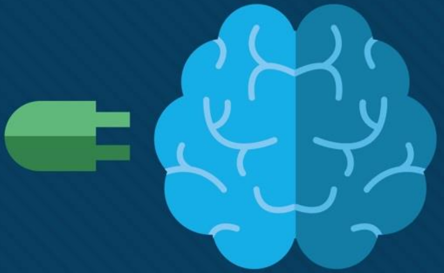
Chapter 3: Protecting Your Data and Privacy



Introduction to Cybersecurity v2.1

Chapter 3 - Sections & Objectives

- 3.1 Protecting Your Data
  - Explain how to protect devices from threats.
    - Explain how to protect your devices and network.
    - Describe safe procedures for data maintenance.
- 3.2 Safeguarding Your Online Privacy
  - Explain how to safeguard your privacy.
    - Describe strong authentication methods.
    - Describe safe online behaviors.

3.1 Protecting Your Data

Protecting Your Computing Devices

- Keep the Firewall On
  - Prevent unauthorized access to your data or computing devices
  - Keep the firewall up to date
- Use Antivirus and Antispyware
  - Prevent unauthorized access to your data or computing devices
  - Only download software from trusted websites
  - Keep the software up to date
- Manage Your Operating System and Browser
  - Set the security settings at medium or higher
  - Update your computer’s operating system and browser
  - Download and install the latest software patches and security updates
- Protect All Your Devices
  - Password protect
  - Encrypt the data
  - Only store necessary information
  - IoT devices

Protecting Your Devices and Network

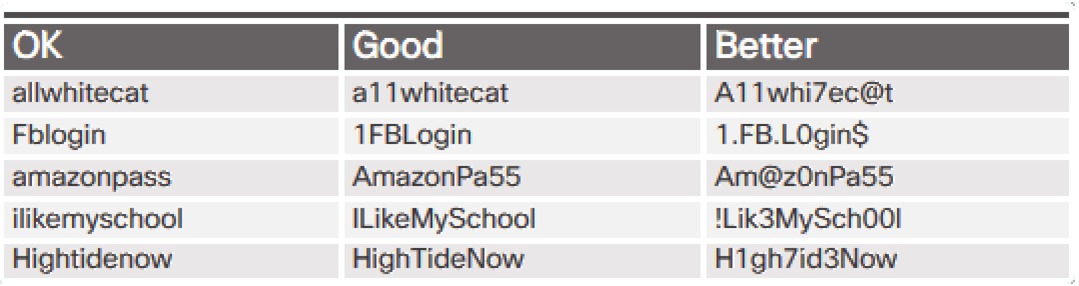
Use Wireless Networks Safely

- Home Wireless Network
  - Change the pre-set SSID and default administrative password on your Wi-Fi router.
  - Disable SSID broadcast
  - Use WPA2 encryption feature
  - Be aware of WPA2 protocol security flaw – KRACK
    - Allows intruder to break the encryption between wireless router and clients
- Use caution when using public Wi-Fi hotspots
  - Avoid accessing or sending sensitive information
  - Use of VPN tunnel can prevent eavesdropping
- Turn off Bluetooth when not in use

Protecting Your Devices and Network

Use Unique Passwords for Each Online Account

- Prevents criminals from accessing all your online accounts using one stolen credentials
- Use password managers to help with remembering passwords
- Tips for choosing a good password:
  - Do not use dictionary words or names in any languages
  - Do not use common misspellings of dictionary words
  - Do not use computer names or account names
  - If possible use special characters, such as ! @ # $ % ^ & * ( )
  - Use a password with ten or more characters

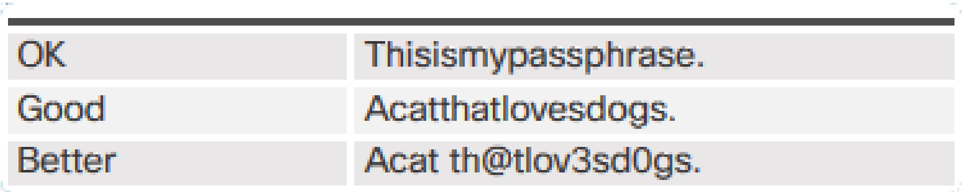


OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

Protecting Your Devices and Network

Use Passphrase Rather Than a Password

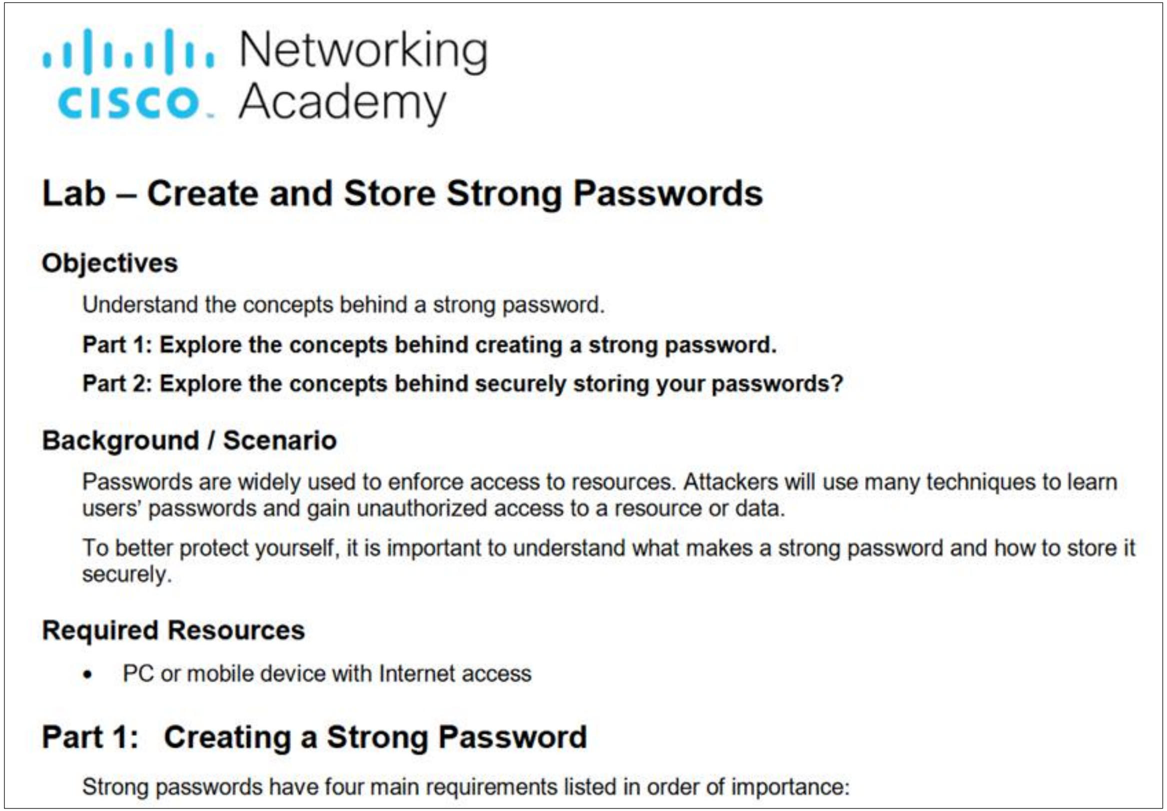
- Tips in choosing a good passphrase:
  - Choose a meaningful statement to you
  - Add special characters, such as ! @ # $ % ^ & * ( )
  - The longer the better
  - Avoid common or famous statements, for example, lyrics from a popular song
- Summary of the new NIST guidelines:
  - 8 characters minimum in length, but no more than 64 characters
  - No common, easily guessed passwords, such as password, abc123
  - No composition rules, such as having to include lowercase and uppercase letters and numbers
  - No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history
  - Improve typing accuracy by allowing the user to see the password while typing
  - All printing characters and spaces are allowed
  - No password hints
  - No periodical or arbitrary password expiration



OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

Protecting Your Devices and Network

Lab – Create and Store Strong Passwords



Networking Academy

Lab – Create and Store Strong Passwords

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

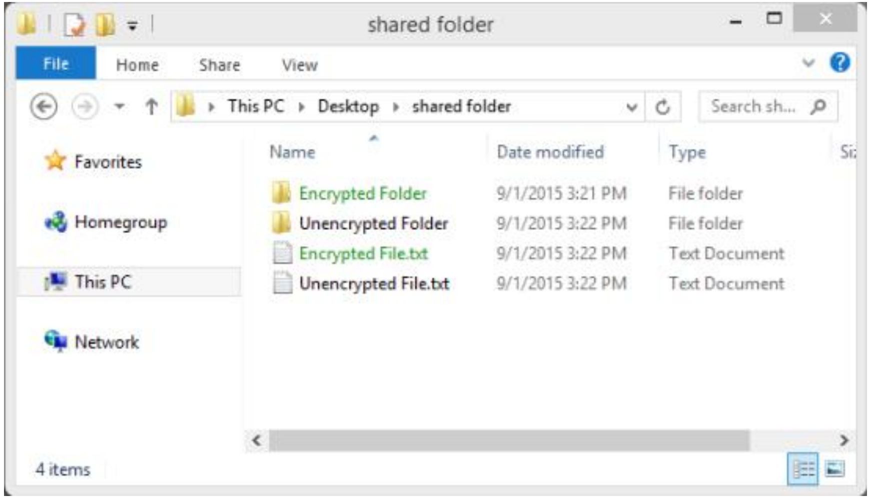
Part 1: Creating a Strong Password

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

Data Maintenance

Encrypt Your Data

- Encrypted data can only be read with the secret key or password
- Prevent unauthorized users from reading the content
- What is Encryption?
  - process of converting the information into a form where an unauthorized party cannot read it



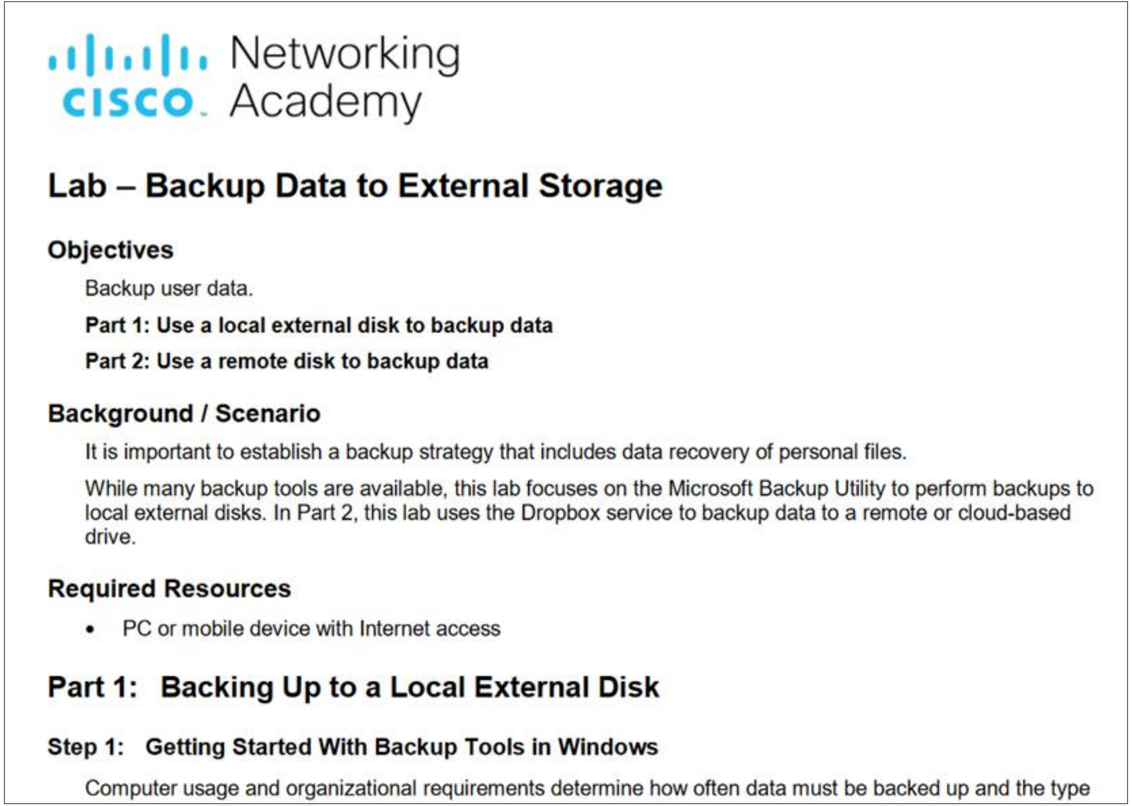
Name	Date modified	Type
Encrypted Folder	9/1/2015 3:21 PM	File folder
Unencrypted Folder	9/1/2015 3:22 PM	File folder
Encrypted File.txt	9/1/2015 3:22 PM	Text Document
Unencrypted File.txt	9/1/2015 3:22 PM	Text Document

Back up Your Data

- Prevent the loss of irreplaceable data
- Need additional storage location for the data
- Copy the data to the backup location regularly and automatically
- Local Backup
  - NAS, external hard drive, CDs/DVDs, thumb drives, or tapes
  - Total control and responsible for the cost and maintenance
- Cloud Storage Service, such as AWS
  - Access to backup as long as you have access to your account
  - may need to be more selective about the data being backed up

Data Maintenance

Lab – Back up Data to External Storage



Networking Academy

Lab – Backup Data to External Storage

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

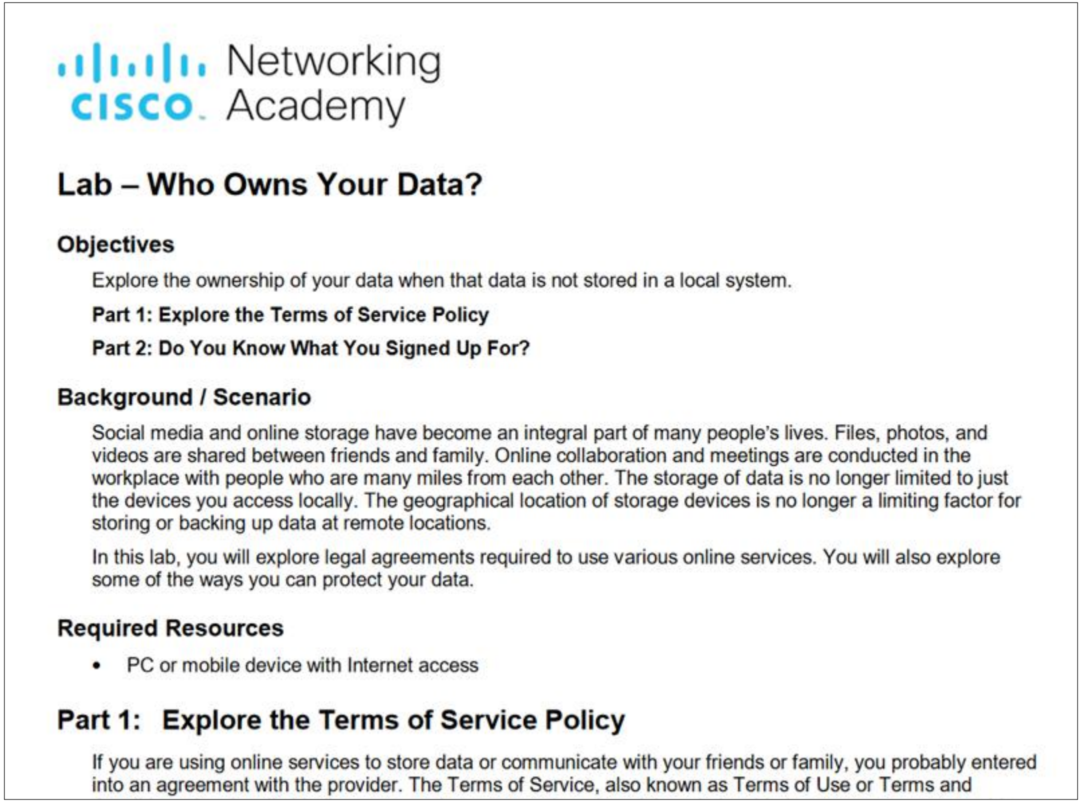
Data Maintenance

Deleting Your Data Permanently

- Use available tools to delete permanently: SDelete and Secure Empty Trash, for example
- Destroy the storage device to ensure that the data is unrecoverable
- Delete the online versions

Data Maintenance

Lab – Who Owns Your Data



Networking Academy

Lab – Who Owns Your Data?

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

3.2 Safeguarding Your Online Privacy

Strong Authentication

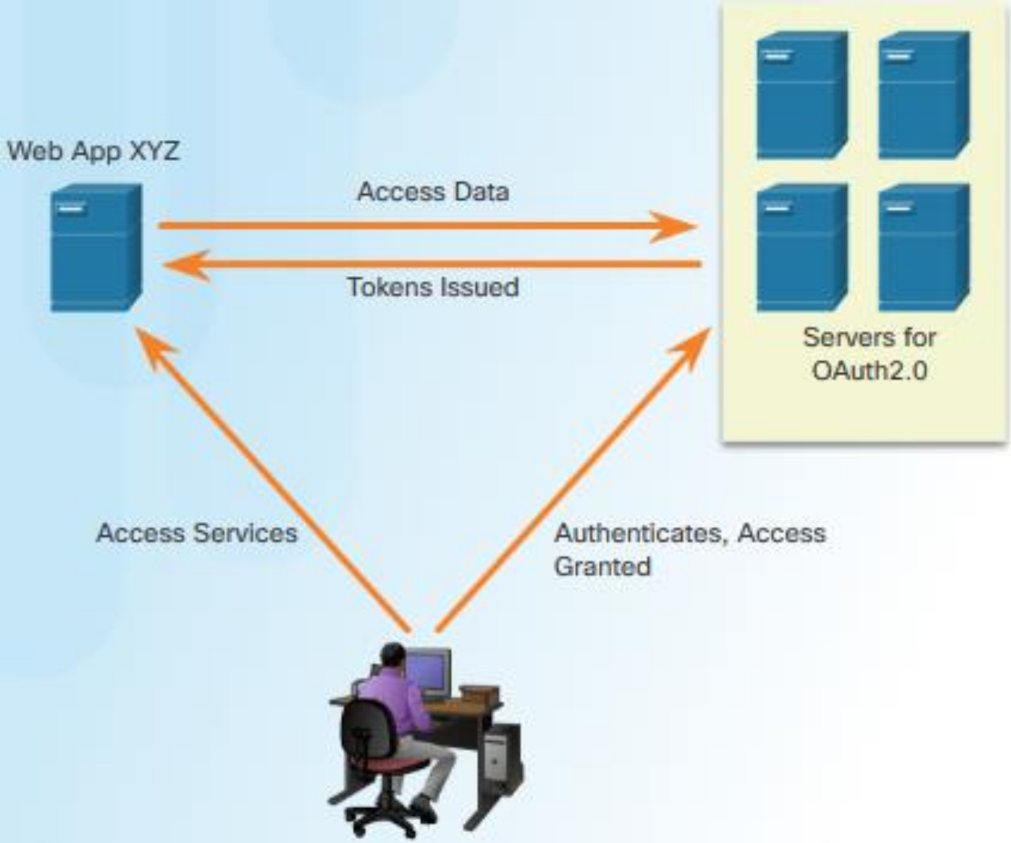
Two Factor Authentication

- Popular online services use two factor authentication
- Need Username / password or PIN and a second token for access:
  - **Physical object** - credit card, ATM card, phone, or fob
  - **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition

Strong Authentication

OAuth 2.0

- An open standard protocol that allows an end user's credentials to access third party applications without exposing the user's password
- Act as the middle man to decide whether to allow end users access to third party applications.



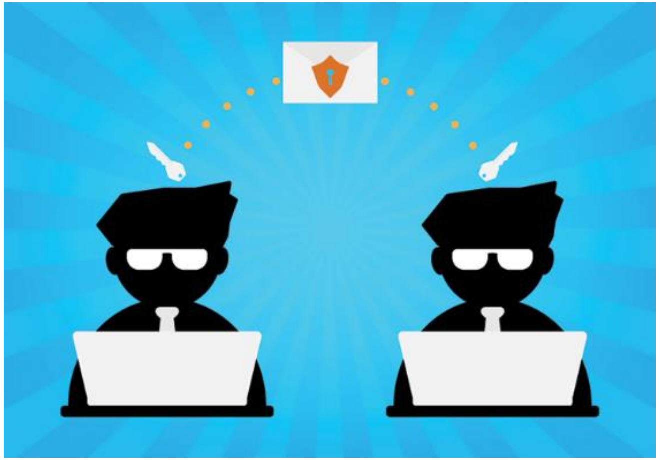
Sharing Too Much Information?

Do Not Share Too Much on Social Media

- Share as little information as possible on social media
- Do not share information such as:
  - Birth date
  - Email address
  - Phone number
- Check your social media settings

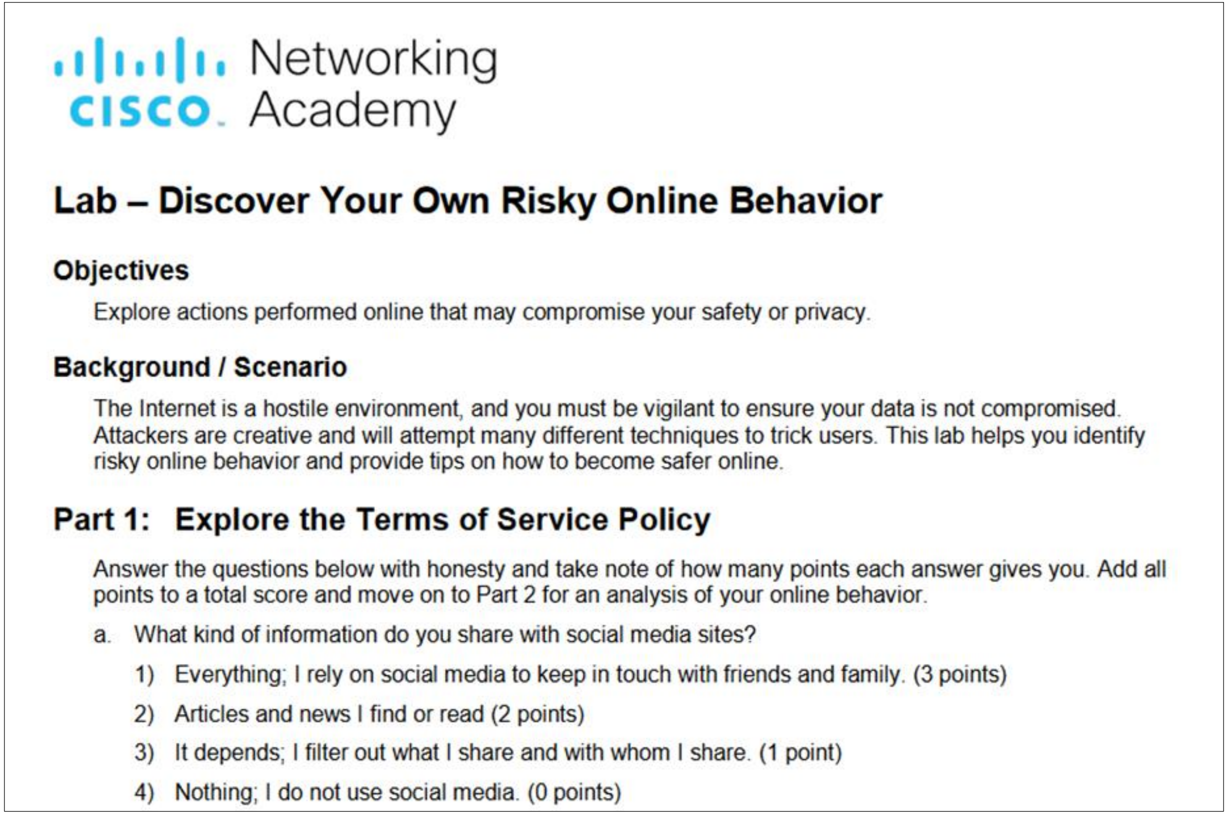
Email and Web Browser Privacy

- Email is like sending a postcard.
- Copies of the email can be read by anyone with access.
- The email is passed among different servers
- Use the private browsing mode can prevent other from gathering information about your online activities.
- Private mode on popular browser
  - **Microsoft Internet Explorer**: InPrivate
  - **Google Chrome**: Incognito
  - **Mozilla Firefox**: Private tab / private window
  - **Safari**: Private: Private browsing



Sharing Too Much Information?

Lab – Discover Your Own Risky Online Behavior



Networking Academy

Lab – Discover Your Own Risky Online Behavior

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)

3.3 Chapter Summary

Summary

- Explain how to protect your devices and network from threats.
- Describe safe procedures for data maintenance.
- Explain how to safeguard your privacy by using strong authentication methods and practicing safe online behaviors.

cisco