גירסה 1.00 – 20.5.2002

אבטחה ב ICQ

Assaf Reshef
ICQ : 15039767
Email : assaf@fullscreen.co.il
Home Page : http://underwar.livedns.co.il

הקדמה

כמה מילים מאת המחבר

במסמך זה אני אדון בגיבוי ושחזור ה ICQ ובהצעות לאבטחת ה ICQ.
הידע הנדרש לפני קריאת המסמך הוא היכולת להתקין ICQ והתמצאות כללית ב ICQ.

במסמך זה אסקור רק חלק מההיבטים של אבטחה ב ICQ. ישנם נושאים נוספים אליהם לא התייחסתי במסמך זה.

בנוגע לחלק של אבטחת ה ICQ : אני מציע לבצע את רוב ההצעות במסמך כדי לשמור על ה ICQ, אבל שכל אחד שיבחר מה שהוא רוצה לעשות בעצמו ושיהיה מודע לכך שהאחריות לבחירתו ולמעשיו היא עליו.

למה לנו בכלל לגבות\להגן על ה ICQ?

כמה סיבות :

1. אם חשוב לנו המספר בו אנחנו משתמשים – שינוי המספר משמע שנצטרך להוסיף את כל הרשימה שלנו מחדש והם יצטרכו להוסיף אותנו. אם מישהו פרץ לנו לחשבון ה ICQ וגנב את המספר שלנו, הוא יכול לשלוח הודעות לחברים ברשימה שלנו ולהתחזות אלינו.

2. אם ההיסטוריה שלנו עם הרשימה היא חשובה\פרטית – אם אנחנו לא רוצים שההיסטוריה שלנו עם הרשימה תימחק או אם אנחנו לא רוצים שמישהו יקרא את ההיסטוריה שלנו.

3. אם אנחנו רוצים לשמור על המחשב שלנו בפני פריצה – אם אנחנו לא ננהג בזהירות ב ICQ, יוכלו אנשים לפרוץ אלינו למחשב.

גיבוי הרשימה

את מה אנחנו בעצם מגבים? - הגיבוי שנעשה יכלול :

- את הרשימה שלנו, האנשים איתם אנחנו מדברים
- את ההיסטוריה שלנו עם אותם אנשים
- את ההגדרות של ICQ האישיות שלנו

כדי לגבות את ה ICQ במקרה שנצטרך להחזיר אותו אנחנו צריכים :

1. את מסד הנתונים שלנו - גיבוי מסד הנתונים שומר על ההיסטוריה (History), על ההגדרות שלנו ובגרסאות ישנות של ICQ (2000 ומטה) גם על רשימת המשתמשים ונרצה לשמור על מסד הנתונים רק אם נרצה לשמור על אלו – לא חובה אבל מומלץ מאוד.

   מסד הנתונים הוא בעצם קבצי הנתונים שלנו – הקבצים עם סיומת DAT. ש ICQ שומר בתיקיית הנתונים שלנו, ואנחנו נרצה לגבות את כולה. התיקייה תלויה בגרסת ה ICQ, והיא נמצאת בתיקיה הראשית של ICQ.
   לדוגמא :
   ב **ICQ 2000b** התיקייה בה נמצאים קבצי הנתונים של ICQ היא
   C:\Program Files\ICQ\2000b

   ב **ICQ 2002a** התיקייה היא
   C:\Program Files\ICQ\2002a

   (בתנאי התיקייה הראשית של ICQ היא **C:\Program Files\ICQ**)

2. מספר ICQ וסיסמא – כמובן שנצטרך לזכור את מספר ה ICQ והסיסמא שלנו כדי להיכנס לחשבון מחדש

3. התקנה של ICQ - את ההתקנה של ICQ נוכל להוריד מהאתר של ICQ בכל שלב. אני ממליץ לשמור התקנה של אותה גירסה שהשתמשנו בה – אבל אפשר גם להוריד ולהתקין גם גירסה יותר מתקדמת

איך נגבה את כל אלו?

כל דרך לגיבוי שנוכל לחשוב עליה היא טובה, ונבחר את הדרך הנוחה לנו : צריבה, העתקה למחשב אחר שברשותנו, שינון הקוד הבינארי של הקבצים בעל פה (אם ממש משעמם לכם :) או כל דרך אחרת.

שחזור הרשימה

כרגע, אנחנו רוצים לשחזר את כל מה שגיבינו.
אם גיבינו את תיקיית הנתונים של ICQ, עדיף שנעתיק אותה למחשב לתיקייה זמנית עד שנשתמש בה.

עכשיו, נלך על פי הצעדים הבאים :

1. **התקנת ICQ חדש ורישום המספר שלנו**

א. נתקין ICQ חדש
ב. אחרי ההתקנה, נפתח לנו חלון ששואל אותנו האם אנחנו רוצים ליצור משתמש חדש (New User) או לרשום משתמש קיים (Existing User). אנחנו נבחר באפשרות השנייה, נקיש את מספר ה ICQ שלנו וסיסמא ובזה רשמנו את מספר ה ICQ במחשב שלנו.
ג. בגרסאות ישנות של ICQ, ייפתח לנו ה ICQ בלי רשימה, ובגרסאות חדשות של ICQ, ייפתח לנו ה ICQ עם רשימה שהוא יוריד מהשרת של ICQ (בתנאי שבעבר השתמשנו בגירסה חדשה ובכך עדכנו את השרת של ICQ ברשימה שלנו), אבל ללא ההיסטוריה עם האנשים שנמצאים אצלנו ברשימה וללא ההגדרות שלנו.

2. **שחזור הרשימה, ההיסטוריה וההגדרות שלנו**

כדי להחזיר לנו את הרשימה, ההיסטוריה וההגדרות נבצע מספר צעדים :

א. נסגור את ה ICQ
ב. נעתיק את כל תוכן התיקייה שגיבינו בהתחלה אל תיקיית הנתונים החדשה שנוצרה לנו כשהתקנו את ה ICQ ונחליף את הקבצים שבתוך התיקייה החדשה לקבצים שגיבינו קודם
ג. נפעיל את ה ICQ מחדש
ד. אם התקנו גירסה חדשה יותר של ICQ ממה שהייתה לנו, מסד הנתונים יומר למסד נתונים של הגירסה החדשה

זה הכל, ה ICQ יעלה עם הרשימה, ההיסטוריה וההגדרות שלנו

מתי חשבון ה ICQ שלנו בסכנה?

יש כמה גורמים שמאפשרים לפורצים להשתלט לנו על חשבון ה ICQ. מישהו יכול לפרוץ לנו לחשבון אם הוא משיג את אחד הבאים :

- **הסיסמא שלנו** – על ידי פיצוח הסיסמא, ניחושה, או על ידי קבלת הסיסמא בעזרת אחת מהשיטות הבאות.

קבצי הנתונים שלנו – את קבצי הנתונים אפשר להשיג על ידי גישה (פיזית או לא) למחשב שלנו. קבצי הנתונים אלו הקבצים עם סיומת DAT. ש ICQ שומר בתיקיית הנתונים שלנו (כדי לדעת בדיוק איפה תיקייה זו ממוקמת – ראה גיבוי ה ICQ בעמוד 2)

- **הדוא"ל שלנו** – מישהו יכול לפרוץ אלינו לחשבון אם הוא פרץ או קיבל גישה לחשבון דוא"ל שרשום אצלנו בפרטים של ה ICQ
- **ההגדרות שלנו** - מישהו יכול לפרוץ אלינו לחשבון אם הוא הצליח לשנות את השרת של ICQ שנמצא אצלנו בהגדרות של ה ICQ
- ועוד...

איך להגן על ה ICQ – הגנות בסיסיות

יש כמה כללים בסיסיים שצריך לשמור עליהם כדי לשמור על הגנה בסיסית על ה ICQ :

- **לא להניח שאנשים הם חברים שלנו** – אם מישהו מוסיף אותנו לרשימה וטוען שהוא חבר שלנו, עדיף לנו לנצל 20 שניות ולשאול אותו משהו אישי שרק שנינו יודעים את התשובה אליו כדי לוודא שזה הוא באמת. אם אנחנו באמת חברים צריכים להיות לנו מספיק דברים קטנים שרק שנינו יודעים.
  מכיוון שאפשר גם לזייף הודעות וגם לפרוץ לאחד החברים שלנו לחשבון, צריך גם לשים לב לדברים שהחברים שלנו ברשימה אומרים ולזהות אם יש משהו חשוד בסגנון כתיבה או בתוכן הדברים שהם אומרים.

- **לא להאמין לכל אחד** – אם מישהו מבקש מאיתנו לעשות משהו בשבילו או לשנות הגדרות בשבילו, עדיף לנו לברר מה זה יעשה קודם כל. נעשה את זה רק אחרי שנהיה בטוחים שהוא מבקש את זה כי הוא צריך את זה וזה לא יפגע בנו בצורה כלשהי.
  דוגמא טובה למשהו שכן יכול לפגוע בנו היא שינוי הדוא"ל שלנו בפרטים, או שינוי השרת של ה ICQ.

- **לבחור בסיסמא קשה לפיצוח** - אם נבחר סיסמאות בסגנון "icq1" או "12345678" לא יהיה קשה לנחש אותן, ומכאן שלא יהיה קשה לפרוץ ל ICQ שלנו. סיסמא קשה לפיצוח היא סיסמא כמו "f3PEnK2r" או "o3N#i&v". אחת השיטות לבחירת סיסמא היא "שיטת כף היד" : להניח את כל כף היד על המקלדת באזור האותיות והמספרים, ללחוץ על כל המקשים ביחד וליצור סיסמא אקראית ☺.

  החלק הבא מדבר על שיטה טובה נוספת לבחירת סיסמא, כדאי לקרוא אבל לא חובה :
  - שיטה אחרת עליה אני ממליץ היא פשוט ליצור סיסמאות שקשורות אישית אלינו עם שינויים – אני לא מתכוון למשהו כמו d0r0n במקום doron אלא משהו קצת יותר מתוחכם. לדוגמא, אני עובד הרבה עם Visual Basic ובאחת הפעמים כתבתי פונקציה בשם SetArrToFileListFromDir ואני זוכר את השם שלה. ניקח את שם הפונקציה, נחליף ונשנה מעט את האותיות ונוכל ליצור סיסמא כמו seTarrt0FileliStFromdiR (האות O [או] הפכה להיות 0 [אפס] ואותיות גדולות הפכו לקטנות ולהיפך). היתרון בסיסמא כזאת היא שאחרי 5-10 פעמים שאני אשתמש בסיסמא זאת אני אזכור אותה בעל פה (במיוחד שאת החלק העיקרי מהסיסמא, את המבנה הכללי שלה, זכרתי עוד לפני כן). יתרון אחר והעיקרי מביניהם הוא שזאת היא סיסמא קשה יחסית, ורק אני יודע איזה פונקציה ספציפית אני זוכר מתוך אלפי הפונקציות שכתבתי, איזה שינויים עשיתי ואת העובדה שהסיסמא שלי היא בכלל בנויה על שם של פונקציה! (ודרך אגב, אני אחסוך לכם כמה דקות ואגיד לכם שזאת רק דוגמא לסיסמא - לא אחת מהסיסמאות שלי). עוד דבר חשוב הוא לזכור את הסיסמאות, או לרשום אותם במקום בטוח (= לא מקום דיגיטלי. פתק מוחבא לדוגמא – וגם זה בתנאי שאתם בטוחים ב 100 אחוזים שהוא לא יגיע לידיים הלא נכונות). לשים על שולחן עבודה קובץ שקוראים לו passwords.txt עם כל הסיסמאות לא יהיה רעיון חכם.

- **לא לקבל קבצים מאנשים זרים** – בדיוק כמו שאימא תמיד אמרה לא לקחת סוכריות מזרים (לדבר עם אנשים זרים זה בסדר ב ICQ :) – ככה אסור לקבל קבצים מאנשים.
  טוב, בשלב הזה אני רוצה להעיר משהו : שמעתי מספיק אנשים וקראתי מספיק מקורות שאומרים שאסור לקבל שום קובץ ומאף בן אדם. לפי דעתי זה קצת מוגזם

ויש הבדל : מחבר קרוב שאנחנו מכירים אותו טוב וסומכים עליו, אפשר לקבל קבצים, במיוחד אם אנחנו יודעים מה הקובץ הזה ולמה הוא שולח אותו, ובמיוחד אם זה קובץ טקסט (Txt), תמונה(Gif, Jpg, Bmp) או מוזיקה (Mp3) ולא קובץ הרצה(Exe, Com, Vbs, Pif, Bat ועוד).

- **<u>לא לפתוח אתר ולא לבדוק דוא"ל דרך השירות של ICQ</u>** – יש והיו מספיק בעיות עם שני השירותים האלה שעדיף לא לגעת בהם. אני הייתי גם ממליץ לא לגעת ב File Sharing כי ההערכה שלי היא שיהיו עם זה עוד בעיות.

- **<u>להשתמש באנטי וירוס טוב</u>** - אני ממליץ על Norton Anti Virus.

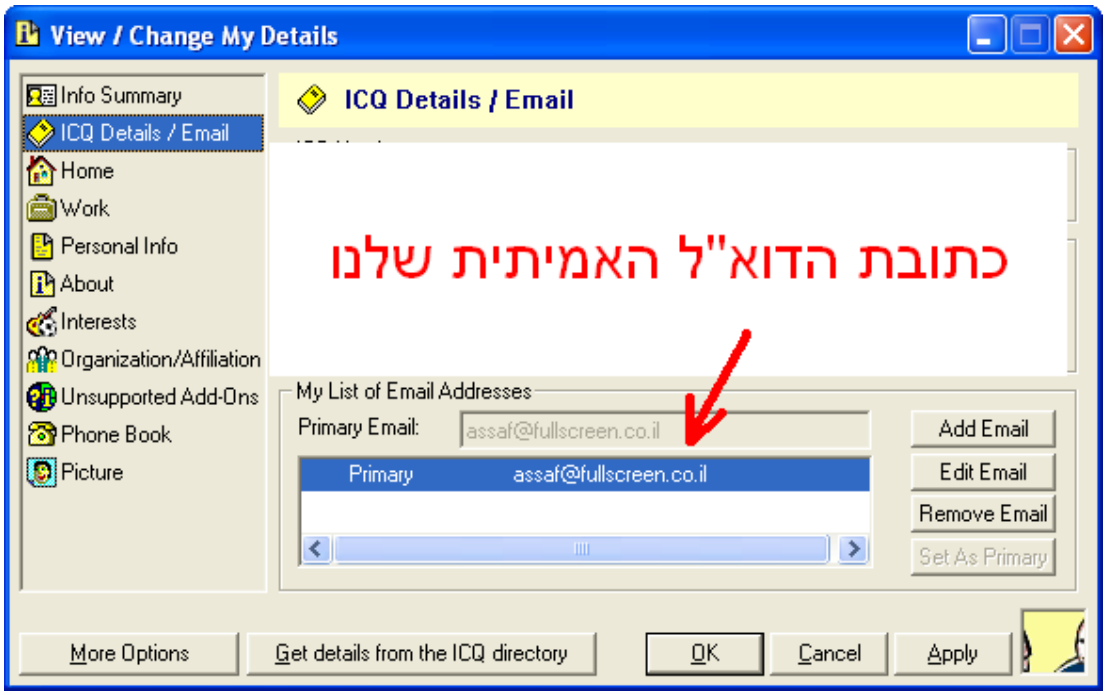
- **<u>להשתמש בחומת אש (Firewall) טובה</u>** – אני ממליץ על ZoneAlarm.

- **<u>לכתוב את כתובת הדוא"ל (Email) האמיתית שלנו בפרטים!</u>** - יש ל ICQ מנגנון ששולח את הסיסמא של ה ICQ במקרה ששכחנו אותה לדוא"ל שכתוב בפרטים של המשתמש. ולכן :

  - אם נכתוב את כתובת הדוא"ל האמיתית שלנו בפרטי ה ICQ ומישהו יפרוץ אלינו לחשבון ה ICQ, נוכל לבקש שהסיסמא הנוכחית של ה ICQ תישלח אלינו לדוא"ל.

  - אם נכתוב דוא"ל של מישהו אחר או נכתוב משהו כמו i_have_no_email@hotmail.com (דוא"ל שלא קיים ושכל אחד יכול לרשום אותו לעצמו), בלחיצת כפתור אחת באתר של ICQ הסיסמא שלנו יכולה להישלח למישהו אחר.

שליחת הסיסמא לדוא"ל נעשית בכתובת http://www.icq.com/password/



<u>הערה</u> : אם הכנסנו כתובת דוא"ל לפרטים שלנו ב ICQ מתאריך 1.9.1999 והלאה, אז

השרתים של ICQ זוכרים אותו, וגם אם רשמנו את הכתובת דוא"ל האמיתית שלנו ומישהו פרץ אלינו בכל זאת ומחק אותה מהפרטים, עדיין נוכל לשחזר את הסיסמא עם הכתובת שנמחקה – תודה לדני על המידע.

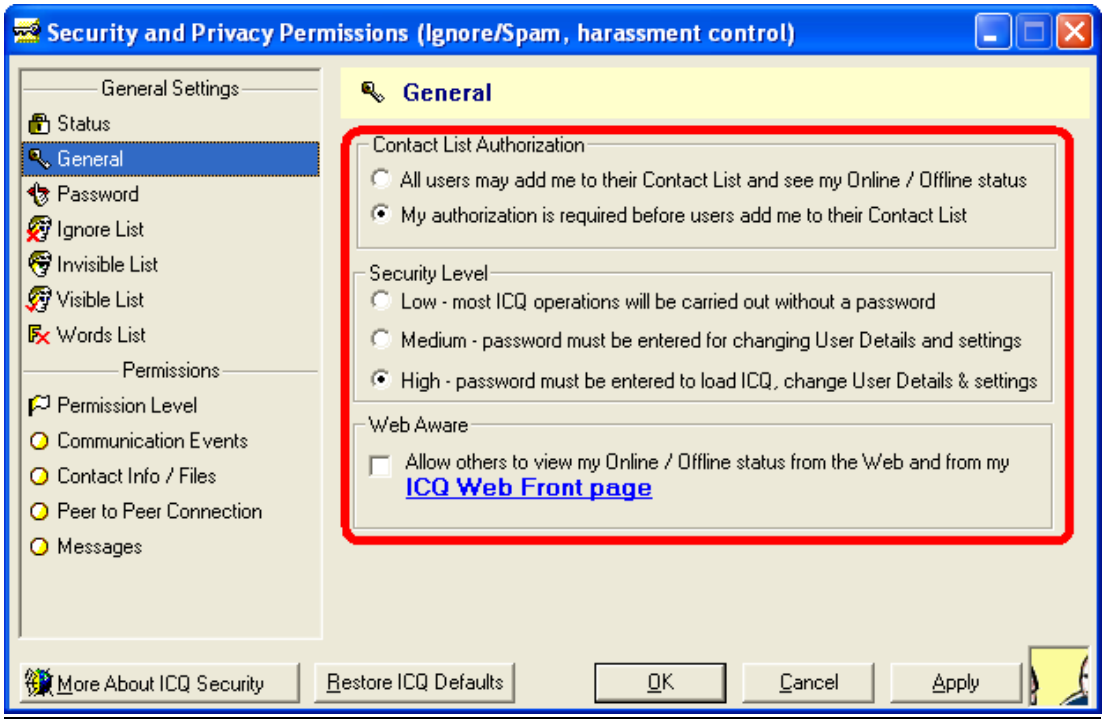
- **<u>לשנות את ההגדרות הראשיות בתפריט Security/Privacy</u>**

בתפריט Security/Privacy נמצא 3 הגדרות אותן נרצה לשנות :

- <u>Contact List Authorization נשנה ל My Authorization is required…</u> - הגדרה זו תגרום לכך שאנשים לא יוכלו להוסיף אותנו לרשימה שלהם בלי האישור שלנו. יש תוכנות שמשנות את הצורה שבה ICQ פועל והן מאפשרות לאנשים בכל זאת להוסיף אותנו לרשימה שלהם בלי אישור, אבל עדיף לקבוע הגדרה זו כדי שניתן את האישור למי שלא שינה את ה ICQ.

- <u>Security Level נשנה ל High</u> – הגדרה זו תגרום לכך שנצטרך להקיש את הסיסמא שלנו כשניכנס ל ICQ וכשנשנה הגדרות, דבר שיוודא שאנחנו עושים את זה ולא מישהו אחר שיש לו גישה פיזית למחשב.

- <u>נסיר את הסימון מ Web Aware</u> – ICQ מאפשר לאנשים לראות דרך האינטרנט אם אנחנו במצב Online או Offline גם אם אנחנו לא ברשימה שלהם והגדרה זו תגרום לכך שהם לא יוכלו.

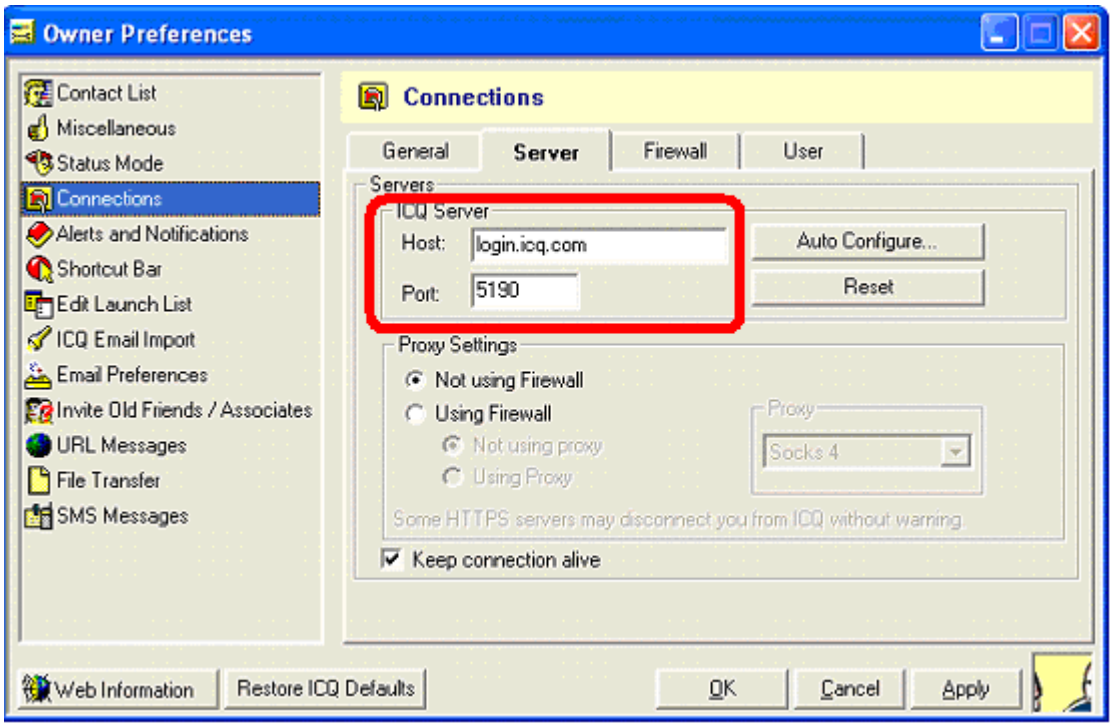


- **<u>לא לשנות את השרת (Server) של ה ICQ שאליו נתחבר</u>** - בגירסאות ICQ98a ICQ99a ICQ99b השרת הוא אחד מהבאים :

icq.mirabilis.com

icq1.mirabilis.com
icq2.mirabilis.com
icq3.mirabilis.com
icq4.mirabilis.com
icq5.mirabilis.com

מגירסה 2000a ומעלה, השרת הוא login.icq.com והפורט הוא 5190.

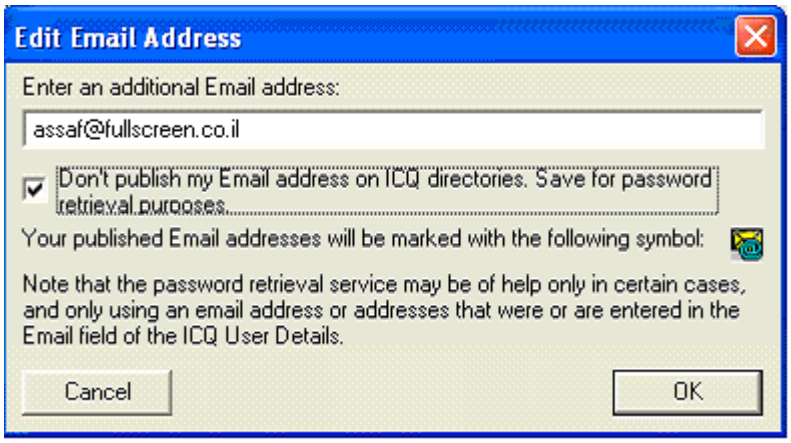


כשאנחנו מתחברים ל ICQ אנחנו שולחים לשרת את מספר ה ICQ והסיסמא שלנו, ולכן אם מישהו גורם לנו לכתוב את הכתובת שלו בתור שרת ה ICQ שלנו, הסיסמא שלנו תישלח אליו ברגע שננסה להתחבר.

איך להגן על ה ICQ – הגנות מתקדמות

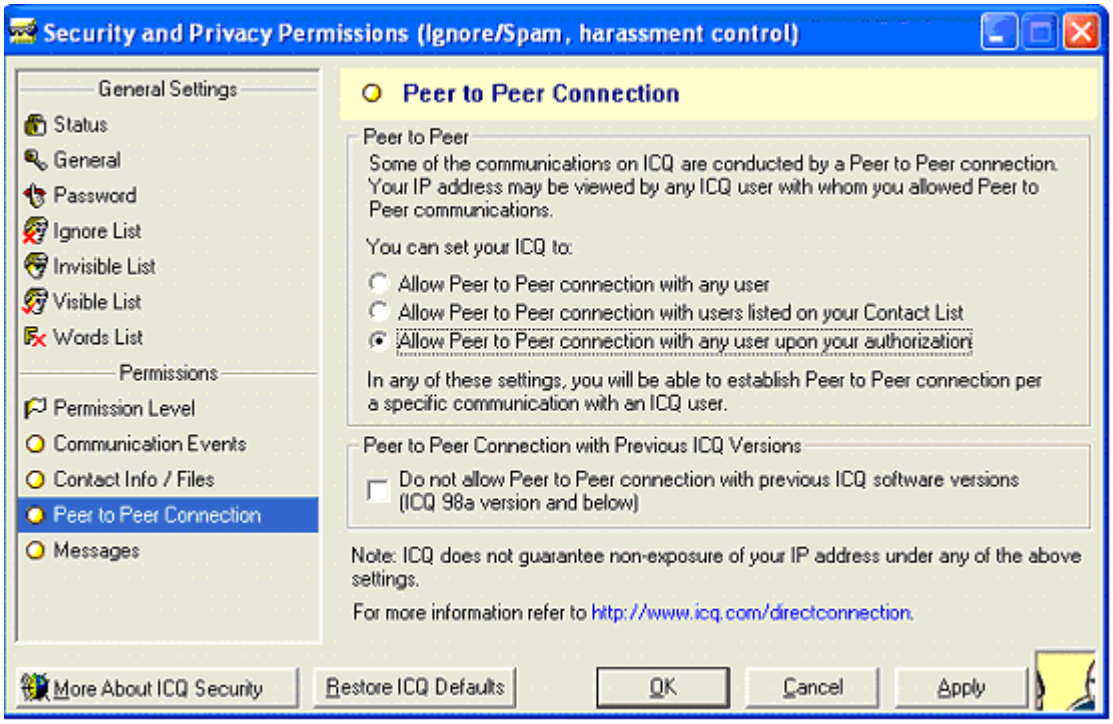
הערה: לא חובה לנקוט ב ההגנות הבאות, ההגנות הבאות רק מוסיפות הגנה על ה ICQ, בנוסף להגנות הבסיסיות.

- **הסתרת הדוא"ל שלנו מהפרטים** – אם מישהו לא רואה את כתובת הדוא"ל שלנו הוא לא יכול לנסות אפילו לפרוץ אותה (אם הוא פרץ את הדוא"ל, הסיסמא יכולה להישלח אליו. כדי להסתיר את הדוא"ל שלנו, נעשה כך:
  1. נלך ל Main/Icq – View / Change My Details – ICQ Details / Email
  2. נשנה את ההגדרות הבאות:
     ב ICQ99 - נסמן את "publish my Email address on ICQ directories. Save for password retrieval purposes"
     ב ICQ2000 ומעלה – נבחר את הכתובת אותה אנחנו רוצים להסתיר, נלחץ על "Edit" ונסמן את "Don't publish my Email address on ICQ directories. Save for password retrieval purposes".
  3. נלחץ OK לאישור



עוד הצעה היא לפתוח חשבון דוא"ל חסוי שיש לו מטרה אחת: לקבל את הסיסמא של ICQ במקרה ששכחנו אותה. היתרון בזה הוא שאם מישהו מכיר אותנו, יודע את הכתובת דוא"ל שלנו ומצליח לפרוץ אותה, הוא לא יוכל להשתלט לנו על ה ICQ, מכיוון שבפרטים רשמנו והסתרנו כתובת דוא"ל שאף אחד לא צריך להכיר ולא את הכתובת העיקרית שלנו.

- **הסתרת כתובת ה IP שלנו** – תוכנות מסוימות מאפשרות לאנשים לראות את כתובת המחשב שלנו (IP) על ידי הזנת מספר ה ICQ, גם אם אנחנו לא נמצאים ברשימה שלהם. כדי להסתיר את כתובת ה IP נצטרך לשנות לבצע את הצעדים הבאים:
  1. נלך ל Main/Icq – Security / Privacy – Peer to Peer Connection
  2. נסמן את Allow Peer to Peer connection with any user upon your authorization
  3. נלחץ OK לאישור



- **<u>הסתרת תיקיית ה ICQ</u>** – ברירת המחדל של ICQ מתקינה את התוכנה בתיקיה C:\Program Files\ICQ\. במקרה ומישהו פרץ אלינו למחשב הוא יכול ללכת לתיקיה הזאת ולהוריד ישר את קובץ הנתונים שלנו, ובכך לפרוץ לנו ל ICQ. לכן, ניצור תיקיה שלא תהיה בולטת ונתקין בה את ה ICQ. לדוגמא: c:\windows\system\help\temp\.

נוכל לבצע עוד מספר פעולות שיעזרו לנו להגן על ה ICQ מפני פריצה:

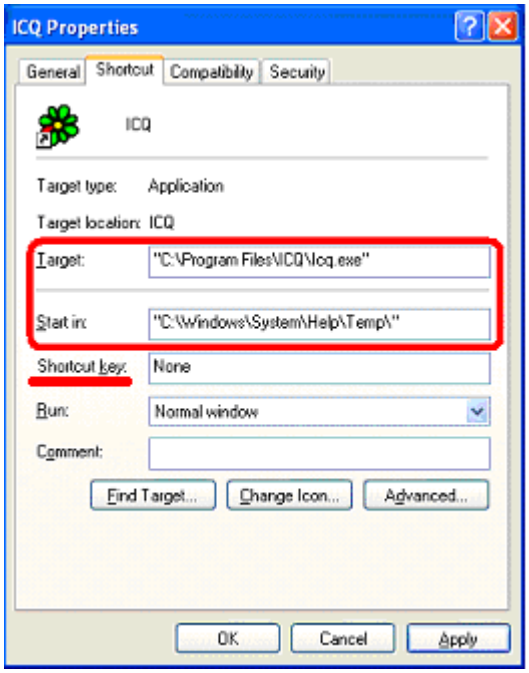
1. אחרי שהתקנו את ה ICQ בתיקיה המוסוות, נוכל ליצור תיקייה מזויפת של ICQ כדי להטעות פורצים במקרה שפרצו אלינו. ניצור את תיקיית ברירת המחדל של ICQ: C:\Program Files\ICQ\ ונעתיק לשם את כל הקבצים מהתיקייה המסוות שיצרנו. עכשיו נותר רק להכין קבצי נתונים מזויפים של ICQ ולהחליף את הקבצים הקיימים בתיקיית הנתונים של ICQ בקבצים המזויפים שיצרנו. אפשרות עדיפה היא להכין קבצים מזויפים אלו מראש ורק להעתיק אותם בתום התקנת ה ICQ.

2. הרבה תוכנות פריצה מאפשרות לראות איזה תוכנות פועלות אצלנו במחשב. אם מישהו יראה שתוכנה בשם c:\windows\system\help\temp\icq.exe פועלת אצלנו במחשב, הוא יסיק בקלות איפה מותקן אצלנו ה ICQ. ולכן, נשנה את השם של הקובץ icq.exe (הקובץ שמפעיל את ה ICQ) לשם "תמים" (לדוגמא Help.exe). שינוי שם הקובץ נבדק ופועל ב ICQ2002a Beta 3727 ואני לא יודע אם הוא עובד בגרסאות אחרות. עכשיו אם מישהו יבדוק איזה תוכנות פועלות, הוא יראה שתוכנה בשם c:\windows\system\help\temp\help.exe פועלת, תוכנה שנראית הרבה יותר "משעממת" בשבילו מתוכנה בשם C:\Program Files\ICQ\icq.exe.

3. אחרי שבסעיף 1 יצרנו תיקייה מזויפת של ICQ, למה שלא נגרום למשתמש לראות

שקובץ בשם C:\Program Files\ICQ\icq.exe פועל אצלנו במחשב, אבל רק אנחנו יודעים שהוא לא האמיתי! שיטה אחת היא פשוט לשים במקום הקובץ C:\Program Files\ICQ\icq.exe המזויף שיצרנו קובץ שפשוט פועל ולא עושה כלום (אם יהיה ביקוש גדול אני יכול לשים את קוד המקור של תוכנה כזאת ב VB :). שיטה אחרת היא פשוט להפעיל את הקובץ icq.exe מהתיקייה המזויפת. אם התקנו את ICQ בתיקיה מסוימת, תיקייה זו נשמרה ב Registry ונוכל להפעיל את icq.exe מכל תיקיה שנרצה וה ICQ יעלה לנו עם הנתונים וההגדרות של התיקייה בה התקנו את ה ICQ.

4. במקרה וסעיף 3 לא עובד נוכל ליצור קיצור דרך ל תוכנה icq.exe בתיקיה המזויפת אבל להגדיר שהתוכנה תפעל מתוך התיקייה שבה התקנו את ה ICQ (יש אפשרות כזאת בתוך המאפיינים של קיצור הדרך – ראה תמונה)



ככה ה ICQ ייראה כאילו הוא רץ מהתיקייה המזויפת. אם נרצה נוכל גם להסתיר את קיצור הדרך הזה בתיקיה כלשהי, במקום לשים אותו במקום גלוי, ולתת לו גם קיצור דרך (Shortcut Key) שיריץ אותו – כדי שיהיה לנו נוח להפעיל אותו, וככה יהיה קשה לגלות אותו ובכך לגלות את התיקייה האמיתית שלנו.

5. הרבה תוכנות שבודקות איפה מותקן ה ICQ לוקחות את הנתיב של ICQ מהמיקום HKEY_LOCAL_MACHINE\Software\Mirabilis\ICQ\DefaultPrefs\ICQPath\ אבל משום מה גם אם נשנה אותו ה ICQ יפעל כמו שצריך, לכן נשנה אותו לנתיב המזויף שלנו ובכך "נעבוד" על כל מיני תוכנות שמנסות לזהות איפה ה ICQ מותקן. כמובן שיש ב Registry עוד מקומות שמהם אפשר להסיק איפה התיקייה המקורית שבה התקנו את ה ICQ, אבל שינוי שלהם יכול לפגוע ב ICQ עצמו. שוב אני אזכיר, המידע הזה לא נבדק על כל גירסה של ICQ ואני לא אחראי לכל נזק שייגרם על ידי שימוש לא נכון ב Registry או כל שימוש אחר במידע זה.

- **<u>תפיסת הפורץ "על חם"</u>** – הרבה פורצים אוהבים לחקור את מה שיש להם ביד לפני שהם עושים איתו משהו. אם מישהו בכל זאת השיג את הסיסמא שלנו והוא התחבר לנו לחשבון ICQ והחליט שהוא "מרחרח" אחרינו לפני שהוא משנה סיסמא, חשוב לנו מאוד לתפוס אותו בשלב הזה ולא בשלב הבא. לשם כך אפשר לנקוט במספר פעולות שיעזרו לנו :

1. הרבה אתרים שנתונים שירות דוא"ל מאפשרים לקבוע בחשבון דבר שנקרא Forward Email שאומר לשרת להעביר אוטומטית כל הודעה שקיבלנו לחשבון דוא"ל אחר. נוכל לפתוח חשבון דוא"ל במיוחד בשביל הצורך הזה, ולהעביר אליו את כל ההודעות שנשלחו אלינו. במידה ומישהו פרץ לנו לחשבון דוא"ל הראשי שלנו וביקש שישלחו לשם סיסמא, וכשהיא הגיעה הוא רשם אותה ומחק את ההודעה מחשבון הדוא"ל, נוכל לראות בדוא"ל המשני שפתחנו את העובדה שמישהו ביקש את הסיסמא, מכיוון שגם שם נמצאת ההודעה של בקשת הסיסמא, ומשם היא לא נמחקה. נוכל לכתוב תוכנה שתבדוק ותנקה מהחשבון המשני הודעות אוטומטית, אלא אם כן היא מוצאת שם הודעה על בקשת סיסמא מ ICQ ובמקרה כזה היא מזהירה אותנו על כך שמישהו השיג את הסיסמא שלנו.

2. נוכל לכתוב תוכנה שתרוץ מתי שסגרנו את ה ICQ, או שנפעיל אותה לפני כל פעם שנצא מהאינטרנט. התוכנה תישלח אלינו לחשבון ICQ הודעה דרך WWPager. מה שיקרה זה שבפעם הבאה שנתחבר ל ICQ נקבל את ההודעה. אם פעם לא נקבל את ההודעה, נדע שמישהו התחבר לחשבון שלנו וקיבל את ההודעה במקומנו, או שהשרתים של ICQ דפוקים ☺. שאלה : מה יקרה אם מי שהתחבר אלינו לחשבון, קיבל את ההודעה, התנתק ושלח שוב בעצמו את אותו WWPager למספר שלנו? לשם כך נוכל לעשות שהתוכנה גם תשמור בקובץ Log את התאריך והשעה שבה ההודעה נשלחה, ומכיוון שהודעת WWPager מכילה גם את התאריך והשעה שבה היא נשלחה, אם מישהו יזייף את ההודעה יותר מאוחר, נוכל לראות זאת על ידי השוואה של התאריך והשעה שרשומים לנו ב ICQ לתאריך והשעה בקובץ LOG שהתוכנה שלנו רשמה. להודעת WWPager מצורף גם מספר ה IP של השולח ולכן יהיה לו עוד יותר קשה לזייף את ההודעה. עוד רעיון זה שבמקום הודעת WWPager, נתחבר ל ICQ על חשבון אחר שלנו ונשלח לחשבון הראשון הודעת Offline Message. במקרה שמישהו התחבר על החשבון הראשי שלנו וקיבל את ההודעה כזאת, יהיה לו קשה מאוד לזייף את ההודעה לפעם הבאה שאנחנו נתחבר כי הוא יצטרך גם לפרוץ את החשבון השני שלנו. ההודעה יכולה להיות תמימה לגמרי כמו "היי" ולא חייבת להיות משהו בסגנון "אני הודעה שמגנה עלי בפני פורצים" וככה מי שפרץ אלינו לא יחשוד שעלינו עליו.