

In Control with no Control: Perceptions and Reality of Windows 10 Home Edition Update Features

Jason Morris, Ingolf Becker, Simon Parkin
University College London
{jason.morris.17, i.becker, s.parkin}@ucl.ac.uk

Abstract—Home computer users are regularly advised to install software updates to stay secure. Windows 10 Home edition is unique as it automatically downloads and installs updates, and restarts the computer automatically if needed. The automatic restarts can be influenced through a number of features, such as ‘active hours’ (the period during which a computer will never automatically restart to finish installing an update) or by explicitly setting a time when to restart the computer.

This research investigates if the features Microsoft provides for managing updates on Windows 10 Home edition are appropriate for computer owners.

We build a model of the update behaviour of Windows 10. The model identifies all interaction points between the update system and the users. We contrast the theory with reality in a survey study with 93 participants which establishes the experiences and perceptions of users of Windows 10 Home.

Windows will not restart a computer outside active hours if the computer is in use. However, if any user of a machine sets an explicit restart time, the computer will restart at that time in order to install quality updates even if the computer is still in active use (potentially by a different user to the one who set the restart time). While overall perceptions of updates were positive, the pattern of use of almost all users was incompatible with the default setting of the ‘active hours’ feature. Only 28% of users knew of its existence. Users are mostly unaware of quality (bug-fix) updates, perceiving that updates act mostly to add features. Half of our participants report unexpected restarts, while half also reported growing concern about the state of their device if an update took a long time. Participants who had previous negative experiences had weaker beliefs about their ability to control updates than those who had not.

We recommend that operating systems obtain explicit permission for restarts consistently; there are opportunities for default features such as active hours and update progress displays to learn from usage activity.

I. INTRODUCTION

A key piece of information security advice given to users by both government organisations [1]–[3] and security companies [4] is to ‘install the latest software and app updates’. Doing so is seen as the way to eliminate software vulnerabilities, toward creating a safer computing environment for the user. Otherwise, vulnerabilities may be exploited readily by attackers with ready access to increasingly off-the-shelf tools to target users of popular operating systems indiscriminately.

Software producers have aimed to make it easier for users to have up-to-date versions of their software by automating the update process. This process is however not without costs and risks for the user. From a cost perspective, software that is updating or installing can interrupt primary tasks. From a risk perspective, should an update fail or break functionality, it could cause a prolonged availability issue. Similarly, an update might change a familiar user interface or piece of functionality, forcing the user to learn new skills before being able to productively resume their work. As user software portfolios have grown over time, these costs and risks have often grown proportionately with them [5].

Updates are arguably most useful if they patch vulnerabilities in a timely fashion [6]. Users may act to postpone updates or not feel a need to concern themselves with updates [7]. To ensure updates are installed, software producers are now seen to automate software updates to the point that they can be scheduled (and rescheduled), but not avoided for long. Most noticeably, the entry level version of Windows 10 aimed at home users (‘Home Edition’) and released in July 2015 removed the ability of users to turn automatic updates off. It will download and install updates as soon as possible, and schedule an automatic restart within the next 24 hours if required to complete the installation, resuming the system from standby if necessary. The user is notified of the scheduled restart, but unable to cancel it. As an operating system provides an execution environment for many applications, an operating system restart has the potential to disrupt other running applications and cause unsaved work to be lost.

In this paper we build a model of the update behaviour of Windows 10 Home Edition. We find that Windows is inconsistent in its restarting behaviour: when an explicit restart time was set by a user it will restart to complete the installation of a quality update even when the computer is in active use. In all other cases it does not restart when the computer is in use. We then use this model to highlight the interactions users have with the system (Section III), and the potential consequences of these interactions for the user should they be mis-configured. Further, we contrast this model with usage experiences through an online survey with 97 UK Windows 10 Home users (Section IV). We find that the default setting of the main feature to control when updates are installed — *active hours* — is unsuitable for 97% of our users. Regardless, 72% do not appear to be aware of the feature. This is supported by about half of participants reporting unexpected restarts. We examine existing research of the challenges of updates for users in Section II. We round off this paper with discussion and conclusions in Sections V and VI.

II. BACKGROUND AND RELATED WORK

A. Motivating the need for software updates

Software may be released that has faults. Features may be changed, or new ones added over time, which may also have faults. These faults may be exploited by malicious parties to access and manipulate a computer. This affects home users and organisations alike. To address these faults, software producers create software security updates or patches that, once applied to a machine, are assumed to eliminate a vulnerability from that machine. By way of an example, during 2017 Microsoft released 681 security updates across their product range [8].

Vania [9] describes security updates as ‘unsolved, solved problems’, referring to the principle that a vulnerability for which a security update exists should not be considered ‘solved’ until the relevant security update is applied to all machines that it needs to be applied to. Indeed, applying security updates in a timely manner is necessary to reduce the window of exposure of a vulnerability¹.

Zero-day vulnerabilities are an extreme example where details of an exploit become widely available before a software update exists to mitigate it. Thus, to reduce the information security risks, software producers need to create security updates quickly; the other side of this is that for updates to work, the expectation is that end users must apply them quickly to their machines [6].

Software producers also create ‘feature updates’ or ‘upgrades’ which add new functions and features, and which arguably should be separated from security updates [9], [12] (where to date may not necessarily be transparent to users). Whereas security updates should typically be invisible to users, feature updates are not. Feature updates may change functionality or the user interface, necessitating changes to users’ ways of working. Consequently, by decoupling the two types, producers can avoid dissuading users from applying a security update for fear it will also draw in a feature update that would disrupt existing ways of working [13].

The economic case for automating the management of software updates is informed by the size of the task for users to keep their software portfolios up-to-date. Frei et al. [5] assessed the software inventories of over two million Windows hosts, calculating that users had an average of 56 packages from 20 different vendors. 90% of observed users needed to handle between 51 and 86 updates per year from 9 to 36 different vendors on average. In light of this burden, and given that security updates typically have no visible benefit for home users, their rejection of security advice to ‘install the latest software and app updates’ can appear rational [14].

In 2007–2009, Duebendorfer et al. compared the effectiveness of different update strategies [15], [16] in web browsers. They found that 97% of Chrome browsers configured with a highly automated ‘silent’ update strategy were updated within three weeks of an update becoming available. Comparatively, Firefox users were initially quicker to update their browser by using a one-click update functionality, but the share of updated browsers never exceeded 85% within 21 days of the release.

¹The day after Microsoft’s ‘Patch Tuesday’ [10] has been labelled ‘Exploit Wednesday’ [11] to reflect this race.

B. The need for human control

While automatically installing software updates minimizes the window of opportunity for vulnerabilities to be exploited, where those updates require a device or software restart, consideration must be given to both the direct cost of disrupting users’ primary tasks and the indirect costs of reducing users’ opportunities to observe and understand the automated update mechanism. Existing research within organisations tells us that users have a limited budget for complying with security demands [17], where the notion of a limited budget for security has broader applicability to home users too [14], [18]. Demands on a user’s ‘compliance budget’ need to be spent wisely; if a user has given all the time and energy to security that they believe is reasonable, any push beyond that limit will promote action to reduce the burden, most directly by circumventing security. Online there are a plethora of forum posts and magazines offering unofficial advice on disabling automatic updates. Tips range from the relatively benign such as marking the computer’s network connection as ‘metered’, to high risk, manual registry changes. To our knowledge, there are two working solutions to disable the automatic restarts: Decker created a ‘Reboot Blocker’ service for free download [19], which continuously adjusts the ‘active hours’ period to include the current time; and one can manually disable the Update Orchestrator Restart Task [20]. Even the mainstream media have felt the need to publish advice on managing updates in advance of Windows 10 feature updates [21].



Fig. 1. Screenshot of Windows update messages when updates fail.

Workarounds are exacerbated by the challenge to make existing functions work correctly. Users who lack understanding of the update mechanism are less likely to be able to identify and troubleshoot problems [22]. A non-functioning update mechanism suggesting to ‘search the web’ (see Figure 1) alongside an 8-digit, hexadecimal error codes may not support a coherent resolution strategy for non-expert users.

It has been widely established that changes to features and interfaces are common reasons for not updating, especially after previous negative experiences [5], [13], [23]–[26]. Bergan and Whittaker [23] explained the impact of changes to interfaces in terms of five key cognitive concepts: a loss of cognitive automation (a need for more attention to the task after a user interface is made less familiar); negative transfer effects (the need to discard skills learned ‘doing things the old way’); the

need to rebuild cognitive maps (such as rediscovering where a menu item is); the need to retrain procedural memory ('even if we know 'in our heads', our 'hands' still do what they used to do with the old interface') and; the demotivating effects on the user of a feeling of loss of overall control.

Wash et al. [22] examined the Windows 7 Update component which allowed users to configure the degree of update automation for key update stages. The authors sought to compare what users intended their computers to do and what they thought it was doing with what it actually did (gained from configuration data on participants' machines). For 25 of their 37 participants the authors identified a discrepancy between actual and expected behaviours, causing them to be less secure and affecting their productivity. They suggested this was a result of 'removing users from the loop'.

Farhang et al. [27] examined the upgrade practices and perceptions of Windows users, focusing on their decision to whether or not to upgrade to Windows 10. They make four practical design recommendations for OS producers to address the issues identified by their survey study.

C. Security automation

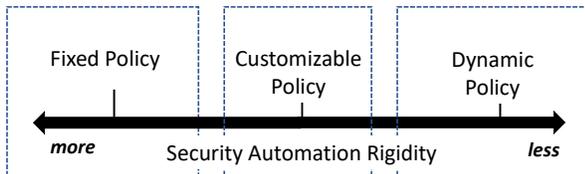


Fig. 2. The spectrum of automation approaches, reproduced from Edwards, Poole, and Stoll [28].

Edwards et al. [28] argue that security automation, removing the user from the decision process, may be more limited than implementers anticipate. This is framed across a spectrum of rigidity for security automation strategies, as in Figure 2, ranging from fixed, 'one-size-fits-all' policies to dynamic policies that allow users to personalise the system's behaviour. A system at the 'fixed policy' end adheres to what Wash describes as the '*stupid user approach*' [29], installing all updates automatically and as quickly as possible (and restarting the device if necessary). Crucially, the system operates independently of the user's working context. The outcome is a maximally secure system, but one that impedes the primary task. We suggest that the update model in Windows 10 Home Edition sits towards this end of the spectrum.

Conversely, a 'dynamic policy' allows the user, rather than the software producer, to control the updating process. The user can selectively install updates and has more control over any associated disruption. The outcome however is a potentially less secure system, as updates may not be applied as quickly. This aligns with Wash's '*education approach*' [29] (though this also relies on the user having been trained appropriately). The update model in Windows 7, as previously noted, is perhaps at this end of the automation spectrum.

III. WINDOWS 10 HOME UPDATE MODEL

Updates for Windows 10 Home Edition, released in July 2015, differ significantly from previous versions of Windows.

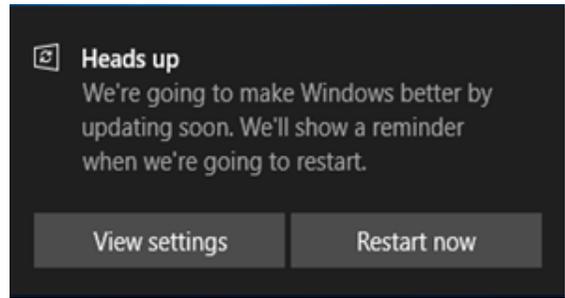


Fig. 3. Initial notification of a pending update requiring a restart.

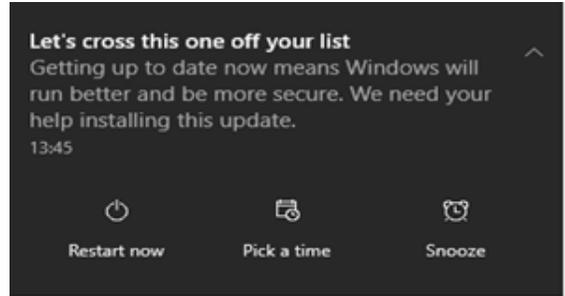


Fig. 4. Example reminder notification of a pending update requiring a restart.

Firstly, updates can no longer be selectively installed. Secondly, update processes were changed to run much more aggressively. Most directly, this culminated in Home Edition users no longer being able to disable automatic updates. Figure 3 shows the notification commonly used to inform users of the need to restart their computer (for updates to finish installing). Figure 4 shows an example of a reminder, where now the option to choose a specific time for the restart has become available.

In the absence of any intervention from the user, downloaded updates for previous Windows versions were installed during a dedicated maintenance cycle scheduled (by default) at 3am. Windows 10 automatically installs updates immediately after download. As the default maintenance cycle was designed to never take machine resources away from an active user [31], this represents a significant change in update behaviour for Windows 10 as resources (and potentially battery life) are consumed while the computer is in use.

For lack of an existing description of the Windows 10 Home automated update, we built a model of its user-facing functionality. In an approach similar to Wash et al.'s documentation of the Windows 7 update model [22], we (i) compiled a list of features and functions described in release announcements and on the official Microsoft Community Support Forum [32], then (ii) verified them in an Oracle Virtual Box environment using a black-box testing approach. The verification began by taking a virtual machine snapshot of a fresh, default installation of Windows 10 Home Edition. Once Microsoft had published subsequent updates, the snapshot was restored to allow the virtual machine to download them. Shortly before the downloaded completed, a further snapshot was taken. By repeatedly restoring to the second snapshot, we were able to efficiently investigate the machine's behaviour as the update was applied with different control paths selected.

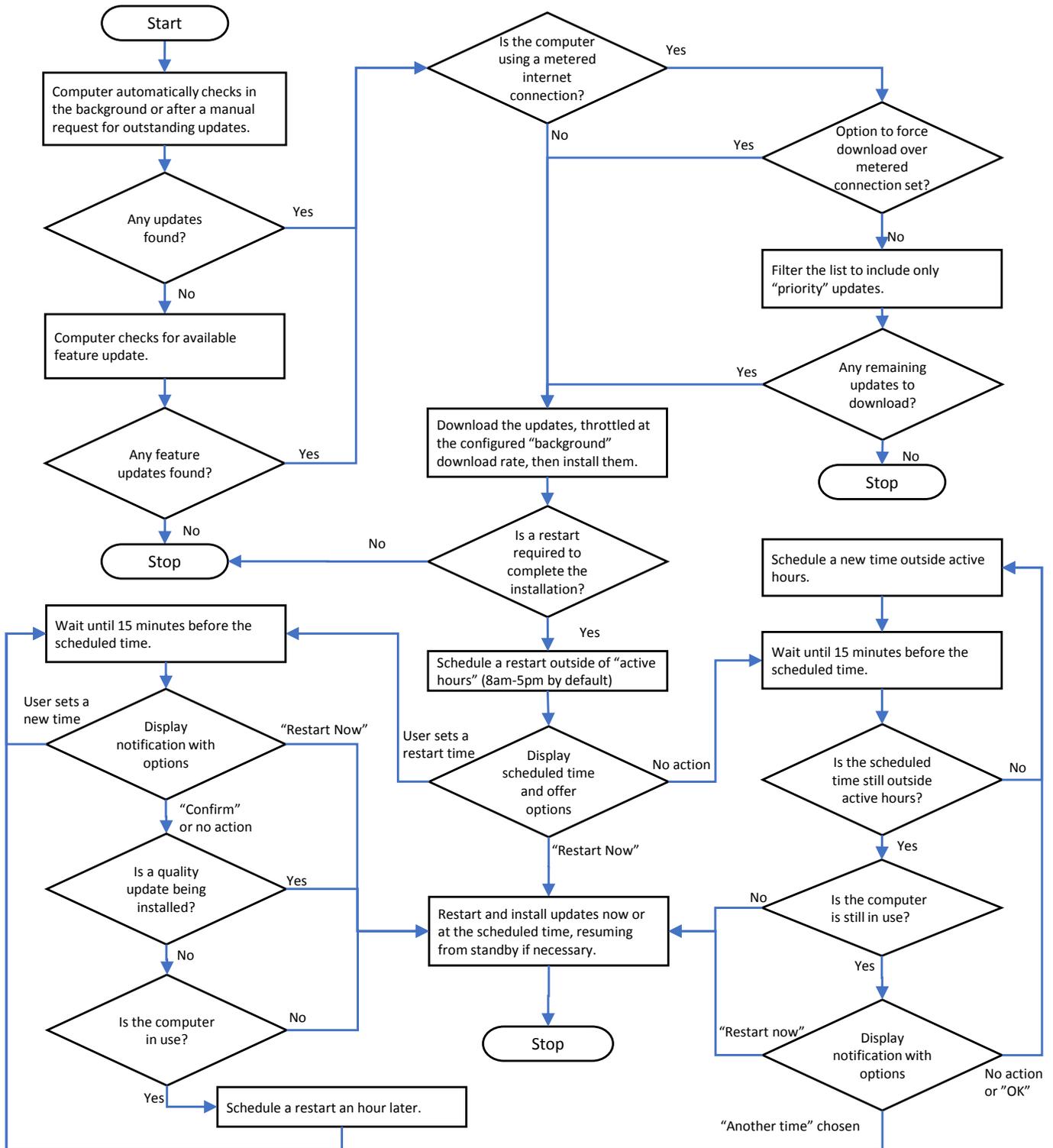


Fig. 5. Windows 10 Update model. As the computer shuts down in preparation for installing an update that requires a restart, the message ‘Configuring Windows Updates – Don’t turn off your computer’ is displayed. During the subsequent start up ‘Working on updates. Don’t turn off your PC. This will take a while.’ is shown. Each stage has a separate progress bar; one during shutdown and one during the restart. If the ‘Sign-in’ option to ‘reopen my apps after an update or restart’ is set, Windows will attempt to restore the state of the user’s desktop to the state it was in before the restart. The text and options in notifications to users to nudge them towards restarting becomes pushier as time passes and the ‘Engaged Restart’ mode is reached [30].

We decided to focus on the most recent release of the operating system, version ‘1803 – April 2018 Update’. The forced update model of the ‘Home Edition’ should then have meant that users regularly connected to the internet would be running it. As the ‘1803’ feature update occurred shortly after the start of our study, we were able to experiment with the installation of this feature update as well as quality updates.

The flow chart in Figure 5 represents the update model of Windows 10 Home version 1803 built using our approach. The process of populating the model was informed by VM experiments and a review of related literature, but not assumed to be exhaustively complete; the discussion that follows is informed by the model. The behaviour of the update mechanism is dependent on a complex range of user and system properties. Windows will check for updates daily, then download and install them without any further interaction or notification of the user. Updates are not downloaded on a metered connection, unless they are critical security fixes. Updates are installed in the background, and unless a restart is required, no notification is displayed to the user.

A. Mapping user interaction with updates

To install updates that require a restart, users must either restart their computer themselves, or ensure that the computer is on or in sleep mode when the update is due to be installed. For the latter, this time will either be outside of the configured ‘active hours’, or at a specific restart time nominated by the user.

With Windows 10 Home Edition, there are now two separate control flows. In the first flow, either the user sets an explicit restart time within the next 7 days or the restart occurs outside the specified ‘active hours’ when the computer is not in use. If the user has selected a specific time for the restart, a notification is displayed 15 minutes before the scheduled restart, at which point the user may select a new time or explicitly initiate a restart at that moment. If the chosen time of restart arrives, we have identified two alternative cases depending on the type of update being installed. If a quality update is being installed (i.e., a bug-fix or security update), the computer is restarted at the chosen time regardless of user action. For other updates, if the computer is in use (see Section III-D for more detail), the restart is automatically rescheduled to occur a short while later (between 30 and 60 minutes in our experiments).

The second control flow relies on the ‘active hours’ feature, intended to minimise disruptive impacts of restarts by preventing restarts during these hours. It is a machine-wide setting that was added in the ‘1607 - Anniversary Update’ (released in July 2016), allowing users to specify a time period of up to twelve hours (and then later eighteen hours in the ‘1703 - Creators Update’ (March 2017)) during which a computer will never automatically restart to finish installing an update. If the setting does not align with a time when the computer is in use, a user who perhaps moves away from their computer outside these hours may return to find their machine having restarted, and any stateful tasks running at the time of the reboot (such as a series of large file downloads) disrupted by the restart. To prevent this, Microsoft provides developers with an ‘Application Recovery and Restart’ API [33] that applications

would need to support to guarantee that their applications are seamlessly restored after a restart. Unfortunately, not many non-Microsoft applications have implemented this feature.

B. Prompts and reminders for updates

As a safeguard, Windows 10 displays a reminder notification 15 minutes before the restart time and checks for the computer being in use (see Section III-D) before restarting. This helps to avoid restarting the computer if actual computer use does not adhere to the active hours configured for the machine. If the computer is in use, the user is offered the chance to select an explicit time for the restart, or to restart the computer at that moment. If the message is ignored, a new time outside active hours is imposed.

Similarly, if updates are downloaded outside of active hours, a user may return to their computer at the resumption of active hours to find it has restarted, with any in-progress tasks having been disrupted. Windows 10 does not provide a user interface for users to control when the background check for updates occurs; indeed, it occurs with an element of randomness to help ensure uniform demand on the servers providing updates [34].

C. Managing disruption caused by updates

Thus, from a security perspective, users need to understand the need to restart their computer to complete the installation of some updates. From the perspective of minimising disruption, users need to understand the ‘active hours’ concept and conversely the configuration of active hours should ideally align with their usage patterns. Failing this, a user cannot reliably expect to leave tasks running outside of ‘active hours’ or expect their desktop state to be fully restored upon resumption of ‘active hours’. This is a major change from previous behaviour. These last two expectations are arguably unnatural, being as they are counter-intuitive to the physical world: if we temporarily leave our possessions unattended but secure, we expect to return to find them how we left them.

D. Computer in use

Windows tries to determine if the computer is in use to avoid restarting it if it is. We used mouse movements and clicks in our virtual environment to simulate the presence of a user in these experiments. Microsoft’s US patent [35] for ‘Initiating update operations’ refers to several tests for detecting user presence but we found watching a video in full-screen mode did not register as one, despite being explicitly being mentioned in the patent.

IV. SURVEY STUDY

In this section we contrast the expectations of the Windows 10 Home update model (Section III) to users’ perceptions and reported experiences using the OS. In particular, we focus on:

- The need to restart a computer when updates are installed;
- The need for restarts to be approved by users;
- The need to reopen applications before being able to resume work after a restart.

We designed an online survey to capture user experience with the above, prefaced with questions about general computer use (such as when the computer is used, whether it is shared with others, and if the participant is wholly responsible for ‘looking after’ the device). Subsequent sections of the survey then captured existing knowledge of what operating system updates do, perception of the risks that security updates are intended to address, and how participants interact with updates and update (prompts) (such as identifying the conditions under which an update may be postponed, and how). Proactive security behaviours were also explored in the survey, alongside questions to determine if participants were aware of features for tailoring the update process, such as configuring the ‘active hours’. The full survey instrument and survey results file are available (see Section VI-B and Appendix). The survey design was informed by our model (Figure 5).

The study was approved by our department’s ethics review process. The survey was open to residents of the United Kingdom aged over 18, who had completed at least 5 prior studies on Prolific and who had an approval rating in excess of 90%. We requested an additional participant filtering criterion on Prolific for the operating system on a participant’s primary computer. At the time of data collection, 1862 potential participants claimed to use Windows 10 Home Edition, 419 Windows 10 Pro Edition, 42 Windows 10 other editions. 621 participants stated that they were using Windows 10, but were unsure of the edition. 479 participants used other Windows versions. We required our participants to be users of ‘Windows 10 Home Edition’ on their primary computer. Participants were compensated 2 GBP for completing the survey. Although we had 98 responses, one participant failed one of two attention questions and was removed from the results. We chose to exclude a further four participants who reported high uncertainty in the answers they provided. This gave a final count of 93 participants.

TABLE I. DEMOGRAPHICS OF THE USER STUDY.

Age groups		Age of computer	
18-24	14	Less than 1 month	2
25-34	32	Between a month and 6 months	7
35-44	18	6-12 months	9
45-54	16	1-2 years	33
55-64	11	2-3 years	14
65-74	2	More than 3 years	28
Gender		Student Status	
Female	58	Student	13
Male	35	Non-student	80
Education		Employment	
No formal qualifications	1	Unemployed (and job seeking)	10
Secondary school/GCSE	9	Not in paid work (e.g. homemaker, retired)	16
College/A levels	28	Part-time	23
Undergraduate degree	42	Full-time	41
Graduate degree	11	Other	3
Doctorate degree	2		

The demographics of our participants can be found in Table I. Compared to the general public, our participants are more likely to be students (14% vs 3% in the wider UK population) and are better educated [36]. Many previous studies about software updating e.g. [7], [22], [26] have also drawn participants from academically biased pools. These participants might be more technically savvy, with more technically accurate mental models of updates. However, we only

observed minor differences in the responses for participants who had ever worked or studied in a computer related field, which do not influence our conclusions. We also asked the age of participants’ computers to give us a very approximate indication of how many monthly update cycles and six-monthly feature updates they had experienced as well as a crude indicator of how much of an impact updates might be having on their system’s performance.

A third (31) of our participants reported having worked or studied for a qualification in a computer related field. 96% (89) participants reported extensive or moderate experience of at least one version of Windows prior to version 10. 82% (76) described their own experience with Windows 10 as extensive and a further 15% (14) as moderate. Two thirds (64) were the sole, regular user of their computer. Many of the remaining participants (26) reported sharing their computer only with other people in their household. 90% reported doing all (48) or most (36) of the maintenance of their computer themselves. Of those reporting how often they used their computer, 90% reported using their computer on at least five days each week. With respect to the participant’s computer itself, around two thirds (64) were laptop devices and 26 were desktop computers. 81% (75) described the speed of their computer as either ‘fast’ or ‘neither noticeably fast nor noticeably slow’ in almost equal numbers. None of the participants described their computer as ‘very slow’. The median reported age of computers was between 1 and 2 years. We then consider that computer performance would not directly exacerbate reported experience of updates (rather than an ageing computer being the fundamental cause of any bad experiences with the operating system).

When computers were not in use, just over half (49) of participants reported ‘shutting down’ their computer. Most of the remainder (39) reported that their computer was left switched on. Whether the computer subsequently entered sleep mode was not important to us because in both cases, by default, the computer would be woken to complete the installation of an update.

With respect to the activities for which participants used their computers, all reported browsing the internet and most reported using office productivity applications and social media. The two categories of uses with the lowest levels reported were for games and video calling, each of which about half of participants reported.

A. Perception of activities related to updates

While participants agreed that updates helped to keep them safe, there was less clarity about what they did. 29% of participants either did not know, or believed that updates rarely or never fixed errors in software. In contrast, 87% thought that updates add new features at least occasionally, implying our participants thought software updates add features more frequently than they fix errors.

Our participants on average perceived updates to be published less frequently than Microsoft’s monthly release cycle. Those with a computing background were about three times less likely to say they did not know (2 out of 31) than those without (11 out of 62), but their answers were not statistically significantly different. 49% (39) of those who

gave an answer thought that new updates were published approximately every two months or less frequently. This was despite an incorrect belief held by half of all participants (47) that they always needed to restart their computer when updates are installed. This needs to be considered in the light that monthly cumulative updates are a subset of all updates and always require a restart. Even if we restricted our analysis to participants who are sole users of their computer (and thus might reasonably be expected to be aware of all activity on it), and who believe updates always require a restart (35), the prevalence of the belief about the incorrectly low frequency of updates was still evident (18).

When asked about the frequency with which updates are installed automatically, only 17% (16) of our participants chose ‘Always’. 42% (39) selected ‘Often’. Aside from 5% who didn’t know, almost all participants believed they are never charged for updates.

B. Use of dedicated Windows 10 update controls

As we wanted to assess how well the Windows 10 update model fitted the needs of users, it was essential to understand how participants used their computer beyond their interactions with updates. Given the key role the ‘active hours’ feature plays in managing the disruptive impact of updates, we assessed whether participants’ reported patterns of use aligned with its assumptions, mainly that for ‘active hours’ there is a period of at least six hours each day when the computer is switched on (or on standby), but is not in use.

We asked ‘What happens to your computer when no one is using it?’ and provided a range of different options, some of which were equivalent from an updating perspective, such as ‘It’s left on all the time’ and ‘It’s put into sleep mode’. This was to reduce the need for participants to convey their interactions with specific interface features and computer functionality. We then asked how many days in an average week the computer was used, and what the typical hours of use on weekdays and weekends were. Given that ‘Patch Tuesday’ occurs on a weekday, the former was particularly important. We separated the day into three-hour intervals, specifically aligned with the default value for ‘active hours’, namely 8am to 5pm. We hypothesized that this might be a poor choice of default for discernible groups of home users (such as those with ‘9 to 5’ jobs, or those in study). As the feature is not referred to during the initial set up of Windows, we also hypothesized users may be simply unaware of its existence. Consequently, we also asked if participants were aware of the feature, and if they were, whether they had configured it. By asking users how often they used their computer, we had hoped to revisit Furnell et al.’s hypothesis [37] that infrequent users had more negative perceptions of updates than frequent users, however only five participants reported using their computer for less than five days a week.

We made two key findings. Firstly, only 28% of our participants were aware of the existence of the active hours feature. Those with a computing background were significantly more likely to be aware of it (15 out of 31) than those without (13 out of 62) ($X^2(1, N = 93) = 6.83, p = 0.009$). Secondly, most of the usage patterns reported among our participants do not fall within the default time window of 8am to 5pm.

All but six of our participants reported typically using their computer on weekday evenings. The hours of use of just three participants fell within these limits. All were sole users of their devices. Looking at whether ‘active hours’ could be set to align with participants’ reported usage, 50 of our 64 participants sole computer users had an unbroken six-hour interval of non-use (as required for the feature to function best).

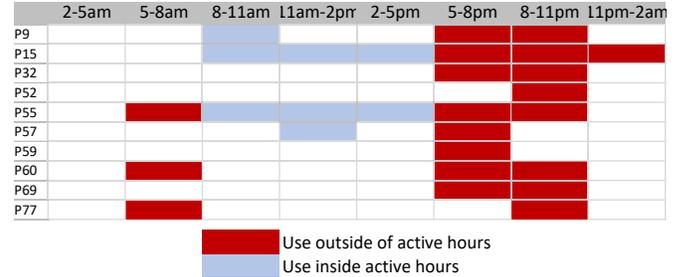


Fig. 6. Usage pattern of participants who reported being aware of ‘active hours’, but are using the default settings despite these being incompatible with their usage behaviours.

We also asked participants who were aware of the feature whether they had changed it from its default setting. Of the 26 participants that were aware of the feature, 10 had not changed it from the default despite their reported usage patterns being incompatible with the defaults (Figure 6). We hypothesise that the users were not aware of this mismatch themselves (being prompted in the survey may have been a first chance to reflect upon this, for instance).

We tested the answers given by those aware of the ‘active hours’ feature to other questions for signs of significantly different experiences, for example whether they had experienced an unexpected restart or whether they felt the computer always sought their permission before restarting, but none of the tests conducted showed statistically significant variations.

C. Proactive check of updates

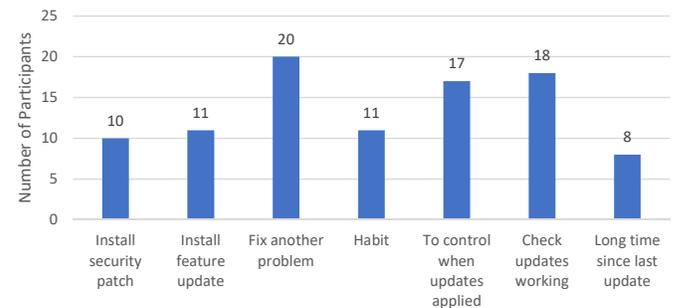


Fig. 7. Reasons why participants proactively checked for updates. Participants were able to select multiple reasons.

Half (46) of participants reported having proactively checked for updates in the past. There was no statistically significant correlation with the participants’ computing background. As to the reasons why participants checked for updates (Figure 7), the most popular reason overall, and particularly amongst participants who chose exactly one of our seven possible answer options, was to fix non-security, technical problems. The second and third most popular choices were

to check that updates are working and to better control when updates are installed. Being more perceptive to security risks was not a predictor of participants' inclination to check for updates, and checking for updates to fix security problems was only our sixth most reported reason. It was selected by none of the 25 participants who chose exactly one reason.

Users can limit the installation of updates by marking a network connection as 'metered'. Only six of our participants reported having employed this workaround. Although some online forums we had encountered had suggested this technique was particularly prevalent amongst gamers, they only accounted for half of the six, approximately the same proportion as across the survey sample.

D. Handling restarts

Due to the potential for restart requests to be particularly disruptive, we specifically wanted to capture how home users handled them. We wanted to understand what choices participants made and whether the features designed to help minimise their disruption were being used. We did this by constructing two hypothetical update scenarios within our survey. The first concerned the installation of a monthly cumulative update requiring a restart. The second, the installation of a feature update. To aid participants' recall, we illustrated our questions with screen images showing notifications for the restart scenarios (sampled from our virtual environment). The images reflected an 'out-of-the-box' Windows 10 desktop with no personalisation. The answer options were intended to elicit how a participant planned to eventually comply with the request for an (inevitable) restart. For both, we asked participants to imagine they were in the middle of an hour-long task on their computer that was important to them when the request appeared. If they chose to 'Restart now', we interpreted that choice as the most disruptive option given the context of the question. Ignoring the notification is potentially the least disruptive option, however if the user forgets about the pending restart but leaves their computer switched on but idle, the computer will restart itself, then possibly resulting in the loss of unsaved work.

We followed each scenario with a question to ask about participants' expectations for how long each restart would take, as a high-level analysis of customer support forums suggested users felt it was too long. Indeed, this has been an area of recent focus for Microsoft [38].

Around 7% of participants reported that they would 'Restart now' for both scenarios. In the first scenario, 30% (28) chose to restart the computer themselves once their task was complete. 40% (37) chose to 'update and shutdown' after they had finished using their computer. 30% of this latter group had previously stated that their computer was left on when not in use. When users were nudged towards picking a restart time in our second scenario, 40% (37) said they would choose this option, however 53% said they would choose to be reminded later with the intention of taking control of the restart themselves (regardless of having chosen a restart time).

With respect to the expected duration of the restart, approximately half (45) of our participants gave identical estimates for both scenarios. 58% of those (26 of 45) expected both restarts to take less than 15 minutes, and only 2 participants

expected to wait for more than 45 minutes. Two participants gave a lower estimate for the 'longer' feature update.

E. Sentiment toward updates

Our participants were generally positive towards updates overall. Referring to Figure 8, participants generally expressed positive sentiments about being given sufficient warning of pending restarts to apply an update; about controlling restarts and; not noticing updates downloading and installing in the background. On our two questions about a worry that the computer will not work after an update and there being too many restarts, desktop users were more complimentary than laptop users, but the result was outside statistical significance. A summary of our results of Likert-scale questions of participants' past experiences with updates can be seen in Figure 8.

Our survey had two sets of comparative questions. The first asked participants with experience of prior versions of Windows to indicate whether they felt updating Windows 10 was firstly easier and secondly causes fewer interruptions. On the former, 53% agreed and only 8% disagreed. On the latter, 43% agreed and 21% disagreed. The second question asked participants to compare their trust in Microsoft's ability to provide updates with other software producers. 95% of participants perceived Microsoft to be better (33%) or as good as (61%) other software producers.

F. Perception of online risks

We wanted to understand participants perception of the computer security risks which updates protect them from. We asked a Likert-scale question to assess if participants thought cyber criminals target 'other people' [39], whether they thought their machine could be used to facilitate crime (e.g., as part of a distributed denial of service attack), and whether participants related their personal security to the security of the web sites they trust.

A majority of our participants agreed with all our positively worded, Likert-scale items about the information security risks mitigated by updates. Levels of disagreement ranged from 24% to 4%. Most users however considered themselves not to be worthwhile targets, consistent with Wash's 'Big Fish' model [39]. These responses did not predict statistically significantly the awareness of the existence of the active hours feature. We did not find any sub-groups with statistically significantly different answers.

G. Impact of updates on other tasks

Just under half (44) of our participants reported experience of their computer restarting unexpectedly to install an update. These same participants were significantly (Fisher's exact test $p < 0.05$) more likely to agree with our statement that there were too many restarts to install updates, disagree with our statement that they had sufficient control over when their computer restarted, and disagree with our statement that their computer gives them sufficient warning when it needs to restart.

While a majority of 57% (52) of participants said the duration of restarts met their expectations, 42% (39) said they took longer than expected. This is similar but slightly

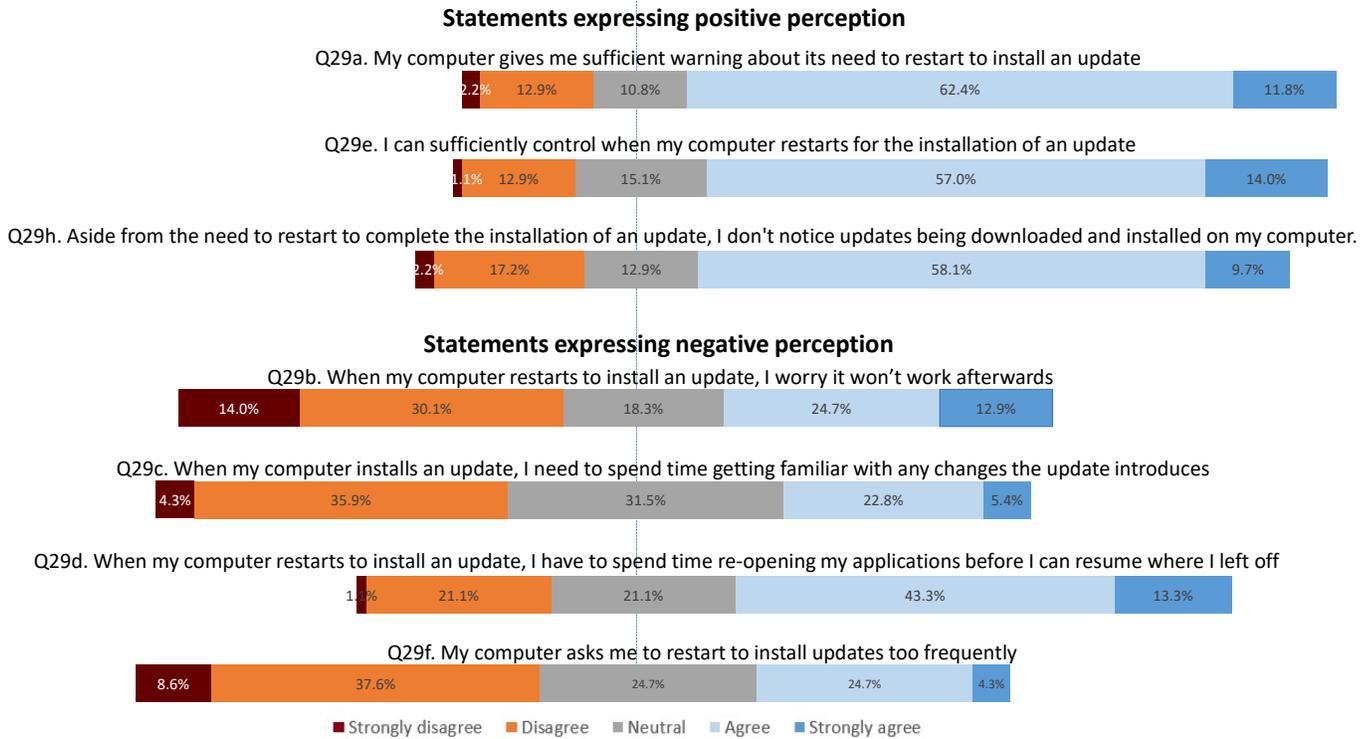


Fig. 8. Participants' perception statements relating to updates.

more positive than Vaniea and Rashidi's finding [40] for their users' perception of update installation times (at 43% and 45% respectively). Only one participant did not express an opinion. In a related question, half of participants agreed that the longer a restart took, the more concerned they became, and 70% of participants were positive about the helpfulness of the notifications in providing progress information during a restart. This latter result appeared to contradict the work of McGrenere et al [41], however they appear to have considered updates to Windows 10 from a previous version number. An aspect of restarting a computer that our participants generally agreed with overall was the need to spend time re-opening applications after a restart before primary tasks could be resumed (57% agreed, while 22% disagreed – see Figure 8).

V. DISCUSSION

A. The silent success story

Our participants perceived that updates added new features more often than fixing errors. Given that feature updates occur approximately every six months and quality updates occur monthly, perception does not match reality. One possible explanation is that users do not notice changes after quality updates, but at the same time do notice them after feature updates. This may be a natural consequence of Microsoft's adoption of practices similar to Vaniea's recommendation [7], to disentangle updates that change the user interface from those that address quality issues. Participants also underestimated the frequency of updates, believing that they occur less frequently than Microsoft's minimum release cycle. It suggests that some updates, including those requiring a restart, are being applied so silently [15] as not to be noticeable or memorable to our

participants. It is perhaps then worth considering that when users are asked for their opinions of updates, what is reported may only refer to a subset of updates (specifically those involving a prompt, and requiring a restart).

B. Keeping the appreciative user adequately informed

Participants did not appear to recognise and appreciate the implications of different types of updates (monthly cumulative vs. feature). The cues used by Windows are subtle, but the implications are potentially significant. As part of our own research, we measured the time taken by a cumulative monthly update in our virtual environment. Where this took 12 minutes, the feature update took 12 times longer². Microsoft claim that the average time for the April 2017 feature release was 82 minutes [38]. Therefore, we think a notification that describes an update as one 'that could take a little longer than other updates' is failing to set accurate expectations to support users in planning around the availability impact of these updates. This may be supported by our general finding that participants believe restarts take longer than expected. Currently, Windows gives neither an estimate before nor during the updating process, and our own research showed the progress indicator can progress unevenly. Vitale et al. [41] made similar observations, enforcing the findings of [40]. They argue 'reasonable [time] estimates must be possible', which we agree with.

C. Designing for consistent update behaviours

We think Windows is not sufficiently explicit in seeking user permission for updates and restarts. It has been designed

²Given our minimally specified virtual environment, our measurement may be close to the worse case.

to nudge users towards updating as quickly as possible. It may give users the impression of having a greater degree of control over restarts than they actually do. Although the initial restart notification offers a ‘Restart now’ option, the implied and less explicit alternative is to restart later at a time of the computer’s choosing, outside of active hours. It then becomes the responsibility of the user to intervene should they wish to stop it. Unlike other consumer-focused operating systems that provide a visual reminder of a pending restart (e.g., [42]), Windows 10 Home Edition does not. Our finding may be explained by the notion that experiencing an unexpected restart may make users more aware about their lack of control.

An existing control which could remedy this is to pick an alternative time within the next seven days for the restart. As discussed in Section III, unlike restart times chosen by the computer, the computer may restart at this time even if in active use. This is a potential source of confusion given the promise to ‘show a reminder when we’re going to restart’. If a user is absorbed by other tasks the computer could, in the mind of the user, appear to restart unexpectedly despite them having been responsible for the chosen time. We think that one’s computer should not reboot while in active use.

The ‘update pending’ notification in Microsoft Windows nudges users towards restarting their computer immediately, with no second chance to postpone a restart if they choose ‘Restart Now’. While we did not specifically ask whether this could have been the cause of any unexpected restarts reported by our participants, it is of note that only 6 participants in our first scenario and 7 participants in the second scenario chose the ‘Restart Now’ option. Constantine and Lockwood’s [43] ‘Simplicity Principle’ of user interface design recommends making common tasks short and simple. Our data suggests ‘Restart Now’ is not a common choice, putting into question whether it is an appropriate option to display.

D. Perceived value of OS updates

Participants conveyed a perception of value in updates. Updates are being applied, and at the same time are not perceived to cause much (if any) disruption. However, the ‘shock’ of updates that create problems is not avoided, an example being the initial release of the ‘1809’ (September 2019) feature update; installation of update 1809 deleted the personal files of a very small number of users with a particular configuration [44]. The update was subsequently withdrawn. To adopt an update model like that of Windows 10 Home Edition is to shift some of the burden of effective updates onto developers, to ensure that updates are not *destructive*, especially if the user has no choice as to whether to avoid the update or not. While Windows offers the ability to uninstall updates, this would not recover lost user data in the above example. Perhaps it is time for Windows to integrate an automatic snapshot feature that allows for immediate roll-back.

E. Limitations

This survey study suffers from similar limitations to other survey studies in security, namely that behaviours are self-reported [45]. One further limitation is that we were unable to query participant’s experiences immediately after the update events. Some of the reported information, such as

perceived event frequencies and impacts, may be informed by experiences distant in time. However, these are nonetheless the perceptions held by participants who are active users of Windows 10 Home Edition. If users were given more capacity to shape the (albeit increasingly unavoidable) update process, their perceptions of past experiences may govern how they configure future interactions with update mechanisms.

VI. CONCLUSIONS

Here we analysed the behaviour of the automatic update feature of Windows 10 Home Edition, contrasting behaviour with an online survey of the experiences and perceptions of 93 UK-based users. A model of Windows 10 Home Edition behaviours highlighted inconsistencies in the restart behaviour: In one circumstance, Windows would reboot to finish installing quality updates even if the device was in active use. The default setting of the ‘active hours’ feature was compatible with the usage pattern of only three survey participants. 28% of participants were aware of the active hours feature. If properly adjusted, the usage pattern of 78% of participants could be captured by the active hours feature. It is not surprising then that around half of participants reported unexpected restarts.

Despite this, the automatic update behaviour of Windows 10 can be considered a (perceived) success. Our participants valued the updates and trust in Microsoft’s ability to provide updates which benefit them. The quality of updates and the delivery of updates appear to be sufficiently reliable that our participants did not report an impact from quality updates.

A. Recommendations

While it is important that security updates are installed in a timely manner, we believe that Windows’ current policy is overly static. Given that many applications do not yet support Microsoft’s restart API (see Section III), restarts should only occur automatically if all running applications support this API. It is not obvious to users if an application supports this feature, where Microsoft could use its market position to improve support. Regardless, we believe that restarts should not occur if the system is in active use (especially so if retrieval of application state is not guaranteed).

The ‘active hours’ feature is arguably flawed. Prompts to users act to shape the installation of updates, but not the shaping of preemptive controls such as active hours: relating adaptability to visibility, the user is in control with no control. Based on the limited use of active hours reported by our participants, an alternative may be for Windows to learn sensible defaults from usage activity and set appropriate restart times automatically. This suggests a strand of further work to anticipate reactions to updates from prior and current interactions with the computer, rather than with updates specifically.

B. Data availability

The full survey text is available in the Appendix, and can also be found alongside participant responses at DOI 10.14324/000.ds.10066165.

Acknowledgements

We would like to thank our reviewers as well as Tristan Caulfield for their constructive, detailed feedback.

REFERENCES

- [1] NCSA. (2017). Malware and Botnets, [Online]. Available: <https://staysafeonline.org/stay-safe-online/online-safety-basics/malware-and-botnets/> (visited on 07/01/2018).
- [2] Cyber Aware. (2016). Software and App Updates, [Online]. Available: <https://www.cyberaware.gov.uk/software-updates> (visited on 11/10/2018).
- [3] US-CERT. (2015). Before You Connect a New Computer to the Internet, [Online]. Available: <https://www.us-cert.gov/ncas/tips/ST15-003> (visited on 08/10/2018).
- [4] Symantec. (2017). The Importance of General Software Updates and Patches, [Online]. Available: <https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html> (visited on 04/01/2018).
- [5] S. Frei, "The Security Exposure of Software Portfolios," Secunia, Tech. Rep., 2010.
- [6] C. Ioannidis, D. Pym, and J. Williams, "Information security trade-offs and optimal patching policies," *European Journal of Operational Research*, vol. 216, no. 2, pp. 434–444, 2012, ISSN: 0377-2217. DOI: 10.1016/j.ejor.2011.05.050.
- [7] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," ACM Press, 2014, pp. 2671–2674, ISBN: 978-1-4503-2473-1. DOI: 10.1145/2556288.2557275.
- [8] Microsoft. (2018). Security Update Guide, [Online]. Available: <https://portal.msrc.microsoft.com/en-us/> (visited on 07/01/2018).
- [9] K. E. Vaniea, Human factors of software updates - Microsoft Research Presentation, 2015.
- [10] Wikipedia. (2018). Patch Tuesday. Page Version ID: 845541287, [Online]. Available: https://en.wikipedia.org/w/index.php?title=Patch_Tuesday&oldid=845541287 (visited on 11/10/2018).
- [11] P. Oliveria. (2006). Patch Tuesday... Exploit Wednesday, [Online]. Available: <https://blog.trendmicro.com/trendlabs-security-intelligence/patch-tuesday-exploit-wednesday/> (visited on 11/10/2018).
- [12] I. Ion, R. Reeder, and S. Consolvo, "'... No one Can Hack My Mind': Comparing Expert and Non-Expert Security Practices.," in *SOUPS*, vol. 15, 2015, pp. 1–20.
- [13] S. Dodier-Lazaro, I. Becker, J. Krinke, and M. A. Sasse, "No Good Reason to Remove Features: Expert Users Value Useful Apps over Secure Ones," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, Springer, Cham, 2017, pp. 25–44. DOI: 10.1007/978-3-319-58460-7_3.
- [14] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, 2009, pp. 133–144.
- [15] T. Duebendorfer and S. Frei, "Why silent updates boost security," ETH Zurich, Technical Report 302, 2009.
- [16] S. Frei, T. Duebendorfer, and B. Plattner, "Firefox (in) security update dynamics exposed," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 16–22, 2008.
- [17] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 New Security Paradigms Workshop*, ACM, 2009, pp. 47–58.
- [18] C. Herley, "More Is Not the Answer," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 14–19, 2014, ISSN: 1540-7993. DOI: 10.1109/MSP.2013.134.
- [19] U. Decker. (2017). Windows 10 - Prevent Auto-Reboot after Installing Updates (Anniversary Update), [Online]. Available: <https://www.udse.de/en/windows-10-reboot-blocker> (visited on 07/01/2018).
- [20] StackExchange Community Wiki. (2016). Sleep - Conclusively stop wake timers from waking Windows 10 desktop, [Online]. Available: <https://superuser.com/a/973029/> (visited on 11/05/2018).
- [21] J. Schofield, "How can I stop an unexpected Windows 10 update?" *The Guardian*, 2018.
- [22] R. Wash, E. Rader, K. Vaniea, and M. Rizor, "Out of the loop: How automated software updates cause unintended security consequences," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014, pp. 89–104.
- [23] O. Bergman and S. Whittaker, "The Cognitive Costs of Upgrades," *Interacting with Computers*, vol. 30, no. 1, pp. 46–52, 2018, ISSN: 0953-5438. DOI: 10.1093/iwc/iwx017.
- [24] A. Mathur, J. Engel, S. Sobti, V. Chang, and M. Chetty, "'They Keep Coming Back Like Zombies': Improving Software Updating Interfaces," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, OCLC: 255312726, Denver, CO, USA: Usenix Association, 2016, ISBN: 978-1-931971-31-7.
- [25] Y. Tian, B. Liu, W. Dai, B. Ur, P. Tague, and L. F. Cranor, "Supporting Privacy-Conscious App Update Decisions with User Reviews," ACM Press, 2015, pp. 51–61, ISBN: 978-1-4503-3819-6. DOI: 10.1145/2808117.2808124.
- [26] M. Fagan, M. M. H. Khan, and N. Nguyen, "How does this message make you feel? A study of user perspectives on software update/warning message design," *Human-centric Computing and Information Sciences*, vol. 5, no. 1, p. 36, 2015, ISSN: 2192-1962. DOI: 10.1186/s13673-015-0053-y.
- [27] S. Farhang, J. Weidman, M. M. Kamani, J. Grossklags, and P. Liu, "Take It or Leave It: A Survey Study on Operating System Upgrade Practices," p. 16, 2018.
- [28] W. K. Edwards, E. S. Poole, and J. Stoll, "Security automation considered harmful?" In *Proceedings of the 2007 Workshop on New Security Paradigms*, ACM, 2008, pp. 33–42.
- [29] R. Wash and E. Rader, "Influencing mental models of security: a research agenda," in *Proceedings of the 2011 New Security Paradigms Workshop*, ACM, 2011, pp. 57–66.
- [30] D. Halfin, B. Lich, nickbrower, nathan-mercier, J. Decker, and L. Poggemeyer. (2017). Manage Device Restarts after Updates (Windows 10), [Online]. Available: <https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart#engaged-restart> (visited on 07/01/2018).
- [31] Microsoft. (2018). Automatic Maintenance (Windows), [Online]. Available: <https://docs.microsoft.com/en-gb/windows/desktop/TaskSchd/task-maintenance> (visited on 10/05/2018).

- [32] —, (2018). Microsoft Community, [Online]. Available: <https://answers.microsoft.com/en-us> (visited on 10/05/2018).
- [33] —, (2018). Registering for Application Restart (Windows), [Online]. Available: <https://docs.microsoft.com/en-gb/windows/desktop/Recovery/registering-for-application-restart> (visited on 07/01/2018).
- [34] C. Gkantsidis, T. Karagiannis, and M. VojnoviC, “Planet Scale Software Updates,” in *Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, ser. SIGCOMM ’06, New York, NY, USA: ACM, 2006, pp. 423–434, ISBN: 978-1-59593-308-9. DOI: 10.1145/1159913.1159961.
- [35] G. Thapar, J. Li, and S. Ramlan, “Initiating update operations,” US9405526B2, 2016.
- [36] Office for National Statistics. (2016). How Has the Student Population Changed? [Online]. Available: <https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/livebirths/articles/howhasthestudentpopulationchanged/2016-09-20> (visited on 10/01/2018).
- [37] S. Furnell, J. van Niekerk, and N. Clarke, “The price of patching,” *Computer Fraud & Security*, vol. 2014, no. 8, pp. 8–13, 2014, ISSN: 13613723. DOI: 10.1016/S1361-3723(14)70521-4.
- [38] J. Conway. (2018). We’re Listening to You — Feature Update Improvements, [Online]. Available: <https://insider.windows.com/en-us/articles/were-listening-to-you/> (visited on 07/01/2018).
- [39] R. Wash, “Folk models of home computer security,” in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ACM, 2010, p. 11.
- [40] K. Vaniea and Y. Rashidi, “Tales of Software Updates: The process of updating software,” in *Proceedings for Computer Human Interaction (CHI) 2016*, San Jose, CA, USA: ACM Press, 2016, pp. 3215–3226, ISBN: 978-1-4503-3362-7. DOI: 10.1145/2858036.2858303.
- [41] F. Vitale, J. McGrenere, A. Tabard, M. Beaudouin-Lafon, and W. Mackay, “High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades,” in *CHI 2017*, Denver, United States: ACM, 2017, pp. 4242–4253. DOI: 10.1145/3025453.3025509.
- [42] Google. (2014). Update Your Chromebook’s Operating System - Chromebook Help, [Online]. Available: <https://support.google.com/chromebook/answer/177889?hl=en-GB> (visited on 10/03/2018).
- [43] L. L. Constantine and L. A. Lockwood, *Software For Use*. Massachusetts 01867: Addison Wesley Longman, Inc., 1999, ISBN: 0-201-92478-1.
- [44] J. Cable. (2018). Updated version of Windows 10 October 2018 Update released to Windows Insiders, [Online]. Available: <https://blogs.windows.com/windowsexperience/2018/10/09/updated-version-of-windows-10-october-2018-update-released-to-windows-insiders/> (visited on 11/23/2018).
- [45] R. Wash and E. J. Rader, “Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users.,” in *SOUPS*, 2015, pp. 309–325.

APPENDIX

This appendix lists the full survey instrument. Note Q1 has been omitted from this listing as it is an administrative question for prolific academic. The original numbering has been maintained for consistency. All text below appeared in the survey. The screenshots appeared immediately after the question. Where the caption of a screenshot describes the content of the screenshot, this description was also included in the survey text. Where there is no description present, none was given in the real survey either.

Q2. Have you ever worked or studied for a qualification in a computer-related field?

For example, answer 'Yes' if you've studied computer science at school or college or if you've worked in a computing related field such as computer programming, IT management or computer networking. [Compulsory, Choose-one]

- Yes
- No

Q3. Which of these answers best describes who takes responsibility for the maintenance of your computer?

Maintenance includes things like installing new applications or creating new accounts for additional people to use your computer. 'Other people' might be a family member, friend or a shop or call centre worker who provides you with a technical support service. [Compulsory, Choose-one]

- I do all of the maintenance myself
- I do most of the maintenance myself but occasionally seek help from other people
- I leave most of the maintenance to other people
- I leave all the maintenance to other people
- Not sure

Q4. Please describe your level of experience of each of these versions of Windows?

[Compulsory, Select for each item from: Used Extensively / Used moderately / Used a little / Not used / Not sure]

- Windows 95
- Windows 98
- Windows ME
- Windows Vista
- Windows 7
- Windows 8
- Windows 10

————— New survey page —————

Q5. Do you use your computer for any of the following purposes?

[Optional, Multiple choice]

- Using websites
- Email
- Gaming
- Running 'office' applications e.g. word processing, spreadsheets and presentations
- Online banking
- Online shopping
- Social media
- Video conferencing e.g. Skype

Q6. Thinking of the things you use your computer for and using the 5 point scale below, how would you describe...
[Compulsory, Select for each item from: Very Slow / Slow / Neither noticeably slow nor noticeably fast // Fast / Very fast]

- the speed of your computer

Q7. Do you share your computer with other people?
[Compulsory, Choose-one]

- Yes, there's at least one other person in my household who uses it regularly
- Yes, there's at least one other person outside my household who uses it regularly.
- Yes, there's at least one other person in my household and at least one other person outside my household who use it regularly.
- No, I'm the only person who uses it regularly

Q8. Which answer best describes what happens to your computer when no one is using it? [Compulsory, Choose-one]

- It's left on all the time
- It's left on all the time but the screen switches off after a period of inactivity.
- It's put into 'sleep' mode
- It's put into 'hibernate' mode
- It's 'shut down'
- I do something else
- I'm not sure

Q9. Approximately on how many days each week is your computer used? [Compulsory, Choose-one]

- At least once a day
- 5-6 days each week
- 2-4 days each week
- At most once a week

Q10. Do you typically use your computer on weekdays?
[Compulsory, Choose-one]

- Yes
- No

Q11. On weekdays when you use your computer, when do you typically use it?

[Compulsory, Multiple choice, Shown if answer to Q10 is 'Yes']

- Between 2 am and 5 am
- Between 5 am and 8 am
- Between 8 am and 11 am
- Between 11 am and 2 pm
- Between 2 pm and 5 pm
- Between 5 pm and 8 pm
- Between 8 pm and 11 pm
- Between 11 pm and 2 am

Q12. Do you typically use your computer on weekends?
[Compulsory, Choose-one]

- Yes
- No

Q13. On weekends when you use your computer, when do you typically use it?

[Compulsory, Multiple choice, Shown if answer to Q12 = 'Yes']

- Between 2 am and 5 am
- Between 5 am and 8 am
- Between 8 am and 11 am
- Between 11 am and 2 pm
- Between 2 pm and 5 pm
- Between 5 pm and 8 pm
- Between 8 pm and 11 pm
- Between 11 pm and 2 am

Q14. Approximately how long have you had your computer?

[Compulsory, Choose-one]

- Less than a month
- Between a month and 6 months
- Between 6 months and 1 year
- Between 1 and 2 years
- Between 2 and 3 years
- 3 years or more

Q15. My computer is...

[Compulsory, Choose-one]

- A laptop computer
- A desktop computer
- A tablet computer
- A combined laptop/tablet computer
- Not sure

————— New survey page —————

Q16. How frequently do you believe each of the following statements about software updates for the Windows 10 operating system is true?

[Compulsory, Select for each item from: Always / Often / Occasionally / Rarely / Never / Don't Know]

- They fix errors in the software on my computer
- They introduce errors into the software on my computer
- They help to keep me safe
- They change the appearance of my system
- They introduce new features
- They remove features
- They stop other software on my computer from working
- Microsoft charge me for them
- They are installed automatically
- Please select 'Never' as the answer to this question
- My computer needs to be restarted when updates are installed
- My computer asks for my permission before it restarts to install an update

Q17. Which answer best describes how often you believe new updates for your Windows 10 computer are released?

[Compulsory, Choose-one]

- There's a new update every six months
- There's a new update every two months
- There's a new update every month
- There's a new update every week

- There's a new update every day
- Not sure

————— New survey page —————

Q18. To what extent do you agree or disagree with each of the following statements?

[Compulsory, Select for each item from: Strongly agree / Agree / Neither agree or disagree / Disagree / Strongly disagree]

- My computer could be affected by cyber criminals
- The data on my computer would be of value to cyber criminals
- My online data would be of value to cyber criminals
- My computer could be used by cyber criminals to affect other people
- Web sites I use could be attacked by cyber criminals

————— New survey page —————

Q19. Is the message shown in Figure 9 familiar to you?

[Compulsory, Choose-one]

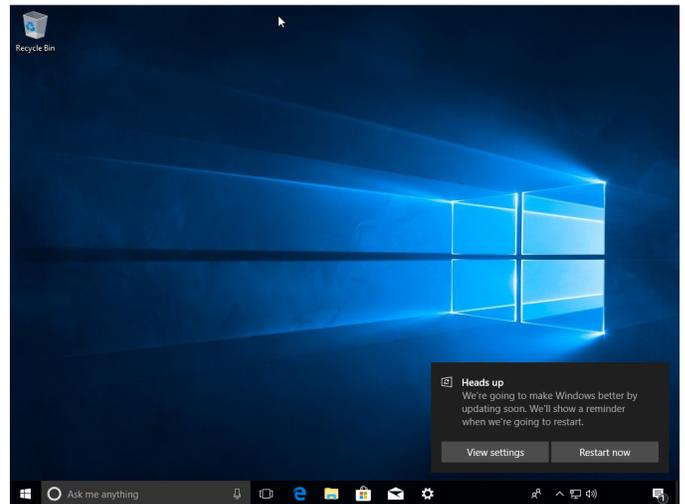


Fig. 9. Screenshot of Windows for Q19. The message in the image reads: 'Heads up. We're going to make Windows better by updating soon. We'll show a reminder when we're going to restart.' The two buttons are labelled 'View settings' and 'Restart now'.

- Yes, I've seen this message before
- No, I don't recall seeing this message before
- Not sure

Q20a. Think back to what you've done in the past when you've seen this message. If you are in the middle of an hour-long task on your computer that is important to you when the message appears, which answer best describes how you would typically respond?

[Compulsory, Choose-one, Shown if answer to Q19 = 'Yes']

- I would ignore the message because I don't understand it
- I would press 'Restart now'
- I would press 'View Settings'
- I would make a special point of 'restarting' later myself after my task is complete

- I would choose to ‘Update and shut down’ later when I’ve finished using my computer
- I would leave my computer to restart on its own later
- I would ask someone else for advice about what to do next

Q20b. If you are in the middle of an hour-long task on your computer that is important to you when the message appears, which answer best describes how you would expect to respond?

[Compulsory, Choose-one, Shown if answer to Q19 = ‘No’ or ‘Not sure’]

- I would ignore the message because I don’t understand it
- I would press ‘Restart now’
- I would press ‘View Settings’
- I would make a special point of restarting my computer myself after my task is complete
- I would choose to ‘Update and shut down’ later when I’ve finished using my computer
- I would leave my computer to restart on its own later
- I would ask someone else for advice about what to do next

Q21. Approximately how much time would you expect the restart required by this update to take on your computer?

[Compulsory, Choose-one]

- Less than 5 minutes
- 5 – 14 minutes
- 15 – 29 minutes
- 30 – 44 minutes
- 45 – 59 minutes
- 60 – 89 minutes
- 90 – 119 minutes
- 2 hours or more

Q22. To the best of your knowledge, has your computer ever restarted to install an update unexpectedly?

[Compulsory, Choose-one]

- Yes
- No
- Not sure

Q23. How would you describe the behaviour of your computer when it restarted unexpectedly?

[Compulsory, Choose at most three, Shown if answer to Q22 = ‘Yes’]

- Disruptive
- Inconsiderate
- Inflexible
- Prudent
- Cautious
- Necessary
- Protective
- Clever
- Forward-thinking

————— New survey page —————

Q24. Like the last section, imagine you are using your computer to work on a task that is important to you when

a message like the one in Figure 10 appears. You must choose an option before you can resume your work. What would you choose to do?

[Compulsory, Choose-one]

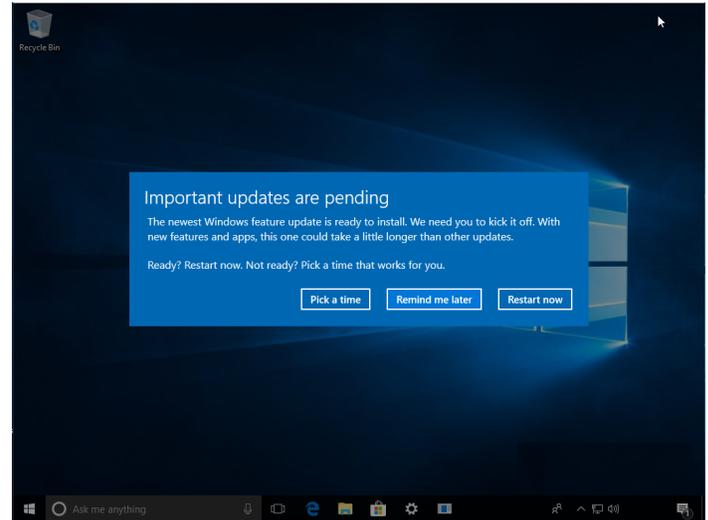


Fig. 10. Screenshot of Windows for Q24. The message in the image reads: ‘Important updates are pending. The newest Windows feature update is ready to install. We need you to kick it off. With new features and apps, this one could take a little longer than other updates. Ready? Restart now. Not ready? Pick a time that works for you.’ The buttons are labelled ‘Pick a time’, ‘Remind me later’ and ‘Restart now’.

- Press ‘Pick a time’
- Press ‘Remind me later’
- Press ‘Restart now’

Q25. How would you eventually choose to restart your computer?

[Compulsory, Choose-one, Shown if answer to Q24 = ‘Remind me later’]

- I would make a special point of restarting my computer myself after my task is complete
- I would choose to ‘Update and shut down’ when I’ve finished using my computer
- I would eventually ‘Pick a time’ and leave my computer to automatically restart itself
- I would ask someone else for advice
- I would do something else

Q26. Approximately how much time would you expect this restart to take on your computer?

[Compulsory, Choose-one]

- Less than 5 minutes
- 5 – 14 minutes
- 15 – 29 minutes
- 30 – 44 minutes
- 45 – 59 minutes
- 60 – 89 minutes
- 90 – 119 minutes
- 2 hours or more

————— New survey page —————

Q27. Sometimes when an update is being installed, a ‘Working on Updates’ or ‘Configuring updates’ screen like the one in Figure 11 is displayed. Is this screen familiar to you?

[Compulsory, Choose-one]

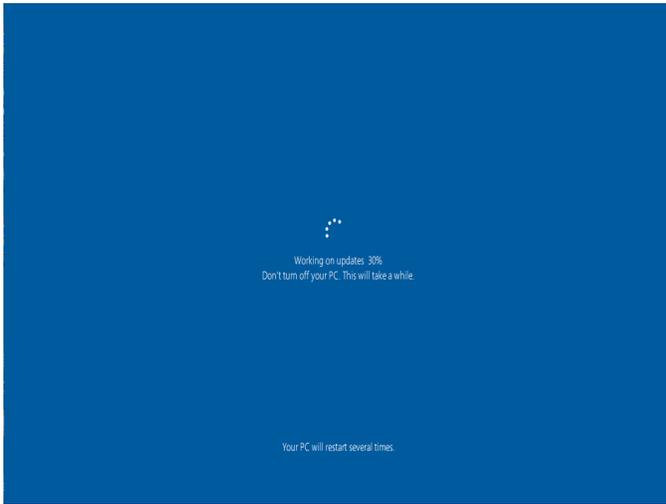


Fig. 11. Screenshot of Windows for Q27.

- Yes, I’ve seen this screen before
- No, I’ve not seen this screen before
- Not sure

Q28. To what extent do you agree or disagree with the following statements?

[Compulsory, Select for each item from: Strongly agree / Agree / Neither agree or disagree / Disagree / Strongly disagree, Only shown if answer to Q27 = ‘Yes’]

- This screen gives me helpful information about the update’s progress
- The longer this screen appears the more concerned I become

————— New survey page —————

Q29. To what extent do you agree or disagree with each of the following statements?

[Compulsory, Select for each item from: Strongly agree / Agree / Neither agree or disagree / Disagree / Strongly disagree / Not sure]

- My computer gives me sufficient warning about its need to restart to install an update
- When my computer restarts to install an update, I worry it won’t work afterwards
- When my computer installs an update, I need to devote time to getting familiar with any changes the update introduces
- When my computer restarts to install an update, I have to spend time re-opening my applications before I can resume where I left off
- I can sufficiently control when my computer restarts for the installation of an update
- My computer asks me to restart to install updates too frequently

- Please select ‘Neither’ as the answer to this question
- Aside from the need to restart to complete the installation of an update, I don’t notice updates being downloaded and installed on my computer

Q30. Restarting my computer to complete the installation of an update takes...

[Compulsory, Select one]

- A lot more time than I expect
- More time than I expect
- About the amount of time I expect
- Less time than I expect
- A lot less time than I expect
- Don’t know

Q31. To what extent do you agree or disagree with each of the following statement?

[Compulsory, Select for each item from: Strongly agree / Agree / Neither agree or disagree / Disagree / Strongly disagree, Only shown if answer to Q4 reports ‘extensive’ or ‘moderate experience’ of any version of Windows prior to Windows 10]

- Updating Windows 10 is easier than previous versions of Windows
- Updating Windows 10 does not interrupt my work as much as previous versions of Windows

Q32. Windows limits the software updates it downloads and installs to the most important ones if the current network connection has been marked as ‘metered’. Have you ever marked a connection as ‘metered’ only because you wanted to reduce the number of updates installed?

A metered network connection is one where the more it’s used, the more you are charged e.g. mobile/cellular networks may charge on this basis. Thus by limiting the number of software updates that are downloaded, Windows tries to limit the charges. [Compulsory, Select one, Shown if answer to Q3 is ‘all’ or ‘most’ maintenance myself]

- Yes
- No
- Not sure

————— New survey page —————

Q33. Windows 10 allows users to proactively check for new updates by pressing the ‘Check for updates’ button in the ‘Settings’ application (as seen in Figure 12). If any are found, it will immediately download and install them. Have you proactively checked for updates in the past?

[Compulsory, Select one]

- Yes
- No
- Not sure

Q34. Why have you proactively checked for updates in the past?

[Compulsory, Multiple choice, Shown if answer to Q33 is ‘Yes’]

- Because I’ve wanted to install an update to fix a security problem I’d heard about

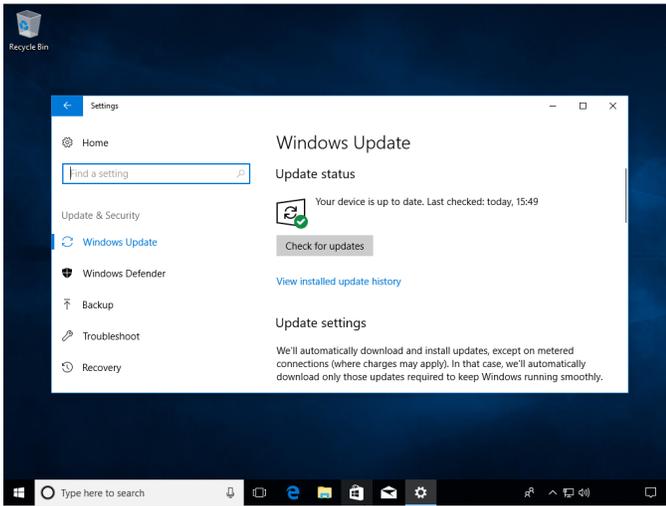


Fig. 12. Screenshot of Windows for Q33.

- Because I've wanted to install a new feature update I'd heard about
- Because I've encountered a problem on my computer that I'd hoped an update might fix
- I make it a habit to regularly check for new updates for security reasons
- Because by proactively checking for new updates I can better control when they get installed
- Because I've wanted to check the update system is working correctly.

————— New survey page —————

Q35. 'Active hours' is a Windows 10 feature that allows users to specify a period of time when their computer is normally in use. If a software update needs to restart the computer, the computer will avoid restarting it during that period. An image of the screen used to set the feature is shown in Figure 13. Prior to this survey, were you aware of this feature?

[Compulsory, Select one]

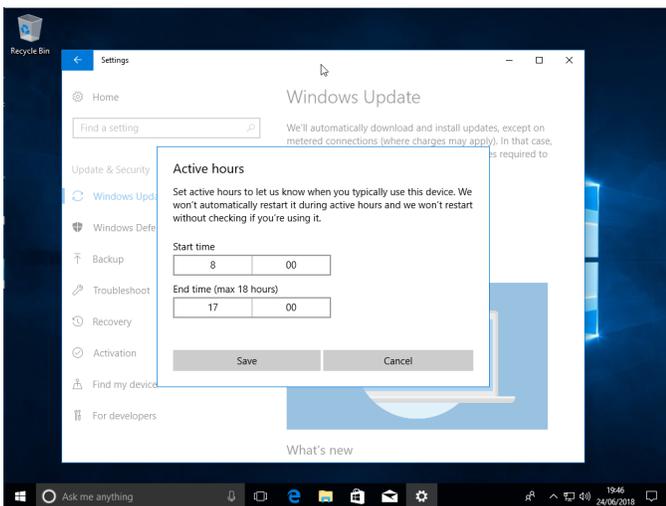


Fig. 13. Screenshot of Windows for Q35.

- Yes
- No

Q36. The default setting for 'Active Hours' is from 8am to 5pm. To the best of your knowledge, has the 'Active Hours' period been changed on your computer?

By 'default setting', we mean when a new Windows 10 computer is used for the first time, 'Active Hours' will be set to 8am to 5pm. You can see the 'Active Hours' period on your computer by opening the 'Settings' application, choosing 'Update & Security' then click on 'Change active hours'. Press the Cancel button to close the window without changing the setting. [Compulsory, Select one, Shown if answer to Q35 is 'Yes']

- Yes
- No
- Not sure

————— New survey page —————

Q37. Windows 10 includes a feature that allows you to limit the amount of your computer's internet bandwidth that it uses to download software updates. For example, it can be limited to 45% of the available capacity. An image of the screen used to set up the feature is shown in Figure 14. Prior to this survey, were you aware of this feature?

[Compulsory, Select one, Shown if answer to Q3 is 'I do

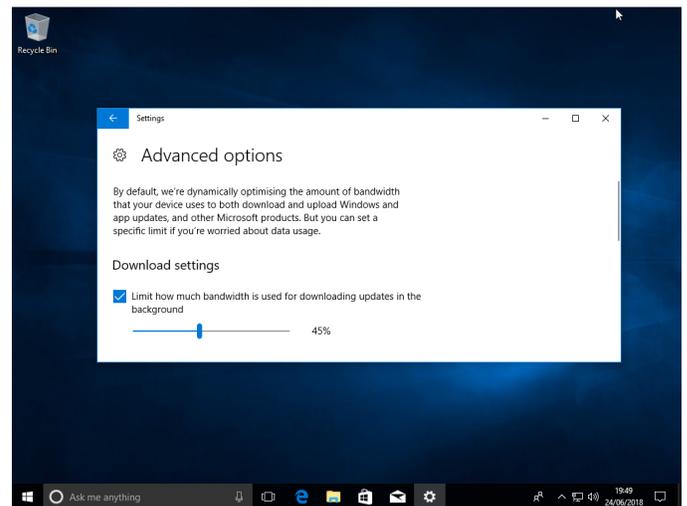


Fig. 14. Screenshot of Windows for Q37.

most of the maintenance myself but occasionally seek help from other people' or 'I do all of the maintenance myself']

- Yes
- No

Q38. Have you used this feature?

[Compulsory, Select one, Shown if answer to Q37 is 'Yes']

- Yes
- No
- Not sure

————— New survey page —————

Q39. Windows 10 includes a ‘Windows Update Troubleshooter’ for identifying and fixing problems with the installation of updates. An image of the screen used to run the trouble-shooter is shown in Figure 15. Prior to this survey, were you aware of this feature?

[Compulsory, Select one, Shown if answer to Q3 is ‘I do

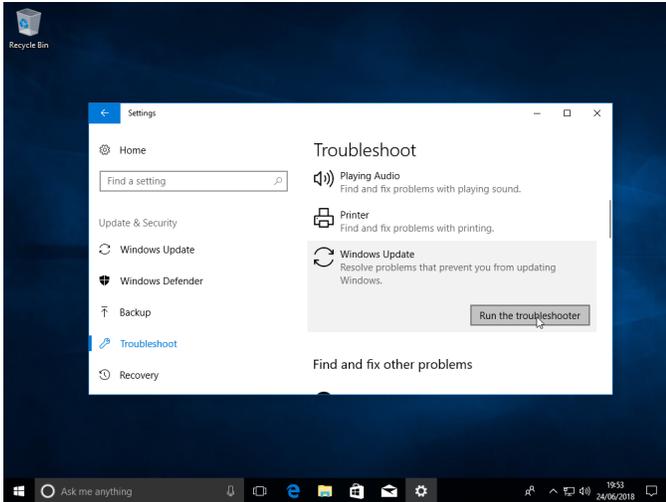


Fig. 15. Screenshot of Windows for Q39.

most of the maintenance myself but occasionally seek help from other people’ or ‘I do all of the maintenance myself’]

- Yes
- No

Q40. Have you tried to use this feature?

[Compulsory, Select one, Shown if answer to Q39 is ‘Yes’]

- Yes
- No
- Not sure

————— New survey page —————

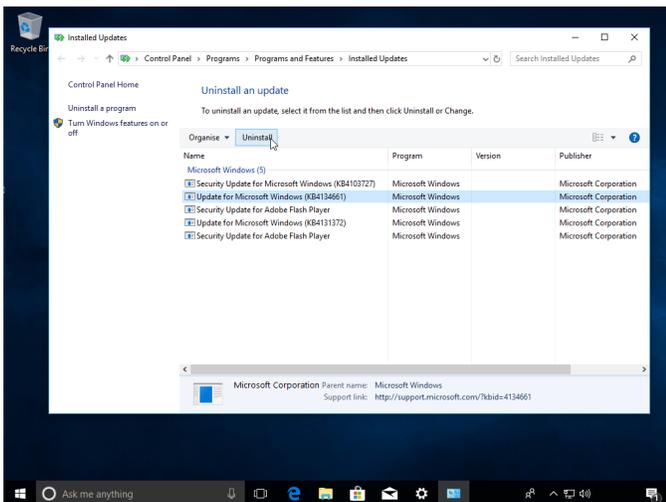


Fig. 16. Screenshot of Windows for Q41.

Q41. Windows 10 includes a feature that allows an update to be un-installed. You might consider doing this if

you suspect a specific update caused a problem with your computer. An image of the screen for the feature is shown in Figure 16. Prior to this survey, were you aware of this feature?

[Compulsory, Select one]

- Yes
- No

Q42. Have you used this feature?

[Compulsory, Select one, Shown if answer to Q41 is ‘Yes’]

- Yes
- No
- Not sure

————— New survey page —————

Q43. To what extent do you agree or disagree with each of the following statements?

[Compulsory, Select for each item from: Strongly agree / Agree / Neither agree or disagree / Disagree / Strongly disagree]

- I trust Microsoft to provide the updates for their software I need to keep my computer safe
- I trust other software producers to provide the updates for their software I need to keep my computer safe
- Updates are convenient
- Updates keep me safe

Q44. How certain are you of the accuracy of your responses to this survey?

[Compulsory, Select one]

- uncertain / guessing
- mostly uncertain
- mostly certain
- certain

Thank you for participating!