



# Introduction to Cybersecurity: Introduction to Cybersecurity 2.1

## Instructor Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the Introduction to Cybersecurity course as part of an official Cisco Networking Academy Program.

## Lab – Compare Data with a Hash (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Use a hashing program to verify the integrity of data.

### Background / Scenario

It is important to understand when data has been corrupted or it has been tampered with. A hashing program can be used to verify if data has changed, or if it has remained the same. A hashing program performs a hash function on data or a file, which returns a (usually much shorter) value. There are many different hash functions, some very simple and some very complex. When the same hash is performed on the same data, the value that is returned is always the same. If any change is performed on the data, the hash value returned will be different.

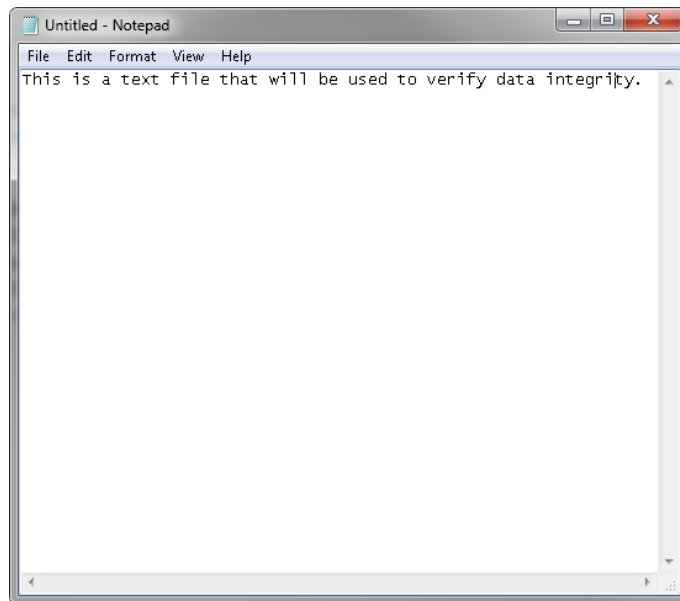
**Note:** You will need installation privileges and some knowledge of the process to install Windows programs.

### Required Resources

- PC with Internet access

#### Step 1: Create a Text file

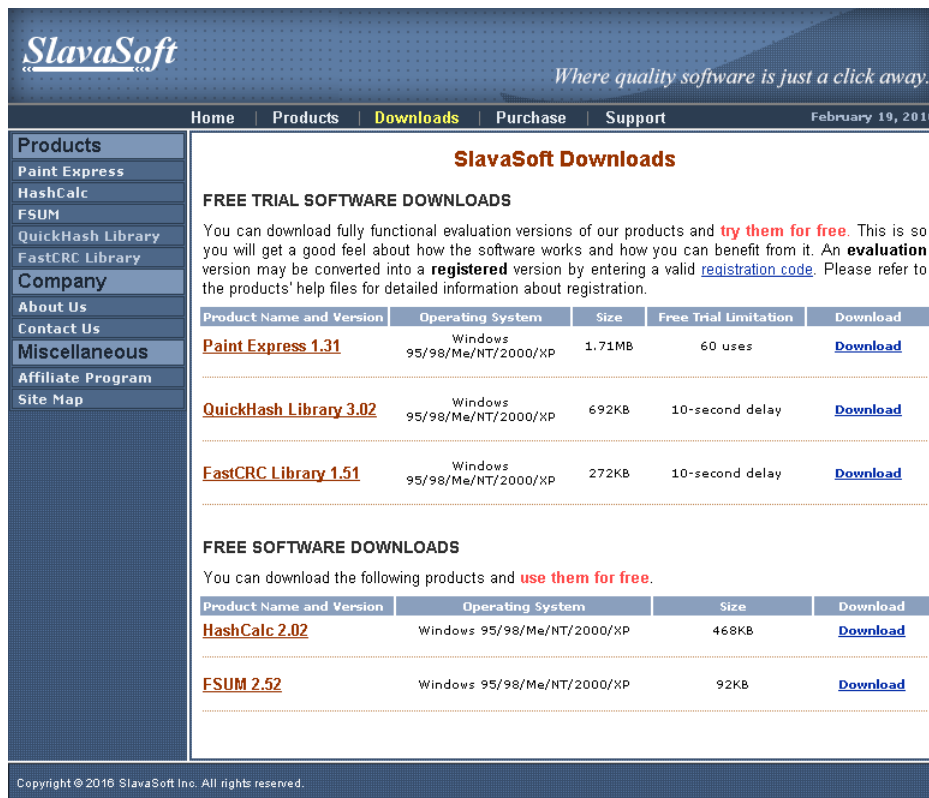
- a. Search your computer for the Notepad program and open it.
- b. Type some text in the program.



- c. Choose **File > Save**.
- d. Navigate to **Desktop**.
- e. Type **Hash** in the **File name:** field, and click **Save**.

### Step 2: Install HashCalc

- a. Open a web browser and navigate to <http://www.slavasoft.com/download.htm>.



**SlavaSoft**  
Where quality software is just a click away.

Home | Products | **Downloads** | Purchase | Support | February 19, 2016

**Products**  
Paint Express  
HashCalc  
FSUM  
QuickHash Library  
FastCRC Library  
**Company**  
About Us  
Contact Us  
Miscellaneous  
Affiliate Program  
Site Map

**SlavaSoft Downloads**

**FREE TRIAL SOFTWARE DOWNLOADS**  
You can download fully functional evaluation versions of our products and **try them for free**. This is so you will get a good feel about how the software works and how you can benefit from it. An **evaluation** version may be converted into a **registered** version by entering a valid [registration code](#). Please refer to the products' help files for detailed information about registration.

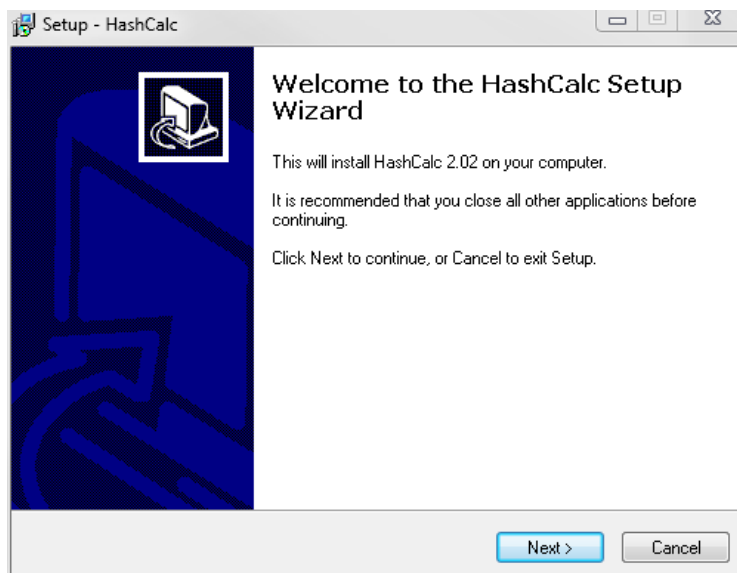
Product Name and Version	Operating System	Size	Free Trial Limitation	Download
<a href="#">Paint Express 1.31</a>	Windows 95/98/Me/NT/2000/XP	1.71MB	60 uses	<a href="#">Download</a>
<a href="#">QuickHash Library 3.02</a>	Windows 95/98/Me/NT/2000/XP	692KB	10-second delay	<a href="#">Download</a>
<a href="#">FastCRC Library 1.51</a>	Windows 95/98/Me/NT/2000/XP	272KB	10-second delay	<a href="#">Download</a>

**FREE SOFTWARE DOWNLOADS**  
You can download the following products and **use them for free**.

Product Name and Version	Operating System	Size	Download
<a href="#">HashCalc 2.02</a>	Windows 95/98/Me/NT/2000/XP	468KB	<a href="#">Download</a>
<a href="#">FSUM 2.52</a>	Windows 95/98/Me/NT/2000/XP	92KB	<a href="#">Download</a>

Copyright © 2016 SlavaSoft Inc. All rights reserved.

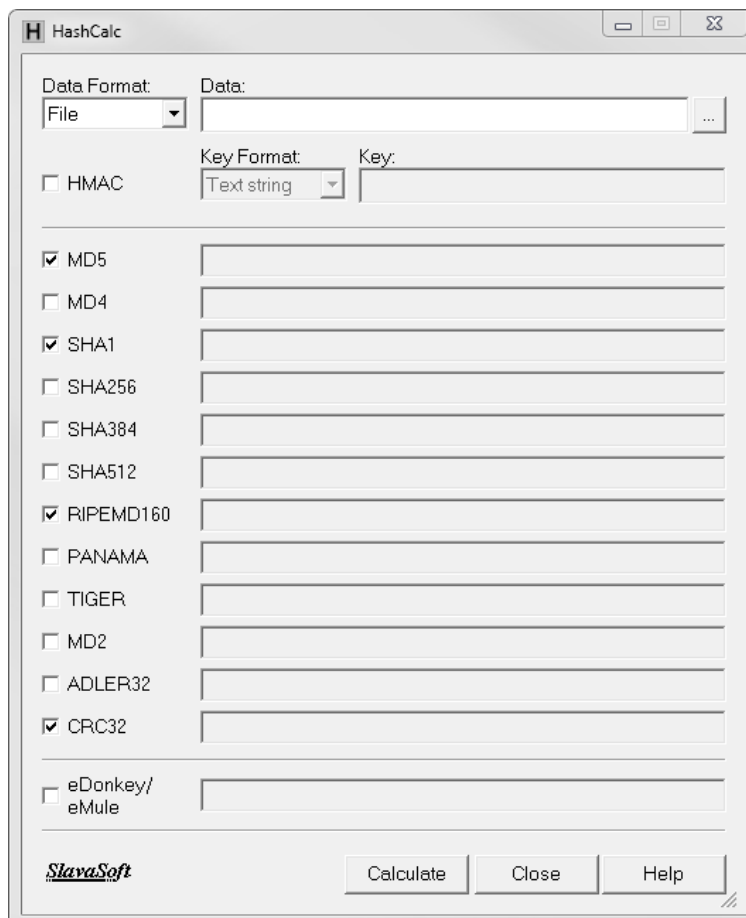
- b. Click **Download** in the **HashCalc 2.02** row.
- c. Open the **hashcalc.zip** file and run the **setup.exe** file inside.



- d. Follow the installation wizard to install HashCalc.

## Lab – Compare Data with a Hash

- e. Click **Finish** on the last screen, and close the **README** file if it opened. You may read the file if you wish.
- f. HashCalc is now installed and running.



### Step 3: Calculate a hash of the Hash.txt file

- a. Set the following items in HashCalc:
  - 1) Data Format: **File**.
  - 2) Data: Click the ... button next to the Data field, navigate to the **Desktop** and choose the **Hash.txt** file.
  - 3) Uncheck **HMAC**.
  - 4) Uncheck all hash types except **MD5**.
- b. Click the **Calculate** button.

What is the value next to **MD5**?

---

Answers may vary. Example: 82e8ac8d4ae929c79e1ce4cf1f0691f4

### Step 4: Make a change to the Hash.txt file

- a. Navigate to the **Desktop** and open the **Hash.txt** file.
- b. Make a minor change to the text, such as deleting a letter, or adding a space or period.

- c. Click **File > Save**, and close **Notepad**.

### Step 5: Calculate a new hash of the Hash.txt file

- a. Click the **Calculate** button in HashCalc again.

What is the value next to **MD5**?

---

Answers may vary, but will be different from Step 3. Example: fb53ad826cefac1dbee8f583a66b7bf4

Is the value different from the value recorded in Step 3?

---

Yes.

- b. Place a check mark next to all of the hash types.
- c. Click **Calculate**.
- d. Notice that many of the hash types create a hash of a different length. Why?

---

Many of the hashes use a different number of bits to produce the hash.

## Lab – Compare Data with a Hash (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Use a hashing program to verify the integrity of data.

### Background / Scenario

It is important to understand when data has been corrupted or it has been tampered with. A hashing program can be used to verify if data has changed, or if it has remained the same. A hashing program performs a hash function on data or a file, which returns a (usually much shorter) value. There are many different hash functions, some very simple and some very complex. When the same hash is performed on the same data, the value that is returned is always the same. If any change is performed on the data, the hash value returned will be different.

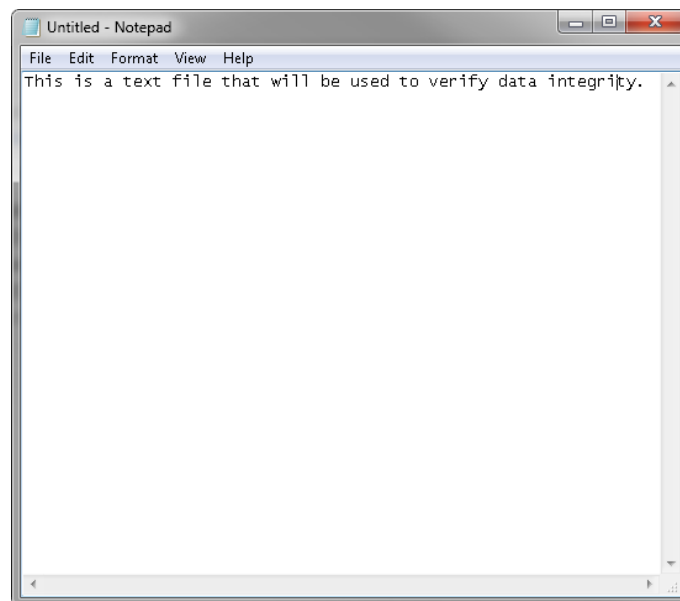
**Note:** You will need installation privileges and some knowledge of the process to install Windows programs.

### Required Resources

- PC with Internet access

#### Step 1: Create a Text file

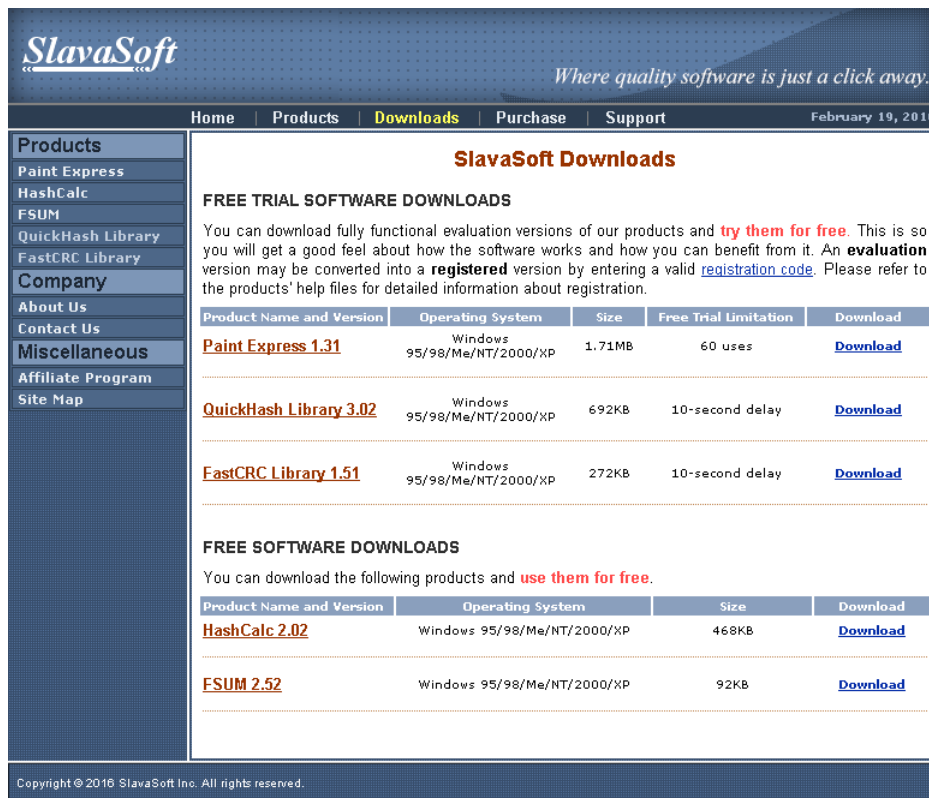
- a. Search your computer for the Notepad program and open it.
- b. Type some text in the program.



- c. Choose **File > Save**.
- d. Navigate to **Desktop**.
- e. Type **Hash** in the **File name:** field, and click **Save**.

### Step 2: Install HashCalc

- Open a web browser and navigate to <http://www.slavasoft.com/download.htm>.



**SlavaSoft**  
Where quality software is just a click away.

Home | Products | **Downloads** | Purchase | Support | February 19, 2016

**Products**  
Paint Express  
HashCalc  
FSUM  
QuickHash Library  
FastCRC Library  
**Company**  
About Us  
Contact Us  
Miscellaneous  
Affiliate Program  
Site Map

**SlavaSoft Downloads**

**FREE TRIAL SOFTWARE DOWNLOADS**  
You can download fully functional evaluation versions of our products and **try them for free**. This is so you will get a good feel about how the software works and how you can benefit from it. An **evaluation** version may be converted into a **registered** version by entering a valid [registration code](#). Please refer to the products' help files for detailed information about registration.

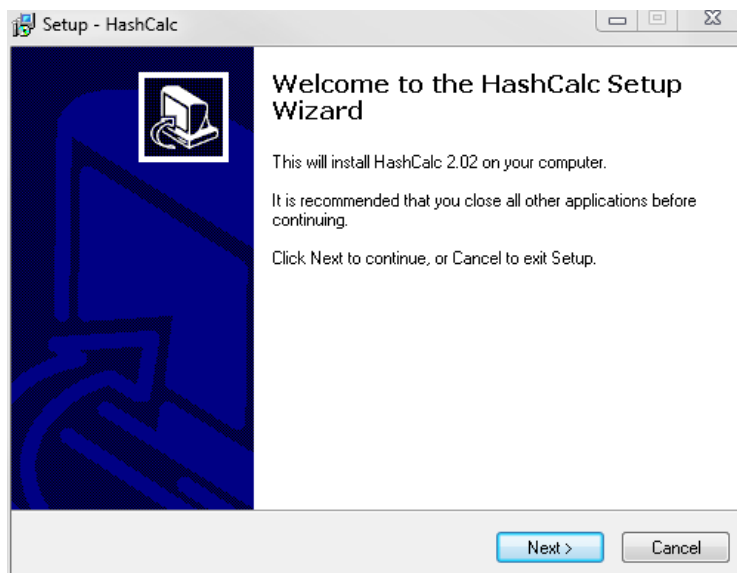
Product Name and Version	Operating System	Size	Free Trial Limitation	Download
<a href="#">Paint Express 1.31</a>	Windows 95/98/Me/NT/2000/XP	1.71MB	60 uses	<a href="#">Download</a>
<a href="#">QuickHash Library 3.02</a>	Windows 95/98/Me/NT/2000/XP	692KB	10-second delay	<a href="#">Download</a>
<a href="#">FastCRC Library 1.51</a>	Windows 95/98/Me/NT/2000/XP	272KB	10-second delay	<a href="#">Download</a>

**FREE SOFTWARE DOWNLOADS**  
You can download the following products and **use them for free**.

Product Name and Version	Operating System	Size	Download
<a href="#">HashCalc 2.02</a>	Windows 95/98/Me/NT/2000/XP	468KB	<a href="#">Download</a>
<a href="#">FSUM 2.52</a>	Windows 95/98/Me/NT/2000/XP	92KB	<a href="#">Download</a>

Copyright © 2016 SlavaSoft Inc. All rights reserved.

- Click **Download** in the **HashCalc 2.02** row.
- Open the **hashcalc.zip** file and run the **setup.exe** file inside.



- Follow the installation wizard to install HashCalc.

## Lab – What was Taken? (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Search for and read about a few recent occurrences of security breaches.

### Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

### Required Resources

- PC or mobile device with Internet access

### Security Breach Research

- a. Use the two provided links to security breaches from different sectors to fill out the table below.
- b. Search for a few additional interesting breaches and record the findings in the table below.



## Lab – What was Taken?

Incident Date	Affected Organization	How many victims? What was Taken?	What exploits were used? How do you protect yourself?	Reference Source
Dec 2015	Neiman Marcus	Approximately 5200 victims with their username and password stolen	Other hacked websites Use unique passwords per site	<a href="#">Securityweek</a>
Between 2009 and 2015	Centene Corp.	950,000 victims and six hard drives containing their personally identifying information i	Physical access to the drives. Use credit and health care monitoring	<a href="#">BBC</a>

## Reflection

After reading about the security breaches, what can you do to prevent these types of breaches?

---

---

---

Answers will vary. Examples: Use unique passwords, avoid opening embedded links in an email

## Lab – Create and Store Strong Passwords (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Understand the concepts behind a strong password.

**Part 1: Explore the concepts behind creating a strong password.**

**Part 2: Explore the concepts behind securely storing your passwords?**

### Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

### Required Resources

- PC or mobile device with Internet access

### Part 1: Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

- 1) The user can easily remember the password.
- 2) It is not trivial for any other person to guess a password.
- 3) It is not trivial for a program to guess or discover a password.
- 4) Must be complex, containing numbers, symbols and a mix of upper case and lower case letters.

Based on the list above, the first requirement is probably the most important because you need to be able to remember your password. For example, the password **#4ssFrX^~aartPOknx25\_70!xAdk<d!** is considered a strong password because it satisfies the last three requirements, but it is very difficult to remember.

Many organizations require passwords to contain a combination of numbers, symbols, and lower and upper case letters. Passwords that conform to that policy are fine as long as they are easy for the user to remember. Below is a sample password policy set for a typical organization:

- The password must be at least 8 characters long
- The password must contain upper- and lower-case letters
- The password must contain a number
- The password must contain a non-alphanumeric character

## Lab – Create and Store Strong Passwords

---

Take a moment to analyze the characteristics of a strong password and the common password policy set shown above. Why does the policy set neglect the first two items? Explain.

---

---

---

---

---

---

Adding symbols, numbers and mixed upper/lower case to a password makes it harder for the user to remember it. Traditionally, when a user finds a password that conforms to a specific set of password policies, the user will re-use the same structure or even the entire password through other services. Some systems will also force the user to change the password periodically, keeping users from using past passwords again. Those users are also very likely to introduce minor changes to the password instead of creating an entirely different password that still conforms to the given password policies.

A good way to create strong passwords is to choose four or more random words and string them together. The password **televisionfrogbootschurch** is stronger than **J0n@than#81**. Notice that while the second password is in compliance with the policies described above, password cracker programs are very efficient at guessing that type of password. While many password policy sets will not accept the first password, **televisionfrogbootschurch**, it is much stronger than the second. It is easier for the user to remember (especially is associated with an image), it is very long and its random factor makes it hard for password crackers to guess it.

Using an online password creation tool, create passwords based on the common company password policy set described above.

- Open a web browser and go to <http://passwordsgenerator.net>
- Select the options to conform to password policy set
- Generate the password.

Is the password generated easy to remember?

---

---

Answers will vary. But it is very likely the password will not be easy to remember.

Using an online password creation tool, create passwords based on random words. Notice that because the words are appended together, they are not seen as dictionary words.

- Open a web browser and go to <http://preshing.com/20110811/xkcd-password-generator/>
- Generate a random word password by clicking **Generate Another!** at the top portion of the webpage.
- Is the password generated easy to remember?

---

---

Answer will vary. But it is very likely the password will be easy to remember.

## Part 2: Securely Storing Passwords

If the user chooses to use a password manager, the first strong password characteristic can be dropped because the user has access to the password manager at all times. Notice that some users only trust their

passwords to their own memory. Password managers, either local or remote, must have a password store, and it can be compromised.

The password manager password store must be strongly encrypted and access to it must be tightly controlled. With mobile phone apps and web interfaces, cloud-based password managers provide anytime, uninterrupted access to its users.

A popular password manager is Last Pass.

Create a trial Lastpass account:

- a. Open a web browser and go to <https://lastpass.com/>
- b. Click **Start Trial** to create a trial account.
- c. Fill out the fields, as instructed.
- d. Set a master password. This password gives you access to your LastPass account.
- e. Download and install the LastPass' client for your operating system.
- f. Open the client and log in with your LastPass master password.
- g. Explore LastPass password manager.

As you add passwords to Lastpass, where are the passwords stored?

---

The passwords are stored on the cloud, on Lastpass' servers.

Besides you, at least one other entity has access to your passwords. Who is that entity?

---

Lastpass

While having all your passwords stored on the same place can be convenient, there are drawbacks. Can you think of any?

---

Answers will vary. Lastpass' servers become a big target for attackers as it contains many users' passwords. The responsibility of maintaining your passwords were now delegated to a third party company which you have no control on their security policies. You choose to trust they are doing a good job at protecting your passwords but there's no guarantees.

### Part 3: What Is a Strong Password Then?

Using on the strong password characteristics given at the beginning of this lab, choose a password that is easy to remember but hard to be guessed. Complex passwords are OK as long as it does not impact more important requirements such as the ability to easily remember it.

If a password manager is used, the need to be easily remembered can be relaxed.

Below is a quick summary:

Choose a password you can remember.

Choose a password that someone else cannot associate with you.

Choose different passwords and never use the same password for different services.

Complex passwords are OK as long as it does not become harder to remember.

## Lab – Backup Data to External Storage (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Backup user data.

**Part 1: Use a local external disk to backup data**

**Part 2: Use a remote disk to backup data**

### Background / Scenario

It is important to establish a backup strategy that includes data recovery of personal files.

While many backup tools are available, this lab focuses on the Microsoft Backup Utility to perform backups to local external disks. In Part 2, this lab uses the Dropbox service to backup data to a remote or cloud-based drive.

### Required Resources

- PC or mobile device with Internet access

## Part 1: Backing Up to a Local External Disk

### Step 1: Getting Started With Backup Tools in Windows

Computer usage and organizational requirements determine how often data must be backed up and the type of backup to perform. It can take a long time to run a backup. If the backup strategy is followed carefully, it is not necessary to back up all files every time. Only the files that have changed since the last backup need to be backed up.

Microsoft Windows includes backup tools that can be used to backup files. In versions earlier than Windows 8, you could use Backup and Restore to backup your files. Windows 8.1 ships with File History which can be used to back up the files in the Documents, Music, Pictures, Videos, and Desktop folders. Over time, File History builds a history of your files, allowing you to go back and recover specific versions of a file. This is a helpful feature if there are damaged or lost files.

Windows 7 and Vista ship with a different backup tool called **Backup and Restore**. When an external drive is selected, Windows 7 will offer the chance to use the new drive as a backup device. Use Backup and Restore to manage backups.

**To access the Backup and Restore utility in Windows 7, follow the steps below:**

- Connect an external drive.
- Execute the Backup and Restore by using the following path:

**Start > Control Panel > Backup and Restore**

**To get started with File History in Windows 8.1, follow the steps below:**

- Connect an external drive.
- Turn on File History by using the following path:

**Control Panel > File History > click Turn on**

**Note:** Other operating systems also have backup tools available. Apple OS X includes Time Machine while Ubuntu Linux includes Déjà Dup, by default.

### Step 2: Backing up the Documents and Pictures folders

Now that the external disk is connected and you know how to find the backup tool, set it up to back up the Documents and Pictures folders every day, at 3 a.m.

- Open **Backup and Restore** (Windows 7) or **File History** (Windows 8.x).
- Select the external disk you want to use to receive the backup.
- Specify what you want to be backed up to the disk. For this lab, choose the **Documents** and **Pictures** folders.
- Set up a backup schedule. For this lab, use daily at 3 a.m.  
Why would you choose to perform backups at 3 a.m.?

---

Because this is likely to be a low-usage time and little to no impact to user operations is expected.

- Start the backup by clicking the **Save settings and run backup**.

## Part 2: Backing Up to a Remote Disk

### Step 1: Getting Familiar With Cloud-Based Backup Services

Another option for a backup destination is a remote disk. This might be a complete cloud service, or simply a NAS connected to the network, remote backups are also very common.

- List a few of cloud-based backup services.

---

Answers will vary. Dropbox, Microsoft OneDrive, Google Drive, Apple iCloud, Amazon AWS.

- Research the services you listed above. Are these services free?

---

Answers will vary. Dropbox, Microsoft OneDrive, Google Drive and Apple iCloud are free for a small and limited amount of storage. If the user needs more storage space, a monthly fee must be paid.

- Are the services listed by you platform dependent?

---

Answers will vary. Most of the popular cloud backup services are not platform dependent and have web interfaces or clients available for all the major platforms.

- d. Can you access your data from all devices you own (desktop, laptop, tablet and phone)?

---

---

Answers will vary. Yes. Most of the popular cloud-based backup services have clients for all computer platforms.

### Step 2: Using Backup and Restore to Back Up Data to the Cloud

Choose a service that fits your needs and backup your copy of your Documents folder to the cloud. Notice that Dropbox and OneDrive allow you to create a folder on your computer that acts as a link to the cloud drive. Once created, files copied to that folder are automatically uploaded to the cloud by the cloud-service client that is always running. This setup is very convenient because you can use any backup tools of your choice to schedule cloud backups. To use Windows Backup and Restore to back up your files to Dropbox, follow the steps below:

- Visit <http://dropbox.com> and sign up for a free Dropbox account.
- When the account is created, Dropbox will display all the files stored in your account. Click **your name** and click **Install** to download and install the appropriate Dropbox client for your operating system.
- Open the downloaded program to install the client.
- After the installation is complete, the Dropbox client will create a folder named Dropbox inside your Home folder. Notice that any files copied into the newly created folder will be automatically copied to Dropbox's cloud-hosted servers.
- Open **Windows Backup and Restore** and configure it to use the new Dropbox folder as a backup destination.

### Reflection

1. What are the benefits of backing up data to a local external disk?

---

---

Local backups are entirely under user's control and no other parties have access to the data. Local backups are always available as it does not depend on an Internet connection.

2. What are the drawbacks of backing up data to a local external disk?

---

---

Measures must be taken if the user wants/needs to access the data from other devices or locations. In case of a disaster such as fire or flooding, the local backup disks are also at risk.

3. What are the benefits of backing up data to a cloud-based disk?

---

---

Because data is replicated to an off-site location, it is more resilient to disaster.

## Lab – Backup Data to External Storage

---

4. What are the drawbacks of backing up data to a cloud-based disk?

---

---

The data is now under the care of a third party company. This company can read and access the data. Also, if the amount of data is high, a storage fee must be paid.



## Lab – Who Owns Your Data? (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Explore the ownership of your data when that data is not stored in a local system.

**Part 1: Explore the Terms of Service Policy**

**Part 2: Do You Know What You Signed Up For?**

### Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

### Required Resources

- PC or mobile device with Internet access

### Part 1: Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and Conditions, is a legally binding contract that governs the rules of the relationship between you, your provider, and others who use the service.

Navigate to the website of an online service that you use and search for the Terms of Service agreement. Below is a list of many popular social media and online storage services.

#### Social Media

Facebook: <https://www.facebook.com/policies>

Instagram: <http://instagram.com/legal/terms/>

Twitter: <https://twitter.com/tos>

Pinterest: <https://about.pinterest.com/en/terms-service>

#### Online Storage

iCloud: <https://www.apple.com/legal/internet-services/icloud/en/terms.html>

Dropbox: <https://www.dropbox.com/terms2014>

OneDrive: <http://windows.microsoft.com/en-us/windows/microsoft-services-agreement>

Review the terms and answer the following questions.

- a. Do you have an account with an online service provider? If so, have you read the Terms of Service agreement?
-

Answer will vary.

- b. What is the data use policy?

---

---

Answer will vary.

- c. What are the privacy settings?

---

---

Answer will vary.

- d. What is the security policy?

---

---

Answer will vary.

- e. What are your rights regarding your data? Can you request a copy of your data?

---

---

Answer will vary.

- f. What can the provider do with the data you upload?

---

---

Answer will vary.

- g. What happens to your data when you close your account?

---

---

Answer will vary.

## Part 2: Do You Know What You Signed Up For?

After you have created an account and agreed to the Terms of Service, do you really know what you have signed up for?

In Part 2, you will explore how the Terms of Service can be interpreted and used by providers.

Use the Internet to search for information regarding how the Terms of Service are interpreted.

Below are a few samples articles to get you started.

Facebook:

<http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html>

iCloud:

[http://www.americanbar.org/publications/law\\_practice\\_today\\_home/law\\_practice\\_today\\_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html](http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html)

Dropbox:

<http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/>

Review the articles and answer the following questions.

- a. What can you do to protect yourself?

---

---

Answers will vary. Read and understand the agreement and check for modification periodically.

- b. What can you do to safeguard your account and protect your data?

---

---

Change your passwords periodically and use a complex password.

## Lab – Discover Your Own Risky Online Behavior (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Objectives

Explore actions performed online that may compromise your safety or privacy.

### Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

### Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

- a. What kind of information do you share with social media sites? \_\_\_\_\_
  - 1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
  - 2) Articles and news I find or read (2 points)
  - 3) It depends; I filter out what I share and with whom I share. (1 point)
  - 4) Nothing; I do not use social media. (0 points)
- b. When you create a new account in an online service, you: \_\_\_\_\_
  - 1) Re-use the same password used in other services to make it easier to remember. (3 points)
  - 2) Create a password that is as easy as possible so you can remember it. (3 points)
  - 3) Create a very complex password and store it in a password manager service. (1 point)
  - 4) Create a new password that is similar to, but different from, a password used in another service. (1 point)
  - 5) Create an entirely new strong password. (0 points)
- c. When you receive an email with links to other sites: \_\_\_\_\_
  - 1) You do not click the link because you never follow links sent to you via email. (0 points)
  - 2) You click the links because the email server has already scanned the email. (3 points)
  - 3) You click all links if the email came from a person you know. (2 points)
  - 4) You hover the mouse on links to verify the destination URL before clicking. (1 point)
- d. A pop-up window is displayed as you visit a website. It states your computer is at risk and you should download and install a diagnostics program to make it safe: \_\_\_\_\_
  - 1) You click, download, and install the program to keep your computer safe. (3 points)
  - 2) You inspect the pop-up windows and hover over the link to verify its validity. (3 points)
  - 3) Ignore the message, making sure you don't click it or download the program and close the website. (0 points)

- e. When you need to log into your financial institution's website to perform a task, you: \_\_\_\_\_
  - 1) Enter your login information immediately. (3 points)
  - 2) You verify the URL to ensure it is the institution you were looking for before entering any information. (0 points)
  - 3) You don't use online banking or any online financial services. (0 points)
- f. You read about a program and decide to give it a try. You look around the Internet and find a trial version on an unknown site, you: \_\_\_\_\_
  - 1) Promptly download and install the program. (3 points)
  - 2) Search for more information about the program creator before downloading it. (1 points)
  - 3) Do not download or install the program. (0 points)
- g. You find a USB drive while walking to work. you: \_\_\_\_\_
  - 1) Pick it up and plug it into your computer to look at its contents. (3 points)
  - 2) Pick it up and plug it into your computer to completely erase its contents before re-using it. (3 points)
  - 3) Pick it up and plug it into your computer to run an anti-virus scan before re-using it for your own files (3 points)
  - 4) Don't pick it up. (0 points)
- h. You need to connect to the Internet and you find an open Wi-Fi hotspot. You: \_\_\_\_\_
  - 1) Connect to it and use the Internet. (3 points)
  - 2) Don't connect to it and wait until you have a trusted connection. (0 points)
  - 3) Connect to it and establishes a VPN to a trusted server before sending any information. (0 points)

## Part 2: Analyze Your Online Behavior

The higher your score, the less safe your online behaviors are. The goal is to be 100% safe by paying attention to all your online interactions. This is very important as it only takes one mistake to compromise your computer and data.

Add up the points from Part 1. Record your score. \_\_\_\_\_

**0:** You are very safe online.

**0 – 3:** You are somewhat safe online but should still change your behavior to be completely safe.

**3 – 17:** You have unsafe behavior online and have a high risk of becoming compromised.

**18 or more:** You are very unsafe online and will be compromised.

Below are a few important online safety tips.

- a. The more information you share on social media, the more you allow an attacker to know you. With more knowledge, an attacker can craft a much more targeted attack. For example, by sharing with the world you went to a car race, an attacker can craft a malicious email coming from the ticketing company responsible for the race event. Because you have just been to the event, the email seems more credible.
- b. Reusing passwords is a bad practice. If you reuse a password in a service under attackers' control, they may be successful when attempting to log in as you in other services.
- c. Emails can be easily forged to look legitimate. Forged emails often contain links to malicious sites or malware. As a general rule, do not click embedded links received via email.

- d. Do not accept any unsolicited software, especially if it comes from a web page. It is extremely unlikely that a web page will have a legitimate software update for you. It is strongly recommended to close the browser and use the operating system tools to check for the updates.
- e. Malicious web pages can be easily made to look like a bank or financial institution website. Before clicking the links or providing any information, double-check the URL to make sure it is the correct web page.
- f. When you allow a program to run on your computer, you give it a lot of power. Choose wisely before allowing a program to run. Research to make sure the company or individual behind the program is a serious and legitimate author. Also, only download the program from the official website of the company or individual.
- g. USB drives and thumb drives include a tiny controller to allow computers to communicate with it. It is possible to infect that controller and instruct it to install malicious software on the host computer. Because the malware is hosted in the USB controller itself and not in the data area, no amount of erasing or anti-virus scanning will detect the malware.
- h. Attackers will often deploy fake Wi-Fi hotspots to lure users. Because the attacker has access to all the information exchanged via the compromised hotspot, users connected to that hotspot are at risk. Never use unknown Wi-Fi hot spots without encrypting your traffic through a VPN. Never provide sensitive data such as credit card numbers while using an unknown network (wired or wireless).

### Reflection

After analyzing your online behavior, what changes would you make to protect yourself online?

---

---

---

---

Answers will vary.