**Week 3 Lab: Hands-on Password Practice**

Please read through the entire lab before you begin, so that you understand what will be expected of you. Then download and fill out the worksheet template file

W03 Hands-on Password Lab Worksheet.dotx

as you work. When you finish, save your worksheet and submit it as instructed.

## Tasks

1. Learn to create strong passwords
2. Identify sites that can help verify you have a strong password
3. Learn to use a password generator
4. Install and use a password manager
5. Teach strong password skills to someone else

## Overview

Right now, login names with secret passwords are the most prevalent tool used for authentication. Maybe someday there will be better technologies that everyone will use to verify identities, but currently, every Internet user currently needs to create and use passwords for various purposes. This lab will help you learn characteristics of strong passwords. You will:

* review patterns that could make a password weak or strong,
* try creating a password that will be easy for you to remember but hard for someone else to guess,
* test your new password, to estimate how long it might take to “crack” it,
* try using a password generator, to create a truly random password,
* test your random password to see how its strength compares to your first password,
* install and learn to use password manager software,
* share what you have learned with others (family or friends) and help them to create their own stronger passwords.

## Task 1: Learn to create strong passwords

There is a good psychological reason why many people use weak passwords: they don’t want to spend their brain power remembering a complex password, because they have better or more important tasks occupying their mind. Unfortunately, adversaries take advantage of such mental inertia when they try to crack passwords. They don’t need to exhaustively guess every possible password; instead, they will try guessing short passwords, common words found in dictionaries, and simple keystroke patterns.

That is the reason why better passwords are longer, have character sequences that don’t match dictionary terms, and do not follow facile patterns. Some systems enforce variety in a password’s keystrokes by requiring combinations of uppercase, lowercase, numerals, or punctuation symbols.

Watch these two videos, and then answer the questions below.

* Consumer Reports, How to Create Strong Passwords. <https://youtu.be/ZL6446ShQ08> (about 4 minutes.)
* First American, Strong Passwords. <https://youtu.be/9LxdtaSvQ3I> (almost 2 minutes.)
* After you become accustomed to a password, it can be annoying to change it and get used to a new password. But there are good reasons for not sticking with the same password for too long. Why should you change your password periodically? Think of and write at least one reason.
* For each of the following passphrases, pass judgment: is it weak or strong?
  1. MyCatLovesMe
  2. myc@t\_lovesme
  3. MyC@t\_L0v3sM3!
  4. Mycatlovesme
* Support your judgments: what is it about each that makes it weak or strong?
* What do you believe are the most important steps you can take to ensure you are using a secure password?

Complete the Task 1 section of the lab worksheet template.

## Task 2: Identify sites that can help verify you have a strong password.

Some web sites have tools that can be used to verify the strength of a password, or to estimate how long it might take for an adversary to crack a password. These online tools usually express the strength of the password using either measurements of complexity or measurements of time (how long the password might be cracked by a hacker). Let’s look at both kinds.

Password strength tests:

* Experiment with the following two web pages:
  1. Password strength test, University of Illinois at Chicago. <https://www.uic.edu/apps/strong-password/>
  2. The Password Meter. <http://www.passwordmeter.com/>

Review the password requirements (they are listed toward the right side on both of those web pages), then create a new password that satisfies those requirements. Type your password into your worksheet. **You will use this password for this lab only!** (Since you must share this password in the document you will submit, make sure to pick one that you have never used before and do not plan to use in the future).

* Enter your new password in the password field of each of the web pages listed above. Observe the complexity level on each. Capture a screen image of each web page’s complexity result. (Do they match?)
* Next, visit this web site:

Dashlane, How Secure Is My Password? <https://howsecureismypassword.net/>

Type or paste your new password on that web site. How long does it estimate it would take to crack it? Capture a screen image of this result.

* Insert or paste your screenshots in your worksheet.

Complete the Task 2 section of the lab worksheet template.

## Tasks 3: Learn to use a password generator

Another useful tool is a password generator. Security practitioners use password generators to automate the creation of random password strings that meet strict complexity requirements. Such strong random passwords are useful to authenticate very sensitive access controls, such as administrator privileges on a server, or secure communication keys between network devices.

Password Generator:

* Visit this web site: Secure Password Generator, <https://passwordsgenerator.net/>

Observe the default settings. Note that the standard password length is set to sixteen characters. Without changing any settings, generate a new random password and copy it to your lab worksheet template.

* How might this password be better than the one you created for Task 2? How might this random password be worse?
* Copy the generated random password. Revisit the “How Secure Is My Password?” site, <https://howsecureismypassword.net/> , and paste the random password in that site. How long does it estimate it would take to crack it? Capture a screen image of your result.
* Insert or paste your screenshot in your worksheet.

Complete the Task 3 section of the lab worksheet template.

## Task 4: Install and use a password manager

Security practitioners caution against re-use of the same password on multiple authentication systems. (For example, don’t use the same password for your online banking that you use for your school account.) Long passphrases and randomly generated passwords are stronger and more difficult to crack, but memorizing dozens of different passwords for various applications and web sites is too much of a burden. A password manager can solve this problem, if it is used correctly and wisely.

Password manager software:

* Watch at least one of the following videos (your choice):
  + Archer News Network, What is a password manager? <https://youtu.be/y4Ak2SXwVLo> (about 3 minutes)
  + Trend Micro, Why Use a Password Manager? <https://youtu.be/0Ce2MsDnk-A> (about 4 minutes)
  + Leo Notenboom, Ask Leo! Are Password Managers Safe? <https://youtu.be/i10BRwNkds0> (about 7 minutes)
* Watch this video:
  + Tekzilla, Get Secure: How To Use A Password Manager. <https://youtu.be/lDIzwxirzgc> (almost 8 minutes, but the last minute is a sponsor’s advertisement; you can skip that if you wish)
* Answer this question in your own words:
  + What is a password manager and why would you want to use one?
* Download and install a password manager application.
  + Recommended: use these instructions in the appendix at the end of this document to install KeePass.

- or -

* + If you would rather use DashLane, 1Password, LastPass, DirectPass, or some other reputable password manager, you are welcome and encouraged to install and use it for this lab.
* Use your new password manager to create a new password database (or “password vault”) and a strong master password for accessing it.
* Create a new credential entry for BYU-Idaho in your new password database. Input your username, password, and [www.byui.edu](https://www.byui.edu) in that new entry. Optionally, you may also store your I-number as an extra note in that entry. Then save your password database.
* Similarly, create a new credential entry for one of your other web sites or applications. Try using your password manager’s password generation feature to create a long random password for that site or app. Again, save your password database. (Remember to always save your database or password vault any time you add or change a credential entry.)
* Test your password manager: use it to sign into BYU-Idaho or your other web site or app. See if you can sign in by having your password manager paste the password, without having to remember or type it in yourself.
* Capture a screen image of your password manager. (If possible, make sure your screen image doesn’t reveal any login names, web site names, etc. which you don’t want to reveal. Edit your screenshot to redact sensitive information as necessary.) Insert or paste your screenshot in your worksheet.

Complete the Task 4 section of the lab worksheet template.

## Task 5: Teach password skills to someone else

Now share your password expertise with a friend, family member, or even a stranger.

Teach password skills and tools:

* Tell them your recommendations for a strong, hard to crack password.
* Help them test their password using <https://howsecureismypassword.net/> and the other password checking tools mentioned in this document. What time or complexity scores did they receive?
* If they aren’t already using one, help them install and learn to use a password manager. If they already use one, ask to compare theirs with yours. Write something you learned by helping or collaborating.

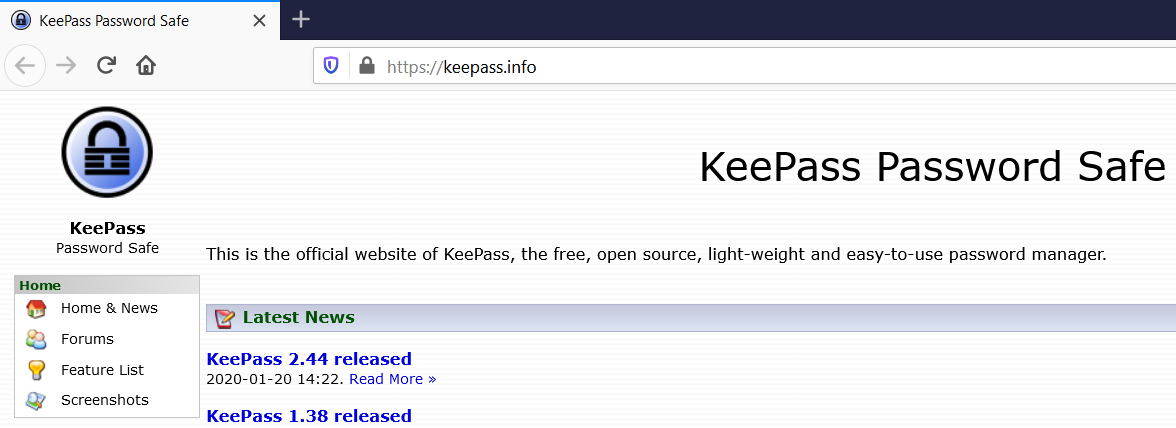
Complete the Task 5 section of the lab worksheet template, including a short reflection about your key take-aways from this lab and something you learned that will help you in the future. Then upload your completed worksheet.

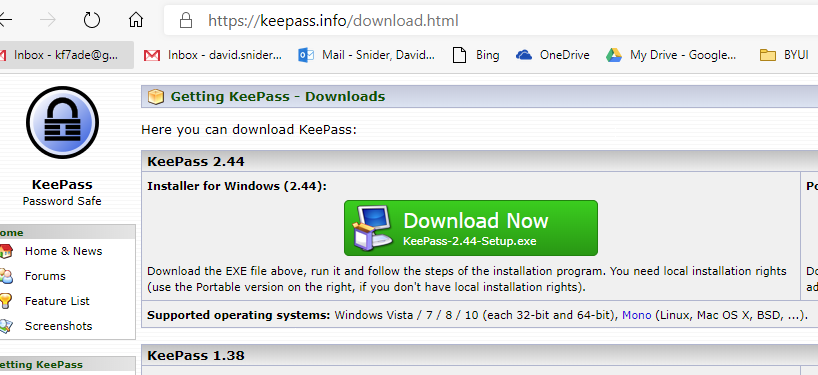
Thank you!

## Appendix: How to install KeePass

These instructions are specific to Microsoft Windows; see step 3 below if you use other operating system platforms.

Download KeePass:

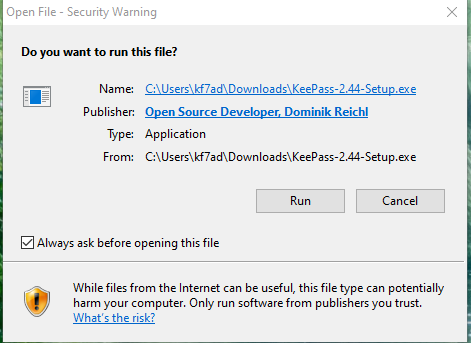
1. Go to <https://keepass.info/>
2. Click the link for the latest release. (When this document was created, the latest release was KeePass 2.44 released 2020-01-20, so that version appears in these instructions; please adjust accordingly for whatever newer version you see.) 
3. Select: **Download KeePass 2.44**. (If you aren’t using Microsoft Windows, select the Downloads link under “Getting KeePass” in the menu on the left, and then scroll down to find Contributed/Unofficial KeePass Ports and Contributed/Unofficial KeePass Packages. Then skip these instructions and instead follow the instructions for your port or package.)
4. Select: **Download Now, KeePass-2.44\_Setup.exe**



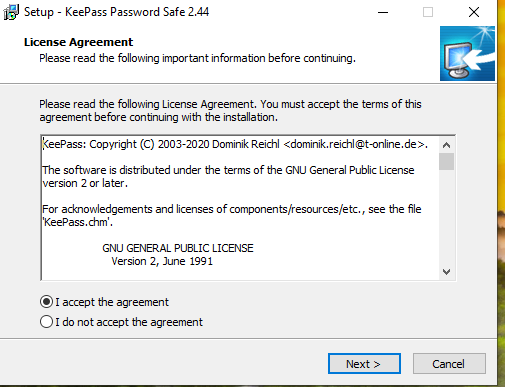
1. Wait a short time for the KeePass-s.44\_Setup.exe file to download.

Install KeePass:

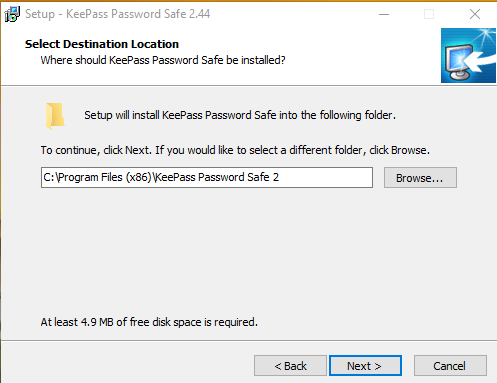
1. Open the downloaded file and click **Run**.



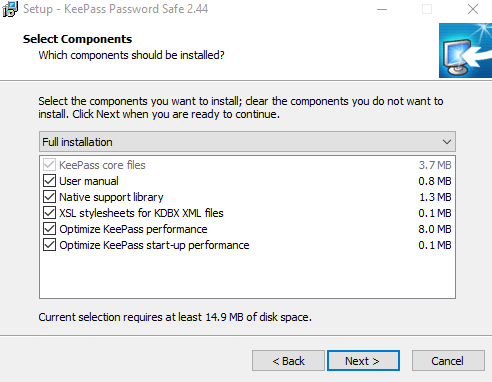
1. Accept the license agreement.



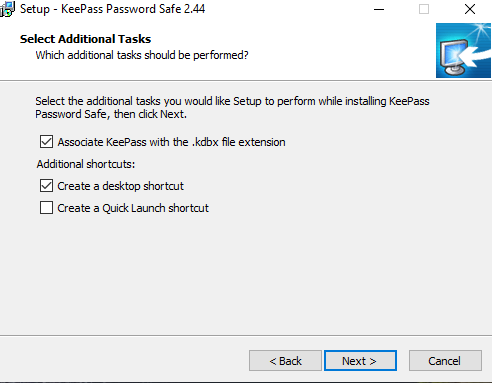
1. Leave the default installation location as it is; click **Next**.



1. Leave the default selected components and click **Next** again.



1. Choose to create a desktop shortcut, then click **Next**.



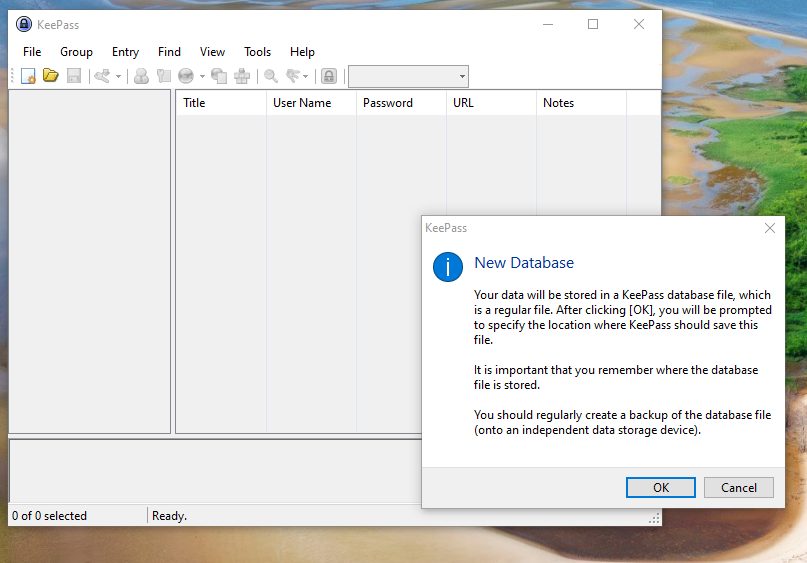
1. Click **Install**. Wait a short moment for installation to complete.
2. Click **Finish**.
3. If asked, allow KeePass to automatically check for updates.

Using KeePass:

1. If KeePass did not launch automatically after it was installed, start it from the desktop by double clicking on the KeePass 2 icon.



1. From the top menu, click **File** > **New** to create a new Database, then click OK.



1. Follow instructions for setting the location of your new KeePass database file.
2. Set the Master Password. (Naturally, this should be a strong password that you *memorize,* using the lessons you learned in tasks 1, 2, and 3 of this lab.) Then click **OK**.
3. KeePass can have more than one user, so you can enter a Database name and a default username for new entries. You can also set a custom color. When set, click **OK**.
4. From the top menu, click **File** > **Print** > **Print Emergency Sheet**. Fill out your printed emergency sheet, and read and follow its instructions.

**-**