# 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
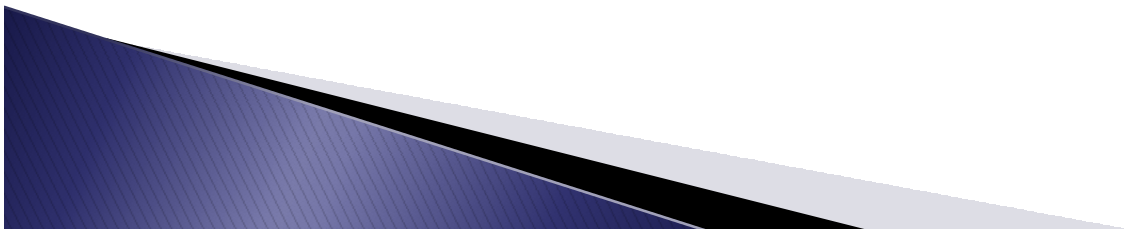
Security Answers Aren't Necessarily Secrets

Robin
@digininja
Follow

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
Follow

They are now doing mothers maiden name and first pet name.

1:33 PM - 9 Jul 2013

Robin
@digininja
Follow

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

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

Please enter a valid Email address or you will not be able to edit your account.

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: *

6

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?

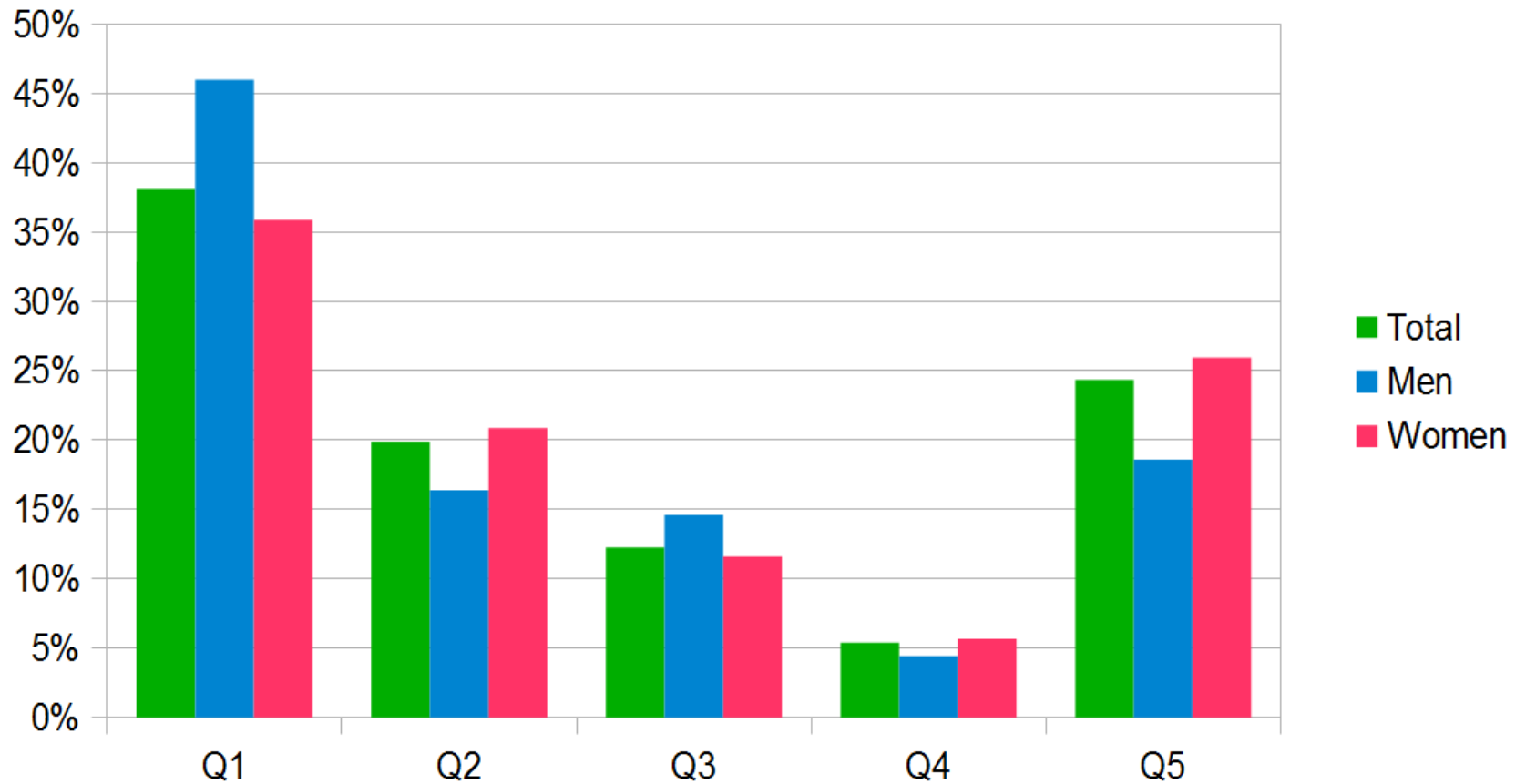5. What is the name of the country of your ultimate dream vacation?
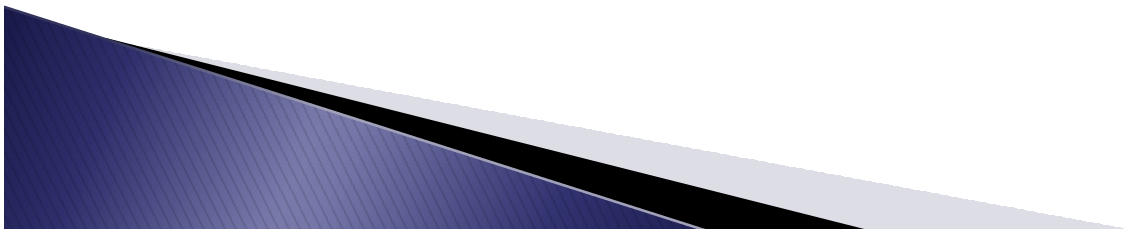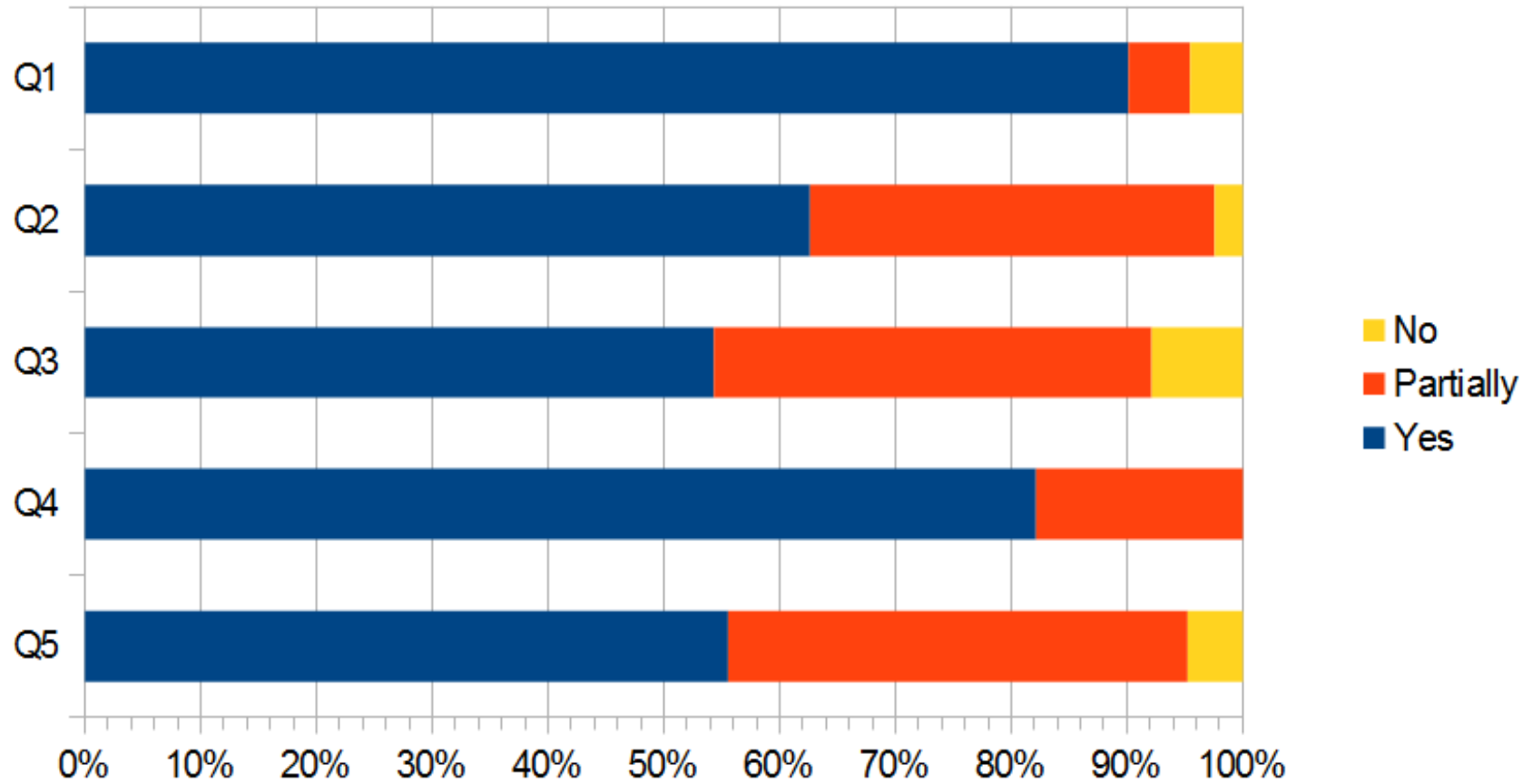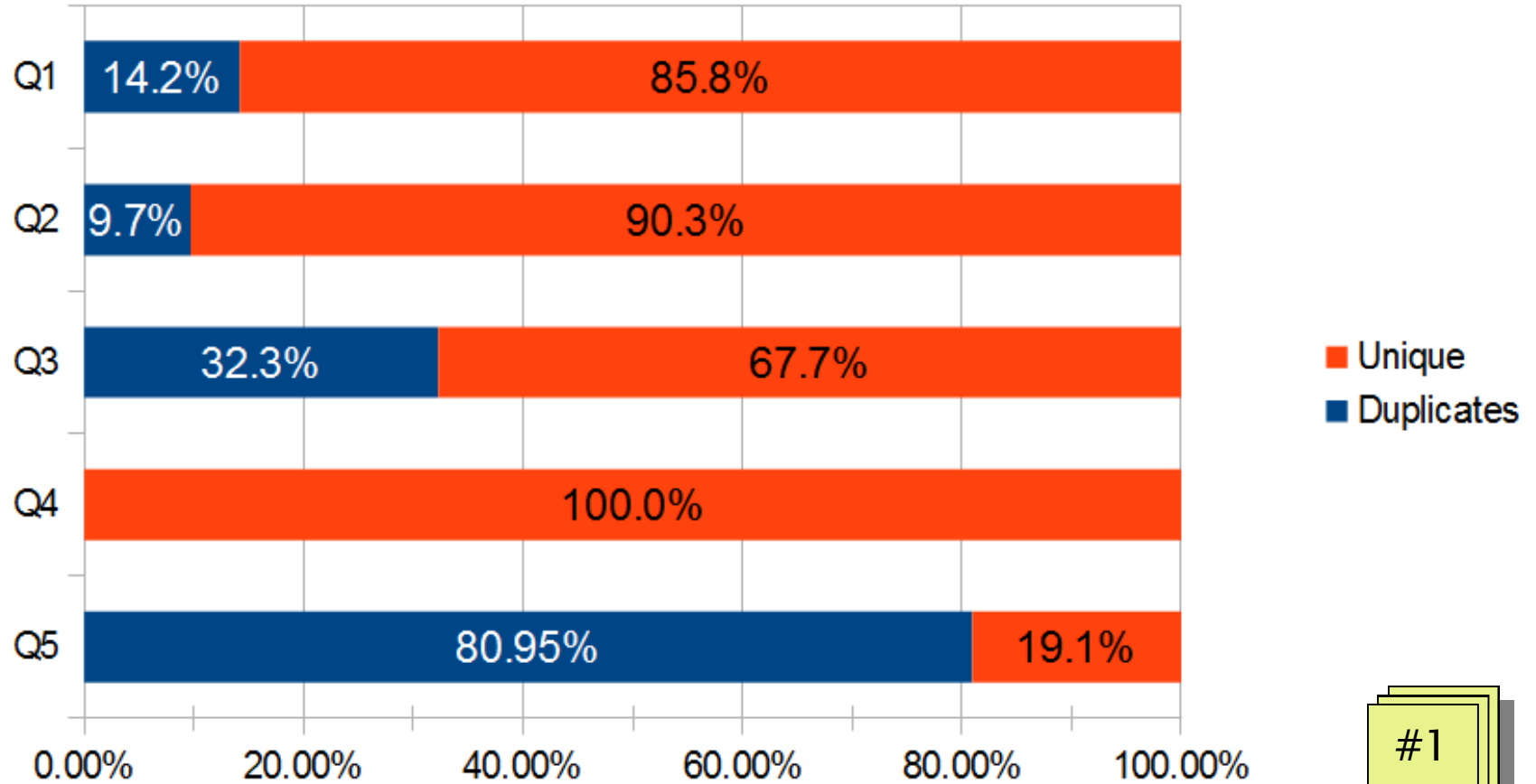
Facts   Opinions

#4

8

Sierra Question Distribution

Sierra Security Answer Relevance

Sierra Security Answer Popularity

Comparative Security Answer Lengths
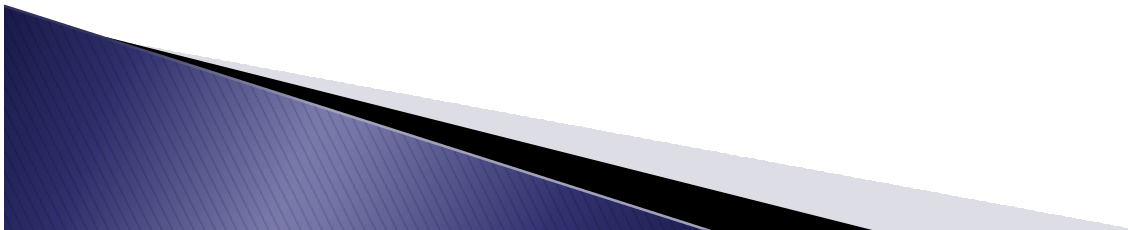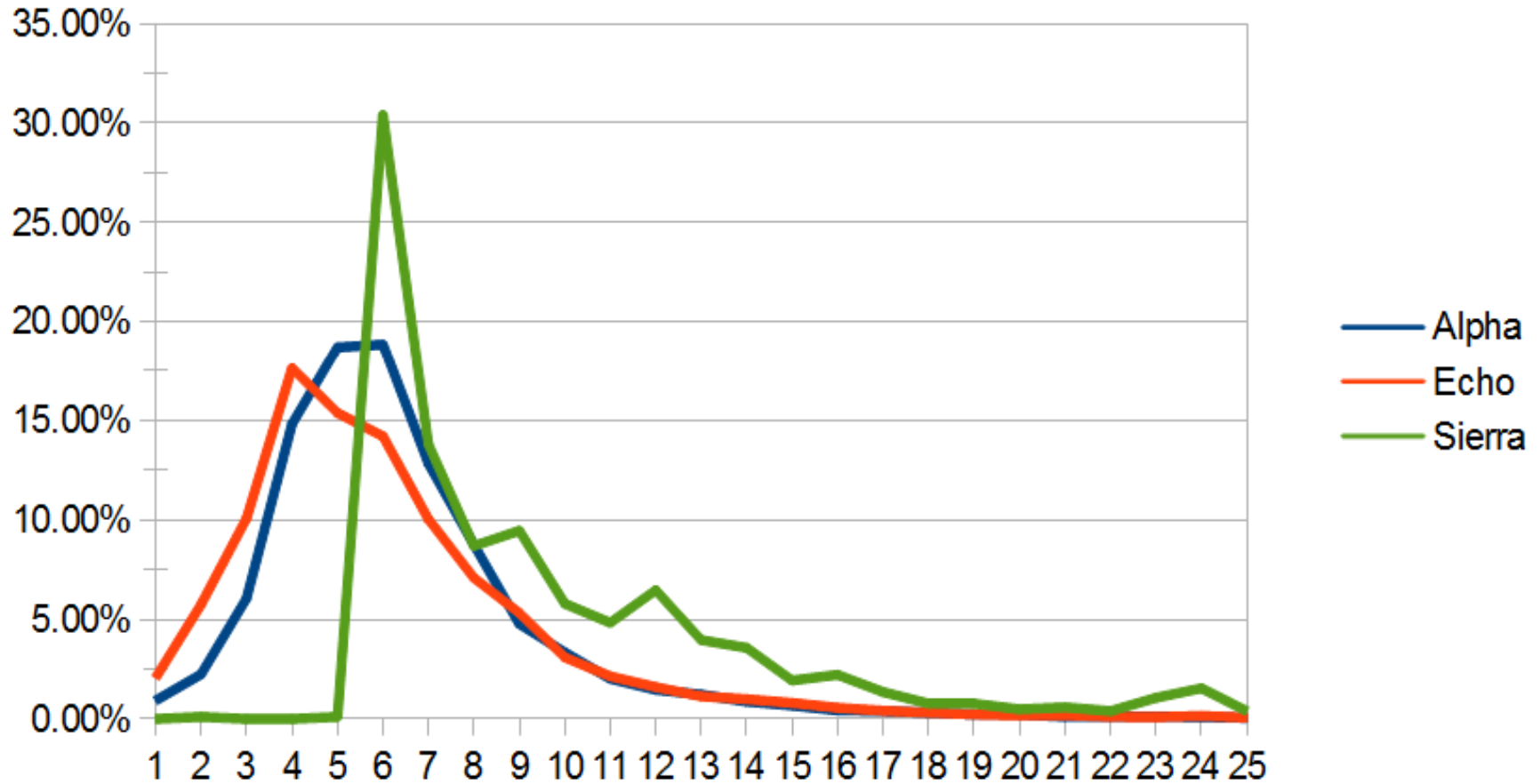
Answer Character Composition

Alpha			Echo			Sierra	
Lowercase	55.5%		Lowercase	67.8%		Lowercase	46.7%
Lower + Upper	20.6%		Lower + Symbol	9.9%		Lower + Symbol	17.2%
Lower + Symbol	6.5%		Number	8.0%		Lower + Upper	15.4%
Number	4.4%		Lower + Upper	6.0%		Lower + Upper + Symbol	14.1%
Lower + Upper + Symbol	4.1%		Lower + Number	2.24%		Uppercase	3.4%

User Data Matches
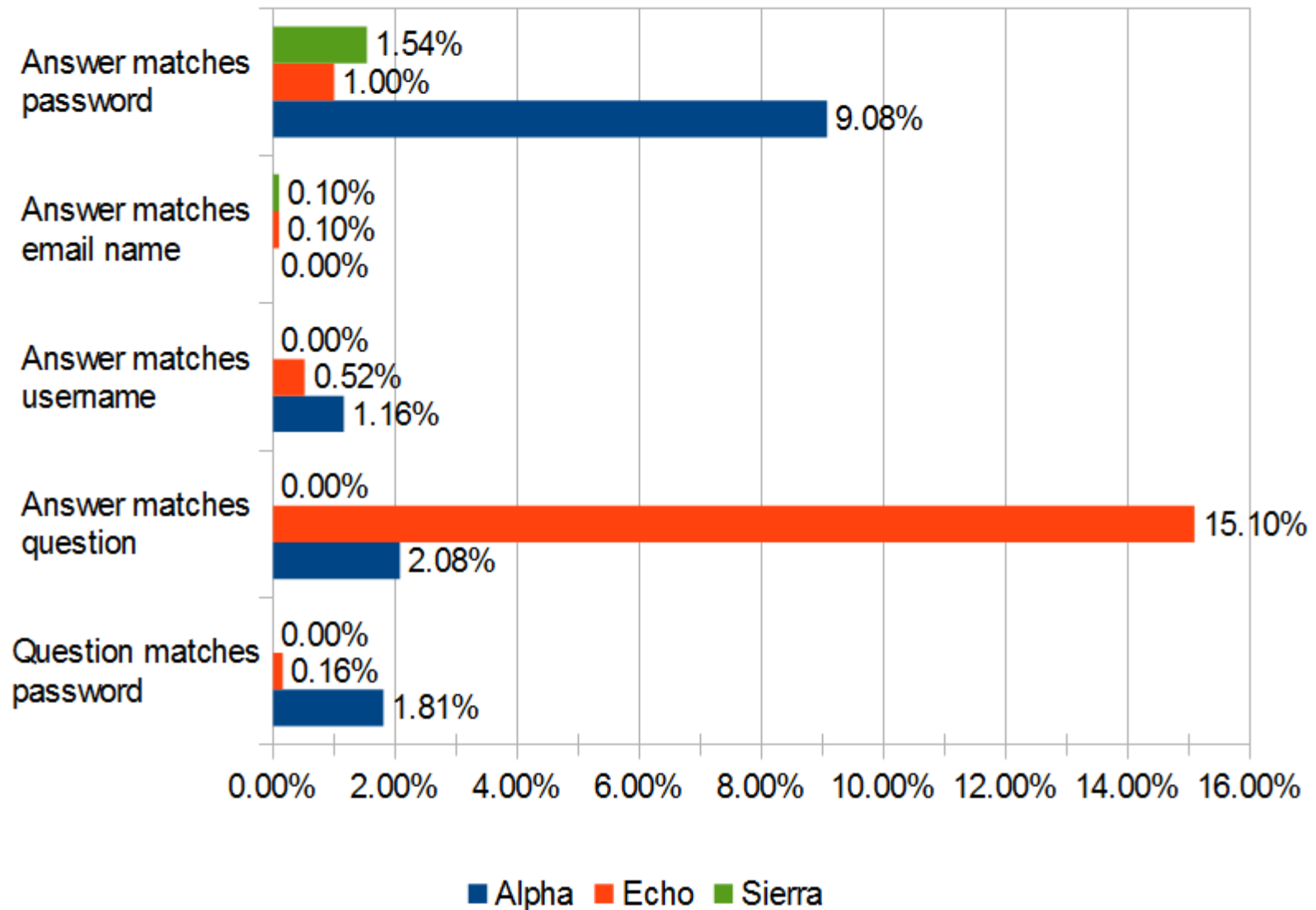
Security Question Suggestions

- 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
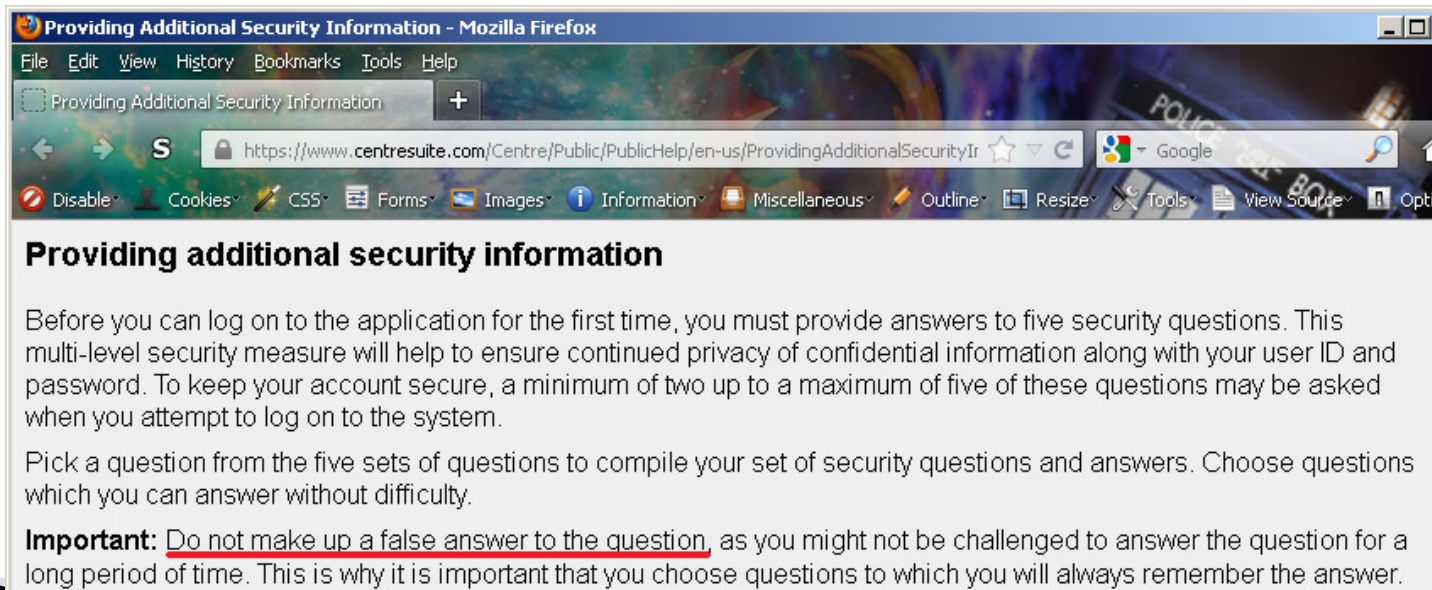
A blog covering security and security technology.

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 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Providing Additional Security Information   +

https://www.centresuite.com/Centre/Public/PublicHelp/en-us/ProvidingAdditionalSecurityIn   Google

Disable   Cookies   CSS   Forms   Images   Information   Miscellaneous   Outline   Resize   Tools   View Source   Opti

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.

16

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

1. Stuart Schechter, AJ Bernheim Brush, Serge Egelman, It's No Secret: Measuring the Security & Reliability of Authentication via 'Secret Questions', SOUPS 2009

2. Ariel Rabkin, Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook, SOUPS 2008

3. Michael Toomim, Xianhang Zhang, James Fogarty, James A. Landay, Access Control by Testing for Shared Knowledge, CHI 2008

4. William J. Haga & Moshe Zviran, Question-and-Answer Passwords: An Empirical Evaluation, Information Systems, Vol 16 No 3, 1991

For More Info

- Slides & Paper: http://bit.ly/secureq or http://www.passwordresearch.com/securityqs.html

- Twitter: @PwdRsch

- Email: bkmarshall@passwordresearch.com

- Blog: http://blog.passwordresearch.com