תוספת לסיסמא (מלח – Salt)

1. רוב האנשים אינם טכנולוגיים. לכן הרבה בוחרים סיסמאות כמו: password, 1234 וכד׳.
2. נניח שהאקר הצליח להסניף את בסיס הנתונים עם הלקוחות שלנו ואז יראה משהו כזה:

Name	other data	password (hashed)
John Doe	.....	Qu674ew89123123
Donald Trump	.....	Qu674ew89123123
Jane Doe	.....	Qu674ew89123123

ההאש נראה זהה כי שלושת האנשים האלה בחרו אותה סיסמא (למשל password).
זה מהווה פתח לניסיון ניחוש סיסמאות.

3. על מנת למנוע זאת, אפשר לייצר ביחד עם כל סיסמא, ערך ראנדומלי שנקרא לו salt (למשל בעזרת פונקציית זמן מחשב) והוא יהיה ייחודי לכל משתמש.. בבסיס הנתונים נשמור האש של השרשור בין הסיסמא וה- salt כערך האש. ביחד עם זאת נשמור גם את ה salt (לא מוצפן).

זה יגרום לכל ערכי ההאש להיות שונים לגמרי גם לאלה שבחרו אותה סיסמא מצד אחד, ומצד שני שמירת ה salt תאפשר לזהות את הסיסמא אם מישהו מנסה לעשות Log in.