A Review of Real World Security Questions & Answers

By Bruce K. Marshall
@PwdRsch / PasswordResearch.com
A Brief History of Security Questions

- User created or site pre-selected questions that a user answers during registration and subsequently uses for authentication
- Typically used for backup authentication or for secondary authentication
- Designed to require a tradeoff between uniqueness and memorability
Security Answers Aren’t Necessarily Secrets

Robin @digininja
Group of 6 adults playing "things you don't know about me" very loud next to me. SE gold if I could be bothered
1:25 PM - 9 Jul 2013

Robin @digininja
They are now doing mothers maiden name and first pet name.
1:33 PM - 9 Jul 2013

Robin @digininja
Tempted to see if I can get them to talk about favourite teacher, first address and favourite colour. Think that would complete the set
1:42 PM - 9 Jul 2013
Maybe Your Info is Safe

28% of trusted acquaintances were able to correctly guess their partner's security question answers.

Forever Secure?
Security Question Case Studies

- **Alpha**: Business resource/networking site located in the USA (but had some int’l users)
  - 17,108 users with security questions/answers

- **Echo**: Gaming discussion forum site located in Europe (large international user base)
  - 789,452 users with security questions/answers

- **Sierra**: Teacher technology education site located in the Philippines (Filipino users only)
  - 1,036 users with security questions/answers
Site Registration Pages

**Alpha**
Create An Account

- Your Name
- Username
- Password
- Secret Question
- Answer To Secret Question
- Email
- Add account

**Echo**

- UserID
- Password
- Repeat Password
- E-Mail
- Repeat E-Mail

*The secret Q/A are used to recover your account if you forget your password*

- Secret Question
- Secret Answer

**Sierra**

- Security Question: Please Select Security Question
- Security Answer: *
EDIT SECURITY QUESTIONS

Select 3 Security Questions
You will be asked these questions in the future if you forget your password.

Select a question or enter your own question...

Question 1
Answer 1
Confirm Answer 1

Question 2
Answer 2
Confirm Answer 2

Question 3
Answer 3
Confirm Answer 3

Select a question or enter your own question...

What is your father's middle name?
What is your oldest cousin's first name?
What is your maternal grandmother's first name?
What is the first name of your first boss?
What is your mother's middle name?
What city was your mother born in?
What year was your mother born?
What year did you graduate from high school?
What street did you live on when you turned 10?
What is your first pet's name?
What elementary school did you attend?
What city did you attend your high school in?
Sierra’s Preset Security Questions

1. What is your pet's name?
2. What is the last name of your favorite teacher?
3. What is the title of your favorite book?
4. What is your oldest cousin's first and last name?
5. What is the name of the country of your ultimate dream vacation?

Facts

Opinions
Sierra Question Distribution

![Bar Chart]

- **Q1**: Green (Total), Blue (Men), Pink (Women)
- **Q2**: Green, Blue, Pink
- **Q3**: Green, Blue, Pink
- **Q4**: Green, Blue, Pink
- **Q5**: Green, Blue, Pink

Legend:
- **Total**
- **Men**
- **Women**
Sierra Security Answer Relevance

- Q1: Yes (90%), Partially (5%), No (1%)
- Q2: Yes (80%), Partially (20%), No (10%)
- Q3: Yes (70%), Partially (30%), No (5%)
- Q4: Yes (60%), Partially (40%), No (5%)
- Q5: Yes (50%), Partially (30%), No (10%)

Legend:
- Yellow: No
- Orange: Partially
- Blue: Yes
Sierra Security Answer Popularity

Q1: 14.2% Unique, 85.8% Duplicates
Q2: 9.7% Unique, 90.3% Duplicates
Q3: 32.3% Unique, 67.7% Duplicates
Q4: 100.0% Unique
Q5: 80.95% Unique, 19.1% Duplicates
Comparative Security Answer Lengths
### Answer Character Composition

<table>
<thead>
<tr>
<th></th>
<th>Alpha</th>
<th>Echo</th>
<th>Sierra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowercase</td>
<td>55.5%</td>
<td>Lowercase</td>
<td>Lowercase</td>
</tr>
<tr>
<td>Lower + Upper</td>
<td>20.6%</td>
<td>Lower + Symbol</td>
<td>Lower + Symbol</td>
</tr>
<tr>
<td>Lower + Symbol</td>
<td>6.5%</td>
<td>Number</td>
<td>Lower + Symbol</td>
</tr>
<tr>
<td>Number</td>
<td>4.4%</td>
<td>Lower + Upper</td>
<td>Lower + Upper</td>
</tr>
<tr>
<td>Lower + Upper + Symbol</td>
<td>4.1%</td>
<td>Lower + Number</td>
<td>Lower + Upper + Symbol</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Uppercase</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lowercase</td>
<td>67.8%</td>
<td>46.7%</td>
<td></td>
</tr>
<tr>
<td>Lower + Symbol</td>
<td>9.9%</td>
<td>17.2%</td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td>8.0%</td>
<td>15.4%</td>
<td></td>
</tr>
<tr>
<td>Lower + Upper</td>
<td>6.0%</td>
<td>14.1%</td>
<td></td>
</tr>
<tr>
<td>Lower + Number</td>
<td>2.24%</td>
<td></td>
<td>3.4%</td>
</tr>
</tbody>
</table>
User Data Matches

- Answer matches password: 9.08% (Alpha), 0.10% (Echo), 0.00% (Sierra)
- Answer matches email name: 0.10% (Alpha, Echo), 0.00% (Sierra)
- Answer matches username: 0.52% (Echo), 1.16% (Alpha)
- Answer matches question: 15.10% (Alpha), 2.08% (Echo)
- Question matches password: 1.81% (Alpha), 0.16% (Echo)
Security Question Suggestions

- Avoid user-generated security questions
- Use combinations of the better questions for authenticating individuals
- Mix with other security controls (e.g. email reset link, prompting for other account info, etc.), ideally risk-based
- Research and offer users alternatives to security questions
- Encourage use of password managers to reduce need to rely on reset mechanisms
Schneier on Security
A blog covering security and security technology.

February 11, 2005

The Curse of the Secret Question
It’s happened to all of us: We sign up for some online account, choose a difficult-to-remember and hard-to-guess password, and are then presented with a "secret question" to answer. Twenty years ago, there was just one secret question: "What’s your mother’s maiden name?" Today, there are more: "What street did you grow up on?" "What’s the name of your first pet?" "What’s your favorite color?" And so on.

... What can one do? My usual technique is to type a completely random answer -- I madly slap at my keyboard for a few seconds -- and then forget about it. This ensures that some attacker can’t bypass my password and try to guess the answer to my secret question, but is pretty unpleasant if I forget my password. The one time this happened to me, I had to call the company to get my password and question reset. (Honestly, I don’t remember how I authenticated myself to the customer service rep at the other end of the phone line.)

Providing additional security information
Before you can log on to the application for the first time, you must provide answers to five security questions. This multi-level security measure will help to ensure continued privacy of confidential information along with your user ID and password. To keep your account secure, a minimum of two up to a maximum of five of these questions may be asked when you attempt to log on to the system.

Pick a question from the five sets of questions to compile your set of security questions and answers. Choose questions which you can answer without difficulty.

**Important:** Do not make up a false answer to the question, as you might not be challenged to answer the question for a long period of time. This is why it is important that you choose questions to which you will always remember the answer.
Additional Research Ideas

- Is there a correlation between the strength of user security answers and their passwords?

- How well do wordlists for popular themes (cities, sports teams, pet names, etc.) match top entries for security answers?

- Are there predictable trends on question or answer selection based on gender/age?
References


For More Info

- Twitter: @PwdRsch
- Email: bkmarshall@passwordresearch.com
- Blog: http://blog.passwordresearch.com