Choose a password:

Your email address:
Microsoft Online Safety

Create strong passwords

Strong passwords are important protections to help you have safer online transactions.

Keys to password strength: length and complexity

An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the letters and characters you use or see most often.

Create a strong password you can remember

There are many ways to create a long, complex password. Here is one way that may make remembering it easier.
How safe is your password?

The first step in protecting your online privacy is creating a safe password - i.e. one that a computer program or persistent individual won’t easily be able to guess in a short period of time. To help you choose a secure password, we’ve created a feature that lets you know visually how safe your password is as soon as you create it.

Tips for creating a secure password:

• Include punctuation marks and/or numbers.
• Mix capital and lowercase letters.
• Include similar looking substitutions, such as the number zero for the letter ‘O’ or ‘$’ for the letter ‘S’.
• Create a unique acronym.
• Include phonetic replacements, such as ‘Luv 2 Lef’ for ‘Love to Laugh’.

Things to avoid:

• Don’t use a password that is listed as an example of how to pick a good password.
• Don’t use a password that contains personal information (name, birth date, etc.)
• Don’t use words or acronyms that can be found in a dictionary.
• Don’t use keyboard patterns (asdf) or sequential numbers (1234).
• Don’t make your password all numbers, uppercase letters or lowercase letters.
• Don’t use repeating characters (aa11).

Tips for keeping your password secure:

• Never tell your password to anyone (this includes significant others, roommates, parrots, etc.).
• Never write your password down.
• Never send your password by email.
• Periodically test your current password and change it to a new one.
Internship Programs @ Microsoft Research

Internship Application - Create Login

Send any technical support questions you may have to interns@microsoft.com

Items marked with "*" are required.

Passwords must have the following characteristics:

- Be at least 8 alphanumeric characters long.
- Contain both uppercase and lowercase characters (e.g., a-z, A-Z).
- One of the first four characters must be an uppercase letter.
- Have at least one digit e.g. 0-9.
- Have at least one punctuation character e.g. !@#$%^&"()_+~-=\{};';,./
- One or more of the characters from the second (2) to sixth (6) positions must not be an alphabet character e.g. between A-Z or a-z.

For example:
- BWtN2ds! - Beware of the neighbors 2 dogs!
- I’shiS2d - I’m so happy its Sunny today

Returning user? Please login to go to your application.

Please enter your email address and password.

Email Address:* 
Password:*
Why are we doing this to our users?
Threat 1: Password file compromised

- stus, 0xCF832A834
- cormac, 0xC86A00386
- michaelm, 0xDB015528
- helenw, 0x5723B9291
- wdcui, 0x24BF98902
- dmolnar, 0x23482AA83
- alexmos, 0x1B200D481
- bparno, 0x88B330
Threat 1: Password file compromised

- stus, 0xCF832A834
- cormac, 0xC86A00386
- michaelm, 0xDB015528
- helenw, 0x5723B9291
- wdcui, 0x24BF98902
- dmolnar, 0x23482AA83
- alexmos, 0xB200D481
- bparno, 0x88B330

0xD1F7255CA
Threat 1: Password file compromised

- "stus,asdf"
- $h_{0xCF832A834}$

cost of one guess = cost to compute $h$

<table>
<thead>
<tr>
<th>Username</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>stus</td>
<td>$0xCF832A834$</td>
</tr>
<tr>
<td>cormac</td>
<td>$0xC86A00386$</td>
</tr>
<tr>
<td>michaelm</td>
<td>$0xDB015528$</td>
</tr>
<tr>
<td>helenw</td>
<td>$0x5723B9291$</td>
</tr>
<tr>
<td>wdcui</td>
<td>$0x24BF98902$</td>
</tr>
<tr>
<td>dmolnar</td>
<td>$0x23482AA83$</td>
</tr>
<tr>
<td>alexmos</td>
<td>$0x1B200D481$</td>
</tr>
<tr>
<td>bparno</td>
<td>$0x88B330$</td>
</tr>
</tbody>
</table>
Threat 1: Password file compromised

RockYou Hack Exposes Names, Passwords of 30M Accounts

Hackers breached a database at social networking application maker RockYou Inc. and accessed username and password information on more than 30 million individuals with accounts at the company.

Jaikumar Vijayan, Computerworld
Threat 1: Password file compromised

- stus, asdf
- cormac, 123456
- michaelm, password1
- helenw, rockyou
- wdcui, princess
- dmolnar, abc123
- alexmos, qwerty
- bparno, monkey
Threat 2: Online dictionary attack

"stus, abc123"

Sorry!
Threat 2a: Online statistical guessing

Common passwords (sorted by popularity)

- password1
- password
- abc123
- asdf
- 1234568
- p@ssword
- iloveyou

"stuck on password1"

Welcome!

Sorry!
Threat 2a: Online statistical guessing

- User-based lockout ineffective
  - 300m users * 10 guesses per user = 3 billion guesses

- IP lockout slightly less ineffective
  - 10m node botnet * 10 guesses per IP = 100M guesses

- Some accounts will be compromised
  - Frequency of most popular password * guesses
  - 100k accounts if 0.1% use most popular password
Here comes the big* idea of the talk...

*yet low carbon
Replace composition rules with one new rule.
Don’t password rules already accomplish this?

http://failblog.org/2008/01/03/fail-camera/
Expected password choices... without rules

Example based on real data... but not real data!

I’m so clever!

Percent of users with password

Password

- password
- <>
- asdf
- 1234
- qwert
- iloveyou
- fuckyou
- asdfkl;
Rule 1: At least 8 characters

Sometimes rules have unintended consequences
Rule 2: At least 1 number

Percent of users with password

Password

password1  12345678 blink182 trustno1 no1knows hard2forget answeris42 ih8rules
Rule 3: At least 1 “special” character

I sure know how to obfuscate! I’m so original!
Large sites favor strength meters over rules
Create your Windows Live ID

It gets you into all Windows Live services—and other places you see.

All information is required.

If you use Hotmail, Messenger, or Xbox Live, you already have a Windows Live ID.

Sign in

popularityiseverything@hotmail.com is available.

Create a password: password1

6-character minimum; case sensitive

Retype password:

Alternate e-mail address:

Or choose a security question for password reset

Windows Live ID: hotmail.com
Create an Account

Your Google Account gives you access to Gmail and other Google services. If you already have a Google account, you can sign in here.

Get started with Gmail

First name: 
Last name: 
Desired Login Name: popularityiseverything@gmail.com
Examples: JSmith, John.Smith
Choose a password: ********
Minimum of 8 characters in length. 
Password strength: Strong
Re-enter password: ********
Composition rules stronger passwords

‘password’ \^ ‘P@$word1’
Your may not choose a popular password (one already in use by n% of other users.)
If we enforced “no popular passwords”...
Enforcing the “no popular passwords” rule

Create your Windows Live ID

Create a password: P@$$word1

6-character minimum; case sensitive

Sorry!
At least 100 other users are already using this password. You’ll need to choose another one.
We must track popularity to prevent it

<table>
<thead>
<tr>
<th>Common passwords (sorted by popularity)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>password1</td>
<td>2805</td>
</tr>
<tr>
<td>password</td>
<td>2280</td>
</tr>
<tr>
<td>abc123</td>
<td>1568</td>
</tr>
<tr>
<td>asdf</td>
<td>1375</td>
</tr>
<tr>
<td>1234568</td>
<td>583</td>
</tr>
<tr>
<td>p@ssword</td>
<td>390</td>
</tr>
<tr>
<td>Iloveyou</td>
<td>334</td>
</tr>
</tbody>
</table>
Dangers of tracking popular passwords

• Attackers will use this data for statistical guessing
  – Against you
  – Against other sites
## Tracking popular passwords

<table>
<thead>
<tr>
<th>Common passwords (sorted by popularity)</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>password1,</td>
<td></td>
</tr>
<tr>
<td>password,</td>
<td></td>
</tr>
<tr>
<td>abc123,</td>
<td></td>
</tr>
<tr>
<td>asdf,</td>
<td></td>
</tr>
<tr>
<td>1234568,</td>
<td></td>
</tr>
<tr>
<td>p@ssword,</td>
<td></td>
</tr>
<tr>
<td>lloveyou,</td>
<td></td>
</tr>
</tbody>
</table>
Dangers of tracking popular passwords

• Attackers will use for statistical guessing attacks
  – Against you
  – Against other sites

• Attackers will use for offline statistical guessing
  – Crack using only passwords in the popularity list
<table>
<thead>
<tr>
<th>Common passwords (sorted by popularity)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>password1,</td>
<td>100</td>
</tr>
<tr>
<td>password,</td>
<td>100</td>
</tr>
<tr>
<td>abc123,</td>
<td>100</td>
</tr>
<tr>
<td>asdf,</td>
<td>100</td>
</tr>
<tr>
<td>1234568,</td>
<td>100</td>
</tr>
<tr>
<td>p@ssword,</td>
<td>100</td>
</tr>
<tr>
<td>Iloveyou,</td>
<td>100</td>
</tr>
</tbody>
</table>
## Tracking popular passwords

<table>
<thead>
<tr>
<th>Common passwords (sorted by popularity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xCF832A834</td>
</tr>
<tr>
<td>0xC86A00386</td>
</tr>
<tr>
<td>0x0DB015528</td>
</tr>
<tr>
<td>0x5723B9291</td>
</tr>
<tr>
<td>0x24BF98902</td>
</tr>
<tr>
<td>0x23482AA83</td>
</tr>
<tr>
<td>0x1B200D481</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>0xA82C010D48</td>
</tr>
</tbody>
</table>
Dangers of tracking popular passwords

• Attackers will use for statistical guessing attacks
  – Against you
  – Against other sites

• Attackers will use for offline statistical guessing
  – Crack using only passwords in the popularity list
### How can we track popular passwords?

Crack popular password file (once for all accounts) to identify passwords to use against salted password file entries.

<table>
<thead>
<tr>
<th>Common passwords (sorted by popularity)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0xCF832A834</td>
<td>100</td>
</tr>
<tr>
<td>0xC86A00386</td>
<td>100</td>
</tr>
<tr>
<td>0x0DB015528</td>
<td>100</td>
</tr>
<tr>
<td>0x5723B9291</td>
<td>100</td>
</tr>
<tr>
<td>0x24BF98902</td>
<td>100</td>
</tr>
<tr>
<td>0x23482AA83</td>
<td>100</td>
</tr>
<tr>
<td>0x1B200D481</td>
<td>100</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>0xA82C010D48</td>
<td>1</td>
</tr>
</tbody>
</table>

**Salt free**
Dangers of tracking popular passwords

• Attackers will use for statistical guessing attacks
  – Against you
  – Against other sites

• Attackers will use for offline statistical guessing
  – Crack using only passwords in the popularity list
  – Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  – Filter candidate password list (with access to oracle)

These seem unavoidable
Requirements for popularity-tracking data structure

add($p$)

Adds the occurrence (use) of a password $p$

count($p$)

Returns # of times $p$ has been added

Need not be exact
count($p$) number of times $p$ added

a few false positives are OK
We’ll implement a probabilistic oracle

- False positives (falsely popular), no false negatives
- Count-min sketch
  - Relative of bloom filter (and counting bloom filter)
Base case (single table) of a count-min sketch

- $h_1$
  - 0x0000 to 0xFFFF
- $h_2$
  - 0x0000 to 0xFFFF
- $h_3$
  - 0x0000 to 0xFFFF
- $h_4$
  - 0x0000 to 0xFFFF
Count-min sketch: add("password")
Count-min sketch: $\text{count(“password”)}$

$\text{count(“password”)} = \min(1,1,1,1) = 1$
add(“ih8rules”)
Count-min sketch: \texttt{add(“password”)}

\texttt{count(“password”)} = \text{min}(2,2,2,2) = 2

Need not be incremented (conservative add)
Count-min sketch: add("password")

count("password") = 100 = MAX_ALLOWED
Dangers of tracking popular passwords

• Attackers will use for statistical guessing attacks
  – Against you
  – Against other sites

• Attackers will use for offline statistical guessing
  – Crack using only passwords in the popularity list
  – Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  – Filter candidate password list (with access to oracle)
False positives to the rescue!

• Randomly generated password $x$ likely to have $\text{count}(x) > 0$
Dangers of tracking user passwords

- Attackers will use for statistical guessing attacks
  - Against you
  - Against other sites

- Attackers will use for offline statistical guessing
  - Crack using only passwords in the popularity list
  - Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  - Filter candidate password list (with access to oracle)
False positives to the rescue, again!

• Assumptions
  – 2% false positive rate for count-min sketch
  – 20% of user password choices are too popular

• Implications
  – 9% of the passwords rejected as too popular were actually false positives

  – Dictionary of $2^{60}$ 10 char passwords, filtered to $2^{54}$
    (2% of $2^{60}$)

    If dictionary cracked, force all passwords to be changed.
Dangers of tracking popular passwords

• Attackers will use for statistical guessing attacks
  – Against you
  – Against other sites

• Attackers will use for offline statistical guessing
  – Walk the password list (if popularity list is plaintext)
  – Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  – Filter candidate password list (with access to oracle)
One last warning

Popular *strategies* can be dangerous even if passwords are unique
Unique passwords, dangerously popular strategies

• Passwords with derivative of username
  – “stuspassword”, “sutspassword”

• Passwords containing text that can be found on web search of user
  – http://binge.com/?q=stus popularityiseverything
You didn’t expect we’d believe this... did you?
I’m sorry dear, but if this represents the best presentation we’ll be capable of, even with millions of additional years to evolve, maybe it’s best that we not reproduce.