Lab - Exploring the World of Cybersecurity Professionals

Objectives

Explore the security features used by organizations like Google and Cisco to keep your data safe.

Part 1: Protecting Your Data

Part 2: Improving your Google Account Security

Background / Scenario

This chapter introduces the student to the cyber world. This cyber world is full of data kingdoms that handle unimaginable amounts of personal and organizational information. As cybersecurity professionals, it is important to understand the types of cybersecurity safeguards an organization must implement in order to protect the data they store, manage, and protect. In this lab, you will explore one of the world's largest data handling organizations, Google. You will watch two videos and then answer a series of questions. Each video presents a different aspect of cybersecurity defense at Google. Upon completion, you will have a better understanding of the security measures and services that organizations like Google take in order to protect information and information systems.

Videos:

How Google Protects Your Data

Security Key

Required Resources

- PC or mobile device with Internet access

Part 1: Protecting Your Data

As one of the world's largest personal data repositories, Google stores massive amounts of data. Google accounts for close to 50% of all internet search activity. To make things even more complicated, Google owns and operates YouTube, the Android operating system, and many other major sources of data collection. In this activity, you will watch a short video and try to identify several of the measures the cybersecurity professionals at Google take to protect your data.

Step 1: Open a browser and view the following video:

How Google Protects Your Data

a. How does Google ensure that the servers they install in their datacenters are not infected with malware by the equipment manufacturers?

Google personally develops custom built hardware and only install necessary software needed by the servers.

b. How does Google protect against physical access to the servers located in the Google datacenters?

Google has 24-hour security personnel and surveillance to monitor all activity at the data centers and does not allow visitors or public tours of the data centers.

c. How does Google protect customer data on a server system?

Data is stored in different locations where files are given random file names and are encrypted as they are stored as random texts.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Step 2: Identify data vulnerabilities.

a. As you can see by the video, data in the Google datacenters are well protected, however, when using Google, not all your data is located in the Google datacenter. Where else can you find your data when using the Google search engine?

One the device that is used to access google servers.

b. Can you take steps to protect data when using the Google search engine? What are a few measures you can use to protect your data?

2-Step Verification and also physical security keys.

Part 2: Improving your Google Account Security

The greatest threat when using web-based services like Google is protecting your personal account information (username and password). To make things worse, these accounts are commonly shared and used to authenticate you to other web-based services, like Facebook, Amazon, or LinkedIn. You have several options to improve the handling of your Google login credentials. These measures include creating a two-step verification or an access code with your username and password. Google also supports the use of security keys. In this activity, you will watch a short video and try to identify measures that can be taken to protect your credentials when using web-based accounts.

Step 1: Open a browser and view the following video:

The Key to Working Smarter, Faster, and Safer

a. What is two-step verification? How can it protect your Google account?

It is a secondary access code required after the password has been authenticated. It protects data by requiring the code from another device such as a mobile phone app or second email.

b. What is a security key and what does it do? Can you use the security key on multiple systems?

It is a physical device used to access a google account, by inserting it into the desired device and tapping it sends a code automatically to the google servers and logs into the registered account. It can

c. Click here for common questions about the Security Key. If you set up your account to use a security key, can you still get in without having the physical key?

Yes, by using other preset verification processes available in the account.

Step 2: Protect Gmail Account Access.

a. The use of a Gmail account has become extremely popular. Google now has over 1 billion active Gmail accounts. One of the convenient features of Gmail accounts is the ability to grant access to other users. This share access feature creates a shared email account. Hackers can use this feature to access your Gmail account. To check your account, log in to your Gmail account, and click the gear icon in the top right corner (settings). When the settings screen opens, a menu bar is displayed under the Settings screen title. (General – Labels – Inbox – Accounts and Import – Filters and Blocked Addresses …)

b. Click the **Accounts and Import** menu item. Check the **Grant access to your account** option. Delete any unauthorized shared users of your account.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Step 3: Check Your Gmail Account Activity.

a. Gmail users can also check the account activity in order to make sure no other users have accessed their personal Gmail account. This feature can identify who has accessed the account and from what locations. Use the **Last account activity** option to determine if someone else has accessed your account. To access the **Last account activity** follow these steps:

   1) Login to your Gmail account.

   2) Select **Last account activity:** found at the bottom of the page. It will display the last time the unauthorized user accessed the account and from where.

   3) Just below this message is a detail hyperlink. Click the detail hyperlink.

b. View the account activity. If you find an unauthorized user, you can disconnect the unauthorized user by clicking the button at the top left **Sign out all other web sessions**. Now change your password to keep the unauthorized user from accessing the account.

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.