בעקבות ברכי לוין- לבחורות מבינות עניין בלבד!

<u>פרק א- אשליית המסך</u>

כידוע בשנים האחרונות העולם כולו עבר לפעילות באינטרנט וזה כולל גם אותך, הקוראת הנכבדה.
היות שהגישה לאינטרנט או לאימייל נעשית בקלות ובנגישות, מתוך מקום נעים ומוכר כמו הבית/העבודה/המכשיר האישי, קל לשגות באשליה שגם האינטרנט הוא מקום מוכר ונעים.
הוא לא!
כניסה לאינטרנט היא ביקור בעולם אחר.
בכניסה לאתר הבנק- יש להתנהג כמו בכניסה לסניף הבנק עצמו .
בכניסה לאתרי קניות- יש להתנהג כמו בכניסה לשוק.
בכניסה לאתרים לא מוכרים, יש להתנהג כמו בכניסה לסימטה חשוכה לבד בלילה .
ובקיצור- **המסך הוא אשליה.**
האינטרנט קיצר מרחקים עבור כולנו, וגם עבור אנשים עם כוונות לא טובות, עבריינים ופושעים.
באינטרנט אפשר לפגוע ולהיפגע בדיוק כמו בעולם האמיתי ולפעמים אפילו יותר.

<u>פרק ב- הפשיעה באינטרנט</u>

לאילו מטרות משתמשים פושעים באינטרנט?
לאותן מטרות שהן מנסים להשיג גם בעולם האמיתי.
מילוי תאוות בצע או תאוות אחרות (לעיתים חולניות ובלתי נשלטות), תאוות שליטה, תאוות נקם ועוד.

בעולם האמיתי....-
גנב צריך לרגל אחר הקורבן.
גנב צריך להסתכן בפריצה לבית.
מטרידן צריך להיחשף בפני מושא הטרדתו.
סחטן צריך לאיים בנשק או איום חזק אחר.
רמאי צריך להתאמץ כדי לשכנע.

בעולם הוירטואלי...-
גנב יכול להסתפק בבדיקה בפייסבוק של הקורבן.
גנב יכול לפרוץ לחשבון הבנק במחי הקשת מקלדת.
מטרידן יכול להסוות את זהותו.
סחטן יכול לאיים בפירסום היסטוריית הגלישה או נעילת המחשב.
רמאי יכול ליצור בקלות את הרושם שהוא רוצה.

לסיכום- בעולם האמיתי, הפושע חייב לארוב לקרבן.
בעולם הוירטואלי- הקרבן יכול להיכנס לרשת מעצמו מתוך תמימות.

<u>פרק ג'- הגנה עצמית</u>

האם יש מה לעשות כדי להתגונן?
הבשורה הטובה היא, כן.

איך?

<u>השלב הראשון הוא להפנים:</u>

האינטרנט אינו אמצעי למציאת קשרים חדשים,

אלא אמצעי לתחזוקת קשרים שנוצרו בעולם האמיתי.

אמת המידה לקיום קשר באינטרנט היא אותה אמת מידה לקיום קשר בעולם האמיתי:
האם אני מבירה את הדמות שעימה אני בקשר, כאדם אמין שניתן לסמוך עליו?

<u>השלב השני הוא להפנים:</u>

לא על כל פנייה צריך לענות.

להיפך, יש הודעות שמיותר או מסוכן לענות להן.
מותר להעז למחוק הודעות נכנסות, (או להעביר לספאם), ומותר להפסיק לענות לאדם שנראה לנו חשוד.
הוא לא יגיע עד אלינו, וגם אם הוא מתחנן, מאיים או מפעיל מניפולציות,
כשהוא יראה שאין קול ואין עונה- הוא יעזוב ויחפש מישהו אחר.
(וגם אם הוא כותב שהוא יודע איפה את גרה, או איומים אחרים, בד"כ זה פשוט לא נכון, אלה מניפולציות שמטרתן לגרום לך לענות.)

<u>השלב השלישי הוא לבנות חומת הגנה מושכלת:</u>

לבצר את מעגל הקשרים הקיימים שלך.

לבחון את אנשי הקשר, לסנן את אלה שאינך סומכת עליהם (כגון, למחוק, או להעביר לתגית "בלתי מוכר זהירות" וכו'), ולהשאיר רק את אלה שהקשר איתם/ן תורם לך.
באופן כללי יש לבחון לפי אמת המידה שצויינה לעיל (עד כמה מבירים את האדם בעולם האמיתי), עם הסתייגויות פה ושם- כגון משרדי ממשלה, ברור שלא מבירים אישית אך אפשר לתת אמון כדי לקבל את השירות, וכדומה. או איש קשר שמובר אישית לאיש קשר שמובר לך אישית. אבל אלה יוצאי דופן, והכלל הוא להשאיר רק את האמינים והמועילים.

<u>השלב הרביעי הוא לא להיות ספאמרית בעצמך:</u>

להעביר אימיילים רק ממי שסומכים עליו, ורק למי שסומכים עליו ,

ובכל העברה למחוק את כל הכתובות הקודמות שבשירשור .

יש הרבה פירסומות שאנו מעבירות זו לזו בלי הרבה מחשבה,
מדובר בספאם בלתי חוקי שיכול לגרום נזקים ממשיים.
מספיק שהשרשור מגיע בסוף למישהו לא הגון או גרוע מכך,
מספיק שאצל המפרסם עובד מישהו עם נטיות עברייניות והוא מעתיק את רשימת הכתובות לשימושו האישי.
מספיק שמישהו אחד בשרשרת הוא עו"ד או צרכן עצבני ויתבע את המפרסם שיינזק מאוד.
ולכן חשוב להקפיד על הכלל דלעיל .

השלב החמישי הוא

לאמץ הרגלי גלישה נכונים:

* לא פותחים קבצים מצורפים אא"כ יודעים מראש במה מדובר.
* לא לוחצים על קישורים באף הודעת אימייל אא"כ כנ"ל יודעים מראש מהו הקישור (כולל לא קישורים שנראים אמינים כמו החלפת סיסמה לבנק וכדו').
* סיסמאות שומרים בדף נייר בבית - לא בארנק ולא בנרתיק של הטלפון.
* מחליפים סיסמאות כל חודשיים-שלושה.
* לא משתמשים באותה סיסמה לכמה אתרים.
* לפני תשלום באשראי מבררים אם מקבל התשלום הוא אכן גורם אמין.
* לא קונים על סמך המלצות באינטרנט אלא רק על סמך המלצות מאנשים אמיתיים בעולם האמיתי.
* משתפים עם אנשי הקשר מידע על הונאות שחווית בעצמך כדי להזהיר.
* לא מעבירים כסף לאף אחד שלא מכירים בעולם האמיתי, ויהיה מה שיהיה.
* כנ"ל לגבי תמונות וסרטונים אישיים.

השלב השישי הוא להתחזק ולהפנים:

אין מי שרוצה בטובתך יותר מה' יתברך ומהאנשים הקרובים לך בעולם האמיתי.

אף פנייה באינטרנט, חברית או מפתה ככל שתהיה, אינה לטובתך-
היא בד"כ תמיד לטובת האינטרסים של הפונה.
(תוכלי לבדוק זאת ע"י הפניות שאת יוזמת-
כמה מהן הן לטובתך, וכמה לטובת הנמען? ומי הם הנמענים שאת דורשת את טובתם?)
זכותך המלאה לאמת כל פנייה ע"י שאלה "תזכיר/י לי מאיפה אני מכירה אותך?",
או ע"י ביצוע בירור אצל מכרים משותפים,
או ע"י בקשת מס' טלפון של בית העסק וביצוע חיפוש בגוגל.

זכותך המלאה להתעלם, למחוק, לחסום, לסרב, ולעשות בפנייה כבל העולה על רוחך.

זכותך המלאה להתעלם, למחוק ולחסום כנ"ל גם אחרי שנוצר קשר ולא רק בהתחלה.

זכותך המלאה לשמור על עצמך ולדאוג לעצמך, זכותך וחובתך- כי אף אחד לא יעשה זאת במקומך.

ואם את מרגישה לא בנוח לגבי משהו שקרה לך באינטרנט -

המעשה הנכון והבוגר ביותר הוא לפנות למישהו מבוגר שאת סומכת עליו/ה:

אמא, אבא, קרוב/ה אחר/ת, מורה או יועצת, אח/ות נשוי/ה- העיקר דמות נאמנה שתוכל לסייע.

פרק ד- התמודדות לאחר מעשה

את לא אשמה!

את לא אשמה בכך שמישהו החליט לפנות אלייך מיוזמתו!
את לא אשמה בכך שנהגת בתמימות ונענית.
את לא אשמה בכך שמישהו עולל לך רע.
גם מנכ"לים של חברות מצאו עצמם קורבן להונאות באינטרנט.
הרבה אנשים טובים היו קורבן לשיימינג, להטרדה או לתופעות שליליות אחרות.
מעטים גם איבדו את חייהם בעקבות כך, ואין סיבה שתגיעי לשם, כי את לא אשמה שנקלעת למצב מסויים כזה או אחר.

<u>אבל אם את מסתירה מהיקרים לך דברים רעים שקורים לך, את אשמה גם אשמה!!!</u>
ההתמודדות הנכונה היא לשוב לחיות את החיים האמיתיים בעולם האמיתי, ובד"כ צריך עזרה מבחוץ בשביל זה. תפני לעזרה! זה המעשה הכי טוב שאת יכולה לעשות בשביל עצמך.

<u>פרק ה- בנקודת הבחירה</u>

יכול להיות שאת מאלה שחושבות "אפשר לחשוב..." או "לי זה לא יקרה" או "אציץ רק לרגע ולא יקרה לי כלום..."
יכול להיות שכרגע את בנקודת הבחירה, שבה עלייך לאזור אומץ ולערוך התמודדות פנימית בתוך עצמך כדי להתנתק מקשר שמשפיע עלייך לרעה.
נקודה זו היא קריטית בשבילך, אל תיכשלי בה מדעת.
כל מי שהצליח לצאת מזה מעיד שמדובר בקשרים אפלים, חשוכים, מעוותים ושליליים, גם אם ממבט ראשון הם מסקרנים ומושכים, זו מלכודת בוץ שנדרשים מאמצים עילאיים לצאת ממנה.
לא כל עולם חדש שמתגלה, הוא עולם ראוי ונכון!
זה ניסיון קשה, אבל הסקרנות הורגת!
האם תרצי לפתוח מכסה שמתחתיו יפרצו אליך גזים רעילים?
האם תרצי לפתוח קופסה שמתוכה יתנפל עלייך שודד בסכין שלופה?
האם תרצי להתבונן במראה שייצור כווייה בעינייך?
אם לא- אל תיכנעי לסקרנות, תרשי לעצמך פעם אחת בחיים להיות תמימה עם ה' ולומר: ה' הטוב, בשבילך אני מוותרת, עוצמת עיניים, מתעלמת ומפנה גב לכל הדברים המסקרנים שאני יכולה לגלות! "טוב ארך אפיים וגו'"- לעשות זה קל, להתנזר זה קשה! נראה אותך!
מה גם שמי שיוצר איתך קשר מסוג זה באינטרנט- הוא לא מנכ"ל מייקרוסופט ולא ראש הממשלה- וזאת בלשון המעטה. רוב הסיכויים שהוא משתייך לצד הלא-יוצלח של העולם, כי הוא עסוק בהתכתבויות למילוי צרכיו החולניים בעוד שאר העולם עסוק בחתירה להצלחה. לאדם נורמלי יש סדר יום, הוא מתפרנס ממשלח יד מקובל, בד"כ בעל תעודה כלשהיא, ישן בלילה וקם בבוקר לעבודה, ולא מסתובב באינטרנט בכל עת מצוא.
מי שמחפש צעירות באינטרנט- הוא אדם שלא אכפת לו ממך, והוא מתכונן להשתמש בך כמו מגבון לח.
תחשבי על העתיד שלך- איפה את רואה את עצמך בעוד 5, 10, 20 שנה? נשואה למישהו שהכרת באינטרנט (במקרה הטוב עדיין נשואה), מנותקת מהעולם שהכרת תמיד? או נטועה היטב במקום מוכר ונוח <u>שאת</u> בחרת בו?
אם עד לפני שנים ספורות היה עוד אפשר להתבלבל ולחשוב שהעולם שבחוץ מסוגל להביא אושר- הרי שהיום זה כבר ברור שלא. העולם המערבי מציע הנאות אך לא שמחה. העולם המערבי מציע

התנתקות וחופשיות אך לא מציע מטרה לשאוף אליה. העולם המערבי כשל- ואין סיבה שאת תהיי חלק מהכשלון הזה, ובוודאי שלא תחווי על בשרך את תחושת הריקנות והאבדון שמחכה לנכשלים.

<u>פרק ה/2- לאחר נקודת הבחירה</u>

נכשלת?
ה' מחכה לך בכל רגע ורגע!
דרך תשובה מוכנה עבורך, עלייך רק לעשות את הצעד הראשון.
כל שעלייך לעשות הוא לפתוח פתח בחודו של מחט, למצוא בתוכך את הרצון להיות נורמלית וטובה, ולפלס את דרכך אל המקום שבו את רוצה באמת להיות.
הצלחת?
אין טעם להכביר במילים, כי את האושר והסיפוק את בוודאי מרגישה בעצמך!!!
(וגם אם הם לא מגיעים מייד, עדיף להמתין להם מאשר לשתות בינתיים מים מלוחים)

<u>נספח- לא לבעלות לב חלש.</u>
כמה דוגמאות למה שפושעים עושים באינטרנט:
* גונבים סיסמאות ונכנסים בעזרתן לאתרים שונים ומתחזים למשתמש עצמו. כך לדוגמה פושע שמשיג את הסיסמה לאלי אקספרס יכול להיכנס לשם ולהזמין בכל העולה על רוחו (לאחר שעידכן את הכתובת למשלוח הפריטים, והם יגיעו אליו באדיבות אמצעי התשלום של המשתמש התמים.)
* שולחים אימיילים עם ניסיונות סחיטה. (אני אישית קיבלתי לא מזמן ניסיון סחיטה בזה, שבו ההאקר כתב שאם לא אעביר לו סכום כסף מסויים בהקדם, הוא יפרסם את היסטוריית הגלישה שלי לכל אנשי הקשר שלי... במקרה זה ספציפית ידעתי שהוא משקר כי הוא ציין אתרים שממש לא נמצאים בהיסטוריית הגלישה שלי ולא עוברים אף חסימה, אבל אנשים שכן נכנסים לאתרים הללו, מאוד חוששים מזה ומסוגלים להיות נתונים לסחיטה.)
* מנסים לגנוב פרטים אישיים ובעיקר פרטי כרטיס אשראי וזה די ברור למה. (חשוב לציין שכל פרט שהם משיגים עוזר להם לבנות את ה"פאזל" של זהות האדם, שמצליבים עם נתונים מהמון אתרים ולכן גם שם וטלפון לא כדאי שיפלו בידיהם.)
* מפיצים וירוס שנועל את כל הקבצים ורק הם יכולים לשחרר אותו באמצעות קוד מסויים, והם עושים זאת אחרי שבעל המחשב משלם את סכום הכסף שדרשו. למעשה "וירוס כופר". לפני כמה שנים כשעבדתי במקום עבודה מסויים אחד הלקוחות שלנו קיבל כזה וירוס והיה צריך להשקיע כספים ומשאבים רבים כדי להציל את המידע שלו. תארי לעצמך שזה קורה לאדם פרטי עם כל התמונות של המשפחה כמה כסף הוא כבר יכול להשקיע בזה?
* מקימים חשבונות מזוייפים בכל מיני אתרים- בעיקר רשתות חברתיות אך לא רק. (חשבון מזוייף הכוונה היא חשבון שלא משקף את הזהות האמיתית של מי שהקים אותו.) איך תרגישי אם תדעי שחצי מההמלצות החמות שגרמו לך לקנות מוצר מסויים נכתבו ע"י כאלה חשבונות? ("בוטים")
* פותחים אתרי מכירה שבהם אפשר לקנות דברים, הקונים משלמים אך לא מקבלים את המוצר וממתינים עד בוש... בעוד הפושע קיבל את הכסף ולא התכונן אפילו לרגע לספק את המוצר.

* שולחים מיילים כביכול מהבנק או מחברת האשראי ומבקשים בתמימות להחליף סיסמה (והמיילים וגם הקישורים נראים אותנטיים לחלוטין כאילו הגיעו מהבנק) המשתמש מזין את הסיסמה הקודמת ו... אופס, הפושע קיבל אותה.
* מנסים להשיג תמונות אישיות, בעיקר של נשים וילדים, בעיקר תמונות כמה שפחות צנועות וד"ל. הם עושים זאת כדי למלא תאוות בלתי נשלטות שבגינן אמורים להתאשפז בבית חולים פסיכיאטרי או בבלא. לא נעים לאף אחת לדעת שהיא מעסיקה את מחשבותיו של פושע זר ונאלח ושוב- ד"ל.
* וזה בלי שמדברים על וירוסים שמצלמים את המסך כל כמה שניות, וירוסים שמדליקים את המצלמה והמיקרופון שמחוברים למחשב, האקרים שמעבירים לעצמם כספים מחשבונות בנק של אנשים תמימים, אנשים משוממים שנהנים להפחיד אחרים ומפיצים ידיעות מפחידות ושקריות, ואין לדבר סוף כי יצר לב האדם רע מנעוריו.
(במאמר מוסגר- אלו רק הפשעים שקיימים באינטרנט הרגיל שכולנו משתמשים בו. מתחתיו, מופעלת מתוך שרתים עלומים ע"י פושעים מקצועיים, רוחשת ה"דארקנט"- העולם התחתון של רשת האינטרנט, שבו ניתן לקנות נשק, סמים מסוכנים, מוצרים מובחרים, ואפילו עבדים ושפחות (בד"כ ילדים) ממקומות עניים בעולם. אין צורך לדאוג, כי לאדם מן השורה אין אפשרות להיכנס ל"דארקנט", שמוגנת היטב ע"י הפושעים המפעילים אותה- אבל לגבי האנשים הרעים שמסתובבים באינטרנט הרגיל, צריך לדאוג גם לדאוג.)
זה אולי נראה רחוק או דמיוני אבל לא לחינם תחום הגנת הסייבר הוא תחום צומח בשנים האחרונות- כי הפושעים הולכים ונעשים מתוחכמים מפעם לפעם ומי שלא מגן על עצמו, אין לו למי לבוא בטענות.
ונסיים בנימה אופטימית:
בגלל שאין לי פייסבוק, אני מנסה להכיר חברים מחוץ לפייסבוק, ומשתמש באותה השיטה: כל יום אני הולך ברחוב ומסביר לאנשים שאני פוגש: מה אכלתי, איך אני מרגיש, מה עשיתי אתמול, מה אני עושה עכשיו, מה אני עומד לעשות, מה אני עושה מחר, אני נותן להם תמונות של אישתי, של הילדים, של הכלב שהיה לי, תמונות שלי שוטף את האוטו ושל אישתי תופרת. אני גם מקשיב לשיחות של אנשים ואומר: "אהבתי!" - וזה עובד! כרגע יש לי כבר 5 אנשים שעוקבים אחריי: 2 שוטרים, 1 פסיכיאטר, 1 פסיכולוג ופראמדיק.