

CONTENT WARNING

The following presentation contains images of unclothed human organs.



Towards reliable storage of 56-bit secrets in *human* memory

My maiden name

MR. Jaeyeon Jung

Spouse of DR. Jaeyeon Jung

Joseph Bonneau
Princeton

~~Stuart Schechter~~
Microsoft Research

Your cruise director for today's excursion

A user-chosen secret can never be *provably* to be hard to guess

At best, we can show that user-chosen secrets are hard to guess using state-of-the-art methods and knowledge available to the defense

Sometimes, a really strong secret is actually worth some extra effort

LastPass ****



iCloud Keychain



1Password



A screenshot of a Windows password change interface. On the left is a grey silhouette of a person. To the right, the title "Change a password" is displayed. Below it are four input fields: "REDMOND\stus" (domain name), "Old password", "New password", and "Confirm password" with a blue arrow button. At the bottom, it says "Sign in to: REDMOND", "How do I sign in to another domain?", and "Sign-in options".



Humans are incapable of securely storing high-quality cryptographic keys... they are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.

Kaufman, Perlman and Speciner
Network Security: Private Communication in a Public World
2002

Why do computer scientists assume humans can't remember secrets?

(1) We start with familiar metaphors



(2) We explain problems using these metaphors



Computer Scientists recognize that writing to brains is harder than disks

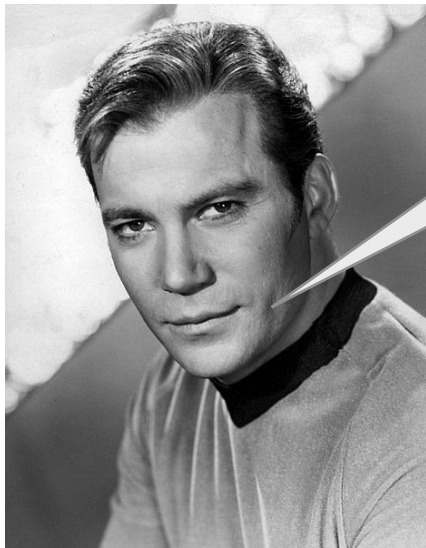
Creative commons attributed image to protect against copyright lawsuits...

http://en.wikipedia.org/wiki/File:Taille_depierre_2.jpg



...won't protect your speaker from a mouse's trademark lawsuit

(3) Our proposed solutions are constrained by these metaphors



Scotty, I need more power!

Captain, just a little more time!

These metaphors hide an important reality for human storage systems

Time + Power + Annoyance \neq Memorization



Your brain is designed to *forget*
random data it only sees only once.

These metaphors hide an important reality for human storage systems

Time + Power + Annoyance \neq *Single-Session* Memorization



Maybe this should be our metaphor
for human storage systems

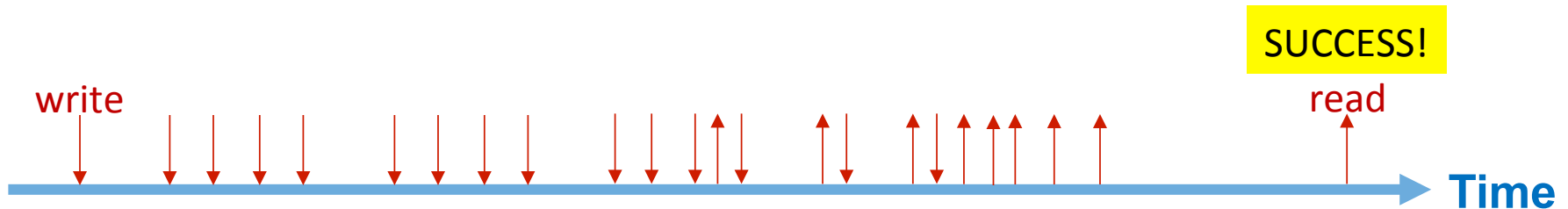


http://en.wikipedia.org/wiki/File:Wavecut_platform_southerndown_pano.jpg

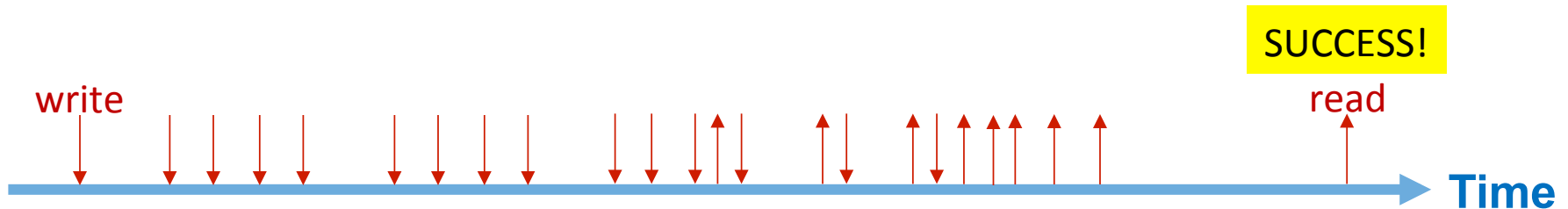
We've all learned through spaced repetition



Learning through spaced repetition (rehearsals)



How to learn passwords through spaced repetition?



How to learn passwords through spaced repetition?

Step 1: Sign-up (*no changes*)

at least 4 characters

User Name

at least 6 characters

Password

Repeat password

How to learn passwords through spaced repetition?

Step 2: Training during login

User Name

Password

How to learn passwords through spaced repetition?

Step 2: Training during login

stuart

User Name

(verifying)

●●●●●●

Password

How to learn passwords through spaced repetition?

Step 2: Training during login

User Name

(not yet correct)

Password

How to learn passwords through spaced repetition?

Step 2: Training during login

(verifying)

stuart

User Name

●●●●●●●●

Password

How to learn passwords through spaced repetition?

Step 2: Training during login

stuart
User Name

verified
●●●●●●●●
Password

first nurse
●●●●●●●●
Security code

How to learn passwords through spaced repetition?

Step 2: Training during login

stuart
User Name

verified
●●●●●●●●
Password

vnun
●●●●
Security code

How to learn passwords through spaced repetition?

Step 2: Training during login² (after login)

stuart
User Name

verified
●●●●●●●●
Password

vnun
●●●●
Security code

How to learn passwords through spaced repetition?

Step 2: Training during login³ (more logins)

stuart
User Name

verified
●●●●●●●●
Password

vnun
●●●●
Security code

How to learn passwords through spaced repetition?

Step 2: Training during login¹⁰

stuart

User Name

verified

●●●●●●●●

Password

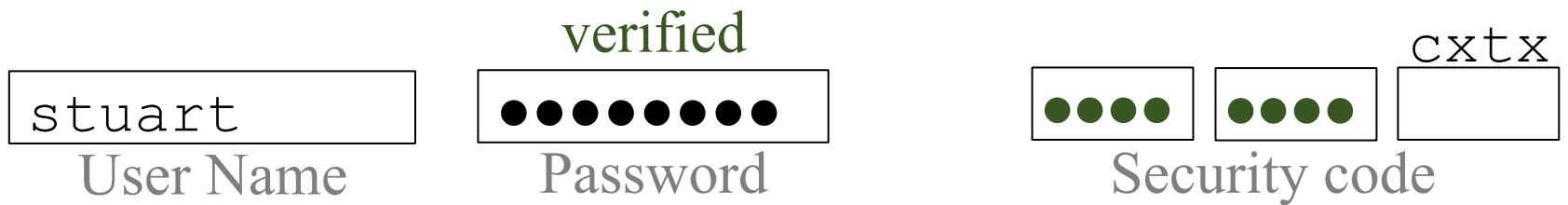
●●●●

Security code

Look, ma! No copying!

How to learn passwords through spaced repetition?

Step 2: Training during login³⁰



But will it work?

You are using the Mechanical Turk Developer Sandbox. This site is for test and development only. [Learn more >](#)

Your Account

HITS

Qualifications

330,637 HITS available now

Sign In

All HITS | HITS Available To You | HITS Assigned To You

Find HITS containing that pay at least \$ 0.00 for which you are qualified require Master Qualification GO

Timer: 00:00:00 of 15 minutes

Want to work on this HIT?

Accept HIT

Total Earned: Unavailable Total HITS Submitted: 0

60-Second Attention Game

Requester: Research Project

Reward: \$0.40 per HIT

HITS Available: 1

Duration: 15 minutes

Qualifications Required: Location is US

Microsoft Research Attention HIT

Instructions

Watch for a word to appear in one of the two boxes below.

If the word "left" appears in either box, type 'f'.

If the word "right" appears in either box, type 'j'.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.

Accept this HIT to begin	

Time remaining (seconds): 60	Total response time (ms): 0
Number of incorrect responses: 0	Penalty for incorrect responses (1000 each): 0
Number of correct responses: 0	Your score (total response time + penalty): 0

Microsoft Research Attention Study

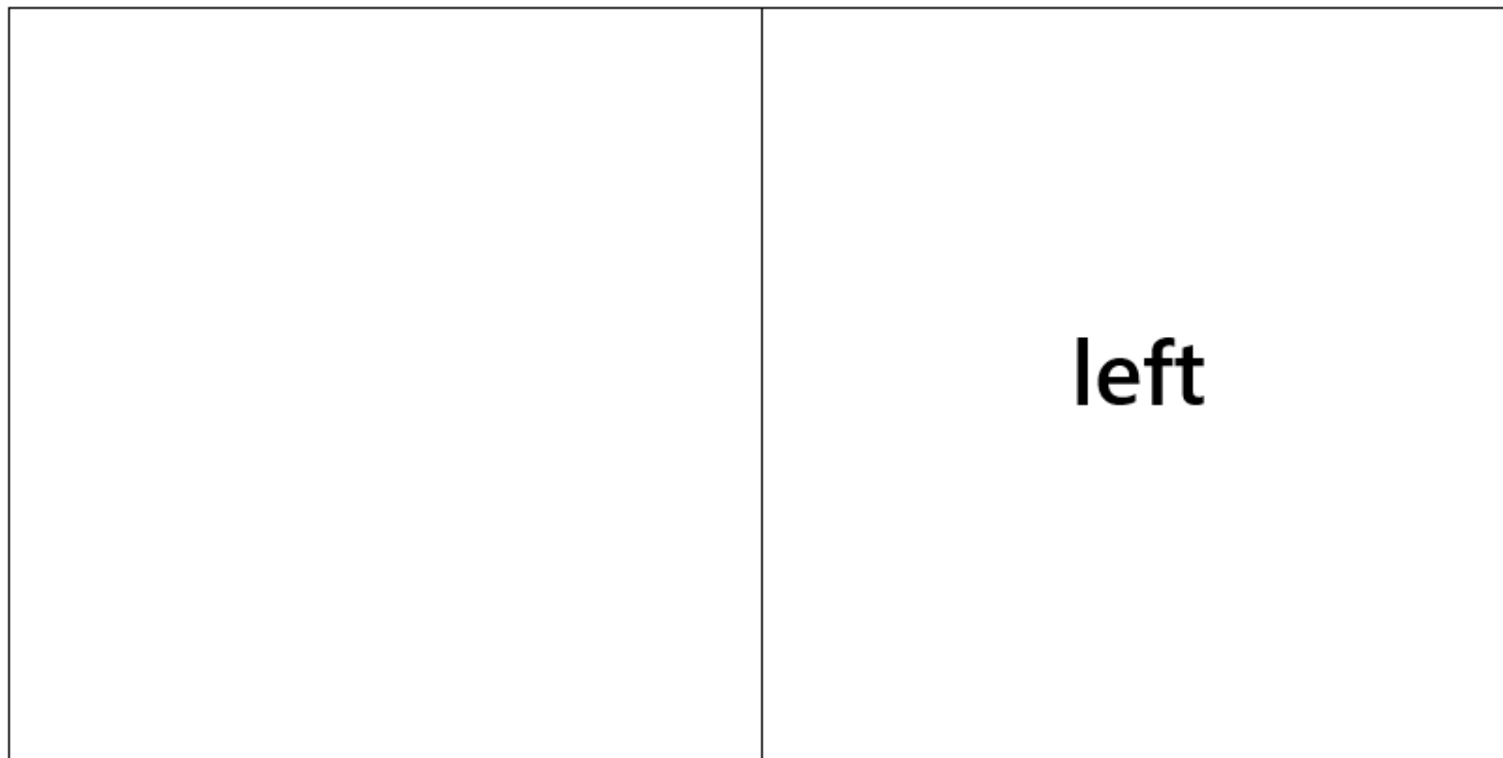
Instructions

Watch for a word to appear in one of the two boxes below.

If the word “left” appears in either box, type ‘f’.

If the word “right” appears in either box, type ‘j’.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.



left

Time remaining (seconds):	20	Total response time (ms):	4565
Number of incorrect responses:	0	Penalty for incorrect responses (1000 each):	0
Number of correct responses:	6	Your score (total response time + penalty):	4565

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Timer: 00:01:17 of 15 minutes

Finished with this HIT? Let someone else do it?

Submit HIT

Return HIT

Total Earned: \$73.04
Total HITs Submitted: 252

Automatically accept the next HIT

60-Second Attention Game

Requester: Research Project

Reward: \$0.40 per HIT

HITs Available: 1

Duration: 15 minutes

Qualifications Required: Location is US

Microsoft Research Attention HIT

Earn \$19 by being part of our extended study (optional)

If you are not interested in this offer, you may proceed to the next heading for instructions on receiving your payment immediately.

If you accept this offer, we will ask you to return to our experiment site for multiple sessions. Each of these sessions should take under three minutes. For each session, you will need to:

1. Login to the study site, which should take less than one minute.
2. Fill out a two-question 30-second survey asking when you last slept, and if you have consumed food, beverages, caffeine, or energy drinks.
3. Perform the same 60-second attention task you just completed.

After you complete each attention test, you will need to wait 30 minutes before starting your next session. You will have 15 days to complete 90 sessions. After the final attention task, we will also ask you to fill out a 10-minute completion survey.

If you complete all 90 sessions and the final survey, we will pay you \$19 in the form of a bonus attached to the HIT you just completed. That comes to \$0.20 per session, plus \$1 for completing the 10-minute survey after your final session. You will not be paid for individual sessions if you fail to complete the study.

To join the study, go to <https://experiment.research.microsoft.com/?workerId=A3A0N4OPTWRYPD>. The page inviting you to join the study will automatically open in a new tab. Do not right click to open a new tab, as it will prevent you from being paid for this HIT. Rather, the HIT in the current browser tab will disappear as we mark the HIT as complete so that you can receive your payment. As you go to the newly-opened tab to sign up for the study, be sure to bookmark the page, or email a copy of the web address (URL) to yourself, so as that you can find website during the study.

Get paid now for your participation in this short experiment

To get paid without joining the longer study, you need only [click here](#). The offer above will disappear.

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Finished with this HIT? Let someone else do it?

Submit HIT

Return HIT

Earn \$19 by being part of our extended study (optional)

If you are not interested in this offer, you may proceed to the next heading for instructions on receiving your payment immediately.

If you accept this offer, we will ask you to return to our experiment site for multiple sessions. Each of these sessions should take under three minutes. For each session, you will need to:

1. Login to the study site, which should take less than one minute.
2. Fill out a two-question 30-second survey asking when you last slept, and if you have consumed food, beverages, caffeine, or energy drinks.
3. Perform the same 60-second attention task you just completed.

After you complete each attention test, you will need to wait 30 minutes before starting your next session. You will have 15 days to complete 90 sessions. After the final attention task, we will also ask you to fill out a 10-minute completion survey.

If you complete all 90 sessions and the final survey, we will pay you \$19 in the form of a bonus attached to the HIT you just completed. That comes to \$0.20 per session, plus \$1 for completing the 10-minute survey after your final session. You will not be paid for individual sessions if you fail to complete the study.

To join the study, go to <https://experiment.research.microsoft.com/?workerId=A3A0N4OPTWRYPD>. The page inviting you to join the study will automatically open in a new tab. Do not right click to open a new tab, as it will prevent you from being paid for this HIT. Rather, the HIT in the current browser tab will disappear as we mark the HIT as complete so that you can receive your payment. As you go to the newly-opened tab to sign up for the study, be sure to bookmark the page, or email a copy of the web address (URL) to yourself, so as that you can find website during the study.

Get paid now for your participation in this short experiment

To get paid without joining the longer study, you need only [click here](#). The offer above will disappear.

Microsoft Research Attention Study

The following agreement governs your participation in this study.

PARTICIPATION AGREEMENT

YOUR AUTHORITY TO PARTICIPATE:

You represent that you have the full right and authority to sign this form, and if you are a minor that you have the consent (as indicated below) of your legal guardian to sign and acknowledge this form, and you will not disclose to Microsoft any non-public information, whether yours or a third party's without notifying Microsoft in advance. YOU ASSUME THE FULL RISK OF ANY INJURIES, DAMAGES, OR LOSSES YOU MAY SUSTAIN AS A RESULT OF YOUR PARTICIPATION IN THE PROJECT. IN ADDITION, YOU AGREE TO RELEASE AND HOLD HARMLESS MICROSOFT AND ITS AFFILIATES FROM ANY AND ALL CLAIMS THAT YOU MAY HAVE NOW OR IN THE FUTURE RELATED TO OR ARISING FROM YOUR PARTICIPATION IN THE RESEARCH PROJECT, AND YOU HEREBY WAIVE ALL SUCH CLAIMS. MICROSOFT WILL NOT BE LIABLE FOR ANY DAMAGES RELATED TO YOUR PARTICIPATION IN THE PROJECT.

INTRODUCTION:

Please note that you have no obligation to participate and you may decide to terminate your participation at any time. Also note that Microsoft has no obligation to disclose any research

Please choose a username and password.

A3A0N4OPTWRYPD

Worker ID

at least 4 characters

User Name

at least 6 characters

Password

Repeat Password

Sign up

Already part of the study? [Sign in](#)

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Microsoft Research Attention Study

How long has it been since you last slept for at least one hour without interruption?

Please indicate if you have consumed any of the following within the last 60 minutes:

- Food
- Beverages
- Caffeinated substances such as coffee or soft drinks
- Energy drinks other than caffeine

Finish

Show why Finish is disabled.

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Microsoft Research Attention Study

Instructions

Watch for a word to appear in one of the two boxes below.

If the word “left” appears in either box, type ‘f’.

If the word “right” appears in either box, type ‘j’.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.



left

Time remaining (seconds):	20	Total response time (ms):	4565
Number of incorrect responses:	0	Penalty for incorrect responses (1000 each):	0
Number of correct responses:	6	Your score (total response time + penalty):	4565

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Microsoft Research Attention Study

Instructions

Watch for a word to appear in one of the two boxes below.

If the word "left" appears in either box, type 'f'.

If the word "right" appears in either box, type 'j'.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.

You have now completed 6 of the 60 attention tests required by Tuesday February 4 at 08:47AM.

Time remaining until you may perform your next attention test:
29:52

Time remaining (seconds): 0

Total response time (ms): 12662

Number of incorrect responses: 0

Penalty for incorrect responses (1000 each): 0

Number of correct responses: 9

Your score (total response time + penalty): 12662

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Microsoft Research Attention Study

testaccount4 (not yet correct)
User Name Password

Not yet part of the study? [Sign up](#) only if you have been invited.

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

Microsoft Research Attention Study

<input type="text" value="testaccount2"/>	verified	<input type="text" value="vnun"/>
User Name	<input type="password" value="••••••"/>	Security Code

Due to concerns about stolen accounts and bonuses, we are giving you an additional security code. To finish logging in, simply type the four letters above the text box. Your code will not change, so once you have learned it, try to type it before the hint appears.

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

	$p=.2$ ↓ <i>Control</i>	$p=.4$ ↓ <i>Letters</i>	$p=.4$ ↓ <i>Words</i>	<i>Total</i>
Signed up for the 'attention' study	41	92	90	223

Four failed to learn the 2nd code

testaccount2

User Name

verified

●●●●●●●●

Password

vnun

□

Security Code

Due to concerns about stolen accounts and bonuses, we are giving you an additional security code. To finish logging in, simply type the four letters above the text box. Your code will not change, so once you have learned it, try to type it before the hint appears.

X

testaccount1

User Name

verified

●●●●●●●●

Password

●●●●●●●●

●●●●●●●●

Security Code

voice baker

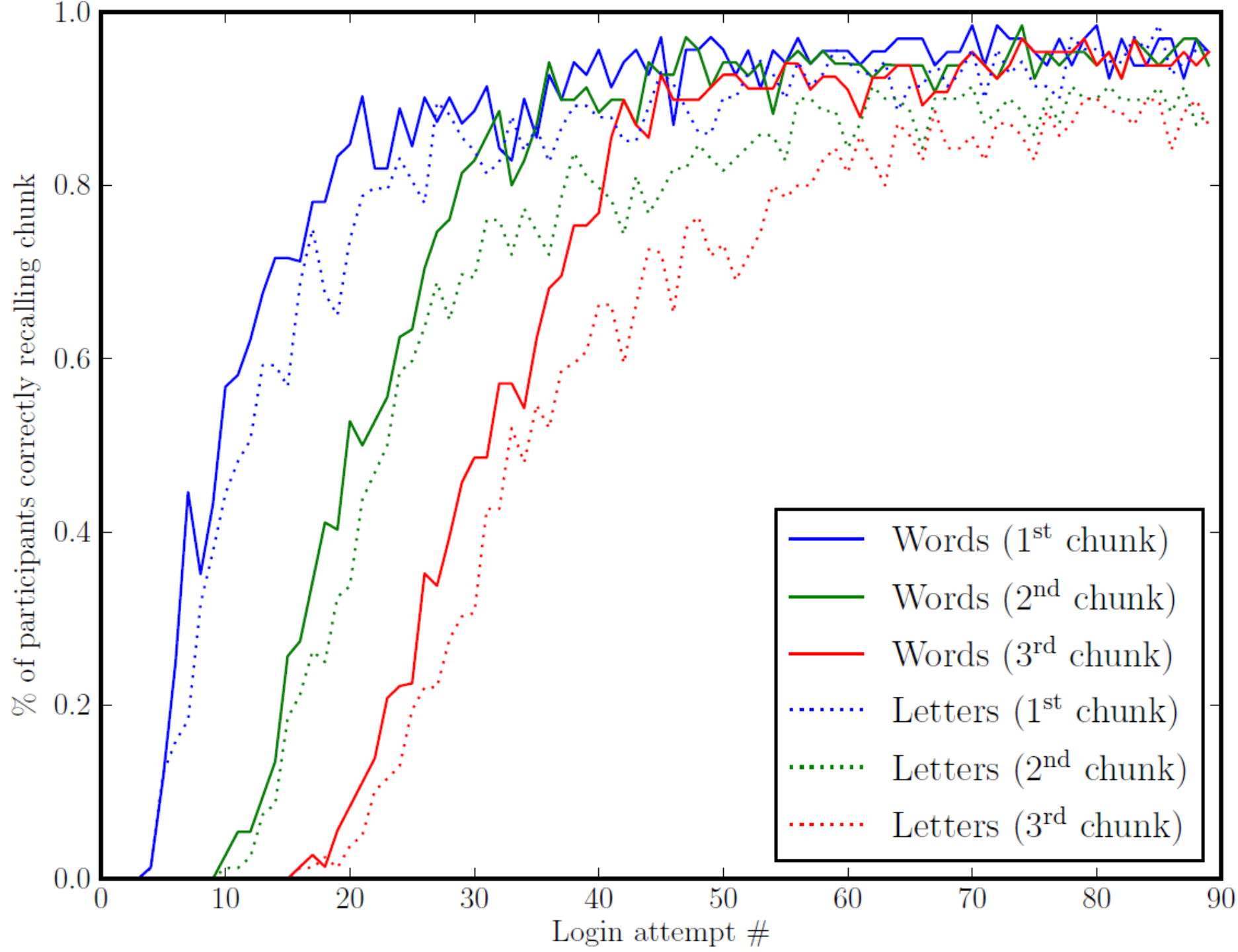
●●●●●● |

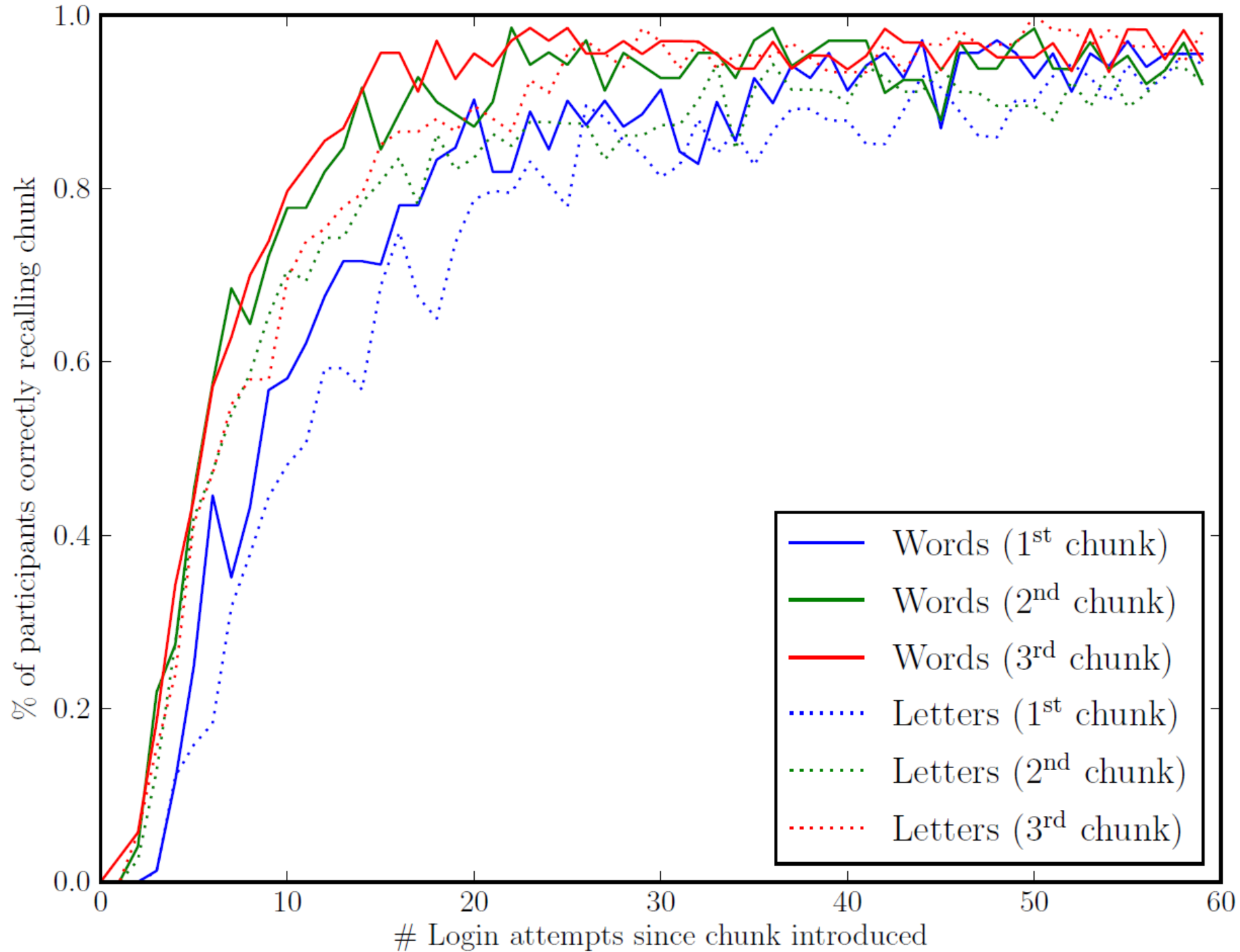
Congratulations! You have learned the first four words of your security code. We have added a final two words. These are the last two words we will ask you to learn. Once you have learned them, you can type them before the hint appears. Once you know the full code, we can use it to protect your account.

X

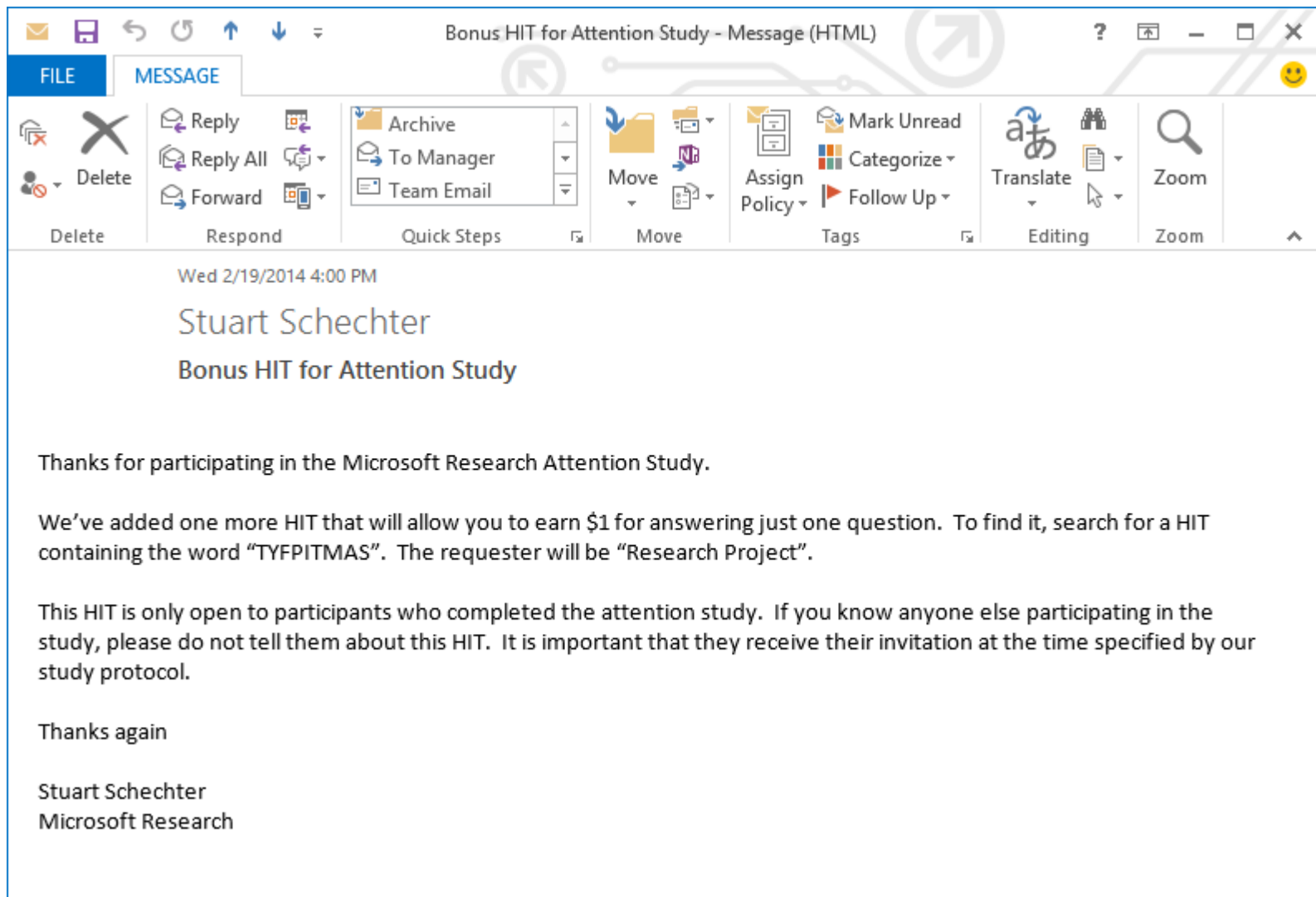
Congratulations! You have learned the first two words of your security code. We have added another two words. Just like the first two words, once you have learned them, you can type them without waiting for the hint to appear.

- “imagine my disappointment when I was rewarded for memorizing the first code by having another one added. I envisioned having code after code added to the end until infinity but I discovered that if I refused to play the game at all then the length of the code never grew more.”
- “it was kind of clear after learning the first pair that this would just result in a third pair and a fourth pair and ...
I have to admit that I was kind of pleased that it worked and I wasn't forced to learn more and more ... Hooray!”
- “I'd rather wait a few seconds and have a shorter code.”
- “Your system should have recorded that I NEVER NOT ONCE typed it in at all before the ``hint" appeared. I doubt my dog would feel like memorizing password just to be given more passwords to memorize. I mean are you serious? If there are people that fell for that please do not tell me as I would be very disappointed and fearful for the future of humanity. lol”





Three days after participants completed the attention study...



	<i>Control</i>		<i>Letters</i>		<i>Words</i>		<i>Total</i>	
Signed up for the ‘attention’ study	41		92		90		223	
<i>Quit after 2 or 3 games</i>	0/41	0%	9/92	10%	12/90	13%	21/223	9%
<i>Otherwise failed to finish</i>	6/41	15%	14/92	15%	12/90	13%	32/223	14%
Completed the ‘attention’ study	35/41	85%	69/92	75%	66/90	73%	170/223	76%
Received full security code	—		63/68	93%	64/65	98%	127/133	95%

	Did you store any part of the additional security code for the study website, such as by writing it down, emailing it to yourself, or adding it to a password manager?							
	‘Yes’				‘No’			
	<i>Letters</i>		<i>Words</i>		<i>Letters</i>		<i>Words</i>	
Completed the study	18/68	26%	10/65	15%	50/68	74%	55/65	85%
<i>Reported storing password</i>	11/18	61%	6/10	60%	2/50	4%	0/55	0%
Received full security code	16/18	89%	9/10	90%	47/50	94%	55/55	100%
Participated in follow-up	14/16	88%	8/9	89%	42/47	89%	48/55	87%
Recalled code correctly	12/14	86%	6/8	75%	34/42	81%	46/48	96%

In comparison to the previous presentation on Telepathwords

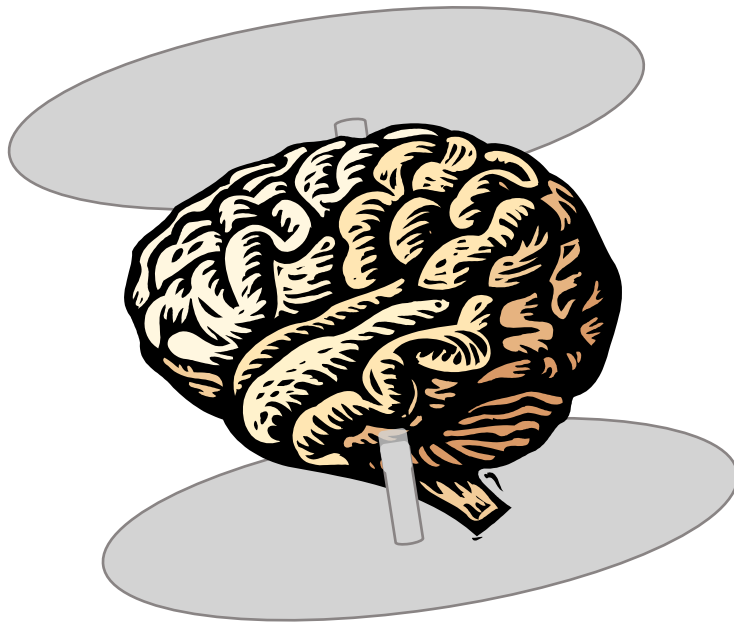
Recall rates maxed out at ~74%

(at least 26% forgot,
vs. 12% in our study)

However, recall rates decrease after 2+ weeks

- Words group: 62% recall rate
- Letters group: 56% recall rate

Summary



“It was surprising that you did this follow up, because I did not expect it.

After having to enter the codes so many times, **the words are branded into my brain.**”

Summary: Some passwords are worth 5-10 aggregate minutes of training

LastPass ****



iCloud Keychain



1Password



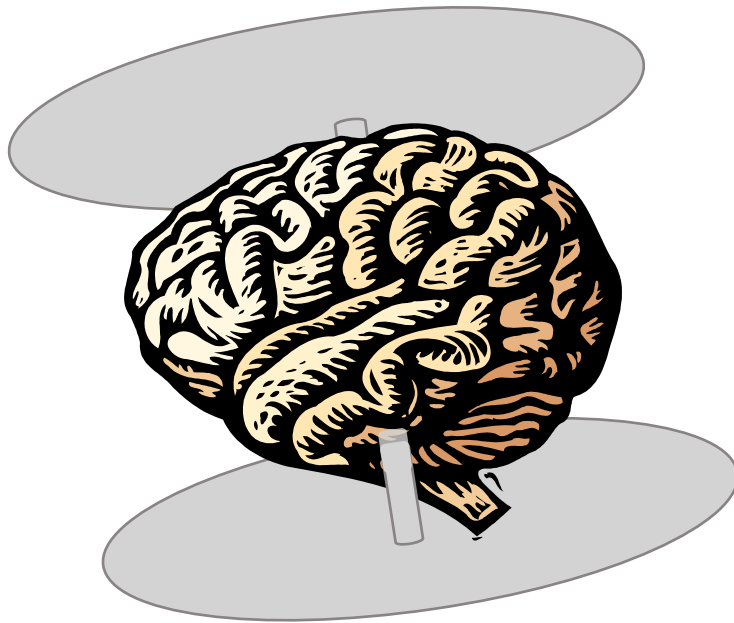
A screenshot of a Windows password change interface. The background is dark blue. On the left, there is a white back arrow icon and a white silhouette of a person's head and shoulders. To the right of the silhouette, the text "Change a password" is displayed in white. Below this, there are four input fields: "REDMOND\stus", "Old password", "New password", and "Confirm password". The "Confirm password" field has a white right-pointing arrow button. At the bottom, there is text: "Sign in to: REDMOND", "How do I sign in to another domain?", and "Sign-in options".

Acknowledgements

- Ross Anderson (Cambridge)
- Craig Agricola (IBM)
- Cristian Bravo-Lillo (CMU)
- Bill Bolosky (Microsoft Research)
- Arvind Narayanan (Princeton)

- The (somewhat) anonymous reviewers
(including the one who word-wraps to very short lines)

Questions?



“It was surprising that you did this follow up, because I did not expect it.

After having to enter the codes so many times, **the words are branded into my brain.**”

Some passwords are worth 5-10 aggregate minutes of training

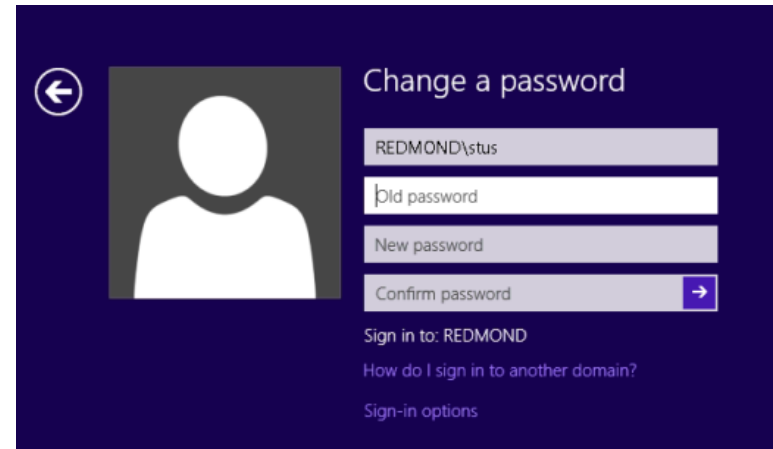
LastPass ****



iCloud Keychain



1Password

A screenshot of a Windows password change dialog box. The background is dark blue. On the left, there is a white back arrow icon and a white silhouette of a person's head and shoulders. To the right of the silhouette, the text "Change a password" is displayed. Below this, there are four input fields: "REDMOND\stus", "Old password", "New password", and "Confirm password". The "Confirm password" field has a blue arrow button to its right. At the bottom, there is text that reads "Sign in to: REDMOND", "How do I sign in to another domain?", and "Sign-in options".

Designing protocols for humans

- Training period
 - Authenticate via your chosen password
 - Learn random assigned password during each login
- High-security period
 - Authenticate via your assigned password

Experience the study for yourself

<https://experiment.research.microsoft.com/Demo.html>

You are using the Mechanical Turk Developer Sandbox. This site is for test and development only. [Learn more >](#)



Your Account

HITS

Qualifications

330,637 HITS available now

Sign In

All HITS | HITS Available To You | HITS Assigned To You

Find HITS containing that pay at least \$ 0.00 for which you are qualified require Master Qualification GO

Timer: 00:00:00 of 15 minutes

Want to work on this HIT?

Accept HIT

Total Earned: Unavailable
Total HITS Submitted: 0

60-Second Attention Game

Requester: Research Project

Reward: \$0.40 per HIT

HITS Available: 1

Duration: 15 minutes

Qualifications Required: Location is US

Microsoft Research Attention HIT

Instructions

Watch for a word to appear in one of the two boxes below.

If the word "left" appears in either box, type 'f'.

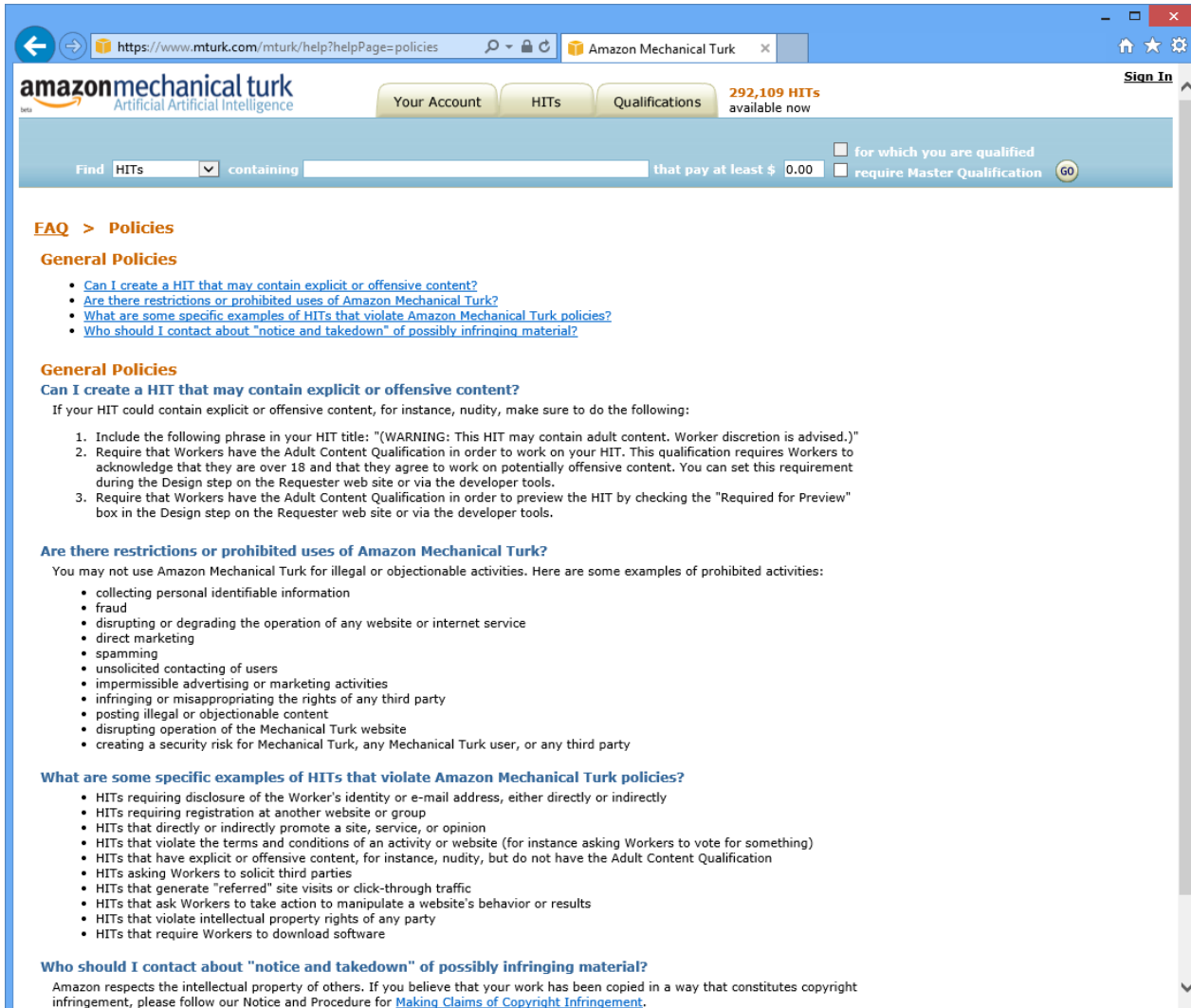
If the word "right" appears in either box, type 'j'.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.

Accept this HIT to begin	

Time remaining (seconds): 60	Total response time (ms): 0
Number of incorrect responses: 0	Penalty for incorrect responses (1000 each): 0
Number of correct responses: 0	Your score (total response time + penalty): 0

One problem



The screenshot shows a web browser window with the URL <https://www.mturk.com/mturk/help?helpPage=policies>. The page header includes the Amazon Mechanical Turk logo, navigation buttons for 'Your Account', 'HITs', and 'Qualifications', and a notification for '292,109 HITs available now'. A search bar is present with the text 'Find HITs containing' and a filter for 'that pay at least \$ 0.00'. The main content area is titled 'FAQ > Policies' and 'General Policies'. It contains several sections with links and text:

- General Policies**
 - [Can I create a HIT that may contain explicit or offensive content?](#)
 - [Are there restrictions or prohibited uses of Amazon Mechanical Turk?](#)
 - [What are some specific examples of HITs that violate Amazon Mechanical Turk policies?](#)
 - [Who should I contact about "notice and takedown" of possibly infringing material?](#)
- General Policies**
 - Can I create a HIT that may contain explicit or offensive content?**

If your HIT could contain explicit or offensive content, for instance, nudity, make sure to do the following:

 1. Include the following phrase in your HIT title: "(WARNING: This HIT may contain adult content. Worker discretion is advised.)"
 2. Require that Workers have the Adult Content Qualification in order to work on your HIT. This qualification requires Workers to acknowledge that they are over 18 and that they agree to work on potentially offensive content. You can set this requirement during the Design step on the Requester web site or via the developer tools.
 3. Require that Workers have the Adult Content Qualification in order to preview the HIT by checking the "Required for Preview" box in the Design step on the Requester web site or via the developer tools.
 - Are there restrictions or prohibited uses of Amazon Mechanical Turk?**

You may not use Amazon Mechanical Turk for illegal or objectionable activities. Here are some examples of prohibited activities:

 - collecting personal identifiable information
 - fraud
 - disrupting or degrading the operation of any website or internet service
 - direct marketing
 - spamming
 - unsolicited contacting of users
 - impermissible advertising or marketing activities
 - infringing or misappropriating the rights of any third party
 - posting illegal or objectionable content
 - disrupting operation of the Mechanical Turk website
 - creating a security risk for Mechanical Turk, any Mechanical Turk user, or any third party
 - What are some specific examples of HITs that violate Amazon Mechanical Turk policies?**
 - HITs requiring disclosure of the Worker's identity or e-mail address, either directly or indirectly
 - HITs requiring registration at another website or group
 - HITs that directly or indirectly promote a site, service, or opinion
 - HITs that violate the terms and conditions of an activity or website (for instance asking Workers to vote for something)
 - HITs that have explicit or offensive content, for instance, nudity, but do not have the Adult Content Qualification
 - HITs asking Workers to solicit third parties
 - HITs that generate "referred" site visits or click-through traffic
 - HITs that ask Workers to take action to manipulate a website's behavior or results
 - HITs that violate intellectual property rights of any party
 - HITs that require Workers to download software
 - Who should I contact about "notice and takedown" of possibly infringing material?**

Amazon respects the intellectual property of others. If you believe that your work has been copied in a way that constitutes copyright infringement, please follow our Notice and Procedure for [Making Claims of Copyright Infringement](#).

One problem

Are there restrictions or prohibited uses of Amazon Mechanical Turk?

You may not use Amazon Mechanical Turk for illegal or objectionable activities. Here are some examples of prohibited activities:

- collecting personal identifiable information
- fraud
- disrupting or degrading the operation of any website or internet service
- direct marketing
- spamming
- unsolicited contacting of users
- impermissible advertising or marketing activities
- infringing or misappropriating the rights of any third party
- posting illegal or objectionable content
- disrupting operation of the Mechanical Turk website
- creating a security risk for Mechanical Turk, any Mechanical Turk user, or any third party

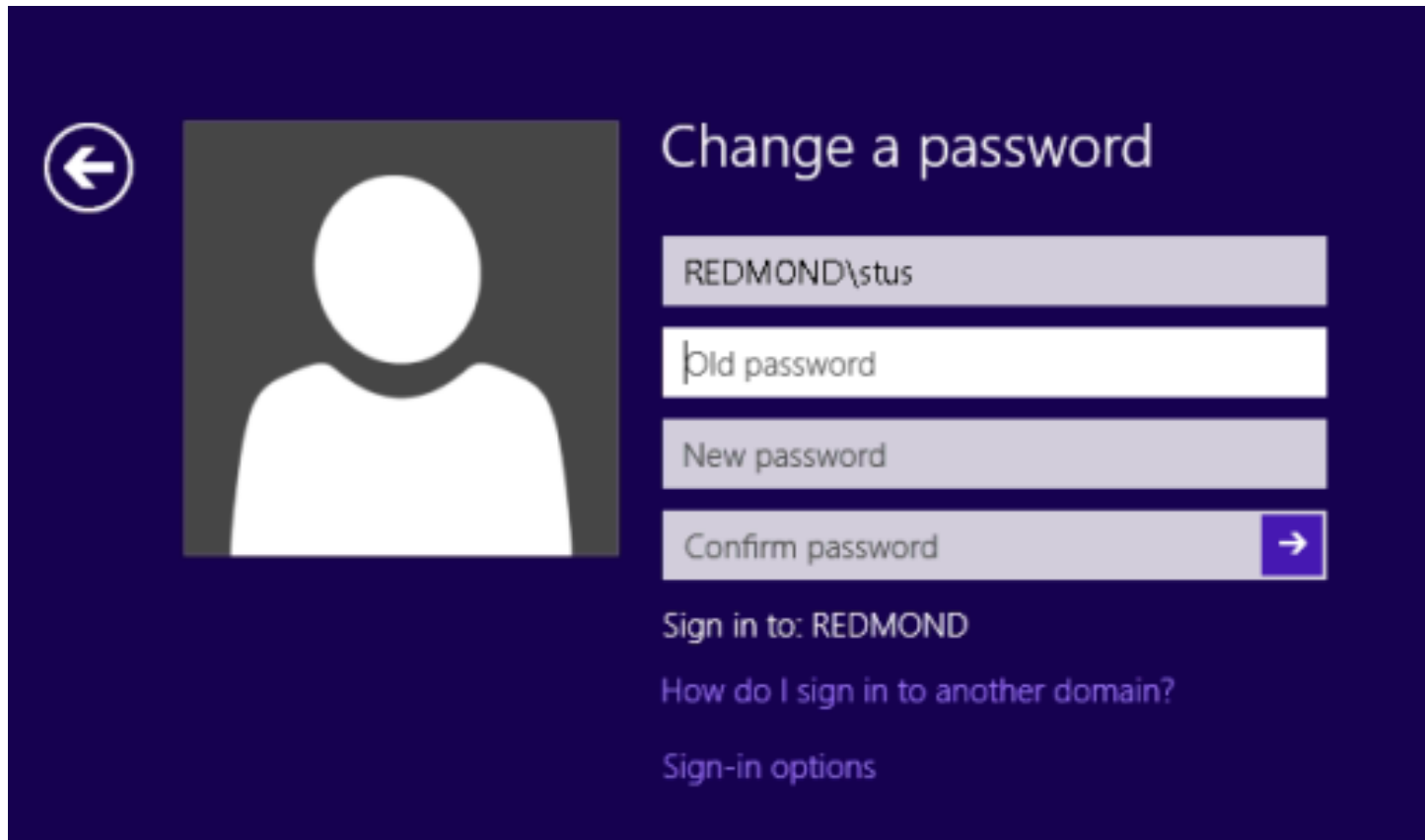
What are some specific examples of HITs that violate Amazon Mechanical Turk policies?

- HITs requiring disclosure of the Worker's identity or e-mail address, either directly or indirectly
- HITs requiring registration at another website or group

Some users choose bad secrets

- password
- qwerty
- p@ssword1
- princess
- monkey
- letmein
- opensesame
- abc123
- 12345678

Humans need to store secrets



A screenshot of a Windows password change dialog box. The background is dark blue. On the left, there is a white circular arrow icon pointing left, and a white silhouette of a person's head and shoulders. To the right of the silhouette, the text "Change a password" is displayed in white. Below this, there are four input fields: the first contains "REDMOND\stus", the second contains "Old password", the third contains "New password", and the fourth contains "Confirm password" with a white arrow icon pointing right. Below the input fields, the text "Sign in to: REDMOND" is displayed in white, followed by "How do I sign in to another domain?" and "Sign-in options" in a lighter blue color.

Change a password

REDMOND\stus

Old password

New password

Confirm password →

Sign in to: REDMOND

[How do I sign in to another domain?](#)

[Sign-in options](#)