Lab - Exploring the World of Cybersecurity Professionals – Rymbayeva Anelya, 20B030299

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?

Only the necessary operating system services and hardware are installed. This helps provide a computing environment that is much less prone to vulnerabilities.

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

Access to Google data centers is tightly controlled. Its in Google policy not to allow public tours or site visits. Security personnel are on duty 24 hours a day, 7 days a week. Google data centers are watched by a comprehensive set of video monitoring cameras. Once granted access to the facility, authorized personnel must check in at a reception area.

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

Google takes great measures to protect its customers' data, and security and protection of that data is paramount. Google's customer data is stored in multiple locations help ensure reliability. The files that stored the data are given random file names and are not stored in clear text. So there're not humanly readable. For each hard drive that is received in one of our data centers, Google rigorously tracks its location and status. When a hard drive fails or begins to exhibit performance problems, its brought to this area where its reformatted and retested. If the hard drive does not pass these tests, its removed from the rotation. The data on the hard drives is then overwritten to help ensure that no customer data remains on it. The data override is then verified with a complete discrete. This process helps ensure that there's no trace of customer data remaining on the hard drive. For hard drives that reach the end of their life, Google has a destruction process that is designed to further ensure that none of the data on that drive can ever be accessed the drives are destroyed in a multi-step process. One device that is used to destroy old hard drives is known as 'the chusher'. A steel piston is pushed through the center of the drive, and the platters are deformed , making them unreadable. Another step in the process is the drive shredder. No one will be likely to get any of Google's customers' data from these drives, after the crushing process, the remains are sent to recycling centers.

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?

Data still resides at your local machine(laptop, PC, smart phones). This data must also be protected.

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?

Use strong passwords, two-factor authentication. Also frequently clear the browse history and cookies. Require device authentication to access your account.

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?

Two – step verification is an enhancement to normal Google account login. Users can create a special ID number that is provided during login.

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

A security key log is registered to your Google account, not a particular computer. You can use your Security Key on any computer with Google Chrome.

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. If you are asked for a Security key and do not have it available, you will always have the option to use a verification code.

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.

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:

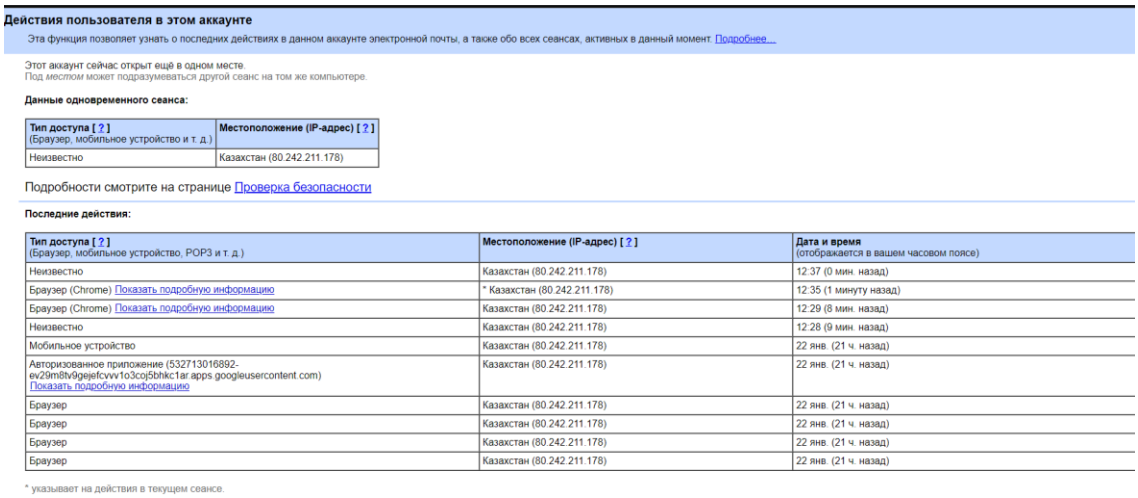
1) Login to your Gmail account.

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.

Последние действия в аккаунте: 21 час назад

Подробные сведения

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



Действия пользователя в этом аккаунте

Эта функция позволяет узнать о последних действиях в данном аккаунте электронной почты, а также обо всех сеансах, активных в данный момент. Подробнее...

Этот аккаунт сейчас открыт ещё в одном месте.
Под *местом* может подразумеваться другой сеанс на том же компьютере.

Данные одновременного сеанса:

Тип доступа [?] (Браузер, мобильное устройство и т. д.)	Местоположение (IP-адрес) [?]
Неизвестно	Казахстан (80.242.211.178)

Подробности смотрите на странице Проверка безопасности

Последние действия:

Тип доступа [?] (Браузер, мобильное устройство, POP3 и т. д.)	Местоположение (IP-адрес) [?]	Дата и время (отображается в вашем часовом поясе)
Неизвестно	Казахстан (80.242.211.178)	12:37 (0 мин. назад)
Браузер (Chrome) Показать подробную информацию	* Казахстан (80.242.211.178)	12:35 (1 минуту назад)
Браузер (Chrome) Показать подробную информацию	Казахстан (80.242.211.178)	12:29 (8 мин. назад)
Неизвестно	Казахстан (80.242.211.178)	12:28 (9 мин. назад)
Мобильное устройство	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)
Авторизованное приложение (532713016892-ev2l9m8fv9gejefcvvv1o3coj5bhkc1ar.apps.googleusercontent.com) Показать подробную информацию	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)
Браузер	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)
Браузер	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)
Браузер	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)
Браузер	Казахстан (80.242.211.178)	22 янв. (21 ч. назад)

* указывает на действия в текущем сеансе.

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.