

ההמלצה שלנו היא להשתמש ב**סיגנל**, האפליקציה כתובה בקוד פתוח (ולכן אפשר לוודא שהיא אכן עושה מה שהיא מבטיחה), מצפינה את ההודעות מקצה לקצה, ולא שומרת מידע או מטא-מידע. למעשה, במקרים שבהם רשויות אכיפה בארה"ב הוציאו צו משפטי שהורה לסיגנל לחשוף מידע על התקשורת שבוצעה בחשבון מסוים, הן קיבלו מהחברה דף ריק, כיוון שסיגנל לא שומרת שום מידע מלכתחילה. נוסף להצפנת קצה לקצה, **סיגנל מאפשרת גם צ'אטים קבוצתיים מוצפנים**, והוסיפה לאחרונה גם את האפשרות **למחיקה אוטומטית של הודעות בין 10 שניות לשבוע לאחר שנקראו לראשונה** (זכרו: עדיין אפשר לבצע צילום מסך). סיגנל מאפשרת גם **שיתוף תמונות תוך טשטוש פנים**, דבר שמאפשר להגן על המצולמות והמצולמים בהפגנות מפני איתור שלהן. אם התמונה מגיעה לידי גורמי האכיפה או גורמים עוינים.



שמרו על המידע שלכם.

שימוש ב-VPN

שימוש ב-VPN – רשת פרטית וירטואלית – מאפשר לך להצפין את תעבורת האינטרנט שלך במלואה, ובכך להגן על הפעילות המקוונת שלך מעיניים סקרניות. הוא מאפשר לך גם להסוות את המיקום שלך, וכך לגשת לאתרים חסומים ולהימנע מצנזורה.



VPN הוא שירות מקוון שמצפין את תעבורת האינטרנט שלך ומסתיר את כתובת ה-IP שלך (הכתובת המזהה של המחשב או הטלפון שלך בזמן חיבור לאינטרנט). זה מתבצע באמצעות ניתוב מאובטח של הגלישה שלך דרך שרתי החברה, שנמצאים בדרך כלל במדינה אחרת. את השירות מספקות חברות מסחריות, בתשלום או בחינם. חשוב לשים לב ממי רוכשים את השירות – גם במקרה זה ישנן חברות שמוכרות מידע אישי של המשתמשים.

ספקי VPN מומלצים לדוגמה הם NordVPN, Surfshark ו-ProtonVPN.

חשוב לזכור: VPN אינו מבטיח אנונימיות מלאה. לאנונימיות מיטבית כדאי לגלוש באמצעות דפדפן Tor, שהגלישה בו מתבצעת דרך שלושה שרתים שונים.

הגנה פיזית על מחשבים וטלפונים ניידים

הדבר הפשוט, הבסיסי וההכרחי ביותר הוא לוודא שההניסה למחשב או לנייד שלך מתבצעת אך ורק באמצעות סיסמה (כמובן שכדאי לבחור סיסמה מורכבת, שקשה לנחש). במקרה של חשש מפני מעקב ממוקד, כדאי גם לכסות את המצלמה של המכשיר במדבקה או כיסוי ייעודי אחר.

נעילה ביומטריית של הטלפון הסלולרי (באמצעות טביעת אצבע או זיהוי פנים) אינה מומלצת במקרה של חשש מפני מעצר. החוק עדיין אינו ברור לגבי הסמכות של גורמי האכיפה בהקשר זה, ולכן מומלץ לבטל את הנעילה הביומטרית לפני אירועי מחאה (נרחיב בנושא בהמשך המסמך).

הצפנת מידע

אם על המחשב שלך שמור מידע שחשוב לך שאיש מלבדך לא יראה, כדאי להצפין אותו. לשם כך אפשר להשתמש בתוכנת הצפנה כמו למשל VeraCrypt או להסתמך על תכונות ההצפנה המובנות במערכות ההפעלה של רוב הסמארטפונים והמחשבים. תכונת ההצפנה של iOS נקראת FileVault, תכונת ההצפנה של וינדוז נקראת BitLocker, ואילו אנדרואיד מציעה אפשרות להצפין את כל תוכן המכשיר (המופעלת אוטומטית ברגע שהמכשיר מוגן באמצעות סיסמה) וכן אפשרות ליצור תיקייה מאובטחת שיכולה להיפתח רק באמצעות סיסמה.

פרטיות במסמכים משותפים

כאשר עובדים על מסמכים ורשימות משותפים בענן (למשל בדרייב של גוגל), חשוב לשים לב להגדרות פרטיות וגישת. תמיד עדיף להקפיד על הגדרות סגורות ומצמצמות, ולהבטיח שהמסמך יהיה זמין רק לבעלי. כתובות מייל מסוימות (ולא פתוח לכל מי שיש להם קישור למסמך).

גלישה וחיפוש אנונימיים

שיטוט באינטרנט במצב "גלישה בסתר" (אינקוגניטו) הוא דרך סבירה להסתיר ממשותמשים אחרים במכשיר את היסטוריית החיפוש והגלישה שלכם, אבל חוץ מזה מדובר באמצעי מוגבל מאוד. מצב "גלישה בסתר" מונע אחסון של נתוני הגלישה במכשיר, אך אינו מונע סוגים אחרים של מעקב: עדיין אפשר לעקוב אחריו באמצעות כתובת ה-IP, ספק האינטרנט עדיין יכול לתעד את האתרים שבהם ביקרו, וכן הלאה.

כדי לבצע חיפוש מאובטח שלא ישאיר עקבות מומלץ להשתמש במנוע חיפוש שאינו שומר את המידע שלך, כמו למשל DuckDuckGo. אם הפרטיות חשובה לך במיוחד, כדאי לשקול לעבור לדפדפן מוכון פרטיות שאינו מאחסן עוגיות, וחוסם פרסומות וכלי מעקב (כמו Brave ופיירפוקס).

במקרה הצורך אפשר גם להשתמש בדפדפנים שונים למטרות שונות. אפשר למשל להשתמש בפיירפוקס כדי לגלוש באתרים הדורשים סיסמה (כמו ג'ימייל ורשתות חברתיות), אבל את החיפושים לבצע אינקוגניטו בדפדפן נקי (למשל כרום), שלא ישמור את היסטוריית הגלישה שלך. הפרדה כזו תסייע למנוע את העמקת המעקב אחריכם. באמצעות מנועי החיפוש והרשתות החברתיות.

* גלישה וחיפוש אנונימיים יכולים גם לחסוך לכם, כסף (לדוגמה בחיפוש לקניות אונליין).



הטלפון הנייד בהפגנות

הטלפון שלנו מייצר כמות אדירה של מידע עלינו ועל האנשים שאנחנו מתקשרים איתם, ומתפקד גם כמכשיר מעקב לכל דבר. בקלות יחסית אפשר לעקוב אחרי מטא-נתונים של שיחות (מי דיבר עם מי ולכמה זמן), לקרוא הודעות טקסט לא מוצפנות, לעקוב אחר הרגלי שימוש באינטרנט, לצבור נתוני מיקום, לשאוב אנשי קשר ועוד ועוד נתונים שהמכשיר יוצר, מאחסן ומפיץ (כמו כן, נתונים רבים שמורים אצל ספקי השירות – סלקום, פרטנר, פלאפון וכו' – שמשתפים בהם גורמים ממשלתיים ומסחריים).

נוסף לכל הנתונים שנוצרים ונשמרים בשימוש סדיר, מכשיר טלפון עלול גם ללכת לאיבוד או להיגנב. חוץ מזה, הרשויות יכולות להחרים אותו – ובמקרה שתהיה להן גישה לתוכן שעמור בו, יהיה בידן שפע נתונים לגבינו ולגבי אנשים שאנחנו מכירים. לדוגמה, הנייד שלך יכול לספק לרשויות גישה למידע על טיב הפעילות המאורגנת ועל מי שמארגנת אותה, ובמקרים מסוימים לספק גם את המידע הדרוש כדי למנוע פעילות וכדי להפחית את המעורבים בה.

במקרים מסוימים הטוב ביותר הוא פשוט להשאיר את הנייד בבית. במקומו אפשר להשתמש בנייד זול חלופי, עם סים נקי וללא מנוי (פריפייד/טוקמן). במכשיר כזה אפשר להשתמש לתקשורת וכדי לתאם פעילויות, וכך להגן על הפרטיות ועל המידע האישי שלך (אפשר גם להשתמש ב"מכשיר טיפשי" שיש בו רק מצלמה ואפשרות לנהל שיחות. במקרים מסוימים אולי תרצו פשוט להצטייד במצלמה דיגיטלית ודי).

אנטנות סלולריות: מגדלי אנטנות סלולריים קולטים מידע שלנו כל הזמן – נתונים כמו מיקום המכשיר, מטא-נתונים כמו שיחות שבוצעו, משך השיחה, תוכן שיחות והודעות טקסט לא מוצפנות. **על פי החוק, מידע זה, שמוחזק על ידי חברות הטלפון, יכול לעבור לידי המשטרה ורשויות אחרות אם השיגו צו בית משפט.**

הכלי: במרץ 2020 החליטה ממשלת ישראל להסמיך את השב"כ לבצע מעקב מגעים ולזהות מיקומים של חולי קורונה ושל כל מי שבא עמם במגע. כך נחשפה תוכנית המעקבים של השב"כ (המכונה "הכלי"). התברר שהשב"כ מקבל באופן רציף וגורף מידע מחברות הסלולר והאינטרנט שלנו, מידע שמאפשר לו לדעת בתוך שעות איפה היינו, עם מי נפגשנו ולכמה זמן. מאגר נתוני התקשורת שבידי השב"כ נאסף ללא צו משפטי, וכמעט אין עליו פיקוח חיצוני.

לפני פעילות, הכינו את הנייד

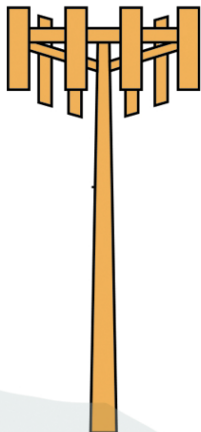
חשוב לוודא שהנייד מוגן באמצעות סיסמה מורכבת, ומומלץ מאוד לבטל את הנעילה הביومترית (כאמור, החוק אינו לגמרי ברור בהקשר זה, ואינו מספק הגנה מלאה מפני פתיחה מאולצת של המכשיר באמצעות טביעת אצבע. כמובן שבמקרה חטיפה אלימה של המכשיר, ניתן לפתוח אותו עם טביעת האצבע שלך פשוט באמצעות כוח פיזי).

בטלו את ההתראות על מסך הנעילה, או לכל הפחות מנעו מאפליקציות המסרים המידיים להציג עליו את תוכן ההודעות ואת פרטי השולח. כך, אם הטלפון נתפס או אבד, לא יהיה צורך לדאוג שמא מישוהו יקרא בקלות את התקשורת הפרטית שלך.

כדאי **להפעיל אימות כפול באפליקציות** המאפשרות את זה, בדגש על האפליקציה שבה מתנהלת רוב התקשורת שלך.

כדאי **לבטל הרשאות** (כמו גישה למצלמה, מיקרופון ונתוני מיקום) ולצאת מכל אפליקציה שיש בה נתונים אישיים, פרטיים או רגשיים (כמו למשל שירותי ענן, מדיה חברתית, דוא"ל וכל שירות אחר שלא היית רוצה שלמשטרה או לאחרים תהיה גישה אליהם).

כדאי מאוד גם **לגבות את המכשיר** למקרה שיאבד, יוחרם או יינזק. אפשר לשקול גם להסיר מהטלפון כל מידע אישי (כמו למשל שם ומספר טלפון למקרה חירום שמופיעים על מסך הנעילה או רשומים פיזית על המכשיר עצמו). קיומו של גיבוי יכול להועיל גם במקרה שהמכשיר אבד, נגנב או הוחרם. במקרה כזה עלול להתעורר הצורך למחוק מרחוק תוכן מסוים, אפליקציה מסוימת ואפילו את כל התוכן בטלפון. הנחיות לביצוע של מחיקה כזו אפשר למצוא בדפי התמיכה של גוגל ושל אפל, בהתאם לסוג המכשיר (ואם יש לך גיבוי של התוכן, זה כמובן יקל על המעבר למכשיר הבא).



זיהוי או אלמוניות?

הגעה אל הפעילות

מומלץ להגיע בלבוש גנרי (חולצת מחאה) ללא סימנים מזהים או סימני היכר מובהקים. במקרה הצורך יועילו גם קפוצ'ון או מסכה (שלא מסכלים בהכרח את כל אמצעי הזיהוי, ובכל זאת מקשים על זיהוי שלכם בעין אנושית).

במקרה שאתה בדרך לפעילות שעצם ההשתתפות בה עלול לשמש נגדכם, כדאי לשקול כמה אמצעים להגן על הפרטיות שלך.

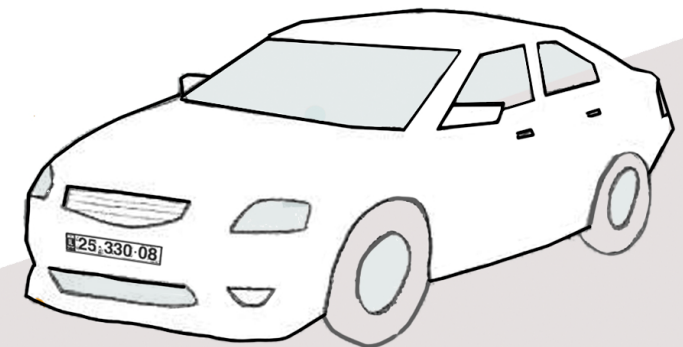
- במידת האפשר, עדיף להגיע ברגל או באופניים.

- אם נוסעים בתחבורה ציבורית, עדיף להשתמש ברב-קו אנונימי או לקנות כרטיס במזומן, כשאפשר.

- אם מגיעים ברכב, צריך לקחת בחשבון שמערכת הנקראת "עין הנץ" מתעדת את תנועתם של כל כלי הרכב בכבישי הארץ באמצעות פענוח לוחית זיהוי הרכב וצילום הנוסעים.

זיהוי פנים

בהפגנות קשה להימנע מזיהוי פנים, אבל אפשר להקשות על המערכת באמצעות חבישת צעיף או כאפייה, כובע ומשקפי שמש. אפשר גם לחבוש מסכת קורונה, וגם סוגים מסוימים של איפור יכולים לעזור. כל אלה לא ימנעו את הזיהוי לגמרי, אבל יקשו עליו.



זיהוי פנים: הזיהוי יכול להתבצע גם בדיעבד וגם דרך המצלמה

בזמן אמיתי. הטכנולוגיה מבוססת על עיבוד של מידע ביומטרי והצלבה שלו עם מאגר קיים של תצלומים ופרטים אישיים.

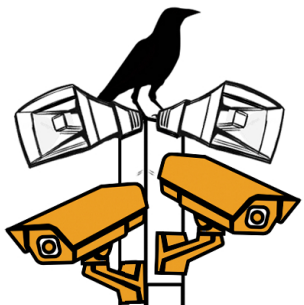
על פי פרסומים בעיתונות, למשטרת ישראל יש מערכת לזיהוי פנים, והיא כבר ביקשה להיות רשאית להפעיל אותה ללא מסגרת חקיקה מסודרת. הבקשה אמנם סורבה, אך בהינתן העובדה שהכלי קיים ושמיש, ניתן להניח שבדי המערכת כבר קיים מאגר פנימי של תצלומי פנים של אזרחים. סוכנויות ביטחון אחרות של המדינה כבר משתמשות במערכות זיהוי פנים, אך נכון להיום אין לנו עדויות על שימוש חוקי בטכנולוגיה על אזרחים ישראלים.

עין הנץ: מערכת עין הנץ אוגרת ושומרת את פרטיהם של כל

האזרחים שכלי הרכב שלהם חלפו על פני המצלמות, כולל צילומי וידיאו וסטילס של הרכב ונוסעיו, השעה והמקום. הנתונים לגבי מספר המצלמות בארץ לא נחשפו בפני הציבור, אך לפי ההערכות מדובר במערכת מקיפה מאוד.

המערכת מאפשרת למשטרה לקבל בלחיצת כפתור מידע פרטי רגיש על מיקומם של האזרחים הנוסעים בכבישי הארץ גם בדיעבד וגם בזמן אמיתי. במילים אחרות, המערכת מאפשרת לזהות את מקום הימצאו של אדם בעבר, לשחזר את מסלול התנועה שלו, ולעתים להתחקות גם אחר מגעים שקיים עם אחרים בעבר.

פעולת המערכת הוסדרה בחוק רק בפברואר 2023, ועד אז עבדה ללא צו משפטי וללא פיקוח. החוק עדיין אינו מאשר למשטרה להשתמש במצלמות מתקדמות לזיהוי פנים במרחב הציבורי, אבל המערכת והאפשרות להשתמש בה קיימות.



בטיחות דיגיטלית בהפגנות

לייב-סטרים ותיעוד של פעולות ספק-חוקיות

עדיף לא לתעד ולהפיץ בזמן אמיתי פעולות שיפילו מפגנים או יעזרו לחזות פעולות מחאה עתידיות ולסכל אותן.

התיעוד החי לרוב נשמר בידי הפלטפורמה ולא בידי המשתמש. אבל המשטרה בהחלט יכולה להקליט ולשמור אותו לצורך הפללה או הגשת כתבי אישום בהמשך, לכן כדאי להיזהר מאוד עם שימוש בשידורים חיים. בזמן המחאות בהונג-קונג, לדוגמה, המשטרה צפתה בשידורים של מפגנים כדי לעקוב אחרי הפעילות בזמן אמיתי ולסכל אותה. יש סיכוי סביר שכך קורה גם בארץ.

כבדו את הפרטיות של החברים. ות למחאה

כאשר אתם מצלמים ומפיצים תמונות, הפעילו שיקול דעת. זכותך לצלם בכל מחאה ברחובות ובמרחב הציבורי, אבל מחאה אינה רקע לאינסטגרם. בפעולות מחאה רגישות, כדאי להימנע מצילום של מפגנים ומפגנים שמציגים בבירור מידע מזהה כמו פנים או קעקועים. בשטחים, העב"כ משתמש בצילומים של פעילים ועיתונאים כדי לאתר משתתפים בהפגנות ואחר כך לעצור אותם בבתייהם (כולל מעצר קטינים). יש חשש שזה יכול לקרות גם בגבולות ישראל.

כדאי להפעיל שיקול דעת, ובמקרים מסוימים לא לתעד מקרוב אנשים בפנים גלויות. גם תמונות שמצולמות מהגב יכולות להיות מרשימות ואפקטיביות.

כפי שכתבנו למעלה, לסיגנל יש אפשרות לשיתוף תמונות תוך טשטוש פנים, דבר שמאפשר להגן על המצולמות והמצולמים בהפגנות מסוימות מפני איתור. יש גם אפליקציות רבות אחרות שעושות את זה.

כמה מאמצעי הזהירות המתוארים פה כרוכים במחירים כבדים כשמדובר בזמינות של המידע ובשיתוף והפצה שלו בזמן אמיתי, ואלה הרי דברים קריטיים במחאה. כדאי פשוט לחשוב ולהחליט: האם מתאים לך לקחת חלק בשיתוף והפצת מידע? האם ברורים לך הסיכונים הכרוכים בכך (שיכולים להיות משמעותיים ויכולים להיות גם זניחים מאוד)?

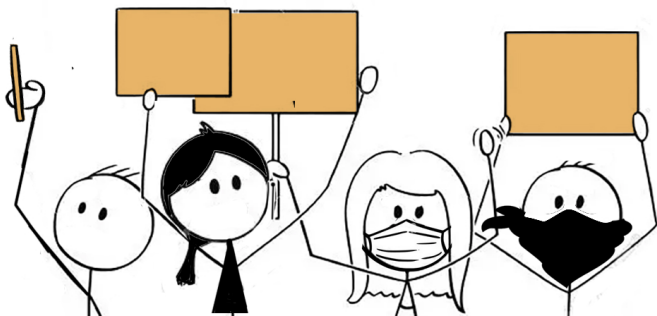
השתתפות בהפגנה אינה פשע, צילום בהפגנה אינו פשע, עמדה פוליטית אינה פשע. במקרים רבים זה בסדר גמור שידעו איפה היית ומה עשית (וכשמדובר בהפגנות, לפעמים זה אפילו מועיל והכרחי). חשוב פשוט להפעיל שיקול דעת.

מצב טיסה

הטלפון שלנו מספק הרבה מידע עלינו גם בזמן אמיתי – בזמן הפגנה או פעילות פוליטית אחרת. במקרה כזה, אפשר לכבות את המכשיר או להעביר אותו למצב טיסה. שימו לב: מצב טיסה אינו משבית את שירותי המיקום, לכן מומלץ לוודא שכל השירותים הללו כבויים. לחלופין, אפשר לכבות רק את הנתונים הסלולריים, את ה-Bluetooth, את שירותי המיקום או את ה-Wi-Fi. בנפרד, ולהפעיל רק מה שצריכים (זה גם שומר על הבטרייה).

השתמשו בהצמדת מסך (App pinning)

במכשירי אנדרואיד ואייפון ניתן לגשת לאפליקציה אחת תוך כדי נעילה של כל שאר הטלפון. זו דרך בטוחה יותר לצלם או לפרסם ברשתות חברתיות במהלך המחאה. היא מועילה גם במקרה שצריך להציג בפני משהו (כולל נציגי רשויות האכיפה) משהו בטלפון, ולעשות זאת בלי שתהיה גישה לכל המידע השמור בו.



אחרי ההפגנה

התנהגות דיגיטלית בטוחה בשוטף

- תרגלו שימוש מושכל ונקי ברשתות חברתיות. לפני שתשתפו מידע, כדאי לחשוב: מה המידע הזה? האם חיוני לשותף אותו? ככלל אצבע, אל תפרסמו דברים שלא הייתם רוצים שאמא שלכם או השוטף השכונתי ידעו.

- היזהרו מהתקפות דיג: היזהרו מכל מיילים, הודעות טקסט או פוסטים במדיה חברתית המבקשים מידע אישי או מציעים ללחוץ על קישור כלשהו. אלו יכולות להיות התקפות שנועדו לגנוב את המידע שלכם או להדביק את המכשיר שלכם בתוכנה זדונית.

- אל תמהרו לחתום על עצומות או להירשם באפליקציות שמבקשות פרטים אישיים כדי "לדעת כמה מתנגדים" או "לספור כמה היו בהפגנה". כאשר מדובר ביישומים שמייצרים מאגר מידע, כדאי לחשוד.

- תקשרו באמצעות אפליקציות מאובטחות (עם הצפנה מקצה לקצה) והקפידו ליצור סיסמאות חזקות. לא כדאי להשתמש באותה סיסמה פעמיים. אם השתמשת בסיסמה מסוימת באתר אחד, עדיף לא להשתמש בה באתר אחר. לעוד מידע וטיפים למחזור של המעקב הדיגיטלי: www.positive-tech.net/post/online-saftey-tips.

- מסמכים שנוצרים בתוכנות אופיס למיניהן כוללים מידע מזהה לגבי מי שיצר. אותם. אפשר למחוק את המידע הזה באחת מלשוניות המאפיינים של המסמך.

- כשאפשר, עדיף לעבוד אנלוגית: להיפגש פנים אל פנים, לכתוב על נייר ולא בנייד או במחשב, וכן הלאה.

העלאת ושיתוף תמונות

- אם התמונות עלולות להפיל או לסבך מפגינים. ואת אחרים. אל תפרסמו אותן בלי רשותם. - קל וחומר שלא בלי לטשטש את הפנים שלהן. בתמונה.

- במקרה שרוצים להסתיר את מיקום הצילום, שימו לב שלא מופיעים בו פרטים כגון שלטי רחוב ונקודות ציון אחרות.

- כאשר משתפים תמונות, עדיף לפרסם צילום מסך של התמונה (זה מוחק ממנה מטא-נתונים כמו מקום, זמן, מכשיר וכדומה).

צילום של גורמי האכיפה

צילום של שוטרים ונציגים אחרים של רשויות האכיפה יכול להגן מפני אלימות משטרתית. הזכות לצלם אותם חוקית ומבוססת, ובכל זאת כדאי לקחת בחשבון שהם עשויים להגיב לכך בכוח.

כאשר מצלמים שוטף, חשוב לעשות זאת בצורה שאינה מתריסה ואינה מפריעה להם למלא את תפקידם (לדוגמה, לעשות זאת מרחוק ולא תוך חדירה למרחב האישי, אחרת זה יכול להיחשב כהפרעה לשוטף).

צילום מפגינות ומפגינים על ידי שוטרים

לעתים קרובות המשטרה מתעדת את המשתתפים בהפגנות ומחאה. הצילום מבוצע קרוב מאוד לפניהם של המפגינים. גם בנסיבות שבהן ההפגנה מתנהלת כסדרה ובשקט, וכן על ידי שוטרים סמויים.

נכון להיום, אין כל פקודה או נוהל משטריים שיסדירו את השימוש המשטירי באמצעי תיעוד בהפגנות (וידיאו, סטילס, רחפנים ועוד). אין כל הנחיה מנהלית שמסדירה את השימוש המשטירי באמצעי תיעוד בהפגנות: אין כל הוראה מתי ואיך ראוי לתעד הפגנות; איך ייאגר התיעוד, היכן יישמר ולמשך כמה זמן; איזה שימוש ייעשה בחומר המתועד; כיצד תובטח אבטחת המידע הנאגר וכו'. כל תחנת משטרה מחליטה לפי ראות עיניה האם להוציא רחפן או צוות צילום וידיאו לתיעוד הפגנה שמתרחשת בתחומה; כל תחנה מחליטה מה לעשות עם החומר המתועד, כמה זמן לשמור אותו וכיצד להפיק ממנו מידע.

