Lab - Privacy and Gaming (Instructor Version)

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

# Objectives

In this activity, you will research the issue of privacy and gaming and configure Windows Privacy and Gaming settings.

Part 1: Privacy and Gaming

Part 2: Mitigation

Part 3: Windows PC Privacy Settings

Part 4: Windows Gaming Settings

# Background / Scenario

The gaming industry has become one of the fastest industries. Video games are designed for everyone. You can play video games on personal computers, game consoles, handhelds, smartphones, or tablets. As you are playing the games, your data is being collected and sent to online servers. Because of its popularity and amount of collected data, it is becoming a prime target for cybercriminals to steal user information, invade privacy or spread malicious content. Your privacy and security can be compromised. Some of the consequences can include stalking, harassment, fraud, identity theft, and possible threats to your physical safety.

In this activity, you will review a few security breaches related to gaming and then you will assess your own gaming privacy risks. You will also configure Windows Privacy settings.

# Required Resources

* Windows PC

# Instructions

## Privacy and Gaming

As gaming becomes more popular, the occurrence of data breaches will also increase. Learning more about how the breaches occur may prevent you from being a victim.

* + - 1. Perform a search on the internet using keywords like gaming data breach and gaming privacy breach.
      2. Choose three gaming data and/or privacy breaches. Share your results in the table below. An example of a breach is included in the table below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Affected Company | First Detected | Games Affected | Loss | Method |
| Zynga | September 2019 | Words with Friends and Draw Something | Users’ personal data:   * login details * email addresses * usernames * Facebook IDs * phone numbers * hashed and salted passwords | Take advantage of a vulnerability to access database with user credentials and information |
| Capcom | November 2021 | Resident Evil, Street Fighter, Dark Stalker | Personal data of 400,000 gamers | Ransomware |
| Electronic Arts (EA) | June 2021 | FIFA 21, Battlefield, Frostbite | Game source code and tools for popular games, no personal data was stolen | Not ransomware. Data mining (cookies) and social engineering |
| Twitch | October 2021 | N/A | Source code and payout information, possible user information | Took advantage of server misconfiguration |

Blank Line, No additional information

## Mitigation

Based on what you learned about the security breach. What can you do to mitigate personal security breaches in the future?

Perform an internet search for gaming privacy. Record your findings on how to avoid oversharing, downloading malware and ransomware, login safety, and other mitigation methods.

* + - 1. Oversharing

Type your answers here.

1) You can limit the amount of shared personal data by using a separated dedicated gaming email address when registered for a gaming account. 2) Review the game’s privacy settings and only activate features that are important for your gaming experience. 3) Beware that when playing online, you can inadvertently share personal information via the camera or microphone. 4) Turn off location information.

* + - 1. Downloading malware and ransomware

Type your answers here.

1) Avoid downloading any game tips, cheat codes, or files from unverified sites or third-party software from unknown sources. 2) Be on the lookout for phishing scams that trick you into downloading and installing malware.

* + - 1. Login safety

Type your answers here.

1) Enable two-factor authentication (2FA) if it is supported. 2) Do not use the same user credentials for gaming and other accounts, such as bank or work accounts. 3) Create strong varied passwords.

* + - 1. Other mitigation methods

Type your answers here.

Answers will vary. Other methods can include: 1) Apply updates on the software and hardware when they become available 2) Be wary when playing on public Wi-Fi 3) Stay up-to-date on any data breaches on the games that you play 4) Log out of your gaming accounts when done playing 5) Use virtual private network (VPN) to keep your online activities private by encrypting your traffic.

## Windows PC Privacy Settings

Changing Windows privacy default settings can help protect you and your private information. The following changes in settings are provided for suggestions only.

* + - 1. Navigate to the Privacy Settings. Click **Start** > **Settings** > **Privacy**.

**Note**: For Windows 11, click **Start** > **Settings** > **Privacy & security** for similar settings.

* + - 1. In the **General** menu option for Windows 10, toggle all four settings to **Off** position.
      2. Navigate to **Location**. Decide which settings should be On in the **Location** menu.

#### Question:

Would you allow location access to the device? Explain.

Type your answers.

Answers will vary. By providing the location information, it can enhance your gaming or mobile device experience; however, your location may become available to threat actors.

* + - 1. Under the **Location history** heading, click **Clear** your location history if location has been on.
      2. Review the rest of the settings and decide which apps can or cannot access your precise location.
      3. Review the Camera and Microphone settings. You can choose which Microsoft apps or desktop apps can access your camera or microphone.

#### Questions:

* 1. How would you allow camera or microphone access to your devices? Explain.
  2. Type your answers.
  3. Answers will vary. Access to the camera or microphone should be allowed on an individual app basis whenever possible. This controlled access hopefully prevents accidental or unauthorized use of the camera or microphone.
     + 1. Under the privacy tab, name at least two more settings that should be changed from default to enhance your privacy. Explain why you chose those two settings

Type your answers here.

Answers will vary. Access to Account Info may expose personal info, such as your name, picture, and other account info. Contacts should only be accessible for apps, such as People, that require the contact to perform correctly.

Cortana, Microsoft’s voice assistant, can be a privacy risk. Perform an internet search to determine how to disable Cortana. You can permanently or temporarily disable Cortana. Document one way to disable Cortana temporarily.

Type your answers here.

Answers will vary. Open Cortana from the Taskbar > Settings > Turn off Keyboard shortcut > Reboot. Turn off Voice activation after reboot. This should prevent Cortana from activating accidentally.

## Windows Gaming Settings

Windows gaming settings can also protect your privacy while you are gaming.

* + - 1. Navigate to the Privacy Settings. Click **Start** > **Settings** > **Gaming**.
      2. Review the options in the **Gaming** settings.

#### Questions:

What are the available Gaming settings?

Type your answers here.

Answers may vary. In Windows 10, the settings are Xbox Game Bar, Captures, Game Mode and Xbox Networking. For Windows 11, Xbox Networking is not available.

Review each setting. What options would you change to enhance your privacy while gaming?

Type your answers here.

Answers may vary. Example: Under the Xbox Game Bar, review the Xbox Game Bar settings and all the shortcuts. You can turn off audio and video recording under the Capture heading.

End of document