

Bachelor thesis
Computing Science



Radboud University

Supply of and Demand for Information Regarding Update Support when Buying Smartphones

Author:

Lisa Kalse
s4338340

Supervisor/assessor:

dr. ir. Eelco Herder
eelcoherder@cs.ru.nl

Second assessor:

dr. Hanna Schraffenberger
hanna.schraffenberger@ru.nl

19 jul. 2021

Abstract

Smartphones only have update support for a limited time. It is important that consumers know this when buying a new smartphone, since out of date software is a big security risk. Are the users aware of this limited update support and do shops inform their customers well enough on this topic? That's why this research aims to answer the question: What is the supply of and demand for information regarding update support when buying smartphones?

Our hypothesis is that the prospective buyers of smartphones do not care for information about update support, since security awareness is low. We also suspect that the supply of information corresponds with the demand, resulting in very little information in the shops regarding update support.

If we look at the scientific context of this research we see fields like update policy, smartphone security and security awareness. Studies about update policies and smartphone security show that many people have outdated phones which means that they are at an increased risk of getting malware. Studies about security awareness show that many people do have insufficient smartphone security awareness. Studies in consumer behaviour show that consumers in different countries value different things in their smartphones.

This research aims to find out if consumers are making informed decisions when buying a phone regarding update support. Therefore we look at both what information they can find and what information they want to find.

We found that most webshops supply barely any information. The physical stores almost only supply information when consumers ask questions to a salesperson. This means that the information supply relies on the awareness of the consumer. We see that 75-80% don't know how long their phone has update support and people would like to receive more information. Consumers value security updates more than version updates, but do value both greatly. So we see that consumers find updates very important but also recognize that they are quite unaware of the update support and do not pay much attention to it when buying a new smartphone.

Contents

Abstract	1
1 Introduction	4
2 Preliminaries	6
2.1 Android updates	6
2.1.1 Original Equipment Manufacturer	6
2.1.2 Google Play System Update	6
2.1.3 Android version update	7
2.1.4 Security update	7
2.1.5 App update	7
2.2 iOS updates	8
2.2.1 Version and security update	8
2.2.2 App update	8
3 Related Work	9
3.1 Update landscape	9
3.1.1 Update policies	9
3.1.1.1 Android	9
3.1.1.2 iOS	10
3.1.2 Versions currently in use	10
3.1.2.1 Android	11
3.1.2.2 iOS	11
3.2 Security risks	12
3.2.1 Vulnerabilities	12
3.2.1.1 Number of fixes per patch	12
3.2.1.2 Severity vulnerabilities	13
3.2.2 Attacks	14
3.2.2.1 Number of attacks per year	14
3.2.2.2 Kinds of attacks	14
3.2.3 Attack prevention by updating	15
3.2.3.1 Version update	15
3.2.3.2 Security update	15
3.2.3.3 App update	15
3.3 User awareness	15
3.3.1 Smartphone security awareness	16
3.3.2 Consumer behaviour	16
4 Research	18
4.1 Method	18
4.1.1 Information supply webshops	18
4.1.2 Physical store visit	18
4.1.3 Survey	18
4.2 Results	19
4.2.1 Webshops	19
4.2.1.1 Coolblue	20
4.2.1.2 Mediamarkt	21

4.2.1.3 Belsimpel	22
4.2.1.4 Bol.com	23
4.2.1.5 BCC	24
4.2.1.6 Summary	24
4.2.2 Physical stores	25
4.2.2.1 Display	25
4.2.2.2 Salesperson	25
4.2.3 Survey	26
4.2.3.1 Store visitation	26
4.2.3.2 Shop information	26
4.2.3.3 Update importance	27
4.2.3.4 Update support duration awareness	29
5 Discussion	33
5.1 Sub-questions	33
5.1.1 How easily can consumers find information about update support in web shops?	33
5.1.2 How easily can consumers find information about update support in physical stores?	33
5.1.3 How much information do consumers want when buying a new smartphone?	34
5.1.4 How important is version update support to consumers when buying a new smartphone?	34
5.1.5 How important is security update support to consumers when buying a new smartphone?	34
5.1.6 Are consumers aware of the limited update support?	34
5.2 Implications	35
5.2.1 Webshops	35
5.2.2 Physical stores	35
5.2.3 Consumers	35
5.3 Limitations	36
5.3.1 Webshops and physical stores	36
5.3.2 Survey	36
5.3.3 Related Research	36
5.4 Future directions	36
5.4.1 Improve survey participants	36
5.4.2 Improve physical store visits	36
5.4.3 Research shopping experience regarding update support	37
5.4.4 Causal relation	37
6 Conclusions	38
Bibliography	39
Appendix	45
Appendix A. Webshops	45
Coolblue	45
Mediamarkt	46
Belsimpel	47
Bol.com	48
BCC	48
Appendix B. Survey	50

1 Introduction

About 90% of the Dutch population has a smartphone (We Are Social Ltd & Hootsuite Inc, 2018). On average a consumer uses a smartphone for 3 years before buying a new one (Techredactie, 2020). Most smartphones receive only about 2 to 3 years of software and security updates, so in a certain way they have some kind of “expiration date”. Seeing that the average consumer keeps phones for as long as the update support of a new phone lasts, most people would have to buy their phone shortly after the release date. Otherwise they would be using a relatively vulnerable smartphone. This leads to this paper's research question: What is the supply of and demand for information regarding update support when buying smartphones?

Bring Your Own Device (BYOD) is becoming increasingly popular, making smartphone security not only a personal issue but a professional one too. Some are even referring to BYOD as “Bring Your Own Danger” (Disterer & Kleiner, 2013).

Once a phone's software is out-of-date it becomes more vulnerable to attacks. The level of vulnerability will become worse as time goes on. The vulnerabilities are announced every time a security patch is released. Not all vulnerabilities will actively be exploited at the time of announcement. Making the vulnerabilities known could result in hackers making use of that vulnerability. For the above stated reason one should always try to keep their software up-to-date. And since phones have update support for a limited time, it is important that people know about update support when buying a phone.

This research aims to get meta-awareness about consumer awareness. Once we know where the issue in awareness lies, this insight might help both consumers and stores that sell smartphones.

A lot of research has been conducted on the security awareness of smartphone users and the wants of smartphone consumers. However, there seems to be no research that looks at both the supply of and demand for information about version and security updates when buying smartphones. We will focus on consumers in the Netherlands.

The average consumer uses Android phones for about 3 years whereas iPhones are used for 4 years. A possible explanation for this disparity could be the duration of the update support (Techredactie, 2020). The average Android phone has 3 years of update support, whereas iPhones have about 5 years of support.

In order to answer this paper's research question, we will answer the following questions:

- How easily can consumers find information about update support in web shops?
- How easily can consumers find information about update support in physical stores?
- How much information do consumers want when buying a new smartphone?
- How important is version update support to consumers when buying a new smartphone?
- How important is security update support to consumers when buying a new smartphone?
- Are consumers aware of the limited update support?

For the supply part of the question, we will take a look at the top 5 most visited web shops and visit one physical store. For the demand part we will conduct a survey. After having analyzed both information sets, we can identify any problems that exist.

There are about three different fields of research that cross this research. We will discuss them in depth in chapter 3. The first field is research about smartphone updates. Here we will see how many actively used smartphones run older versions of iOS and Android. We will also dive into update policies.

The second field is smartphone security. Here we dive into the result of these versions in use and update policies. Kaspersky shows that outdated smartphones are at a higher risk of getting malware. Garg et al. show how many vulnerabilities get patched by the security updates and the severity of them. Kaspersky shows the effects of the attacks that result from these vulnerabilities.

The last field is smartphone security awareness. To see how people perceive these security risks. Watson & Zheng show that IT trained people are more security aware and more likely to follow security recommendations. Koyuncu & Pusatli show that overall smartphone security awareness is low, especially in young (<21) and older (>50). People who are trained in IT or are highly educated, have a higher level of security awareness. We will also discuss how smartphone security awareness translates into consumer behaviour. Ndibwile et al. show that people look for cheap phones in Tanzania and in Japan people look for good batteries. This shows that different countries have different priorities when it comes to buying phones.

In chapter 2, the preliminaries, we will define the different kinds of updates. In chapter 3 we will discuss related work. In chapter 4 we will dive into the research, explaining the method and results. Chapter 5 is the discussion and in chapter 6 we will show the conclusion.

2 Preliminaries

There are two operating systems that have almost all of the smartphone market. These are Android (87%) and iOS (13%) (O'Dea, 2021). Since both operating systems have different ways of updating, we will explain how both systems work in this regard. We will define different kinds of updates, so that we can use these definitions throughout the rest of this thesis.

2.1 Android updates

There are different kinds of updates on Android phones. We will first dive into Original Equipment Manufacturers (OEMs), because they are in charge of some of the updates. Then we will explain more about Google Play System Updates, Android version updates, security updates and app updates.

2.1.1 Original Equipment Manufacturer

In order to look at how the different kinds of Android updates work, we first need to look at Original Equipment Manufacturers. They are important, because they are responsible for some of the updates. Since Android is open and free, a lot of smartphone manufacturers make use of Android. Concurrently there are about 6 big OEMs and some small ones (O'Dea, 2021). OEMs place either “vanilla” Android on their smartphones or, more commonly, fork Android to make their own version of the OS. In order for Android to be successful, there needs to be cooperation between them and the OEMs.

OEMs are in charge of firmware updates. Firmware is a specific type of software that directly controls the hardware. Firmware is the layer between hardware and OS. Firmware is stored on the hardware component it controls. OEMs are also in charge of the OS, if they use their own version of Android.

2.1.2 Google Play System Update

Google had a problem in 2015 with a bug in Stagefright found by Joshua Drake of Zimperium (Avraham, 2015). One of the biggest issues was that Google could not fix the Google Play Services component in Android to fix this, which is a patchwork solution Google often used (Hoffman, 2015). This means that they had to wait for the over-the-air firmware update, which would take a long time.

The problem was that this part of the software was managed by the OEM. Since more devices than just Google devices run Android, Google could not fix this problem on its own. After this incident Google introduced Google Play System Update, which takes care of 12 core components. Now Google can update these 12 components without a full firmware update or involving the manufacturer (Fedewa, 2021).

This feature, called Project Mainline, was introduced in Android 10, which means that 8,2% of the android users benefit from this feature. By modularizing media components, they can now patch nearly 40% of the recently patched vulnerabilities themselves, instead of having to wait for the OEM (Ghuloum, 2019).

This is the kind of update that is out of the scope of this research. This is because we can not find a limited support time for these updates. We suspect that there is no limitation on the support time due to the nature of these updates. They are fully controlled by Google

and fit all Android phones that can run Android 10 and higher. Therefore, it doesn't matter when you buy the phone and that is why it is not interesting for this research.

2.1.3 Android version update

When a new major version releases, new functionality is added to Android. This ranges from a fresh look of the UI to security functionality. For example, there is also an increased number of updatable core OS components in Google Play from 12 to 21 (Cuthbertson, 2020). Android releases about 1 version upgrade each year. (*Android Version History*, 2021)

For phones that have a special version of Android, made by the OEM, the version upgrade can take several months. For example, Xiaomi has their own OS named MIUI. Version 12.5 is the first version of MIUI to be a fork of Android 11. Android 11 came out on september 2020 and MIUI 12.5 in march 2021. With a new Android version releasing every year, this is a significant delay.

2.1.4 Security update

Each month the Android Open Source Project (AOSP) posts an Android security bulletin. In these bulletins they post the vulnerabilities with their own code (CVE) and a patch. These vulnerabilities come from the AOSP, the upstream Linux kernel, and system-on-chip (SOC) manufacturers and get their CVEs from a CVE Numbering Authority. (*Android Security Bulletins*, 2021)

As mentioned in 2.1.1, the OEMs have their own version of Android and each phone has its own hardware. This means that each of them needs to test and alter the security patches so that they will work on their own phones. On top of that, because each of the operating systems is different, they might have their own security holes to patch. Since Google has all the links in the chain of their own phones, Google Pixel phones are all updated very quickly after the security bulletin release each month. It takes quite some time for vulnerabilities to be patched. It all begins with Google posting CVE's 2-3 months after discovering them and then it takes 2-3 more months before OEMs release the patch (Zhang et al., 2021).

2.1.5 App update

There are three ways to update your apps:

- Update all apps automatically
- Update individual apps automatically
- Update all apps manually

(Google, n.d.)

In this research we will not look at app updates, because the update support of apps is directly tied to the Android version. We will look at the version update support instead, since it strictly encompasses more.

2.2 iOS updates

2.2.1 Version and security update

iOS is quite different from Android, since it is a closed system. Apple has full control of the hardware and software that goes into iPhones. iOS has their OS and security updates bundled into 1 update. For example their most recent version, 14.6 comes with security patches (Apple, 2021), bug fixes and added functionality (Apple, n.d.). But we will make the same distinction as in Android and will call the functionality part of the update, the version update. And we will call the CVE patches part of the update, the security update. We have chosen this approach, because we want to make a distinction between security and functionality and see what the consumers value and why.

2.2.2 App update

iOS has the App Store where users can download apps. These apps can be updated manually or automatically. If you choose to update manually, you can update through the App Store by clicking “Update” next to an app to update only that app or click “Update All” to update all of your apps. (Apple, 2021)

Similar to Android, app update support is tied to the OS version, so we will not look into app updates specifically.

3 Related Work

First we will take a look at the update landscape. Then we can take a look at the risks that come with the current update landscape. And lastly we will see how aware users are of the update landscape and the security risks.

3.1 Update landscape

We will first take a look into what update policies Android and iOS have. Then we will look at the effect these policies have on the versions currently in use.

3.1.1 Update policies

Support periods and updates schedules vary highly. OEMs make their update support decisions based on:

- Device age
- Device popularity
- Cost of support
- Partner input
- Severity of vulnerability
- Regularly scheduled releases
- Device price

(Federal Trade Commission, 2018)

Some data suggests that support period length for some manufacturers is more closely related with device price and age than popularity. New phones are prioritized in update support. It was not part of any update policy to notify users of when their update support stops. (Federal Trade Commission, 2018)

Some carriers, for example Microsoft, Samsung and Google, clearly state the end of support date on their own websites. For some OEMs like LG, you need to go to a model first and then select a carrier. Chances are that you only get information about the current version, without the end of support date stated anywhere. A few OEM websites do mention the speed of the update delivery. (Federal Trade Commission, 2018)

We chose to not include these websites in our research, because we don't expect consumers to visit these sites when looking to buy a smartphone.

3.1.1.1 Android

The Verge obtained a contract that requires Android OEMs to install updates for at least 2 years. This contract started on January 31st 2019. They require partners to provide at least four security updates within the first year of the phone's launch. The second year requires security updates too, although there is no specific minimum for that year. OEMs that do not follow these requirements, do not get the license to use the Google suite for its apps. (Kastrenakes & Brandom, 2018)

There is also a more strict contract that Google has with partners named Android One. These phones promise, next to the standard security updates for 2 years, to deploy a security update each month and 2 years of OS upgrades. (Android, n.d.)

Some OEMs have support for longer than these 2 years. For example, we can see that Samsung pledges to update the version for at least 3 generations (Samsung, 2020) and

deploy 4 years of security updates (Samsung, 2021). The update frequency and update speed also widely varies between OEMs or even models.

3.1.1.2 iOS

From the iPhone 5s that came out in 2013 onward, all iPhones have received 5 years of version upgrades. The iPhone 6s is going to be the first generation to have 7 iOS versions. (Richter, 2021) We can see that the iPhone 5s is still receiving security updates up to this day. The newest OS is getting an update about every month. (*Apple Security Updates*, 2021)



Figure 1. Historical iOS compatibility of every iPhone model to date. (Richter, 2021)

3.1.2 Versions currently in use

Many people wait very long or don't install their updates at all and rather buy a new phone (Mansfield-Devine, 2012). We will take a closer look at the differences between Android and iOS.

3.1.2.1 Android

In figure 2 we can see the big disadvantage of not having the whole chain in your own possession. Only 53,5% of the users have Android Oreo 8.1 or newer. That means that almost half of all active Android users have an OS that predates December 5, 2017, which is over 3 years ago. Android versions below 8.0 are not supported anymore, which means they will not receive security updates. (End of Life, n.d.)

ANDROID PLATFORM VERSION	API LEVEL	CUMULATIVE DISTRIBUTION
4.0 Ice Cream Sandwich	15	
4.1 Jelly Bean	16	99.8%
4.2 Jelly Bean	17	99.2%
4.3 Jelly Bean	18	98.4%
4.4 KitKat	19	98.1%
5.0 Lollipop	21	94.1%
5.1 Lollipop	22	92.3%
6.0 Marshmallow	23	84.9%
7.0 Nougat	24	73.7%
7.1 Nougat	25	66.2%
8.0 Oreo	26	60.8%
8.1 Oreo	27	53.5%
9.0 Pie	28	39.5%
10. Android 10	29	8.2%

Figure 2. Android version distribution. (Google, 2021)

3.1.2.2 iOS

In figure 1 we can see the usage of iOS versions. If we compare iOS with Android, we can see that a way bigger group of people is on the newest version. 86% of all iOS users run iOS 14 and 12% iOS 13, which was released on September 19, 2019. This means that 98% has an OS that is a maximum of 2 years old, which is quite a big contrast compared to Android.

iOS and iPadOS Usage

As measured by the App Store on February 24, 2021.

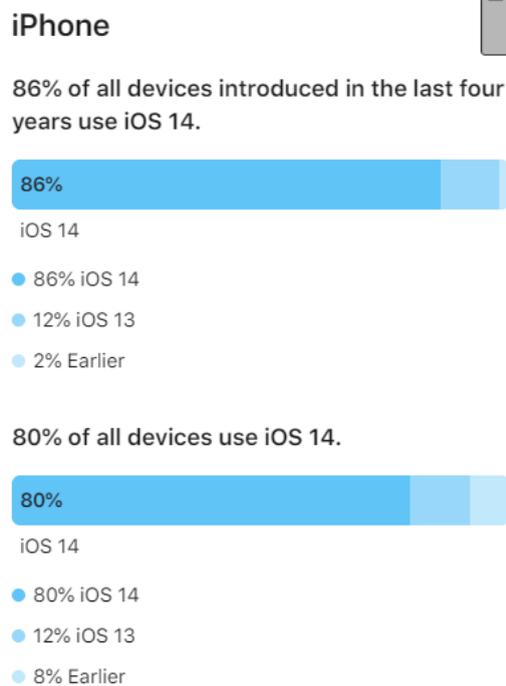


Figure 3. iOS Version Usage. (Apple, n.d.)

3.2 Security risks

We will first take a look at vulnerabilities. Then we will take a look at what attacks are being executed that make use of these vulnerabilities. Lastly we will explain how different updates can help defend against these attacks.

3.2.1 Vulnerabilities

We will first look at how many vulnerabilities are found and how severe the vulnerabilities are.

3.2.1.1 Number of fixes per patch

As mentioned in the preliminaries, Common Vulnerabilities and Exposures (CVE) is a list of security flaws. Google and Apple release the list of vulnerabilities once they have found a patch for them. They register their CVE at a CVE Numbering Authority like MITRE.

As we can see from the study of Garg & Baliyan, in 2019 Android posted 414 CVEs and iOS 156. According to them the decrease in CVEs can be attributed to the use of machine learning and deep learning algorithms.

This means that if your smartphone missed a year of updates in 2019, you have around 156 - 414 security flaws that are known to attackers, as seen in figure 4.

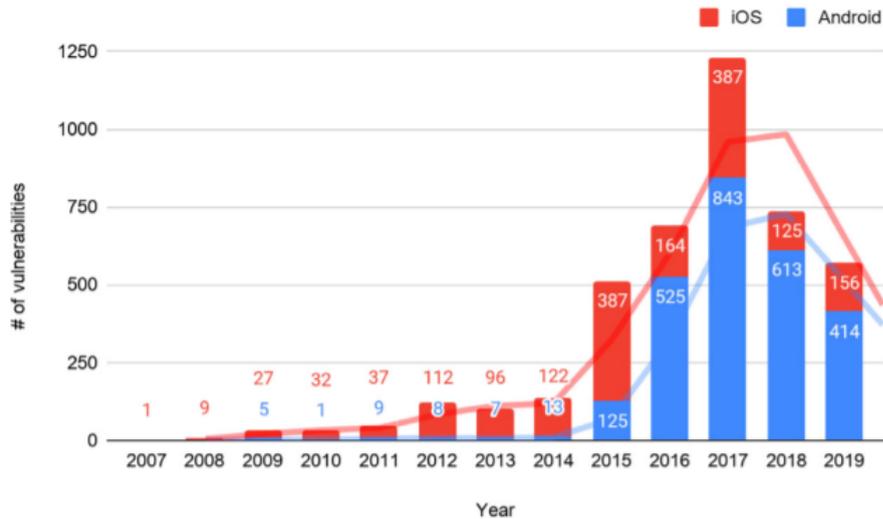


Figure 4. Trend of Android & iOS vulnerabilities for 2007-2019. (Garg & Baliyan, 2021)

This does beg the question, how bad are these vulnerabilities?

3.2.1.2 Severity vulnerabilities

Let's take a look at how severe the vulnerabilities mentioned before are. Garg & Baliyan measured their severity score by looking at the impact on confidentiality, integrity and availability, access level and access complexity. This is the same as CVSS v2, but without the authentication part.

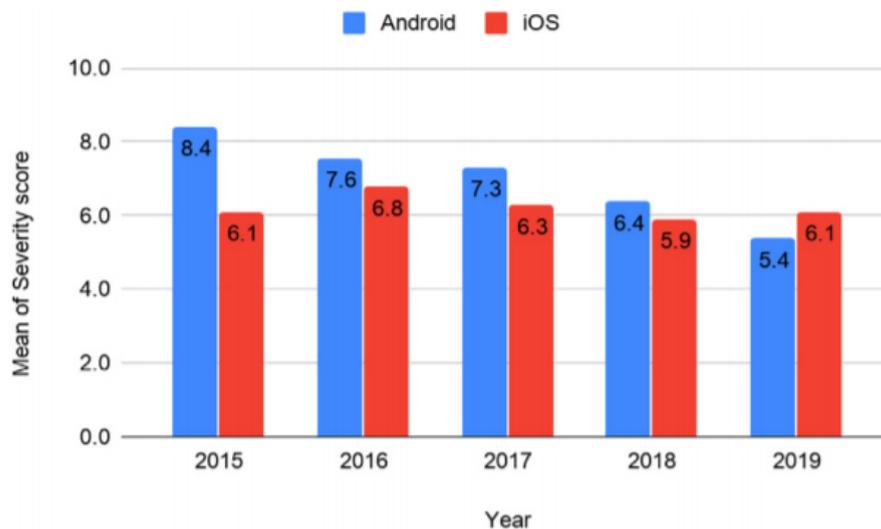


Figure 5. Mean severity scores of Android & iOS vulnerabilities. (Garg & Baliyan, 2021)

Here we can see that the mean severity of iOS vulnerabilities has stayed roughly the same from 2015 to 2019 and that Android is on the decline. Still, 5,4 and 6,1 are medium severity scores. Now that we know how severe vulnerabilities are, let us take a look at the attacks that make use of these vulnerabilities.

3.2.2 Attacks

First we will take a look at the amount of attacks. Then we will take a look at different kinds of attacks.

3.2.2.1 Number of attacks per year

In 2016 Kaspersky Lab detected 8,526,221 malicious installation packages. From the beginning of January till the end of December 2016, Kaspersky Lab registered nearly 40 million attacks by malicious mobile software and protected 4,018,234 unique users of Android-based devices. (Kaspersky Lab, 2016)

The following figure shows that the Netherlands make up less than 9,99% of the unique victims in 2016.

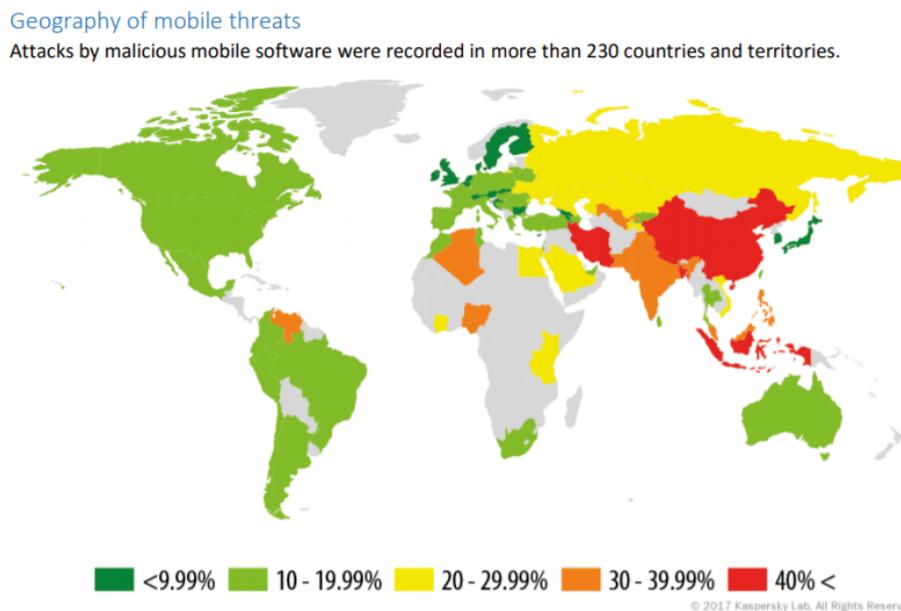


Figure 6. The geography of mobile threats by number of attacked users. (Kaspersky Lab, 2016)

3.2.2.2 Kinds of attacks

An attack usually makes use of multiple exploits. We can roughly categorize these attacks into three categories: Malware (82,17%), adware (14,62) and riskware (3,21) (Chebyshev, 2021). But what do these terms mean?

Adware is a kind of software that places advertisements on your device. It tries to make you install additional software, click on or view ads in order to earn money (Kaspersky, n.d.). It also tries to get more information about you, like browsing history, in order to sell that information. Adware can be very annoying, because your phone can become practically unusable from the amount of ads.

Riskware is the set of legitimate programs that have a vulnerability that can be exploited (Kaspersky, n.d.). For example, some view weather apps as riskware. If a weather app is not secure, hackers can get the GPS data from the user. The use of GPS data in a weather app is legitimate, but if the app is vulnerable, it becomes riskware. A version update might help with minimizing exposure to riskware. For example, Android 11 automatically revokes permission after not using an app for a few months. But updating apps regularly might be the best way to combat riskware.

Malware is an umbrella term. It stands for “malicious malware” that can do things like:

- Deletion countermeasures
- Detection countermeasures
- Privilege escalation
- etc.

Adware is a specific type of malware. One could argue that riskware is not malware, because it was not meant to be malicious, but in general it is viewed as malware.

One of the things popular malware does is gain super-user privileges. With these privileges, hackers can for example (Chebyshev, 2021)(Kaspersky Lab, 2016):

- Download advertising applications
- Make it impossible to use the smartphone
- Buy apps via Google Play
- Install other malware
- Steal credential information of for example Facebook

In short, there are many serious attacks that exploit vulnerabilities on smartphones. These vulnerabilities can come from the OS software and from apps. These attacks can do some serious damage. They can make your phone unusable, spend your money or steal your credentials.

3.2.3 Attack prevention by updating

3.2.3.1 Version update

In 2016, the most prevalent kind of attack uses vulnerabilities that were known to have been patched. So the majority of victims were smartphone users with outdated OS versions. Through these vulnerabilities, attackers were able to escalate their privileges to gain super-user privileges. (Kaspersky Lab, 2016) Version updates also help against riskware and adware (Kaspersky, n.d.) (Kaspersky, n.d.).

3.2.3.2 Security update

Security updates patch many exploits like gaining privileges, code execution and denial of service. It patches many exploits that form the building blocks of an attack.

3.2.3.3 App update

App updates could help against riskware. Unsupported apps are more often probed by hackers for vulnerabilities in hopes of getting personal data (Kaspersky, n.d.). Updating the app could reduce both this risk and patch any security holes the app might have. App updates also help against adware (Kaspersky, n.d.).

3.3 User awareness

There are two parts of user awareness that tie into this research. The first part is security awareness and the second part is how this awareness manifests itself in consumer behaviour.

3.3.1 Smartphone security awareness

This research fits into the broader context of user security awareness. The update support has a direct influence on the security of the smartphone. If the user is aware about the update support, they can take active steps to improve their security. With security awareness we mean the awareness of security risks and recommendations.

Research found that users with a strong IT familiarity are more security aware and follow more security recommendations than those without a strong IT familiarity (Watson & Zheng, 2017).

The study from Koyuncu and Pusatli on security awareness among smartphone users, pointed out that:

1. Overall level of security awareness is not satisfactory.
2. Older (>50) and younger (<21) people have the lowest awareness level.
3. Higher educated people have a higher level of awareness.
4. People trained in IT have a higher level of awareness.
5. Smartphone users have a low security awareness level.

(Koyuncu & Pusatli, 2019)

Ndibwile et al. show that security awareness does not necessarily translate into acting in accordance with that knowledge. For example, Japanese who are equally security aware as Tanzanians, mention security as the major motivation for updating. Tanzanians mention “improved performance and user interface”. Updating the OS depends much more on factors like trying to save phone battery, income and needing the smartphone for a hotspot. (Ndibwile et al., 2018)

So overall we can conclude that research points out that smartphone security awareness is still at a low level and educating people helps to raise the level of security awareness. This research tries to aid in that endeavor. But we also see that awareness does not necessarily directly translate into behaviour.

3.3.2 Consumer behaviour

We can also see security awareness reflected in consumer behaviour.

Update support is also very important when buying a refurbished smartphone. Since the phones are older, you will probably have less update support compared to a new phone. In table 1 we see that update support ranked quite high, with “Guaranteed software updates” being ranked number 2.

Incentives	Category	Mean	SD
Upgraded battery	Product	6.44	0.94
Guaranteed software updates	Product	6.25	0.99
Upgraded performance	Product	5.91	1.24
Classification system	Information	5.69	1.10
Info on refurbishing process	Information	5.65	1.24
Quality certification	Information	5.50	1.39
Upgraded internal storage	Product	5.39	1.45
Upgraded screen	Product	5.34	1.45
Unbiased testimonials	Information	5.16	1.45
Upgraded camera	Product	5.13	1.62
Extendable protection period	Service	4.99	1.64
More innovative features	Product	4.84	1.78
Extended trial period	Service	4.57	1.82
Extendable protection coverage	Service	4.26	1.82
Updated appearance	Product	3.96	1.82
Leasing option	Service	3.64	2.08

Table 1. An overview of the proposed incentives arranged from having the most to least impact on consumers’ purchase intention. (Mugge et al., 2017)

Consumers seem to focus only on basic features that are advertised or recommended by other people. The basic specs are the focus and they are not being informed on security risks or recommendations. (Khan & Kongar, 2014)

We see that there seems to be a difference between the findings of Khan & Kongar and Mugge et al. It might be that one of the researches is wrong. It could also be that a lot has changed in the 3 years between these researches. Or maybe people who buy refurbished phones are more focussed on software updates compared to people who buy new phones. This would make sense, because the refurbished phones are older, which means that they probably get less update support.

4 Research

4.1 Method

The method consists of three parts. In the first part we will take a look at the most visited websites for buying smartphones. Here we will take a look at what information is given about the update support. In the second part we will take a look at physical stores. Here we will take a look at the shopping layout and talk with a salesperson to find out more about their experiences. In the third part we will take a look at the survey we have conducted.

4.1.1 Information supply webshops

In order to determine how good the information supply is in the webshops, we will take a closer look at the 5 most visited webshops for smartphones. We have picked these websites by using Google by searching for “telefoon kopen”, since we want to know how well specifically Dutch websites do. These are the 5 websites:

1. Coolblue
2. Mediamarkt
3. Belsimpel
4. Bol.com
5. BCC

On these websites we will take the top 10 smartphones that appear on top of the filtered “meest verkocht”(most sold) or similar (see Appendix A). We will take a look at what information is given and check whether the information is correct.

4.1.2 Physical store visit

Since it is not feasible to visit a lot of stores and since we want to limit our movement due to the coronavirus, we will only visit one store. Since the BCC operates under a certain formula, one store is representative of all 62 Dutch stores in the chain. This is not representative of all different kinds of stores, but it will hopefully give us some insights.

We will investigate the presentation of the smartphones in the store and speak to the salesperson that is in charge of the smartphone section of the store. By investigating the presentation we can see what information a customer gets without asking for any help. By speaking to the salesperson we can see what information a customer gets when they do ask for help. Speaking to the salesperson might also give us more insights as to the information demand of the customer. Unfortunately, we were not allowed to record the interview.

4.1.3 Survey

We want to see whether consumers are aware of the limited duration of update support and how big of a role it plays when buying a new phone. This is why we conducted a survey. See Appendix B for the contents of the survey.

The survey has initially been sent to fellow students, family, and friends through WhatsApp. We have asked them to share it in their social circles in hopes to get a more representative picture of all smartphone consumers in the Netherlands. This means that we have a convenience sample.

We have stressed that the survey is conducted anonymously and that they will not get judged on the answers they give. You can read the full text of the survey in Appendix B. We felt like it was important to stress the anonymity, because people could adjust their answers in order to feel less ashamed of their (self-perceived) lack of awareness. We also asked them not to look up any info and go with their gut feeling.

We conducted this survey online using LimeSurvey. We looked at the sub-questions we had and came up with matching questions to ask our participants. We then added some more questions to verify answers. For example, after we asked participants whether they knew how long their update support would last, we asked them to try and name the exact duration. We tested these questions on family members, who we then excluded from the final survey. Some questions were unclear, so we had to rephrase them and we got a good idea of how long the survey would take. We also added more in depth questions. For example, when we asked them how important they thought certain updates were, we also asked them why they thought that. We tried to ask enough questions to get a clear view of the information needs and awareness of the participants, but not too much so we could keep the survey short in hopes of attracting more participants.

We added short descriptions of our definitions of version updates and security updates. At the end we also asked our participants to share the survey within their social circle.

4.2 Results

4.2.1 Webshops

We will look at the 5 most visited webshops in the Netherlands:

- Coolblue
- Mediamarkt
- Belsimpel
- Bol.com
- BCC

For each webshop we will take a look at what information we can find about update support.

We will focus on the following 7 things:

- Included OS version
- Introduction date
- Update duration
- Update end date
- Update frequency
- Interpretation information
- Correct information

In the first 8 things we will check for the presence of the information and lastly we will check whether that information is correct or not. For each webshop we will include some screenshots to illustrate how the information is presented.

4.2.1.1 Coolblue

As seen in figure 7, coolblue has a deliberate overview of update policies. They make the distinction between OS updates and security updates. The information is up-to-date and mostly accurate. It is easy to find. You have to press “specificaties” (specifications) or scroll down until you reach the specifications. Then you will find all the update support information under “OS and update policy”.

Besturingssysteem en updatebeleid	
 Introductiejaar	2020
 Introductiemaand	November
 Besturingssysteem	iOS
 iOS versie bij introductie	iOS 14
 Update mogelijk naar iOS versie	iOS 14
 Nieuwste iOS versie	✓
 Verwachte aantal resterende iOS updates	6
 Beoordeling resterende iOS updates	Standaard
 Verwachte frequentie beveiligingsupdates	Elk kwartaal
 Verwachte datum laatste beveiligingsupdate	Oktober 2025
 Beoordeling resterende beveiligingsupdates	Uitstekend
 Beoordeling updatebeleid	Zeer goed

Figure 7. OS and policy coolblue. (coolblue, n.d.)

They greatly help the consumer by giving a rating for how well the update policy is. This helps a lot with knowing how to interpret all of the other statistics that they give in the update policy overview. You can click on a bar to get more information. For example this is what you will see if you press on “Beoordeling updatebeleid” (evaluation update policy):

Beoordeling updatebeleid



Voor de beoordeling van het updatebeleid hebben we gekeken naar software updates en beveiligingsupdates. Software updates komen elk jaar uit en brengen grote vernieuwingen, waardoor je telefoon sneller wordt en nieuwe functies krijgt.

Beveiligingsupdates dichten de meest actuele veiligheidslekken en verschijnen meerdere keren per jaar. Omdat fabrikanten informatie over deze updates niet altijd delen, is deze beoordeling deels een verwachting. Hiervoor hebben we alle beschikbare informatie gecombineerd met historische data. We updaten deze beoordeling elke maand.



Matig

Deze telefoon is niet up-to-date en niet lang meer veilig. We verwachten dat je geen enkele software update meer krijgt. Als je nog beveiligingsupdates ontvangt, krijg je deze nog maar korter dan een jaar. Meestal duurt het ook nog eens lang voordat je deze ontvangt.

Standaard

We verwachten dat je nog 1 software update ontvangt, maar dit duurt nog minstens een 6 maanden nadat de update uitkomt. Ook ontvang je ofwel korter dan een jaar maandelijkse beveiligingsupdates, dan wel anderhalf jaar elke 3 maanden beveiligingsupdates.

Goed

Je krijgt nog minimaal 1 software update, maar vaak zelfs nog 2. Het duurt dan vaak wel 6 maanden of langer voordat je deze updates krijgt. Verder ontvang je nog 12 tot 24 maanden beveiligingsupdates. Deze ontvang je meestal binnen 3 maanden.

Zeer goed

We verwachten dat je nog minstens 2 software updates ontvangt. Deze installeer je vaak 3 maanden nadat deze uitkomen. Deze smartphones ontvangen tussen de 24 en 32 maanden elke maand een beveiligingsupdate.

Uitstekend

Jouw telefoon is voor lange tijd up-to-date en veilig. Je ontvangt nog minstens 2 software updates binnen 3 maanden nadat deze uitkomen. Verder installeer je nog minstens 30 maanden elke maand een beveiligingsupdate.

Figure 8. Explanation coolblue. (coolblue, n.d.)

All 10 smartphone web pages of coolblue we checked had complete and correct information and looked very much like Figure 7 and 8.

4.2.1.2 Mediamarkt

Mediamarkt shows the OS version that is included with the purchase of the smartphone directly underneath the photos.

Besturingssysteem: Android 10.0
Geheugencapaciteit: 128 GB
Specificaties camera: 64 + 12 + 5 + 5 megapixel
Beeldscherm diagonaal (cm/inch): 17.02 cm / 6.7 inch
Capaciteit batterij: 4500 mAh

Figure 9. Quick overview mobile specifications MediaMarkt. (MediaMarkt, n.d.)

If you open all the specifications, as seen in figure 10, then you also get to see the update policy. They clearly denote that the support duration starts at the introduction date of the smartphone, not the date of purchase.

UPDATEBELEID

✓ Modeljaar:	2020
✓ Introductiedatum:	2020-01-04
✓ Software-updates vanuit fabrikant:	ja
✓ Min. duur van software-updates vanaf productintroductie:	2 jaar
✓ Aanvullende update-informatie:	Geen aanvullende update-informatie
✓ Update policy:	Onbekend

Figure 10. Extensive overview mobile specifications MediaMarkt. (MediaMarkt, n.d.)

Unfortunately, the data is not always complete or correct. 9 out of 10 times it says “Update policy: Onbekend” (Update policy: Unknown) as shown above and 1 out of 10 times it says 2 years. For example, Samsung has announced that they will support their Galaxy phones for 4 years. Mediamarkt says that the phones will get a minimum of 2 years of support, but I will mark this as incorrect information, since more accurate information is available. On top of that, there is no distinction between version updates and security updates even though for some smartphones there seems to be a difference in support duration. It also does not mention anything about the frequency of the updates. They also do not help customers with the interpretation of the information, but that’s not necessary since they do not give much information that needs to be interpreted.

4.2.1.3 Belsimpel

Belsimpel has very minimal information for all 10 web pages we checked. It only mentions the included OS version in the short specifications:

Specificaties Apple iPhone 12 64GB Zwart

 146.7 x 71.5 x 7.4 mm 162 gram	 6.1 inch 2532x1170 pixels
 4096 MB Werkgeheugen Hexa-core processor	 5G-internet
 iOS Versie bij release: 14	 12 megapixels 4k video
 64 GB opslag Niet-uitbreidbaar	 Simlockvrij Geschikt voor alle providers

Figure 11. Belsimpel quick overview specifications. (Belsimpel, n.d.)

There are links to manuals, but they rarely ever mention something about the update policy. It sometimes mentions the “Besturingssysteem skin” (Operating system skin), which is the OEM’s own version of Android.

This information is quite hard to find, since you first have to go to the specifications and then click on “Meer specificaties” (More specifications). Here you can find the introduction date. You can also get a little bit more information about the included OS when

you hover the “i” as seen in figure 12, but it is still very little information. The kinds of information given about each phone was the same for all 10 web pages.

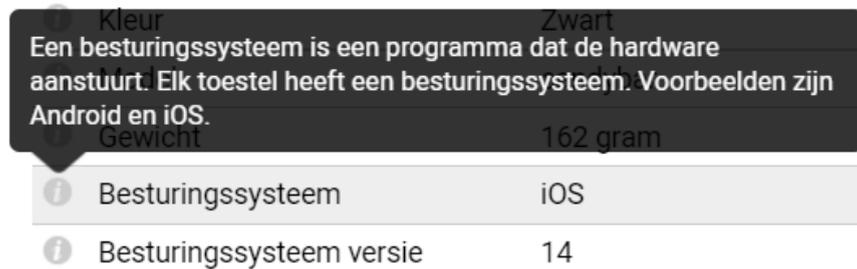


Figure 12. More information specifications Belsimpel. (Belsimpel, n.d.)

Belsimpel does not inform the consumer of the frequency of the updates, the duration and end date of the updates and does not help interpreting the information. All information on the 10 web pages is correct.

4.2.1.4 Bol.com

Bol.com is both a platform and a shop. This is the reason why we see a big difference in the amount of information supplied. Bol.com has correct and complete information for 7 out of 10 web pages, but with other models there is some information missing like the duration of support (1 out of 10) and the frequency of the security support (2 out of 10).

Let us take a look at one of the sales by bol.com themselves. The first bits of the specifications are already high up on the page. It mentions the year of release and the included OS. You can hover the “i” for more information as seen in figure 13.



Figure 13. More information specifications bol.com. (bol.com, n.d.)

It is very hard to get a good feeling of how good the update policy is. You cannot see all the required information at a glance, since it is split between “Introductie en ondersteuning” (Introduction and support) and “Overige kenmerken” (Other characteristics). It is also unclear whether “Ondersteuning met updates” (Update support) refers to OS version updates or security updates.

Introductie en ondersteuning

Introductiejaar	: 2021
Introductiemaand	: Maart
Ondersteuning met updates	: Minimaal 48 maanden na introductiedatum

Table 14. Introduction and support bol.com. (bol.com, n.d.)

Frequentie beveiligingsupdates	: Maandelijks
Verwachte laatste beveiligingsupdate	: Maart 2025

Figure 15. Other characteristics bol.com. (bol.com, n.d.)

Bol.com also sells refurbished smartphones. The information on these pages regarding update support are the same as the new smartphones.

4.2.1.5 BCC

The BCC often only shows the included OS. What is confusing is that the OS version is mentioned two times on the website. One time it shows it under the heading of “Minimale systeemeisen” (minimal system requirements) which is a bit unclear. And under “Software” it just presents the OS version as “10”, not specifying that it is “Android 10”.

Minimale systeemeisen

Besturingssysteem	Android 10.0
-------------------	--------------

Figure 16. Minimal system requirements specifications BCC. (BCC, n.d.)

Software

Besturingssysteem versie	10
--------------------------	----

Figure 17. Software specifications BCC. (BCC, n.d.)

There were 2 exceptions. 1 out of 10 displayed a different OS, Android Q Go. To users it might not be clear what this means, since most of the time the android version is followed by a number on the BCC website. 2 out of 10 web pages displayed only “Android” as the OS, without mentioning the version.

4.2.1.6 Summary

If we look at all these webshops, we can roughly summarize the results as following:

The yellow squares show that on some of the pages of the webshop the information is complete and on others it is not. Green shows that on all 10 web pages the information was complete and red shows that none of the web pages had complete information. The last row denotes whether the given information on all 10 web pages is correct (green), on some webpages correct (yellow) or on all pages incorrect (red).

	Coolblue	Mediamarkt	Belsimpel	bol.com	BCC
Included OS version	Green	Green	Green	Green	Yellow
Introduction date	Green	Green	Green	Green	Red
Update duration	Green	Yellow	Red	Yellow	Red
Update end date	Green	Yellow	Red	Yellow	Red
Update frequency	Green	Red	Red	Yellow	Red
Interpretation information	Green	Red	Red	Red	Red
Correct information	Green	Yellow	Green	Green	Green

Table 2. Information correctness and completeness in webshops.

4.2.2 Physical stores

For this part we visited a BCC. This is a non-representative sample. This part serves only to get an impression of physical stores. We looked at both the information on displays and the information you get by talking to the salesperson.

4.2.2.1 Display

The stand we visited had about 20 phones. Only 1 display next to an iPhone showed us what OS was included with the phone. Only 2 displays next to Huawei phones showed us that there were no Google apps on the phone, but that it did use AOSP with Huawei apps. All other phones had no information about the OS or update support.

4.2.2.2 Salesperson

When speaking with the salesperson, it became clear that they tailor the information they give based on the demand of the customer. This often results in barely any information being given, because people seem not to be aware of update support. They often do attend customers on the fact that if they buy a model that is from the previous year, that they will have one year less of update support. If somebody were to ask for update support, the salesperson says that most devices only have support for 2 years, but that Samsung might sometimes decide to support for a longer period of time.

If we take a look at what the salesperson reports about the customers we see the following. About 90% of customers do not know that there is limited update support. Almost nobody asks for more information about it. Many people, mostly elderly, walk into the store with a phone where half of the apps are not working anymore. Some people even have notifications on their phone that show that a version update is waiting. People have probably never clicked it, since they simply do not know what it is or what to do with it. People do not seem to connect half of their apps not working and a lack of updates. When people ask how long they will be able to use a new phone, they mostly focus on the duration of the battery, which degrades over time.

4.2.3 Survey

We have asked 15 questions to our respondents and we have grouped them together per subject so that we can compare the results. We have asked the respondents to try not to think too much about the answers and go with their gut feeling. We have received 124 responses, of which 86 were complete. We don't include the incomplete responses, since they will skew the results. We had anticipated that it would take about 2-4 minutes, which corresponds with the following timing data:

Average interview time: 4 min. 33 sec.

Median: 2 min. 20 sec.

4.2.3.1 Store visitation

We asked the respondents which kind(s) of store they visited when shopping for a smartphone. We can see in figure 18 that more people went shopping in webshops (78%) than in physical stores (31%). As we can see there is some overlap, which means that some people visited both kinds of stores.

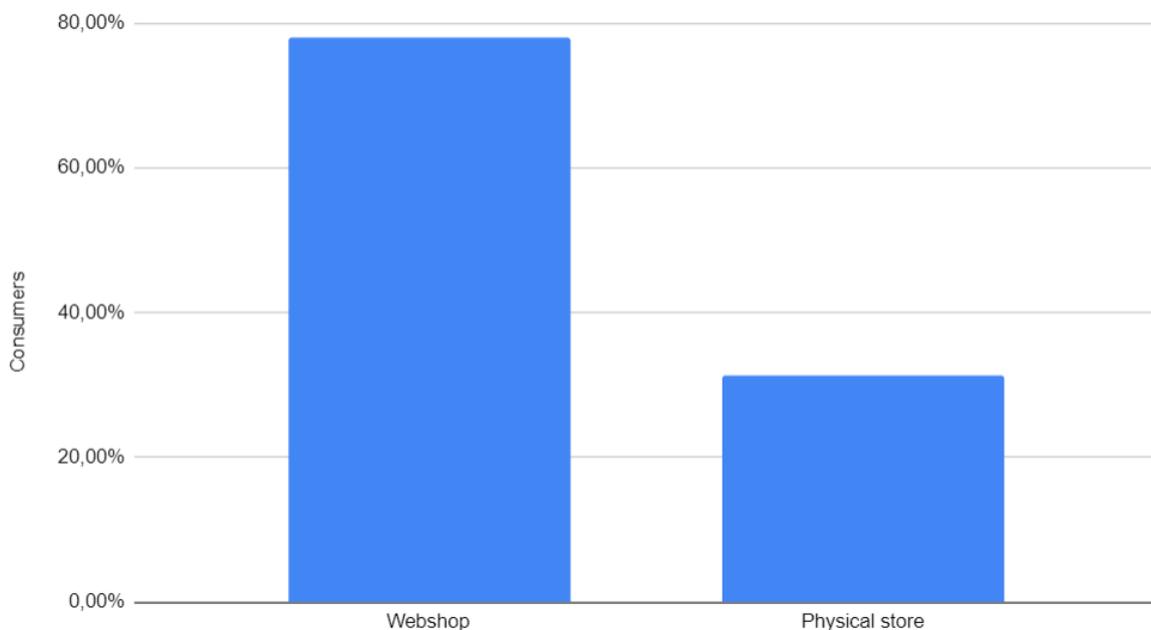


Figure 18. Webshop versus physical store visit.

4.2.3.2 Shop information

We ask respondents what they thought about the amount of information they receive while shopping.

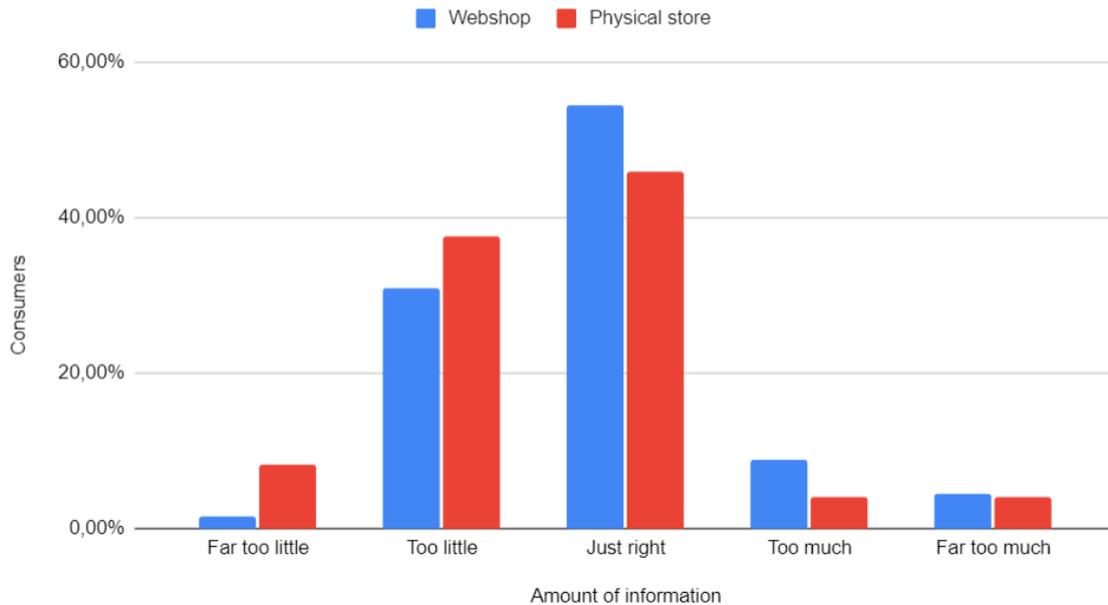


Figure 19. Webshop versus physical store information.

In figure 19 we can see that webshops (average 2,83) seem to have a bit more information than physical stores (average 2,58), but this does not seem as a significant enough difference. In general, people seem to be either happy with the amount of information or want to see a bit more. A respondent remarked “You have to be able to know what the end-of-life time is of a product, especially when you spent around €1000,00 for the product (iPhone 11)”.

4.2.3.3 Update importance

We ask respondents what they thought about the importance of updates. In figure 20 we can see that the respondents value both updates, but value security updates (average 4,36) more than version updates (average 3,60).

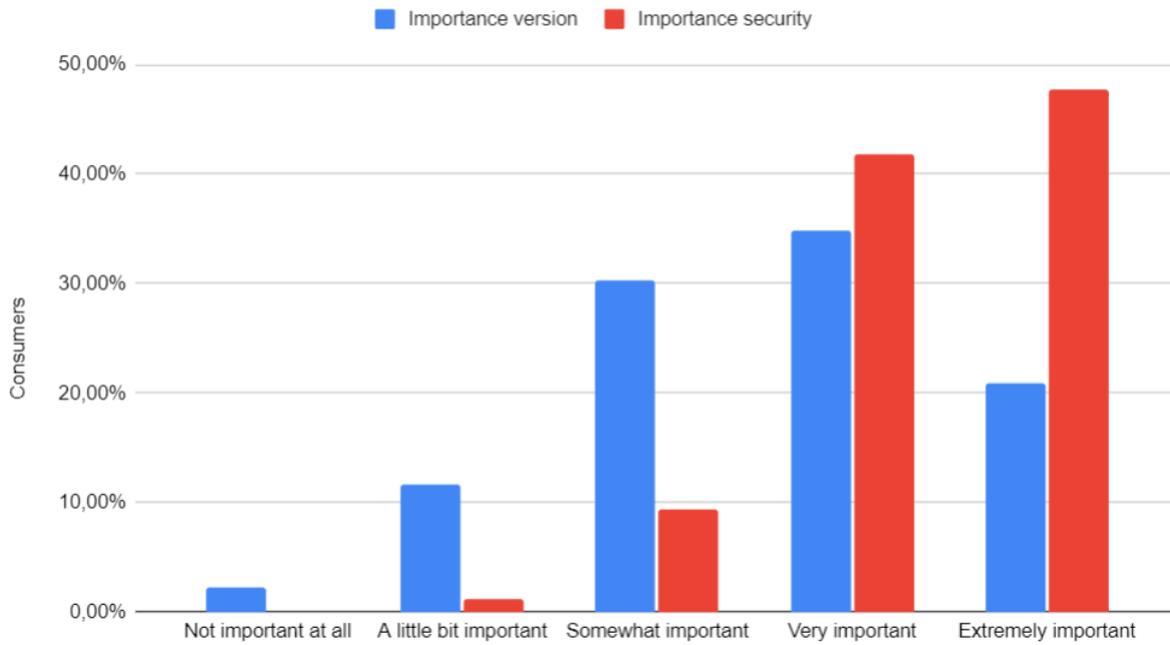


Figure 20. Version versus security update importance.

Respondents also noted that “Even though I value updates, I never spent much time thinking about it when buying a phone”.

When we asked respondents why they thought version updates were (not) important their answers can roughly be categorized as follows:

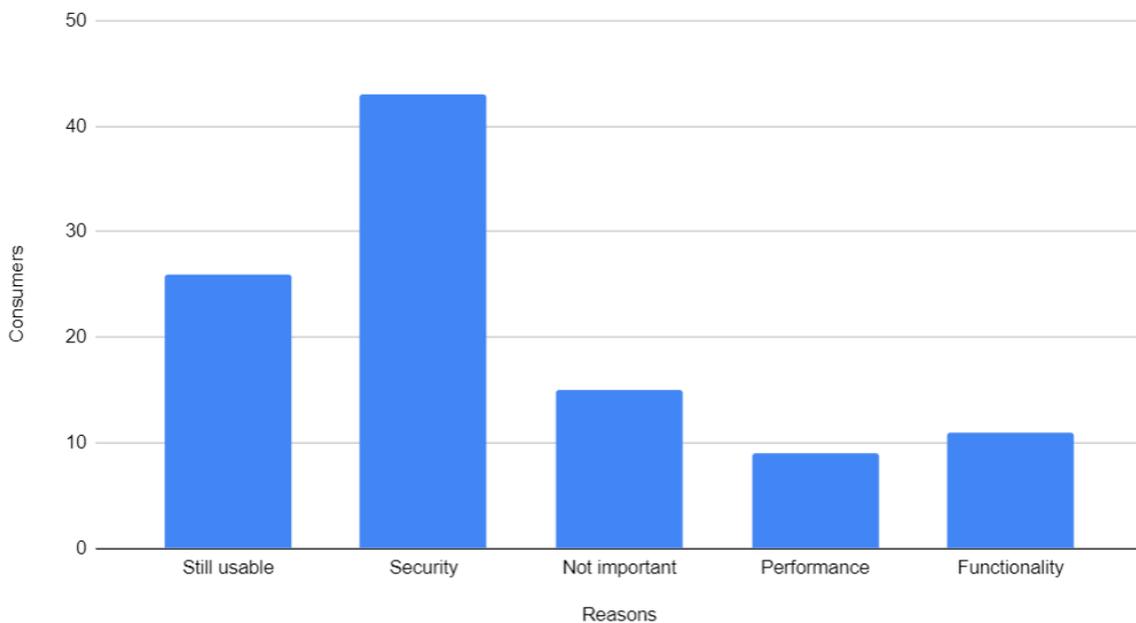


Figure 21. Reason importance version update.

Note that some respondents gave more than 1 reason, resulting in the total of reasons adding up to more than 86. The main reason people want to have version updates is because of security. One respondent mentioned “I think it is important to have the latest software, so that I know that vulnerabilities have been patched”.The second most important reason was that they want to be able to use their phone for a long time and they want to

keep using their apps. One respondent noted “I want to be able to use my phone until it breaks”. People also valued added or improved functionality and a performance increase. For example, one respondent said “Without updates phones feel old quite quickly, because they miss new features and patches and the like.” Some people did not find version updates important. Their reasons ranged from “I have no clue what to expect” to “Sometimes a new update is worse than the previous version”.

We split the reasons for finding security updates important into 4 categories as seen in figure 22. The main reason people value security updates is that they want to feel secure or safe. The second reason is that people know they have private information on their phones and want to protect this information. For example, one respondent said “You do a lot of important stuff on your phone, like banking, saving photos and chatting and I’d rather not give other people access to that”. The third reason is that people are afraid of their phones getting hacked. As one respondent put it “My phone has to stay MY phone”. The last category is the “Other category”. Some people said that valuing security updates just made sense, others said that they don’t know what security updates do, but they’d probably be important. Some people said that they wanted to protect their phones from viruses and some said that they want to be able to continue using their phone.

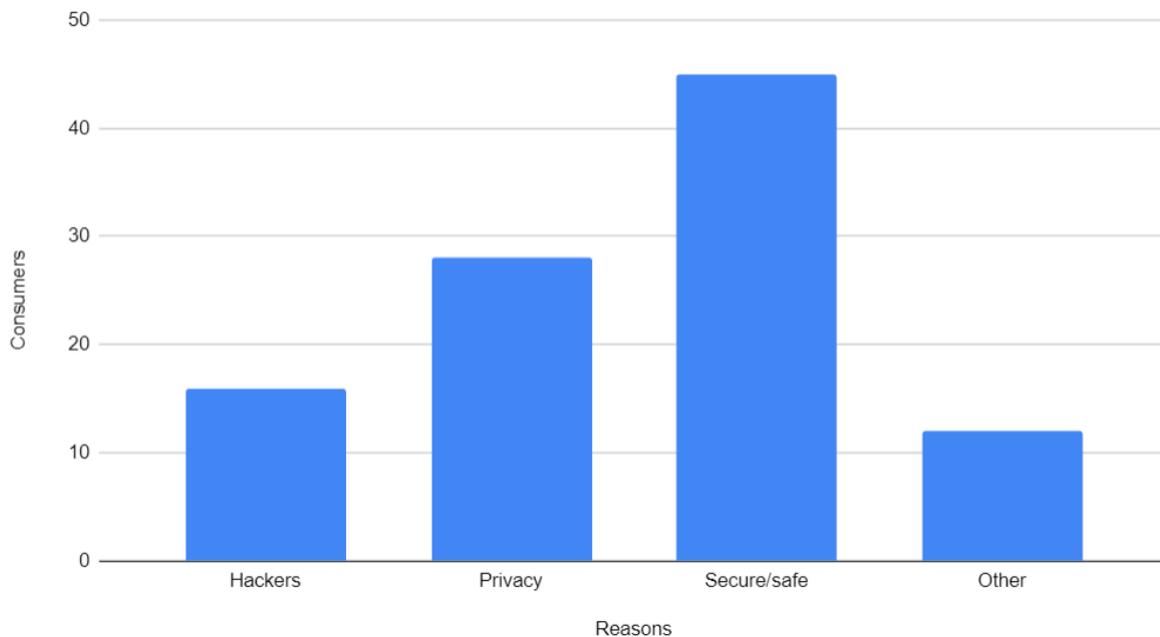


Figure 22. Reason importance security update.

4.2.3.4 Update support duration awareness

We asked respondents whether they know how long their updates last. We can see in figure 23 that 75-80% of respondents do not know how long their updates last. This can be seen by one respondent that told us “You make me aware of something I have not thought about before. I will definitely look into it.”. In the first question, the blue color in the graph, we asked respondents whether they knew how long their phone would have update support at the time of buying. The version and security update questions asked about current awareness. We can see that over time, the awareness does not really change.

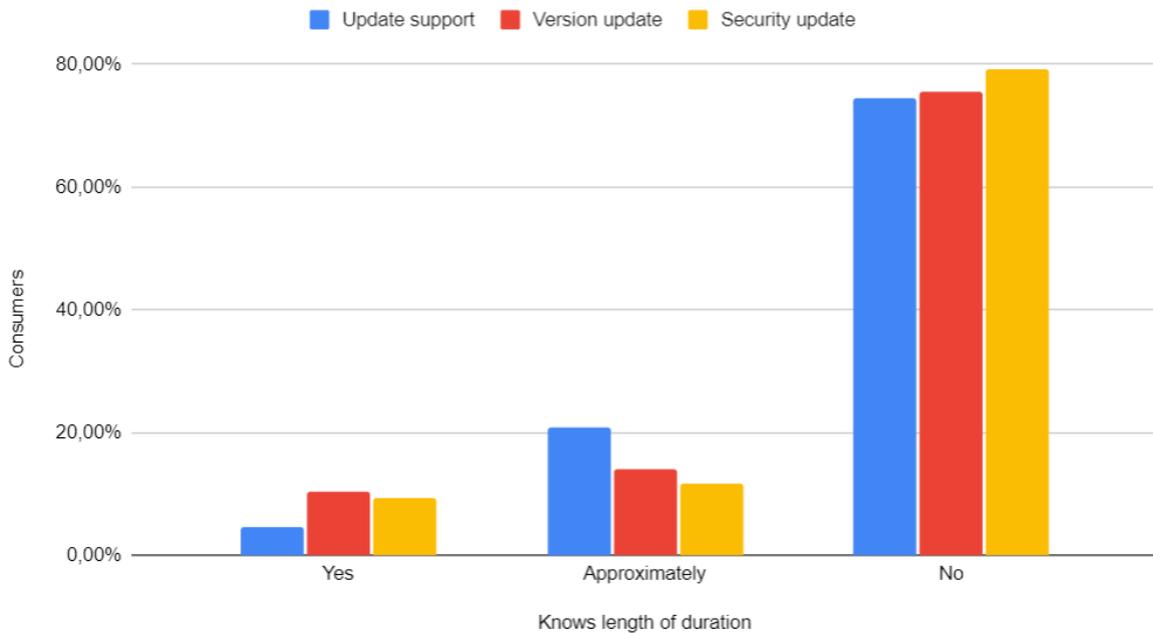


Figure 23. Update support duration awareness

So if we then look at the people that filled in that they (approximately) knew how long their update support would last at the time of buying. As we can see in figure 24, everyone got phone updates less than 4 years after buying the phone or 5 - 7 years. The 5 - 7 years corresponds with the duration of update support that Apple guarantees. The 2 - 4 years correspond with Google. The 0 and 1 years are a bit weird. This could be explained by people having old phones from when update support wasn't valued as much. It might also be that people misread the question, bought the smartphone many years ago, bought a second hand smartphone or bought a smartphone with a different OS. This proves that most, if not all, of these people indeed had an idea of how long their phone's update support would last. One responded with "Updates stopped a few months after I bought the phone" indicating that this person knows the updates have stopped.

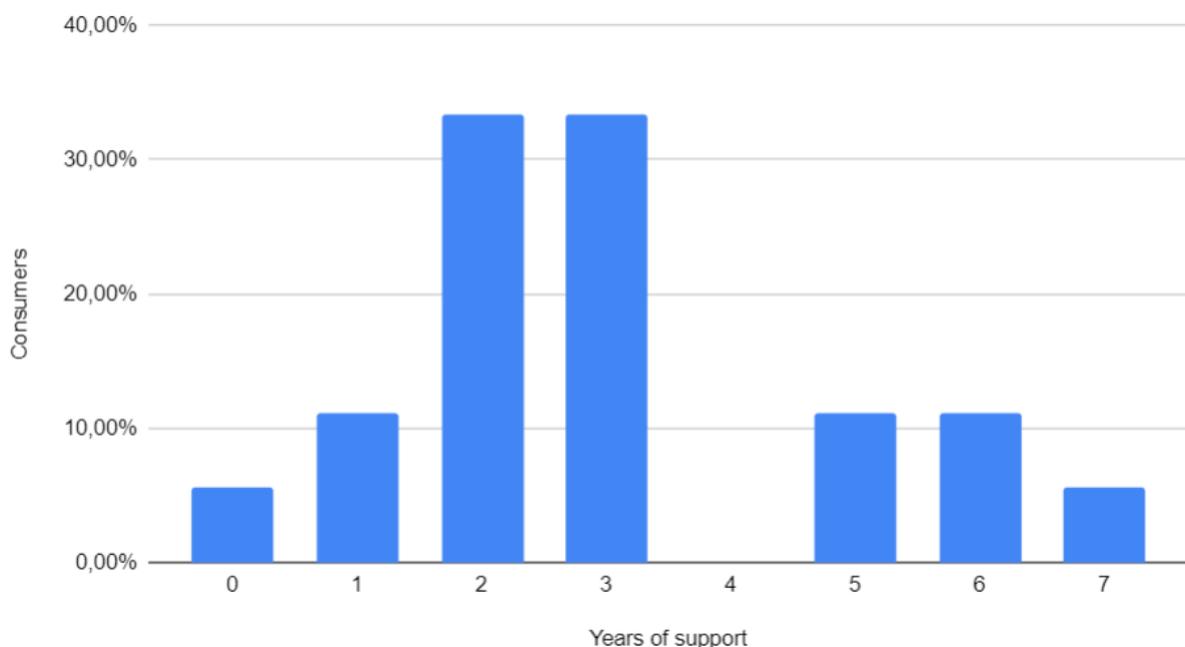


Figure 24. Duration of update support at time of buying.

If we look at the people who don't know how long their phone support would last we see quotes like "I don't know" and "I received updates up until now". The last quote at least points out that the consumer is aware that the updates are still being deployed.

If we look at the data from the security updates in figure 25, we see that of the people who know how long their security update support lasts, 13,33% do not get security updates anymore. The vast majority, 40% will receive 1 more year of security updates.

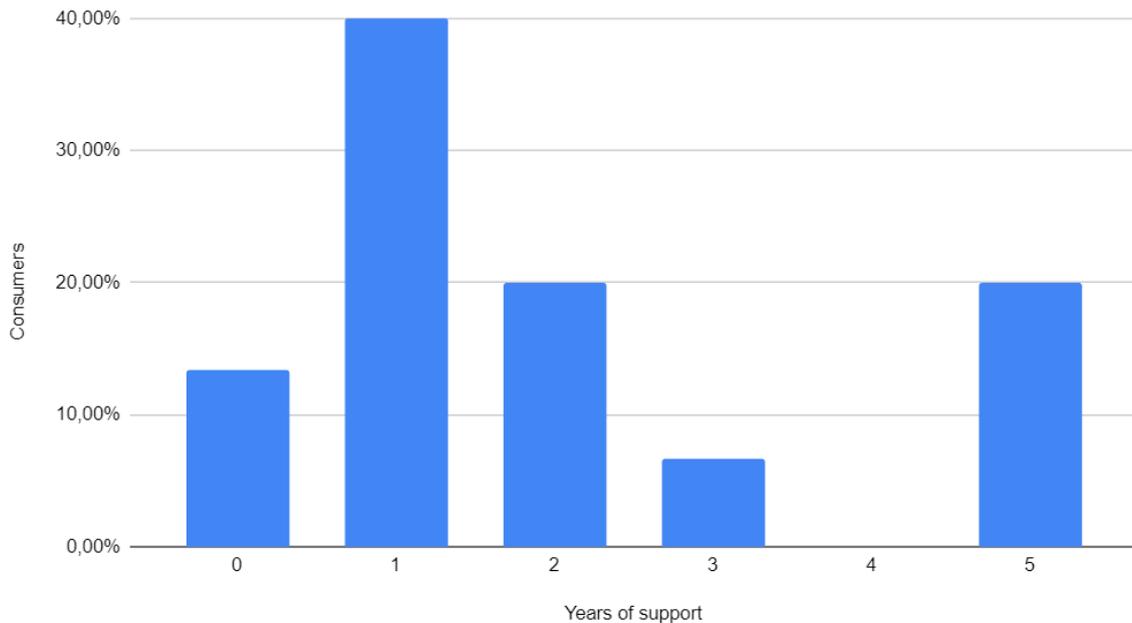


Figure 25. Remaining security update support duration

Now if we take a look at version support in figure 26, we see something very similar. This makes sense, because most of the time security update and version update support duration go hand in hand. The 1 year of support comes out on top and 19% of people who know their support duration think that they don't receive version updates anymore.

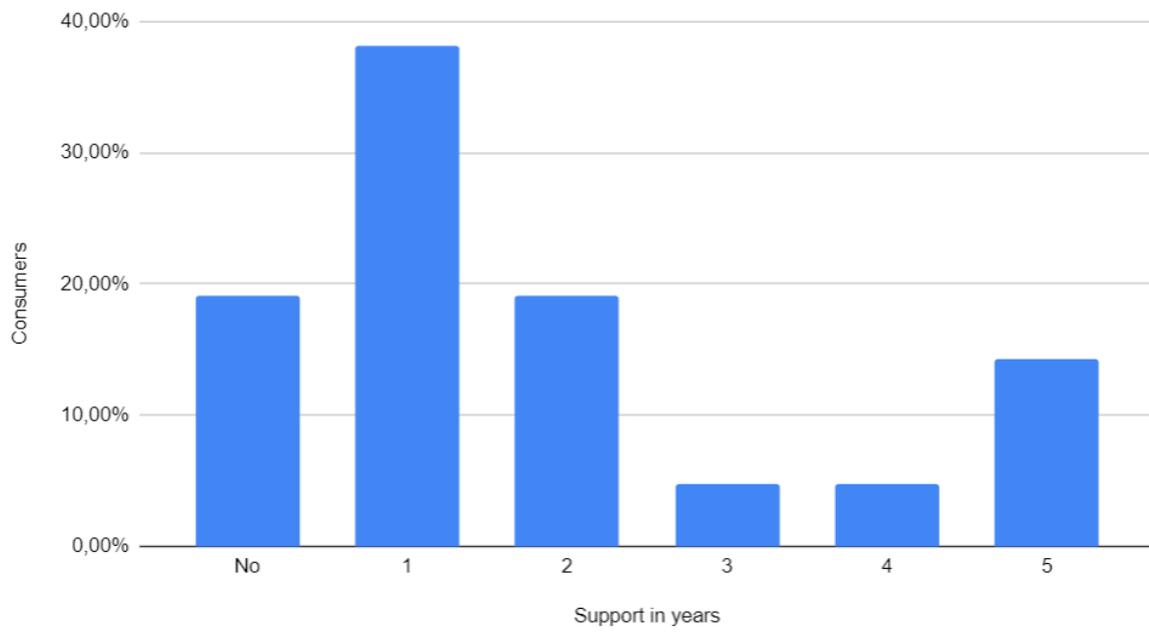


Figure 26. Remaining version update support duration

5 Discussion

We will interpret the results of chapter 4, so that we can answer the research question. We will do this on the basis of the sub-questions. Afterwards we will talk about implications, limitations and future directions.

5.1 Sub-questions

5.1.1 How easily can consumers find information about update support in web shops?

The quantity and quality of information in web shops differs greatly. The smallest amount of information we have found is from BCC, which only stated the OS version included with the phone. The biggest amount of information can be found at Coolblue. They have information about the included OS version, introduction date, update duration, update end date and update frequency.

The quality of the information ranges greatly too. For example the Mediamarkt often states to have no information on the update duration. In contrast, Coolblue even goes the extra mile and explains to their visitors how to interpret the given information. It also clearly states the differences between the different kinds of updates.

In figure 19, we can see that participants in the surveys also mention that they want to have more information. This could mean that they are not able to easily find the information that is there or that the information is missing or incorrect. We can also see in figure 19 that people are happier with the amount of information from webshops (average 2,83) than from physical stores (average 2,58).

In conclusion, even though there is a webshop that has correct and complete information, we cannot expect the user to find it. Some webshops have conflicting information and we cannot expect from consumers to find out what information is correct. The low level of information regarding update support on most webshops corresponds with our hypothesis.

5.1.2 How easily can consumers find information about update support in physical stores?

There is no information on the displays about update support, only some phone displays show the current OS version. This means that all other information regarding update support should be gained from a salesperson. Depending on the knowledge and skills of the salesperson it is quite easy to get advice. The only information you are likely to get without asking for it, is that older phones have a shorter duration of update support. In figure 23 we can see that 75-80% of consumers are not aware of the limited duration of update support. So the chances that people bring this up while talking to the salesperson are very slim.

In figure 19, we can see that survey participants mention that they want to have more information. This could mean that they are not able to easily find the information that is there, especially compared to in the webshops.

Since information gathering in the physical stores is completely dependent on the information needed by the consumer, it is likely most consumers will not find any information

regarding update support. The low level of information regarding update support in the physical stores corresponds with our hypothesis.

5.1.3 How much information do consumers want when buying a new smartphone?

The respondents seem to want a little bit more information when shopping, as seen in figure 19. On average the webshops seem to have a slightly better amount of information compared to the physical stores, which have too little information. This is both reflected in the analysis of the web pages of the webshops and in the survey. Respondents shop more in webshops than in physical stores. This could be a sign that respondents do want more information and therefore shop in the webshops, where the information is easier to find.

In conclusion, consumers seem to want a little more information, especially from physical stores.

5.1.4 How important is version update support to consumers when buying a new smartphone?

As seen in figure 20, over 50% of the respondents found version update support to be quite important to very important. As seen in figure 21, the most mentioned reasons are being able to use apps, security and getting new features so the phone does not feel old.

Some respondents are hesitant towards version updates. They sometimes think that an update might make things worse. For example, it might put extra bloat on your phone or the new features might be bad. Other respondents do not understand what version updates are for, so they do not bother with it.

On the other hand, one could argue that since 75,6% consumers do not know how long their version support lasts, as shown in figure 2, they do not really find version updates all that important. However, this can also be explained by that information is hard to find, as shown in 5.1.1 and 5.1.2. People also report that it is something they think they should pay more attention to.

In general, consumers say they find version update support to be quite important to very important to consumers. These findings correspond with the results of Mugge et al., who found that software update support was the number 2 specification people looked at when buying a refurbished phone.

5.1.5 How important is security update support to consumers when buying a new smartphone?

All of the respondents thought security to be reasonably to extremely important. They value security updates more than version updates, as seen in figure 20. The reasons why they value security updates can be found in figure 22. Many of the respondents seem to be very aware of the fact that they use their phone for a lot of personal affairs. They want to protect their private messages, photo's and banking in particular. They also seem to be afraid of hackers and viruses.

On the other hand, one could argue that since 79,1% consumers do not know how long their security support lasts, as shown in figure 2, they do not really find security updates all that important. However, this can also be explained by that information is hard to find, as

shown in 5.1.1 and 5.1.2. People also report that it is something they think they should pay more attention to.

In conclusion, security update support is very important to consumers. It is valued more than version updates. Even though consumers say they value the security updates a lot, we see that they do not know how long they will get security updates.

5.1.6 Are consumers aware of the limited update support?

Our survey shows that 20-25% of respondents did approximately know how long their phone would have update support. They told us that their support lasted for 2-3 years or 5-7 years at the time of buying. These numbers correspond with Android and iOS support respectively, proving that these people actually know how long their support lasts.

It is not surprising that consumers are not aware. As mentioned in 5.1.1 and 5.1.2 it can be quite hard to find information about update support. In webshops the information is often missing, incorrect or hard to understand. In physical stores consumers actively need to ask about update support in order to get information about it.

In conclusion, 75-80% of consumers are not aware of the limited update support. That is not surprising, because it matches earlier research as seen in 3.3. This is a chicken-and-egg problem. What came first, the little information in the shops or the lack of awareness in consumers?

5.2 Implications

5.2.1 Webshops

Since 75-80% of consumers are not aware of the limited update support (as seen in figure 23), it might be an indication of consumers not paying attention to this information when buying a smartphone. This means that it might not be worth it for webshops to spend resources into making sure the information regarding update support is complete and correct.

But in general, people do express that they want to have a bit more information (as seen in figure 19). So depending on whether information supply might be a reason people order from a different webshop, it might be worth it after all. It might also be a reason why people use webshops instead of or next to physical stores more often (as seen in figure 18). Webshops might be interested in A/B testing with different amounts of information.

5.2.2 Physical stores

Since the displays are meant to give a short summary of the smartphone, it is understandable that update support information is not on there (as discussed in 4.2.2.1).

Normally salespersons do not tell consumers about update support unless specifically asked about it. They might only mention that older models have updates for a shorter period of time (as discussed in 4.2.2.2). Since it is likely consumers will not bring it up themselves, but do care about update support (as seen in figure 20), it is important for salespeople to bring it up themselves. It might increase consumer satisfaction.

5.2.3 Consumers

Consumers admit that they value update support greatly (as seen in figure 20 and by the research of Mugge et al.), but do not pay much attention to it when buying a smartphone. Consumers may want to use webshops more (as seen in figure 18) because in general, more information can easily be found there. You might be more likely to find the information about update support without actively looking for it. Consumers that do decide to go to physical stores might want to ask the salesperson specifically about the update support of smartphones. However, this does require consumers to be aware of update support.

As long as consumers are not aware of the limited update support, they will likely buy smartphones with little update support. They might not be aware of when the update support ends and might not buy a new phone. As seen in 3.2.1.1 and 3.2.1.2, this leaves a lot of severe vulnerabilities unpatched. As seen in 3.2.3.1 and 3.2.3.2 both version and security updates are key in defending against attacks.

However, Khan & Kongar say that people buy phones based on recommendations of others and advertised specs. So maybe only informing users of the update support is not enough and actively advertising with update support is needed in order to raise awareness.

5.3 Limitations

5.3.1 Webshops and physical stores

We recognize that it can be quite a while ago when respondents last bought their smartphone. In the meantime, a lot could have changed. So this information might already be outdated.

Respondents could also have bought their smartphones at different webshops or physical stores than the ones examined in this research. That might cause discrepancies between the supply and the demand part of this research.

In the BCC we were not allowed to record the interview. It was offered that we could e-mail the headquarters to ask for permission. Due to time constraints, we decided to conduct the interview without recording.

5.3.2 Survey

We recognize that we only have a small subset of the whole population of Dutch smartphone consumers. The further this survey gets spread around from the initial social circle, the more representative the results get. We think that we might have an overrepresentation of people who are highly educated or have an IT education. These two factors lead to a higher level of security awareness when it comes to smartphones (Koyuncu & Pusatli, 2019).

We also recognize that this survey is based on self-reporting. This means that we are depending on the self-awareness, memory and honesty of the respondents.

5.3.3 Related Research

It was hard to find numbers on some of the smartphone security statistics. We ended up using Kaspersky research. We recognize that this party has financial interest and might want to stress the importance of using Kaspersky products. This could result in them overstating security risks.

5.4 Future directions

5.4.1 Improve survey participants

In this research we have a convenience sample. We suspect we have more highly educated people and people trained in IT. For example, this skews our results such that we expect to have a sample that is more security aware than the Dutch population. We had to pick a convenience sample due to the time and money constraints on this research.

This research can be conducted with a bigger and more representative sample. This would give a better representation of the update support information wants and needs and the security awareness of the Dutch population.

5.4.2 Improve physical store visits

In this research, we only visited one BCC. This does give us some idea as to the state of the physical stores, but does not give us a representative sample. New research could visit more different store chains and maybe more than one store per chain. This would give a way more accurate idea of the current state of information supply regarding update support in the physical stores. This would also be interesting because it would enable the researcher to compare different stores and store chains. Maybe the interviews could also be recorded, which was not possible for this research due to time constraints.

5.4.3 Research shopping experience regarding update support

The next possible future research focuses on how we can improve the shopping experience regarding update support. Maybe customers would prefer to see the update support information on the displays or hear it from the salesperson without asking for it. This could either be done by asking people through surveys or by splitting the participants into multiple groups that get their information through different means and see how they would rate their satisfaction. This can be done for both the physical stores and webshops. With webshops you could test this with simple A/B tests.

5.4.4 Causal relation

In 5.1.6 we asked what comes first, the lack of awareness or the little information in stores? One could research whether a causal relationship exists between the level of awareness and the amount of information in the stores. For example, we could split the participants in multiple groups that get a different amount of information about update support in the stores. Afterwards we can see if their level of awareness changes. One might even want to see if the changes in awareness are long-term or short-term.

6 Conclusions

The research question can be split into two parts: supply and demand. In order to answer the research question in a clear fashion, we will look at these two parts separately.

The supply of information in web shops greatly differs. Some web shops only inform the consumer of the OS included with the device, while others have a detailed summary of the update support including helpful context. Since many web shops display incomplete or even false information, it cannot be expected of people to confidently find the correct information.

The supply of information in physical stores consists of two parts. The first part is the store display. Users see phones with a short description next to it. That description at most mentions the included OS and version, but nothing about the update support. The second part is the information you get by talking to a salesperson. They will give you information based on your information needs. If you do not ask about update support, you will likely only get a warning that buying an older model will result in less updates. This brings us to the demand for information.

Respondents value both OS and security updates, with the latter being valued most. Version updates are valued for being able to keep using apps and keeping the phone feeling fresh and secure. Security updates are valued for keeping photos, messages and mobile banking secure and protecting against viruses and hackers.

Even though respondents value the updates, 75-80% of the respondents did not know how long their phone would receive updates. Some respondents said that they did not look for this information, because they did not know about the limited duration of update support. Some admitted that they think update support is very important, yet they did not look for it while shopping for a new smartphone.

Respondents say that they would like to receive more information while shopping, regardless of shopping in webshops or physical stores.

The supply of information is not sufficient, since consumers want to have more information. If we look at the webshops and physical stores, we can see that it is hard to find complete and correct information.

Generally, consumers are not aware of how long their phone has update support and express that it is something they do care about, but they do not actively look for information when buying a smartphone.

Bibliography

Bibliography

- Android. (n.d.). *Secure, up-to-date and easy to use*. Android. Retrieved June 21, 2021, from <https://www.android.com/one/>
- Android Security Bulletins*. (2021, May 3). Android Security Bulletins. Retrieved May 28, 2021, from <https://source.android.com/security/bulletin>
- Android version history*. (2021, May 28). Wikipedia. Retrieved May 28, 2021, from https://en.wikipedia.org/wiki/Android_version_history
- Apple. (n.d.). *About iOS 14 Updates*. Apple support. Retrieved June 1, 2021, from <https://support.apple.com/en-us/HT211808#146>
- Apple. (n.d.). *App Store*. Apple developer. Retrieved April 20, 2021, from <https://developer.apple.com/support/app-store/>
- Apple. (2021, May 14). *How to manually update apps on your Apple device*. Apple support. Retrieved July 19, 2021, from <https://support.apple.com/en-us/HT202180>
- Apple. (2021, May 24). *About the security content of iOS 14.6 and iPadOS 14.6*. Apple support. Retrieved June 1, 2021, from <https://support.apple.com/en-us/HT212528>
- Apple security updates*. (2021, June 17). Apple Support. Retrieved June 21, 2021, from <https://support.apple.com/en-us/HT201222>
- Avraham, Z. (2015, July 27). *Experts Found a Unicorn in the Heart of Android*. Zimperium. Retrieved April 21, 2021, from <https://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/>
- BCC. (n.d.). *Samsung Galaxy A51 (Zwart)*. BCC. Retrieved June 2, 2021, from <https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a51-zwart/279316>
- Belsimpel. (n.d.). *Apple iPhone 12 64GB Zwart*. belsimpel. Retrieved May 14, 2021, from <https://www.belsimpel.nl/apple-iphone-12/zwart#panel>

- bol.com. (n.d.). *Samsung Galaxy A52 4G - 128GB - Awesome Black*. Bol.com. Retrieved May 14, 2021, from https://www.bol.com/nl/p/samsung-galaxy-a52-4g-128gb-awesome-black/9300000020732477/?bltgh=hL8ibcffPbQ2yh0IEJpH6A.4_54.55.ProductTitle#product_specifications
- Chebyshev, V. (2021, March 1). *Mobile malware evolution 2020*. Securelist by Kaspersky. Retrieved March 17, 2021, from <https://securelist.com/mobile-malware-evolution-2020/101029/>
- coolblue. (n.d.). *Apple iPhone 12 128GB Zwart + Apple Usb C Oplader 20W*. coolblue. Retrieved May 14, 2021, from <https://www.coolblue.nl/product/872169/apple-iphone-12-128gb-zwart-apple-usb-c-oplader-20w.html#product-information>
- Cuthbertson, S. (2020, June 10). *Unwrapping the Android 11 Beta, plus more developer updates*. Android Developers Blog. Retrieved May 28, 2021, from <https://android-developers.googleblog.com/2020/06/unwrapping-android-11-beta-plus-more.html>
- Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device. *Procedia Technology*, 9(BYOD Bring Your Own Device), 43-53. sciencedirect.com. <https://doi.org/10.1016/j.protcy.2013.12.005>
- End of Life. (n.d.). *Android OS End of Life*. End of Life. Retrieved June 15, 2021, from <https://endoflife.date/android>
- Federal Trade Commission. (2018, February). *Mobile Security Updates: Understanding the Issues* [Commission Report]. ftc.gov. Retrieved May 20, 2021, from https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf
- Fedewa, J. (2021, January 14). *What Are Google Play System Updates on Android, and Are They Important?* How To Geek. Retrieved April 21, 2021, from

<https://www.howtogeek.com/686927/what-are-google-play-system-updates-on-android-and-are-they-important/>

Garg, S., & Baliyan, N. (2021, February 13). Comparative analysis of Android and iOS from security viewpoint. *Computer Science Review*, 40, 1-13. Science Direct.

<https://doi.org/10.1016/j.cosrev.2021.100372>

Ghuloum, A. (2019, May 8). *Fresher OS with Projects Treble and Mainline*. Android Developers Blog. Retrieved March 21, 2021, from <https://android-developers.googleblog.com/2019/05/fresher-os-with-projects-treble-and-mainline.html>

Google. (n.d.). *Update your Android apps*. Google Play Help. Retrieved June 15, 2021, from <https://support.google.com/googleplay/answer/113412?hl=en>

Google. (2021, March). Android Platform version percentile [Android Platform version percentile]. In *Android Platform version percentile* [Android Studio]. Google.

Hoffman, C. (2015, August 12). *Android's Stagefright Exploit: What You Need to Know and How to Protect Yourself*. How To Geek. Retrieved April 21, 2021, from <https://www.howtogeek.com/225834/stagefright-what-you-need-to-know-and-how-to-protect-yourself/>

Kaspersky. (n.d.). *What is Adware? – Definition and Explanation*. What is Adware | Kaspersky. Retrieved June 25, 2021, from <https://www.kaspersky.com/resource-center/threats/adware>

Kaspersky. (n.d.). *What is Riskware? Riskware: What Is It and How to Avoid It* | Kaspersky. Retrieved June 25, 2021, from <https://www.kaspersky.com/resource-center/threats/riskware>

Kaspersky Lab. (2016). *MOBILE MALWARE EVOLUTION 2016*. Kaspersky Content Hub. Retrieved Mei 20, 2021, from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180734/Mobile_report_2016.pdf

- Kastrenakes, J., & Brandom, R. (2018, October 24). *Google mandates two years of security updates for popular phones in new Android contract*. The Verge. Retrieved May 20, 2021, from <https://www.theverge.com/2018/10/24/18019356/android-security-update-mandate-google-contract>
- Khan, N., & Kongar, E. (2014, April). Innovation and Development of New Product for Customer Satisfaction, Applying on Smart Phone's Security. *ASEE 2014 Zone I Conference*, 1-7. <http://www.asee.org/documents/zones/zone1/2014/Student/PDFs/262.pdf>
- Koyuncu, M., & Pusatli, T. (2019, May 13). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems, 2019, vol 2*(Security Awareness Level of Smartphone Users: An Exploratory Case Study). <https://doi.org/10.1155/2019/2786913>
- Mansfield-Devine, S. (2012, October). Android architecture: attacking the weak points. *Volume 2012, Issue 10*, 5-12. Science Direct. [https://doi.org/10.1016/S1353-4858\(12\)70092-2](https://doi.org/10.1016/S1353-4858(12)70092-2)
- MediaMarkt. (n.d.). *SAMSUNG Galaxy A71 - 128 GB Dual-sim Zwart*. MediaMarkt. Retrieved May 14, 2021, from https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a71-128-gb-dual-sim-zwart-1650085.html
- Mugge, R., Jockin, B., & Bocken, N. (2017, March 20). How to sell refurbished smartphones? An investigation of different customer groups and appropriate incentives. *Journal of Cleaner Production, Volume 147*(How to sell refurbished smartphones? An investigation of different customer groups and appropriate incentives), 284-296. ScienceDirect. <https://doi.org/10.1016/j.jclepro.2017.01.111>
- Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., & Kadobayashi, Y. (2018, September). Smart4Gap: Factors that Influence Smartphone Security Decisions in

Developing and Developed Countries. *Research Gate*, 4-15. DOI:

10.1145/3285957.3285980

O'Dea, S. (2021, May 5). *Global smartphone market share from 4th quarter 2009 to 4th quarter 2020*. Statista. Retrieved June 9, 2021, from <https://www.statista.com/statistics/271496/global-market-share-held-by-smartphone-validators-since-4th-quarter-2009/>

O'Dea, S. (2021, May 19). *Share of global smartphone shipments by operating system from 2014 to 2023*. Statista. Retrieved May 21, 2021, from <https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/#:~:text=Smartphones%20running%20the%20Android%20operating,percent%20share%20of%20the%20market>

Richter, F. (2021, June 11). *How Long Does Apple Support Older iPhone Models?* Statista. Retrieved June 21, 2021, from <https://www.statista.com/chart/5824/ios-iphone-compatibility/>

Samsung. (2020, August 18). *Samsung Raises the Bar for Mobile Experience Innovation Committing to Three Generations of Android OS Upgrades*. Samsung Newsroom. Retrieved May 20, 2021, from <https://news.samsung.com/global/samsung-raises-the-bar-for-mobile-experience-innovation-committing-to-three-generations-of-android-os-upgrades>

Samsung. (2021, February 22). *Samsung Takes Galaxy Security to the Next Level by Extending Updates*. Samsung Newsroom. Retrieved May 20, 2021, from <https://news.samsung.com/global/samsung-takes-galaxy-security-to-the-next-level-by-extending-updates>

Sharma, A. (2021, May 10). *Yet another phone maker is now promising 3 years of major Android updates*. Android Authority. Retrieved May 20, 2021, from <https://www.androidauthority.com/vivo-three-years-android-updates-1224225/>

Techredactie. (2020, August 24). *Dit is waarom veel smartphones het maar drie jaar volhouden*. AD. Dit is waarom veel smartphones het maar drie jaar volhouden

Watson, B., & Zheng, J. (2017, April 13). On the User Awareness of Mobile Security Recommendations. *ACM SE '17: Proceedings of the SouthEast Conference, 2017*, 120-127. ACM digital library. <https://doi.org/10.1145/3077286.3077563>

We Are Social Ltd & Hootsuite Inc. (2018, January 29). *Digital in 2018 in Western Europe*. Digital in 2018 in Western Europe. Retrieved May 26, 2021, from <https://www.slideshare.net/wearesocial/digital-in-2018-in-northern-europe-part-1-west-86864045>

Zhang, Z., Zhang, H., Qian, Z., & Lau, B. (2021). An Investigation of the Android Kernel Patch Ecosystem. *30th Usenix Security Symposium*. https://www.usenix.org/system/files/sec21summer_zhang.pdf

Appendix

Appendix A. Webshops

Coolblue

Coolblue has the option to filter by smartphone and sort by “best verkocht” (best sold). These were the top 10 smartphones on June 24th 2021.

Nr	Phone	Link
1	Samsung Galaxy S20 FE 128GB Blauw 4G + Clear View Book Case Blauw	https://www.coolblue.nl/product/874356/samsung-galaxy-s20-fe-128gb-blauw-4g-clear-view-book-case-blauw.html
2	Samsung Galaxy A51 128 GB Zwart	https://www.coolblue.nl/product/854584/samsung-galaxy-a51-128-gb-zwart.html
3	Apple iPhone 12 128GB Zwart + Apple Usb C Oplader 20W	https://www.coolblue.nl/product/872169/apple-iphone-12-128gb-zwart-apple-usb-c-oplader-20w.html
4	Samsung Galaxy A32 128GB Zwart	https://www.coolblue.nl/product/876618/samsung-galaxy-a32-128gb-zwart.html
5	Apple iPhone SE 64GB Zwart + Apple Usb C Oplader 20W	https://www.coolblue.nl/product/881927/apple-iphone-se-64gb-zwart-apple-usb-c-oplader-20w.html
6	Apple iPhone SE 64 GB Zwart	https://www.coolblue.nl/product/861017/apple-iphone-se-64-gb-zwart.html
7	OnePlus Nord 128GB Grijs 5G	https://www.coolblue.nl/product/864663/oneplus-nord-128gb-grijs-5g.html
8	Samsung Galaxy A52 128GB Zwart 4G Enterprise Editie	https://www.coolblue.nl/product/880553/samsung-galaxy-a52-128gb-zwart-4g-enterprise-editie.html
9	Samsung Galaxy A52 128GB Zwart 5G + Samsung Smart S View Wallet Cover Zwart	https://www.coolblue.nl/product/879509/samsung-galaxy-a52-128gb-zwart-5g-samsung-smart-s-view-wallet-cover-zwart.html
10	Samsung Galaxy A52 128GB Zwart 5G	https://www.coolblue.nl/product/877961/samsung-galaxy-a52-128gb-zwart-5g.html#product-specifications

All information for these 10 smartphones seems to be complete and correct.

Mediamarkt

Mediamarkt has the option to filter by smartphone and sort by “meest gekocht” (bought most). These were the top 10 smartphones on June 24th 2021.

Nr	Phone	Link
1	SAMSUNG Galaxy A51 - 128 GB Dual-sim Zwart	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a51-128-gb-dual-sim-zwart-1650082.html
2	SAMSUNG Galaxy A12 - 64 GB Zwart	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a12-64-gb-zwart-1684452.html
3	SAMSUNG Galaxy A12 - 128 GB Zwart	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a12-128-gb-zwart-1684450.html
4	APPLE iPhone 12 - 128 GB Zwart 5G	https://www.mediamarkt.nl/nl/product/_apple-iphone-12-128-gb-zwart-5g-1676564.html
5	SAMSUNG Galaxy A12 - 32 GB Zwart	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a12-32-gb-zwart-1691115.html
6	APPLE iPhone 12 Pro - 128 GB Grafiet 5G	https://www.mediamarkt.nl/nl/product/_apple-iphone-12-pro-128-gb-grafiet-5g-1676576.html
7	APPLE iPhone 11 - 64 GB Zwart	https://www.mediamarkt.nl/nl/product/_apple-iphone-11-64-gb-zwart-1677771.html
8	SAMSUNG Galaxy S20 FE - 128 GB Donkerblauw	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-s20-fe-128-gb-donkerblauw-1673332.html
9	APPLE iPhone 12 mini - 128 GB Zwart 5G	https://www.mediamarkt.nl/nl/product/_apple-iphone-12-mini-128-gb-zwart-5g-1676549.html
10	SAMSUNG Galaxy A32 4G - 128 GB Zwart	https://www.mediamarkt.nl/nl/product/_samsung-galaxy-a32-4g-128-gb-zwart-1686722.html

In general, all smartphones had only their current OS version and release date stated. The only exception was number 10, which had a minimum duration of update support of 2 years.

Belsimpel

Belsimpel has the option to filter by phone and sort by “aanbevolen” (recommended). These were the top 10 smartphones on June 24th 2021.

Nr	Phone	Link
1	Apple iPhone 12 64GB Zwart	https://www.belsimpel.nl/apple-iphone-12/zwart
2	Apple iPhone 11 64GB Black	https://www.belsimpel.nl/apple-iphone-11/zwart
3	Samsung Galaxy A52 A525 128GB Zwart	https://www.belsimpel.nl/samsung-galaxy-a52-4g/zwart
4	Samsung Galaxy A32 4G 128GB Zwart	https://www.belsimpel.nl/samsung-galaxy-a32-4g/128gb-zwart
5	Samsung Galaxy A51 4G Black	https://www.belsimpel.nl/samsung-galaxy-a51/zwart
6	Apple iPhone 12 Pro Max 128GB Zwart	https://www.belsimpel.nl/apple-iphone-12-pro-max/zwart
7	Apple iPhone 12 Pro 128GB Zwart	https://www.belsimpel.nl/apple-iphone-12-pro/128gb-zwart
8	Apple iPhone SE 2020 64GB Black	https://www.belsimpel.nl/apple-iphone-se-2020/64gb-zwart
9	Google Pixel 4a 128GB Black	https://www.belsimpel.nl/google-pixel-4a/128gb-zwart
10	Apple iPhone 12 Mini 64GB Zwart	https://www.belsimpel.nl/apple-iphone-12-mini/zwart

All these webpages only show the included OS version and introduction date.

Bol.com

Bel.com has the option to filter by phone and sort by “aanbevolen” (recommended). These were the top 10 smartphones on June 24th 2021.

Nr	Phone	Link
1	Samsung Galaxy A51 - 128GB - Zwart	https://www.bol.com/nl/nl/p/samsung-galaxy-a51-128gb-zwart/9200000127101717/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.55.ProductTitle
2	Motorola Moto E7i Power - 32GB - Rood	https://www.bol.com/nl/nl/p/motorola-moto-e7i-power-32gb-rood/9300000021262612/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.56.ProductTitle
3	TCL 20 SE – 64GB – Groen	https://www.bol.com/nl/nl/p/tcl-20-se-64gb-groen/9300000032501300/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.57.ProductTitle
4	Samsung Galaxy A20e - 32GB - Zwart	https://www.bol.com/nl/nl/p/samsung-galaxy-a20e-32gb-zwart/9200000109073236/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.58.ProductTitle
5	Samsung Galaxy A12 - 128GB - Zwart	https://www.bol.com/nl/nl/p/samsung-galaxy-a12-128gb-zwart/9300000019419396/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.59.ProductTitle
6	Samsung Galaxy A02s - 32GB - Zwart	https://www.bol.com/nl/nl/p/samsung-galaxy-a02s-32gb-zwart/9300000020547718/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.60.ProductTitle
7	Apple iPhone 12 Mini - 64GB - Zwart	https://www.bol.com/nl/nl/p/apple-iphone-12-mini-64gb-zwart/9300000013742257/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.61.ProductTitle
8	Apple iPhone 12 - 64GB - Zwart	https://www.bol.com/nl/nl/p/apple-iphone-12-64gb-zwart/9300000013742278/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.62.ProductTitle
9	Samsung Galaxy A21s - 64GB - Zwart	https://www.bol.com/nl/nl/p/samsung-galaxy-a21s-64gb-zwart/9300000000132986/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.63.ProductTitle
10	Apple iPhone SE (2020) - 64GB - Zwart	https://www.bol.com/nl/nl/p/apple-iphone-se-64gb-zwart/9300000000886605/?bltgh=u4BgiXpbYZV7usby-qxBow.4_54.64.ProductTitle

All of the webpages above mention the year and month of introduction, months of support, included OS and the frequency of security updates. The exceptions are:

- Nr 4, “ondersteuning met updates” lists “informatie niet beschikbaar”
- Nr 5 and 6, “Frequentie beveiligingsupdates” lists “Niet bekend”

BCC

BCC has the option to filter by smartphone and sort by “meest verkocht” (most sold) . These were the top 10 smartphones on June 24th 2021.

Nr	Phone	Link
1	Samsung Galaxy A52 5G 128GB (Zwart)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a52-5g-128gb-zwart/302633
2	Apple iPhone 12 - 64GB (Zwart)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/apple-iphone-12-64gb-zwart/290603
3	Nokia smartphone 3.4 inclusief Lyca SIM kaart	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/nokia-smartphone-34-inclusief-lyca-sim-kaart/307212
4	Samsung Galaxy A52 4G 128GB (Wit)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a52-4g-128gb-wit/302630
5	Samsung Galaxy A02s 32GB (Zwart)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a02s-32gb-zwart/300970
6	Samsung Galaxy A52 4G 128GB (Paars)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a52-4g-128gb-paars/302627
7	Motorola smartphone Moto e6i (Grijs)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/motorola-smartphone-moto-e6i-grijs/305862
8	OPPO smartphone A72 128GB (Zwart)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/oppo-smartphone-a72-128gb-zwart/303787
9	Samsung Galaxy A12 128GB (Zwart) inc Clear Cover	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a12-128gb-zwart-inc-clear-cover/306527
10	Samsung Galaxy A52 4G 128GB (Zwart)	https://www.bcc.nl/navigatie-en-telefoon/mobiele-telefoon/smartphone/samsung-galaxy-a52-4g-128gb-zwart/302629

In general these webpages all had only the OS mentioned quite clearly. The exceptions are:

- Number 7 has a different OS than usual: Android Q Go. This is the lightweight version of Android 10.
- Number 8 and 9 only “Android” as OS, no version.

Appendix B. Survey

Deze vragenlijst gaat over hoe belangrijk consumenten de update-ondersteuning vinden bij het aanschaffen van een smartphone. Als u nog nooit een smartphone hebt gekocht, vragen wij u niet deel te nemen aan dit onderzoek. De vragenlijst duurt ongeveer 4 minuten. Gelieve deze vragenlijst naar eerlijkheid in te vullen. U wordt niet persoonlijk beoordeeld op hoe u dit invult, antwoorden zijn anoniem. Zoek geen informatie op, denk niet te lang na en vul uw eerste ingeving in. Omdat het belangrijk is dat u met uw eerste ingeving gaat, is het niet mogelijk om terug te gaan naar een vorige vraag.

1. Bent u wezen winkelen voor een smartphone in een fysieke winkel?
2. Zo ja, hoe vond u de hoeveelheid informatie bij het winkelen in de fysieke winkel?
3. Bent u wezen winkelen voor een smartphone in een webwinkel?
4. Zo ja, hoe vond u de hoeveelheid informatie bij het winkelen in de webwinkel?
5. Wist u hoe lang u nog update-ondersteuning zou hebben bij aanschaf van uw smartphone?
6. Hoelang na aanschaf kreeg u nog update-ondersteuning? (Als u nee antwoordde op de vorige vraag mag u deze overslaan. Als u 'Ongeveer' heeft geantwoord, gelieve een inschatting te plaatsen van de duur.)

Dit deel van de vragenlijst gaat over versie updates van besturingssystemen. Deze updates zorgen vooral voor nieuwe functionaliteit op uw smartphone. Denk bijvoorbeeld aan een andere manier van ingekomen berichten weergeven. Als uw besturingssysteem verouderd is, kunnen apps onbruikbaar worden op uw smartphone. Een voorbeeld van de versie van een besturingssysteem op een smartphone is Android 11 of iOS 14.

7. Hoe belangrijk vindt u het om versie-updates te ontvangen?
8. Waarom vindt u versie-updates (niet) belangrijk?
9. Weet u hoe lang u nog versie-updates ontvangt?
10. Hoelang heeft u nog versie-update-ondersteuning? (Als u nee antwoordde op de vorige vraag mag u deze overslaan. Als u 'Ongeveer' heeft geantwoord, gelieve een inschatting te plaatsen van de duur.)

Dit deel van de vragenlijst gaat over beveiligingsupdates. Zoals de naam suggereert hebben deze updates te maken met de beveiliging van je smartphone.

11. Hoe belangrijk vindt u dat u beveiligingsupdates ontvangt?
12. Waarom vindt u beveiligingsupdates belangrijk?
13. Weet u hoe lang u nog beveiligingsupdates ontvangt?
14. Hoelang heeft u nog beveiligingsupdate ondersteuning? (Als u nee antwoordde op de vorige vraag mag u deze overslaan. Als u 'Ongeveer' heeft geantwoord, gelieve een inschatting te plaatsen van de duur.)
15. Heeft u nog vragen en/of opmerkingen? Dan kunt u deze hier nog kwijt. Vergeet niet de survey af te sluiten door op "Verzenden" te klikken.

Hartelijk bedankt voor uw deelname! Als u zo vriendelijk zou willen zijn om de survey te delen, zou dat zeer gewaardeerd worden. De link is: