**(Continue Security for an app)**

**12. Using anti-malware for security of an app-**

**Anti-malware** is a piece of software that you knowingly install on your computer with the purpose of protecting your system from malware infiltration and infection. Anti-malware programs are able to do this in three ways: they detect malware on your computer, safely remove it, and clean up any of the damage to the computer that the malware may have caused.

**How it works?**

**One way is** anti-malware (AM) detects bad software is a form of analysis called heuristics. Heuristic analysis allows anti-malware programs to detect threats that were not previously discovered. Heuristics identifies malware by behaviors and characteristics, instead of comparing against a list of known malware.

**Another way is by** AM software can find malware is by running a program it suspects to be malicious in a sandbox, which is a protected space on the computer.

**13. Parental Control-**  **Parental Controls** allows **parents** to monitor, as well as filter, activity on an Android device. It has a child-safe browser function and can also filter content in other Android browsers. In addition, the **app** has**monitoring** capability for texts, calls and usage.

**How can it be used?**

The different levels of protection available are as follows:

* **Operating system-** Microsoft's Windows, Apple's Mac OS, and Google Chrome come with robust built-in parental controls. To get the most benefits, you need to use the most updated version of the operating system, and each user has to log in under his or her profile.
* **Web browsers-** Browsers, for example Mozilla Firefox, Google Chrome, and Apple Safari, are the software you use to go on the Internet. Each one offers different ways of filtering out websites you don't want your kids to visit.
* **Smart phones and tablets-** Some mobile devices come with basic parental controls -- but the options vary a lot depending on what you have. You can also download apps such as [Bark](https://www.bark.us/),[Limitly](http://pumpic.com/limitly-parental-app/), and [TeenSafe](http://www.teensafe.com/)to track and control online activity, including text messaging and social media. If you're an Amazon user, Kindle Fire tablets come preloaded with Kindle FreeTime parental controls.

**14. Safe QR Code-** QR code (or Quick Response code) is a matrix bar code which can be read by an imaging device (camera) and then processed to read its data.

**How can we secure our app from a malicious QR code?**

* **Don’t scan QR codes in the form of stickers placed randomly on walls.**
* **Be extra careful if your smartphone works on the Android mobile operating system-**
* **Install a mobile security app right away.**

**15. Content Filter- Content-control software** is [software](https://en.wikipedia.org/wiki/Software) designed to restrict or control the content a reader is authorised to access, especially when utilised to restrict material delivered over the [Internet](https://en.wikipedia.org/wiki/Internet) via the [Web](https://en.wikipedia.org/wiki/World_Wide_Web), [e-mail](https://en.wikipedia.org/wiki/E-mail), or other means. Content-control software determines what content will be available or perhaps more often what content will be blocked.

**16. Firewall- already discussed in previous doc.**

**17. App Blacklisting- It** is a network administration practice used to prevent the execution of undesirable programs.  Such programs include not only those known to contain security threats or vulnerabilities but also those that are deemed inappropriate within a given organization.

**How it works?**

* Blacklisting works by maintaining a list of applications that are to be denied system access and preventing them from installing or running.

**18. Cloud Backup-** is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site [server](http://whatis.techtarget.com/definition/server). The server is usually hosted by a [third-party service provider](http://searchcloudstorage.techtarget.com/definition/cloud-storage-providers), who charges the backup customer a fee based on capacity, [bandwidth](http://searchenterprisewan.techtarget.com/definition/bandwidth) or number of users

Examples of cloud data backup vendor options include the following:

* **Acronis** offers Backup to Cloud, a cloud subscription add-on to its other backup plans to create a [hybrid cloud](http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud) and local backup service. Acronis Backup to Cloud protects and can recover files, folders, applications or a complete system.
* **Unitrends** allows customers to back up indefinitely to its [private cloud](http://searchcloudcomputing.techtarget.com/definition/private-cloud) with Forever Cloud. It retains the most recent successful backups from the previous four weeks, 12 months and a comprehensive backup for the year.

**19. Anti-virus-** Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

**How it works?**

* Scan specific files or directories for any malware or known malicious patterns
* Allow you to schedule scans to automatically run for you
* Allow you to initiate a scan of a specific file or of your computer, or of a CD or flash drive at any time.
* Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.

20. Remote wipe- Remote [wipe](http://whatis.techtarget.com/definition/wipe) is a security feature that allows a network administrator or device owner to send a command to a computing device and delete data.   A remote wipe may delete data in selected folders, repeatedly overwrite stored data to prevent forensic recovery, return the device to factory settings or remove all programming on the device, essentially turning it into a brick, meaning that it is no longer of any use to anyone.

How it works?

* **Start with a strong password**
* **Combine passwords with full-device encryption.**
* **Beware of data left behind after device wipe.**

**21. Security scan-** A [**web application security**](https://en.wikipedia.org/wiki/Web_application_security)**scanner** is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses. It performs a [black-box](https://en.wikipedia.org/wiki/Black-box) test.

**Examples:**

* The free Web application vulnerability scanner from [Vega](http://subgraph.com/products.html) runs on Linux, OS X and Windows. The open source tool includes an automated scanner for quick tests and an intercepting proxy to inspect HTTP requests and responses.
* The[Netsparker Community Edition](https://www.mavitunasecurity.com/communityedition/) scanner gives possible solutions for any issues it finds.
* [Skipfish](http://code.google.com/p/skipfish/) is a tool that can spot a range of flaws. It works slightly differently than most scanners by preparing an interactive annotated sitemap, which provides a great starting point for a deeper security assessment.
* Another useful scanner to try is [Wapiti](http://www.ict-romulus.eu/web/wapiti/home), which tests for a variety of injection-based vulnerabilities. However, it has to be run from a terminal, as it currently lacks a GUI.

22. Threat alert-