

**National Institute of Standards and Technology (NIST)  
Information Technology Laboratory (ITL)  
Computer Security Division (CSD)  
Password Generation Study Post-Task Questionnaire**

***About the Password Generation Study***

**1. How would you rate the experience of generating passwords to satisfy the password requirements?**

a. “password requirement set 1”

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

b. “password requirement set 2”

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

**2. How would you rate the strength (i.e., in protecting the account) of the password requirements?**

a. “password requirement set 1”

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

b. “password requirement set 2”

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

**3. For the password you selected for “account type 1,” please rate:**

a. The strength (i.e., in protecting the account) of the password

1 Very Weak	2 Weak	3 Neutral	4 Strong	5 Very Strong
----------------	-----------	--------------	-------------	------------------

b. The ease of remembering the password

1 Very Difficult	2 Difficult	3 Neutral	4 Easy	5 Very Easy
---------------------	----------------	--------------	-----------	----------------

c. The ease of typing the password

1 Very Difficult	2 Difficult	3 Neutral	4 Easy	5 Very Easy
---------------------	----------------	--------------	-----------	----------------

**4. For the password you selected for “account type 2,” please rate:**

a. The strength (i.e., in protecting the account) of the password

1 Very Weak	2 Weak	3 Neutral	4 Strong	5 Very Strong
----------------	-----------	--------------	-------------	------------------

b. The ease of remembering the password

1 Very Difficult	2 Difficult	3 Neutral	4 Easy	5 Very Easy
---------------------	----------------	--------------	-----------	----------------

c. The ease of typing the password

1 Very Difficult	2 Difficult	3 Neutral	4 Easy	5 Very Easy
---------------------	----------------	--------------	-----------	----------------

**5. For the password you selected for “account type 3,” please rate:**

a. The strength (i.e., in protecting the account) of the password

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

b. The ease of remembering the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

c. The ease of typing the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

**6. For the password you selected for “account type 4,” please rate:**

a. The strength (i.e., in protecting the account) of the password

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

b. The ease of remembering the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

c. The ease of typing the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

**7. For the password you selected for a desktop computer, please rate:**

a. The strength (i.e., in protecting the account) of the password

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

b. The ease of remembering the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

c. The ease of typing the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

**8. For the password you selected for a mobile computing device, please rate:**

a. The strength (i.e., in protecting the account) of the password

1	2	3	4	5
Very Weak	Weak	Neutral	Strong	Very Strong

b. The ease of remembering the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

c. The ease of typing the password

1	2	3	4	5
Very Difficult	Difficult	Neutral	Easy	Very Easy

9. What, if any strategies, did you use to generate the passwords in this study?

---

***About yourself and your experience with passwords***

**1. Gender:**

- Male
- Female

**2. Age:** \_\_\_\_\_ (in years)

**3. Highest education (degree/level attained):**

- High school or equivalent
- Associate degree
- Bachelor’s degree
- Master’s degree (e.g. MS, MA, etc.)
- Doctoral degree (e.g. PhD)
- Professional degree (e.g. MD, JD, etc.)
- (Other), please specify \_\_\_\_\_

**4. Occupation:** \_\_\_\_\_

**5. Your level of experience using computers:**

- Novice
- Average
- Advanced
- Expert

**6. Do you have **personal accounts** in the categories listed below that require a **password**? If yes, enter the number of accounts in that category and select how often you use those accounts.**

	Number of accounts	Several times a day	About once a day	Several times a week	About once a week	Several times a month	Several times a year
Email		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personal computers requiring passwords		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile devices requiring passwords (e.g., smartphones, tablets)		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social Networks (e.g., Facebook, MySpace, Twitter)		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online Chat/Instant Messaging		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Banking online		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Bill payment online		0	0	0	0	0	0
Shopping online		0	0	0	0	0	0
Financial management online (e.g. investment, 401K)		0	0	0	0	0	0
Healthcare management online (e.g. health insurance, Medicare)		0	0	0	0	0	0
Classifieds/auctions online (e.g. Craigslist, ebay)		0	0	0	0	0	0
Entertainment online (e.g. music, videos/movies)		0	0	0	0	0	0
Games online		0	0	0	0	0	0
News online		0	0	0	0	0	0

If you have other personal accounts not listed above, please describe the nature of the account(s): \_\_\_\_\_

7. How often do you use the **same password** for **different personal accounts**?

- Never or almost never
- Less than half of the time
- About half of the time
- More than half of the time
- Always or almost always

8. Tell us about any overall **strategy** you use to manage your passwords for **different personal accounts**.

(An example of such strategy is to have 3 passwords with different security levels: a strong password for accounts with great importance to you; a medium-strength password for less important accounts; and a low-strength password for accounts that are more casual.)

---

9. What **strategies** do you use to create the passwords of your **personal accounts**? (check all that apply)

- Create from a password root, where a few characters are always the same (e.g., 2PwDRt&, PwDRt42%, or tXpwdRT@)
- Let system assign password
- Make minor change(s) to an existing password (e.g., %elvis1, #elvis2, or \$elvis3)
- Recycle old passwords (e.g., old passwords that are not in current password history)
- Use a common name, word, or phrase (e.g., Boston12)
- Use a meaningful or pronounceable mnemonic (e.g., 2beOrnOt@toBee from “to be or not to be”)

- Use a random combination of words, letters, or characters
- Use character repetitions (e.g. !!!AAAbbb999)
- Use existing passwords from other accounts
- Other –describe strategies generically. Do **not** provide an example of an actual password or enough information to guess your password. \_\_\_\_\_

10. How **important** are these **considerations** to you when you create the password of a **personal email account**?

	Not at all Important	Only a little Important	Somewhat Important	Very Important
Easy to enter/type	0	0	0	0
Easy to remember	0	0	0	0
Strong, i.e., hard to guess/crack	0	0	0	0
Synchronized with passwords for other accounts	0	0	0	0
Compliant with the password requirements	0	0	0	0

11. How do you **keep track** of the passwords of your **personal accounts**? (check all that apply)

- Memorize the passwords
- Let browser/computer auto-fill
- Use mnemonics, e.g. meaningful or pronounceable phrase
- Rely on hints provided by the computer
- Do not track, use “forgot password” feature
- Share with someone (e.g., a family member or friend)
- Write entire password down on paper and place in a non-locked location
- Write entire password down on paper and store securely in a locked location
- Write down on paper, but disguise in some way (e.g. only write down the common word without the special characters)
- Save in a document/file, protected with encryption or password
- Save in a document/file, not protected (i.e. without encryption or password)
- Use password management software
- Store in unencrypted electronic devices, e.g., USB key, PDA, cell phone, etc.
- Store in encrypted electronic devices, e.g. BlackBerry
- Other – please describe \_\_\_\_\_

12. In the past **6 months**, how much **frustration** have these **problems** with your personal accounts caused you?

	None	A little	Some	A lot
Forgetting your User name or ID	0	0	0	0
Forgetting your password	0	0	0	0
Forgetting your PIN	0	0	0	0
Forgetting which password goes with which account	0	0	0	0
Getting locked out of an account	0	0	0	0
Mistyping a password	0	0	0	0
Getting error messages when trying to change a password	0	0	0	0
Getting error messages when trying to recover a password	0	0	0	0
Dealing with slow or unhelpful system support	0	0	0	0
Valid password rejected for unclear reason	0	0	0	0
Other, please describe below	0	0	0	0

If "Other", describe problem(s): \_\_\_\_\_

13. In your opinion, how many characters long should personal account **passwords** be? Please give a whole number. \_\_\_\_\_

14. How do you feel about the **amount of effort** it takes you to **create and manage passwords** to do what you want to do online?

\_\_\_\_\_

**NOTE:** This survey contains collection of information requirements subject to the Paperwork Reduction Act. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB control number. The estimated response time for this survey is **25** minutes. The response time includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information." Send Comments regarding this estimate or any other aspects of this collection of information, including suggestions for reducing the length of this questionnaire, to the National Institute of Standards and Technology, Attn., Mary Theofanos, at [mary.theofanos@nist.gov](mailto:mary.theofanos@nist.gov)

**OMB Control No. 0693-0043 Expiration Date: 3/31/2016**