**Shape

Description automatically generated with medium confidenceGraphical user interface

Description automatically generated**

**Mission 5 - Activity Sheet**

**Story so far**

*Our Alien,* ***Alex****, is internet connected, has locked his device securely, has installed software and apps, & has also just started creating accounts.*

*Your task this time is to help* ***Alex*** *make sure her/his device is as up to date as it can be, as well as understand things to be careful of.*

**Questions you will need to consider looking into.**

* How to you know if there is a new update
* Can you find out if there is no notification
* What is an update/fix/patch
* Why does a new device with recent downloads need updating anyway?
* What might be the risk of not updating software
* Why do hackers care about whether a device is updated

**Next session objective – discussion topic**

What advice are you going to give Alex about updates and where they come from.

**Everyone likes to learn in their favourite way. Here is a list of things you may want to look at if you are stuck or what an idea of things to think about. There are lots more out there, perhaps you can find better ones!**

**I asked Chat GPT to help me out here. Here is what it said!**

Introduction:

Have you ever received a notification on your phone or computer to update your software, but chose to ignore it? You're not alone! Many people put off software updates because they can be time-consuming or seem unnecessary. However, failing to update your software can have serious consequences. In this lesson, we'll explore why it's important to keep your software up to date.

Body:

1. Security Risks:

One of the main reasons why you should update your software is to protect yourself from security risks. Outdated software can be vulnerable to hacking, viruses, and other forms of cyber attacks. Hackers are constantly looking for ways to exploit software vulnerabilities, and outdated software can provide an easy target. By updating your software, you ensure that you have the latest security features and patches to protect against these threats.

1. Improved Functionality:

Software updates often include new features, bug fixes, and performance enhancements. By updating your software, you can take advantage of these improvements, which can make your computer or device run more smoothly and efficiently. Updates can also provide new tools and capabilities that can improve your productivity or make your experience more enjoyable.

1. Compatibility:

As new software and hardware are developed, older software may become incompatible. This means that if you don't update your software, you may not be able to use it with newer devices or programs. For example, if you're using an outdated version of a web browser, you may have trouble accessing certain websites or features that require the latest version.

Conclusion:

Updating your software may seem like a hassle, but it's an important part of keeping your computer or device safe, secure, and functional. By staying up to date, you can protect yourself from security risks, take advantage of new features, and ensure compatibility with new technology.

Resources:

From the NCSC

<https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date/>

"Why You Should Always Update Your Software" by NortonLifeLock: <https://uk.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches>

"The Importance of Software Updates" by Digital Trends: <https://www.digitaltrends.com/mobile/buying-cheap-phones-warning-signs-look-out-for/#dt-heading-the-importance-of-software-updates>

"Why Updating Your Software is Critical for Cybersecurity" by McAfee: <https://www.mcafee.com/blogs/internet-security/software-updates-important/>

A few others to try:

**What are lists of knows bugs (CVE)**

[**https://en.wikipedia.org/wiki/Common\_Vulnerabilities\_and\_Exposures**](https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures)

**What are the stages hackers follow?**

**https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html**