Understanding Home Router Configuration Habits & Attitudes

Junjian Ye
Nanjing University of Posts and Telecommunications
Nanjing, China
jjy470742953@gmail.com

Xavier de Carné de Carnavalet
Radboud University
Nijmegen, The Netherlands
xavier.carnavalet@ru.nl

Lianying Zhao
Carleton University
Ottawa, Canada
lianying.zhao@carleton.ca

Lifa Wu
Nanjing University of Posts and Telecommunications
Nanjing, China
wulifa@njupt.edu.cn

Mengyuan Zhang
Vrije Universiteit Amsterdam
Amsterdam, The Netherlands
m.zhang@vu.nl

Abstract

Home routers serve as a gateway to the Internet and configuration issues such as weak passwords can simply be introduced by users that configured them, potentially leading to severe consequences. The most critical phase in the lifecycle of a home router is perhaps the initial setup intended for users to complete. Yet, the mindset and behavior of users during this process remain under-explored. In a comprehensive online survey of 392 participants across several regions, we find that router settings and user behavior vary significantly between China and English-speaking countries, influenced by factors like IT background, age, gender, and education. A majority of participants go through the configuration of their own routers, but many also admit keeping the default settings and are not actively maintaining their router firmware up-to-date, leaving security vulnerabilities unfixed. We estimate that 91% of participant routers run with default settings, which should push router manufacturers to focus on safe defaults. Moreover, while default passwords are often changed, some participants report coping strategies. With noteworthy differences that we have observed across user backgrounds, we believe that our takeaways can shed some light on advancing the area of home network security.

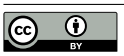
CCS Concepts

• **Human-centered computing** → **Empirical studies in HCI**; **Empirical studies in HCI**; • **Security and privacy** → *Embedded systems security*.

Keywords

Home router security, configuration habits, password selection, automatic updates

ACM Reference Format:
Junjian Ye, Xavier de Carné de Carnavalet, Lianying Zhao, Lifa Wu, and Mengyuan Zhang. 2025. Understanding Home Router Configuration Habits & Attitudes. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3706598.3714231



CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3714231

1 Introduction

As of 2025, there have been 5.52 billion active Internet users worldwide, accounting for 67.5% of the global population [25]. Home routers are common network devices used to connect home users to the Internet [7]. Most home routers (hereafter called routers) support Wi-Fi communications to connect smartphones, laptops, and IoT devices [4].

While router manufacturers have a share of the responsibility to make secure products, currently, part of the burden to keep a router secure remains on the end user. Routers provide various features and options, whose proper configuration determines security. For instance, if users create an open Wi-Fi network without any access restriction (e.g., no passphrase), anyone within the home or in close proximity will be able to connect to that network and potentially gain unauthorized access to connected devices and sensitive information. Moreover, default settings often prioritize convenience over security. For example, many routers come with default administrator usernames and passwords (e.g., admin/admin) that are easily guessable or publicly documented [23], enabling attackers to gain control over the router's settings (cf. the Mirai botnet [19]). An attacker with control over the router can modify DNS settings to redirect users to fraudulent websites [2, 3], or enable port forwarding to expose internal network services to the public Internet, both of which could have severe security implications. Infected routers could also become part of a botnet and leveraged by attackers in Distributed Denial of Service (DDoS) attacks [19].

Even when WiFi networks are encrypted, some default passphrases are guessable due to predictable algorithms [18] or may not have enough entropy [10]. In the current state-of-the-practice, users are often expected to change such settings to ensure security.

Furthermore, the advent of the Internet of Things (IoT) has resulted in a proliferation of smart devices that are connected to home networks, increasing the stakes when it comes to router security. An attacker who gains control of a router could not only compromise computers and smartphones but also smart home devices like security cameras, door locks, and thermostats.

After a new router is purchased, the initial setup (or setup wizard) is often the first point of contact that users have with their

device's security features. During this crucial stage, users are guided through a sequence of steps for basic settings, which often include setting an administrator password, configuring Wi-Fi networks, and proceeding to upgrade the firmware [34]. Routers may work right out-of-the-box, which we call plug-and-play routers, for which a manual setup is not necessary for connecting to the Internet. Defaults are therefore even more likely to remain in place.

While prior studies explored user behaviors towards password selection [16, 27, 33] and attitude towards software updates [13, 17], home router setup is unique in that it combines changing two passwords (admin and WiFi), ensuring safe WiFi protocols, managing (auto-)updates, and possibly configuring other services, e.g., registering the device with the vendor or creating an account for remote management, and more importantly has higher security impact if not properly done, due to the router's critical network roles. This step could thus be found particularly long and cumbersome by users, and quickly forgotten afterwards. Plug-and-play routers already make all such decisions for the user, focusing on ease of use. Routers are also expected to work seamlessly for the remaining of their life, with no particular user interaction.

In this paper, we aim to study whether default settings tend to be kept for routers and the attitude of home router users towards making such decisions if they do change part of the defaults. To this end, we explore the answers to four questions:

RQ1: To what extent are users involved in the configuration of their home routers and do they make changes?

RQ2: How do users react to important questions during the initial setup of home routers?

RQ3: What strategy would users adopt to create an admin password?

RQ4: Do users keep routers updated?

To answer these questions, we conducted an exploratory user survey by spreading an online questionnaire in several countries and regions. We collected and analyzed the questionnaire results of 392 participants who answered a Chinese or English version of our survey, enabling us to compare habits between Chinese, Hong Kong and Macao, and residents in other regions. We also compare habits between age groups, levels of education, gender, and with/without an Information Technology (IT)-related background. In summary, a significant number of participants admit that they do not change the default settings on their routers and may neglect firmware updates. Part of the reason is related to a lack of understanding of the technical jargon presented to users during the initial setup phase. English survey participants with no IT background were much less likely to even read setup questions than their Chinese survey participant counterpart. This pattern should inform design choices by manufacturers towards safe default settings. Further differences between the Chinese and English surveys highlight cultural/regional differences with relevance to how home routers are secured by users. Additionally, we also share the limitations and lessons learned during the survey to help future researchers avoid issues in questionnaire design.

2 Background and Design of the Survey

The initial setup wizard and accessing management pages thereafter are common methods for users to configure home routers, where the former is often required. The guidance provided by the router and user habits and attitudes determine whether the router can run with secure settings. In this section, we first introduce important configuration aspects and the initial setup process of home routers. We then discuss related work and describe the design of the survey.

2.1 Background

When a router is powered on for the first time, it will usually guide the user to access the management page and complete the initial setup to configure basic settings. Some routers are "plug-and-play" and do not require the user to attend an initial setup (one could be optional). This initial setup can guide users to connect to the Internet and set Wi-Fi and admin passphrases that are crucial for the security of routers. Wi-Fi passphrases are used to connect to the Wi-Fi and admin passphrases are used to login to the management page of the router. If the passphrase is hard-coded and weak, adversaries can crack it and control the router, e.g., by brute-forcing it. The initial setup tends to leverage passphrase strength requirements and meters to guide users to set strong passphrases [34]. However, users may still choose to set a simple passphrase that meets the requirements (e.g. "!Aa12345") for convenience [30].

Additionally, firmware update is also a common step of the initial setup. The factory firmware version of the router may not be the latest, so the initial setup will guide users to update the firmware to the latest version to fix known vulnerabilities prior to connecting to the Internet. As shown in Figure 1b, firmware update is usually not mandatory, and users can also choose not to update.

In a word, the guidance provided by the initial setup and users' habits and attitudes determine what settings the router will run with for a long time.

2.2 Related Work

Router manufacturers face an increased attention from security researchers. Researchers found that insecure default settings and users' misconfiguration of features can bring security risks. For example, for Wi-Fi security protocols, vulnerabilities in outdated protocols (e.g. WEP and WPA/WPA2-TKIP) may be exploited by adversaries to eavesdrop or forge packets [28, 29]. Lorente et al. [18] also show certain routers may have been shipped with insecure default password/phrases. Ye et al. [34] also found that IPv6 configuration could expose local devices unprotected, vulnerable Wi-Fi security protocols could be selected by default, including open (unencrypted) Wi-Fi networks, and trivial admin passwords could be set by default in plug-and-play routers. Other smart home-related studies [12, 35, 37] also bring significant insights into the field. However, those works are different than ours, e.g., a small number of participants for non-router devices. We focus on the initial setup phase of home routers and study the behavior/attitude of end users in terms of default settings.

Frameworks have been developed to automatically analyze router firmware [6, 15, 24, 32], leading to numerous discovered vulnerabilities [14]. As a result, routers should be kept updated with the latest firmware that fixes newly discovered vulnerabilities. Routers could either implement an auto-update mechanism or rely on users to apply updates.

Prange et al. [22] found that manufacturers can guide users to employ more secure configurations by providing nudges with concrete and concise details on vulnerabilities, consequences and required steps to employ countermeasures. Several previous works studied users' concerns about privacy and security in smart home devices [5, 31, 36], smartphones [1, 9] and risk-based authentication [20], but users' habits and attitudes towards home router configuration have not yet received the attention they deserve. Ho et al. [11] conducted a city-wide survey and interviews, discovering that home router users were likely to stick with the default WiFi protocol and the use of encrypted WiFi networks varied across neighborhoods. In response, they designed and implemented a new configuration process aimed at securing routers, though their approach focused solely on password management and MAC address filtering.

2.3 Study Design

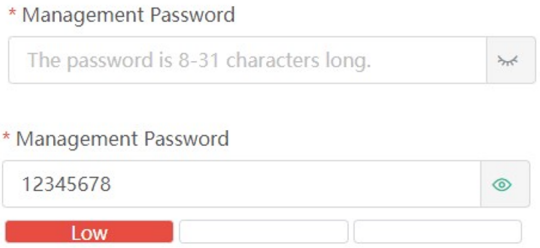
To answer the research questions raised in Section 1, we ask participants about their experience towards their own home router configuration, and also present them with hypothetical situations and ask what their reaction would be. We designed a questionnaire and conducted an anonymous online survey to quickly and widely spread this questionnaire. We obtained the IRB approval from our university before conducting this online survey.

2.3.1 Design of the Survey. The survey consists of 15 questions divided into five parts. In the first part (Q1–7), we collect the demographics of respondents, including age, gender, education level, occupation, region, familiarity with information technology (IT), and whether they subscribe to an Internet plan (or are provided Internet access otherwise, e.g., via mobile data). Then, we build questions (Q8–9) to understand whether participants configured their home routers (e.g., whether the participant owns a router or is provided one by the Internet Service Provider (ISP), whether they configured the router or a technician did it).

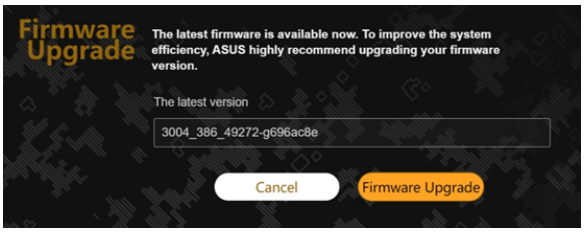
The third part of the questionnaire (Q10-12) focuses on the password-related issues. We first focus on whether participants will change the Wi-Fi or admin page passwords. Then, we provide an immersive question with the prompt on Figure 1a to study what kind of passwords the participants may choose.

The fourth part of the questionnaire (Q13–14) is about router firmware updates. We surveyed the habit of how the participants update their router firmware (Q13: "Do you perform updates on your routers?"). We also provide an immersive question with the prompt on Figure 1b to study the user behavior in terms of firmware update during a hypothetical setup page prompted the user to perform an update. In literature [34], researchers have shown that 30% of the routers will prompt updates during initial settings.

The last question (Q15) is about how participants behave when they set up a new IT equipment. This question tends to convey the message of whether most of the participants will keep the default settings. The full questionnaire can be found in Appendix A.



(a) Setup Admin Password



(b) Firmware Update Prompt [34]

Figure 1: Screenshots extracted from real home routers and presented to survey participants in immersive questions

2.3.2 Survey Distribution. We used Wenjuanxing[1] to host the Chinese version of this questionnaire and SurveyMonkey[2] for the English version. The questions and options in both versions are equivalent. We followed the snowball sampling method to distribute the survey (Section 5.1 discusses the limitation of this method). In our case, the Chinese version gets distributed via WeChat to the participants we have personal connections with (seed participants). Then, those participants will forward the survey to their acquaintances or in their social groups. The English version is spread through our personal contacts. We spread the links of those two surveys out from August to September 2023. The surveys reached China (Mainland), China (HKG, Macao), North America, and Europe. In the end, we collected a total of 392 responses (321 Chinese and 71 English). We refer to the English version when quoting questions in this paper. In all the results, 22 participants did not have Internet plans, so their results were excluded in the later study.

3 Results

In this section, we present the results we collected from our online surveys. Section 3.1 details the demographic information of our participants, Section 3.2 discusses RQ1 (who owns and configures routers), Section 3.3 studies the configuration behavior of participants (RQ2), Section 3.4 explores password selection preferences (RQ3) and Section 3.5 exposes user behavior towards firmware updates (RQ4).

3.1 Participants

We conducted an online survey for n = 392 participants across several regions. In the Chinese online survey, our participants (n = 321) span a wide range of ages, from 18 to 60 and above. Among the

[1] https://www.wjx.cn/
[2] https://www.surveymonkey.com/

Table 1: Demographic information based on the online survey results. n(C) denotes the results from the Chinese online survey, while n(E) denotes the results from the English online survey

Features	n(C)	%	n(E)	%
Age				
18-29	88	27.41	22	30.99
30-39	47	14.64	18	25.35
40-49	81	25.23	14	19.72
50-59	72	22.4	9	12.68
60+	27	8.4	7	9.86
I prefer not to say	6	1.87	1	1.41
Gender				
Female	145	45.17	28	39.44
Male	166	51.7	42	59.15
Other	10	3.11	1	1.41
Education				
High school or equivalent	60	18.69	0	0
College (pre-university)	41	12.77	3	4.23
Bachelor	111	34.58	23	32.39
Master's	78	24.3	25	35.21
Doctorate	31	9.66	20	28.17
Occupation				
Student	47	14.64	22	30.99
Worker	222	69.16	42	59.15
Retiree	52	16.2	6	8.45
Unemployed	0	0	1	1.41
Region				
China (Mainland)	287	89.4	0	0
China (HKG, Macao)	29	9.03	47	66.20
North America	3	0.93	15	21.12
Europe	0	0	7	9.86
Other	2	0.62	2	2.82
Education background or job related to information technologies (IT)				
Yes	133	41.43	33	46.48
No	188	58.57	38	53.52
Subscribe to a home Internet plan				
Yes	303	94.39	68	95.77
No	18	5.6	3	4.23

participants who provided their age (n = 315, 98.1%), we observe a balanced distribution between the age groups of 18-29, 40-49, and 50-59. However, there were fewer participants in the 60+ age group (n = 27, 8.39%) and moderately fewer in the 30-39 age group (n = 47, 14.6%). In terms of IT-related background, slightly more participants in the Chinese survey (58.7% vs. 41.3%) do not have a background in IT. Moving on to the English online survey (n = 71), we noticed that there are slightly more participants in the 30-39 age group compared to the Chinese survey (25.3% vs. 14.6%). This helps to balance out the smaller percentage of participants in this age group in the Chinese survey. We also observed that the number of female participants in the English version is lower compared to the Chinese version (39.4% vs. 45.3%). Additionally, the education level of participants in the English survey is higher than that of the Chinese survey with a minimum college level in the former and 63% achieving at least a master's degree compared to only 34% in the Chinese survey. We notice the China (Mainland) group always follows the trend with the Chinese survey participants closely, mainly because all the participants in this group took the Chinese survey. Therefore, we only further divide into China (Hong Kong, Macao) and overseas. Moreover, the English survey includes 66% of Chinese (Hong Kong, Macao) participants, which significantly skews the results for this survey towards these regions. We provide further breakdown of our results where appropriate.

Furthermore, there are a larger number of participants without an IT-related background in the English survey. It is worth noting that a significant majority of participants in both surveys (94.41% and 96.77% in the Chinese and English, resp.) subscribe to a home Internet plan, which means they will likely experience a router initial setup process. Table 1 summarizes participants' age, gender, education, occupation, region, related to IT, and subscription to a home Internet plan in both Chinese and English online surveys. In the remainder of this paper, we will use "C" to refer to the Chinese survey and "E" for the English survey for brevity.

3.2 RQ1: Who Performs the Router Configuration

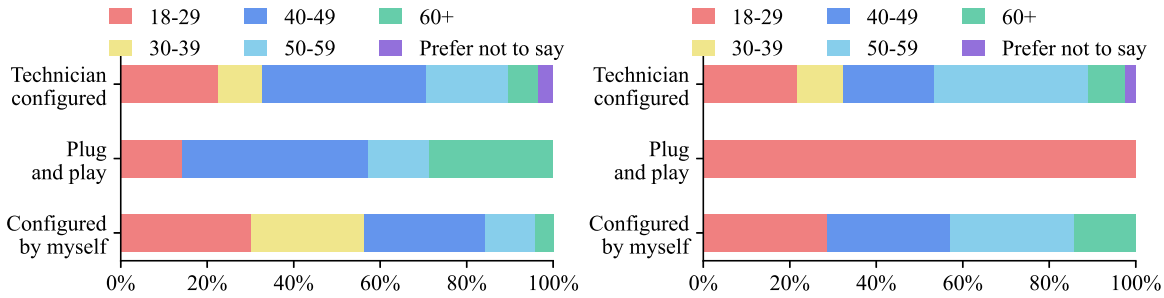
In this part, we first explore whether users leverage their own router or are provided one by their ISP, then we investigate who performs the initial setup of the router (through the setup wizard, if any), and look into the demographic details of such users.

3.2.1 Router types. In the Chinese survey, among participants who subscribed to an Internet plan (303, 94.39%), a total of 161 of them (53.13%) own their home router, while 132 of them (43.5%) receive their router from their ISP. The breakdown by age for users who own their router is 27.2% for 18-29, 19.1% for 30-39, 32.1% for 40-49, 14.2% for 50-59 and 6.2% for 60+, with an over-representation of 40-49, and under-representation of 50-59 compared to the overall age distribution. For ISP-provided routers, the breakdown is 25% of 18-29, 9.8% for 30-39, 20.5% for 40-49, 34.1% for 50-59 and 8.3% for 60+. There is a notable under-representation of 30-39 and over-representation of 50-59.

In the English survey, where 68 subscribed to an Internet plan by themselves (95.8%), 31 participants (45.6%) own a router, while 35 (51.5%) utilize ISP-provided routers. The age breakdown is 19%, 29%, 19%, 16%, 16% and 46%, 20%, 14%, 11%, 6%, 3% for the age groups 18-29, 30-39, 40-49, 50-59 and 60+ in the case of using their own router or ISP-provided router, respectively. There are more 18-39 participants using their own router. Overall, both types of routers are fairly popular in both surveys, with a slight preference for ISP-provided routers in the English survey.

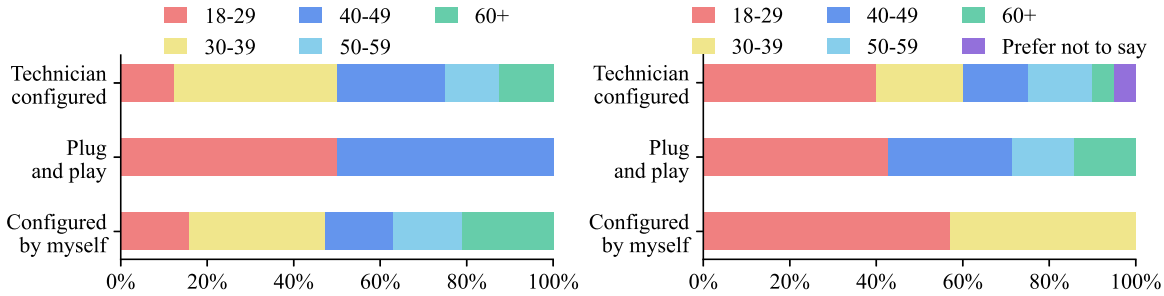
3.2.2 User configuration. When participants use their own routers, a majority (59% in the Chinese survey, 61.3% in the English survey) configure them. Others (65 or 40.1% in C, and 10 or 32.3% in E) either leverage the plug-and-play feature of routers or rely on the technician to set up everything.

Among participants using ISP-provided routers, a substantial 120 (91%) Chinese survey participants chose to retain the router's settings post-configuration by the ISP technician while only 20 (57.1%) did so in the English survey. However, see RQ2 (Section 3.3) for details on how further changes are made by the users who claim to not configure the routers.



(a) Own Router (C) (b) ISP Router (C)

Figure 2: Router configuration in different age groups (Chinese online survey participants)



(a) Own Router (E) (b) ISP Router (E)

Figure 3: Router configuration in different age groups (English online survey participants)

3.2.3 Demographics. Figure 2 and Figure 3 illustrate the high-level configuration results based on different age groups. Participants in the Chinese survey under 40 are less likely to rely on technician assistance to configure routers than those in the English survey (35% vs. 50-60%). Conversely, older participants in the Chinese survey rely more often on technician assistance. In the English survey, only younger participants configure ISP-provided routers, but all age groups configure their own routers (though predominantly younger participants, with about 50% of 39 and below). The trend is opposite in the Chinese survey where 70% of participants who configure ISP routers are 40+ but only represent 45% of participants when having their own routers. Younger participants are more likely to rely on plug-and-play routers when provided by the ISP in China (100% of plug-and-play router users are 18-29), but not with their own routers (only 15%).

To further study the demographic differences for this question, we separated our data into three groups: China (Mainland), China (Hong Kong, Macao), and overseas (North America, Europe, and Other). The results show that 141/287 participants (49%) in Mainland China own a home router, compared to 38/63 participants (60%) in Hong Kong and Macao, and 9/24 participants (37.5%) in overseas regions. Participants from Hong Kong and Macao exhibit the highest rate of home router ownership.

The age distribution for overseas and Hong Kong/Macao participants aligns with the results from the English survey, while the Mainland China participants' age distribution aligns with that of the Chinese survey results.

3.3 RQ2: How Home Users Configure Routers

Below, we investigate the configuration strategies selected by participants regarding the configuration of their router (Q15). Then, we study whether users change the routers' default WiFi passphrase and admin password (Q10–11).

3.3.1 Accepting default settings. Overall, 60.6% of participants report configuring their home router mainly accepting the default settings (71.6% (E) and 58.3% (C)). Reasons include issues with the technical jargon, settings perceived as "good enough", or eagerness to use the router, further detailed below.

Technical jargon. One concerning finding is that a significant number of participants without an IT background (30.16% (C) and 44.4% (E) in Figure 4a and Figure 4b) admitted not understanding the technical jargon and tended to accept and proceed with the default settings. Fewer participants with an IT background (15% (C) and 3% (E)) agree with this confusion about the technical jargon.

With further demographic analysis, the China (Mainland) group exhibits a similar ratio of technical jargon issues as the overall Chinese survey results, with 48/163 non-IT background participants (29%) compared to 19/123 IT background participants (15%). The China (Hong Kong and Macao) group shows the highest confusion with technical jargon among non-IT participants, with 20 out of 46 (43%) reporting difficulties, while IT participants in this group show a lower confusion ratio, at 2 out of 18 (11%). The overseas group has fewer participants but shows a confusion rate of 1 out of 5 (20%) in the non-IT group and 0% in the IT group.

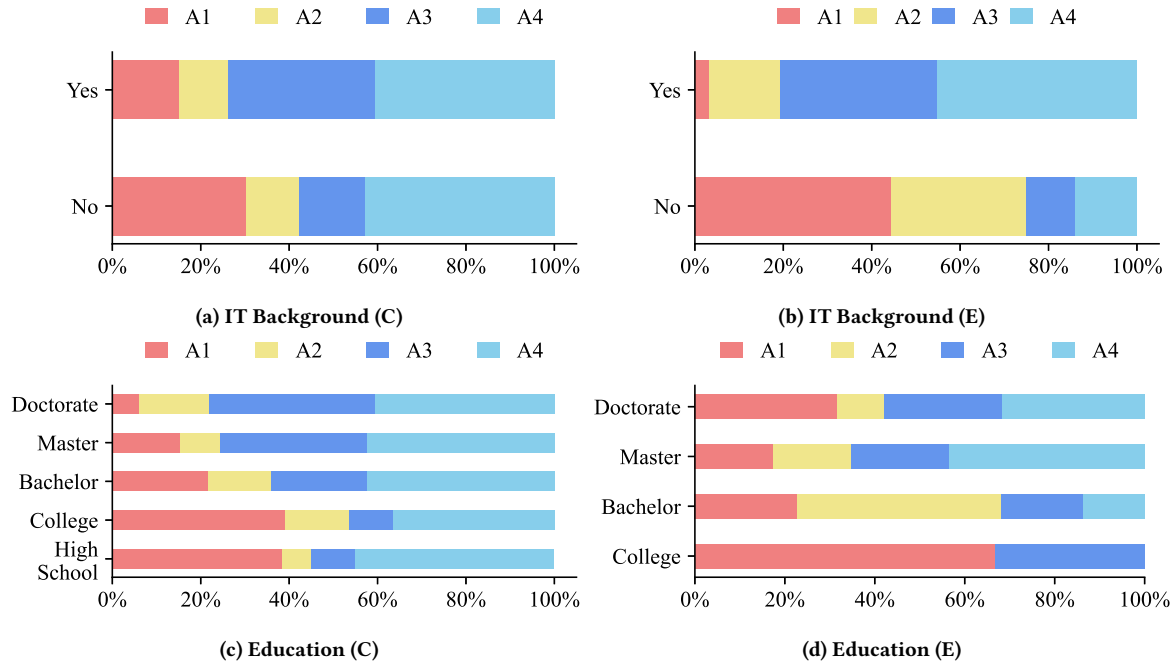


Figure 4: New IT equipment configuration in w or w/o IT background (a) and (b) and in different education backgrounds (c) and (d) (*A1*: I do not understand the technical jargon and tend to accept/proceed; *A2*: I mostly accept the default settings because I think they are good enough; *A3*: I mostly accept the default settings because I want to use my equipment quickly and I will change the configuration later if necessary; *A4*: I read the questions and settings shown to me and make configuration changes as I consider appropriate)

Good-enough settings. Among participants who accept default settings because they view them as "good enough", Chinese survey participants (12.17% non-IT and 11.2% IT) accept them less compared to English survey participants (30.56% non-IT and 16.13% IT). Surprisingly, after aggregating the data further into the China (Hong Kong and Macao) group and the overseas group, default settings adoption remained around 15% and 20% for non-IT participants in both groups and 16.7% and 5% for IT participants. The perception of default settings may vary by population, but see related limitations in Section 5.3.

Eagerness. Non-IT Chinese survey participants (14.81%) fared comparably to non-IT English survey participants (11.11%) when they accept default settings for quick equipment usage and plan to modify configuration later if necessary. However, IT-related participants in both surveys indicated this reason more often (33% in C and 35% in E) than non-IT participants. This trend remains in the specific demographic separation; 44% and 47% of IT-related participants in the China (Hong Kong and Macao) group and the overseas group prioritize usability over security settings. This finding seems counter-intuitive as IT participants may be likely to make custom changes to the default settings, e.g., to fine-tune the configuration. This could suggest that both groups prioritize convenience and quick usability of their equipment in particular in the participants with IT backgrounds.

3.3.2 Reading settings. Lastly, the remaining participants report that they "actively read the configuration questions and settings and make appropriate changes." There is a significant gap between both surveys, with participants of the English survey less engaged with the configuration (28.4% (E) vs. 41.7% (C)). This difference is further exacerbated by looking at the non IT-related population (13% (E) vs. 42% (C)), reflecting the above conjecture that English survey participants may either have higher confidence in the default configuration or care less about the configuration process. However, participants with an IT background in both surveys reported more comparably (40.9% (C) vs. 45.68% (E)).

In the demographic breakdown study, the China (Hong Kong and Macao) group demonstrated the lowest willingness to read the questions, with around 26% in both IT and non-IT participants, while the overseas group showed higher willingness, at 40% for non-IT participants and 47% for IT participants, closer to the results of the Chinese survey.

3.3.3 Education factor. We further analyze the results based on different education groups (Figure 4c and Figure 4d). We collected responses from participants in four education groups: High school or equivalent, College (pre-university), Bachelor, Master, and Doctorate.

In both surveys, higher education correlates with more engagement in configuration, though the acceptance of default settings remains common, reflecting a compromise between convenience and security. For participants with pre-university education (high

school and college), a significant portion tends to proceed without understanding technical jargon (38.33% (C: high school), 39.02% (C: College), and 66.7% (E)). Participants with a bachelor's degree are more inclined to read questions and settings and make configuration changes based on their judgment (42.34% (C: Bachelor), 42.31% (C: Master), 40.62% (C: Doctorate), 43.5% (E: Master), and 31.6% (E: Doctorate)). Higher educated people in the English survey dropped by 12% in reading the questions, which is counter-intuitive.

However, even among higher educated groups, a substantial portion still accepts the default settings initially (36%, 42.4%, and 53% in Chinese survey participants, and 63.6%, 39.12%, and 36.8% in English survey participants, respectively to the education level). Opposite trends are observed based on the education level between Chinese survey participants and English survey participants. This trend is consistent across different demographic regions; at least 40% of the participants with higher education levels will accept the default settings without changes.

3.3.4 Changing WiFi Passphrases. A large majority of participants change the WiFi passphrase when they claim to configure the router by themselves (96/102 (93.14%) in C, 24/26 (92.3%) in E), whether they own (90/95 (94.7%) in C, 17/19 (89.5%) in E) or use ISP-provided routers (6/7 (85.71%) in C, 7/7 (100%) in E). This percentage decreases (6/10 or 60% in C and 4/9 or 44.4% in E) for participants with plug-and-play routers, but note that such participants first responded that those routers need not be configured.

For users who claim to enjoy their routers as plug-and-play or have it configured by an ISP technician, many also change the WiFi passphrase (65.6% (126/192) in C, 56.8% (21/37) in E). To explain this behavior, we posit that the ISP technicians may have recommended a password change on their own, or the change was made at a later point for reasons other than the initial setup.

The WiFi passphrase observation is consistent with further demographic breakdown studies: 92% and 100% of participants in both groups (China (Hong Kong and Macao) and Overseas) change the passphrase when they configure the router themselves. However, only 50% of participants do so when the router is provided as a plug-and-play device.

3.3.5 Changing Admin Passwords. Similarly, a large majority of participants change the admin password when they configure their own routers (82/95 (86.3%) in C and 15/19 (78.9%) in E) or an ISP-provided router (5/7 (71.4%) in C and 5/7 (71.4%) in E). This percentage decreases for participants using plug-and-play routers, with 3/7 (42.9%) in C and 1/2 (50%) in E changing the admin password, and even further for those with ISP-provided plug-and-play routers (1/3 (33.3%) in C and 2/7 (28.5%) in E). Similarly, for technician-configured routers, 35/58 (60%) in C and 4/8 (37.5%) in E of participants with their own routers and 48/120 (40%) in C and 6/20 (30%) in E with ISP-provided routers changed the admin password.

In the China (Hong Kong and Macao) group, participants demonstrate a relatively high rate of changing admin passwords across the three scenarios: 78% when configured by themselves, 40% for plug-and-play devices, and 47% when set up by a technician. In contrast, the overseas group shows a similar trend in the first two scenarios but has the lowest rate of changing admin passwords when devices are configured by a technician, at only 22%.

3.4 RQ3: Password Selection Preferences

In the study on password awareness, we observed that a significant portion of participants showed varying behaviors when it comes to changing passwords. Specifically, 19% (C) and 25% (E) of participants indicated that they did not change either their Wi-Fi or admin passwords. On the other hand, 53% (C) and 69.6% (E) changed both passwords. We observe that 87% (C) and 100% (E) of the individuals who do not change their Wi-Fi passphrase also chose not to change their admin password.

Among the participants who chose to change both passwords, we dig into their strategy to change passwords. In particular, the options the participants can choose from are:

(1) I would set a random password that can make the meter display "very strong";
(2) I would set a random password that meets minimum password strength requirements;
(3) I would set a simple password that can make the meter display "very strong" (e.g., "!Aa12345");
(4) I would set a simple password that meets minimum password strength requirements (e.g., "password", "12345678");
(5) I would use personal information such as birthdates and names to create a password that can make the meter display "very strong";
(6) I would use personal information such as birthdates and names to create a password that meets the minimum password strength requirements.

In the Chinese survey, we observed that in different age groups, participants share a similar preference in choosing a simple password that could display a "very strong" rating on the password strength meter (answer (3): 30.1% in 18-29, 31.9% in 30-39, 40.2% in 40-49, 36.1% in 50-59, and 33.33% in 60+) and (answer (5): 35% in 18-29, 36% in 30-39, 26.8% in 40-49, 0.22% in 50-59). This indicates that people like to choose easy passwords while guided by the meters. Younger generations favor the use of personal data (birthday and name) to create passwords (51% in the age groups below 39). An increasing trend is observed in utilizing pure simple pattern passwords (answer (3) and answer (4)) with the increase of age; more than 50% of the participants choose (3) or (4) when they are in the age groups above 40. In the English survey, a higher proportion of participants (38.7%) expressed a willingness to set a truly random password that can make the meter display "very strong". Most of the participants (44%∼47%) in different age groups expressed a willingness to use random passwords (answer (1) and (2)). None of them want to use simple patterns such as "12345678".

To further study the impact of each demographic factor (e.g., Age, Gender, Education) and behaviors (e.g., changing Wi-Fi password) on password choices, we conducted a hypothesis test with the null hypothesis (H_0): "There is no significant relationship between the demographic or behavioral factor and password choices." Table 2 presents the results for both Chinese and English survey participants, with a significance level of 0.05. The Chi-Square test results reveal distinct differences between these groups. For Chinese participants, age (χ^2(25, N=321) = 58, p = 0.0002), education (χ^2(20, N=321) = 41.34, p = 0.003), and occupation (χ^2(10, N=321) = 51.19, p = 1.6e-07) significantly influence password behavior, and those who change their Wi-Fi and admin passwords are more likely to choose

Table 2: χ^2 test against password choices

	Age	Gender	Education	Occupation	Related to IT	Change WiFi-pwd	Change Admin-pwd
χ^2 (C: p-value)	0.0002	0.75	0.003	1.6e-07	0.478	0.02	0.00068
χ^2 (E: p-value)	0.067	0.034	0.76	0.71	0.108	0.80	0.53

stronger passwords. In contrast, for English participants, gender ($\chi^2(10, N=71) = 19.46$, $p = 0.034$) is a significant factor, while age, education, and occupation are less influential. Notably, changing admin passwords does not significantly impact English participants' password behavior, unlike Chinese participants.

In the China (Hong Kong and Macao) group, different age groups predominantly prefer answer (3), with at least 37.5% of participants younger than 60 selecting this option. In contrast, the overseas group shows a strong preference for answer (1), with at least 37.5% of participants younger than 60 choosing it. Notably, around 30% of participants in both groups still use personal information to generate passwords (answers (5) and (6)). The age groups selecting simple passwords (answer (4)) also differ between the two demographics. In the China (Hong Kong and Macao) group, the highest proportions are seen in ages 18–29 (26.7%) and 50–59 (21.4%), whereas in the overseas group, the largest proportions are in ages 30–39 (25%) and 40–49 (20%).

3.5 RQ4: Router Firmware Update Behavior

Firmware updates play a crucial role in ensuring the security of routers. In this subsection, we examine the behavior of the participants regarding router firmware updates and their implications for security. Participants who reported not performing firmware updates, or lacked knowledge about them, showed varying behaviors when faced with a firmware update prompt during the router setup phase. A significant percentage (41.07% (C) and 22.7% (E)) indicated that they would click "Cancel" without performing the update. This behavior raises concerns, as it leaves their routers vulnerable to security threats that could be mitigated through timely updates. Furthermore, 32.14% (C) and 77% (E) of participants mentioned they would click "Firmware Upgrade".

Regarding participants who consistently perform firmware updates upon receiving a notification, the majority (67.33% (C) and 77% (E)) expressed their willingness to proceed with the update by clicking "Firmware Upgrade" during the initial setup. However, it is concerning that 32% (C) and 22% (E) mentioned they would click "Cancel" or close the page, potentially neglecting and never performing an update.

Participants who regularly checked for firmware updates tend to either skip more often this initial update in the Chinese survey (only 59.26% would choose "Firmware Upgrade"), or more actively proceed with the update in the English survey (85%); highlighting another subtle deviation in regional patterns.

Participants who reported that their routers automatically update themselves (a router behavior that may not be easily known by participants) also demonstrated safer attitude towards the initial update than participants who do not regularly update (64.06% (C) and 80% (E) would proceed).

Both the China (Hong Kong and Macao) and overseas groups demonstrate a high willingness to upgrade firmware, with 73% and 83% of participants, respectively. However, participants with a high willingness to perform upgrades may still cancel updates during the initial setup phase–10% in the China (Hong Kong and Macao) group and 33% in the overseas group. Notably, even among participants who choose the automatic update function for routers, 22% in the China (Hong Kong and Macao) group and 10% in the overseas group still refuse updates during the initial setup phase. This inconsistency highlights that users tend to prioritize usability over security.

4 Insights and Discussion

We first summarize the insights gained through our survey results below, and offer recommendations to users, manufacturers, and other paths forward.

4.1 Takeaways

RQ1. Router users spread across all age groups with minor deviations. Possessing their own router and leveraging an ISP-provided one are both fairly common. Younger participants are associated with less reliance on technician assistance, especially among Chinese participants. However, mid-age and older Chinese participants tend to configure routers more often than their counterparts in the English survey.

RQ2. A majority of participants (60.6% across both surveys) mostly accept default settings. Non-IT English survey participants tend to accept default settings more often due to a lack of understanding of the technical jargon than their Chinese counterparts. This lack of technical knowledge and understanding in non-IT background users can have serious security consequences, as users may not be aware of potential vulnerabilities or risks associated with default configurations; indicating a need for clear explanations during the configuration process to ensure that security settings are not overlooked or misunderstood.

Participants in the English survey (both IT and non-IT) are more likely to trust and accept default settings compared to Chinese participants while Chinese non-IT participants are more willing to read and adjust settings. Higher education was also linked to more careful configuration attitude in the Chinese survey but less so in the English survey.

Perhaps the most striking finding, though not unexpected, is the fact that among participants who effectively own a router and reported configuring it, 48.2% (57.9% (E) and 46.3% (C)) also claimed they accepted default settings. In addition to users owning a router but keeping it as "plug-and-play", plus the majority of participants using an ISP router without configuration or with a technician configuration, the proportion of users effectively running any type of router with default settings is overwhelming. If we only omit the users who configured their or the ISP's router without keeping default settings, and assuming that technicians follow the default

settings, we estimate that 91% of router owners in our survey operate with default settings.

RQ3. A substantial proportion of participants in both surveys neglect to change their Wi-Fi and admin passwords, with a strong correlation between the two. Chinese participants tend to favor simple passwords that appear strong on password meters, with younger individuals more likely to use personal information. In contrast, English-speaking participants show a greater preference for truly random passwords. Note that this difference could be due to biases in the education levels between both populations. Statistical analysis reveals that password choices among Chinese participants are significantly influenced by age, education, and occupation, whereas gender plays a more significant role among English participants.

RQ4. English survey participants were significantly more likely to perform a firmware upgrade during the initial setup than their Chinese counterpart.

The study highlights concerning behaviors regarding router firmware updates, with a significant portion of participants opting to cancel or skip updates during initial setup, leaving their devices vulnerable.

While many participants express willingness to update firmware when notified, inconsistencies arise, particularly among those who rely on automatic updates or regularly check for updates, yet still skip the initial prompt. Furthermore, users who do not regularly check for firmware updates are also less likely to update the firmware at the initial setup. These users will remain permanently outdated. Therefore, we recommend manufacturers to specially consider the frequent situation where routers are never updated after manufacturing due to (possibly misguided) user decision and poor security hygiene practices. We suggest that an auto-update mechanism be considered the default, unless opted out by the user for specific reasons (e.g., possibility for unwanted breaking changes or downtime).

Regional differences are also observed, with English survey participants being more proactive in updating compared to Chinese participants. Even among security-conscious users, usability concerns often outweigh security considerations, leading to missed updates despite high overall awareness.

4.2 Ways Forward

With the exposure of default settings in home routers, manufacturers (and ISPs) bear an important responsibility to ensure safe defaults —or to provide an intuitive configuration process resulting in safe configurations, especially for the customer population without IT knowledge. Legislation could be introduced that mandates such secure defaults for vendors so that users can simply rely on them, including automatic updates. This is already happening in some parts of the world, e.g., in the EU with the Cyber Resilience Act (CRA) [26].

Guidelines or certification programs for vendors should be developed to support them in choosing sensible defaults by providing proven procedures, e.g., choosing secure default passwords for both, the router's WiFi and the router's user interface that are unique to each manufactured unit. The ETSI standard "Cyber Security for Consumer Internet of Things" [8] provides promising baseline requirements.

ISPs could also run information campaigns to alert users of possible misconfiguration of customer routers, especially if they are not controlled by the ISP. ISP-provided routers are more easily kept up-to-date, if automatic updates are turned on from the beginning.

5 Limitations

We discuss below limitations of our study. Some unexpected results (e.g., a large number of non-IT users (42.8%) claiming to understand and change the configuration, perhaps due to our suboptimal option ordering) caught our attention. Thus, we also discuss the lessons learned from our design of such surveys.

5.1 Snowball Sampling

In general, a major limitation of snowball sampling is its reliance on referrals, which can introduce biases by producing samples based on the preferences of the initial participants (seed participants) rather than generating random samples [21]. It is worth noting that, as a result, the collected data from the snowball sampling method may predominantly include participants from a single ethnic group or contain an imbalance in gender distribution, potentially due to a higher likelihood of cooperation among female participants. In our case, the Chinese survey was not meant to reach another ethnic group, and despite the inherent limitations of snowball sampling, we successfully obtained a balanced gender distribution among participants between female (n=145, 45%) ad male (n=166, 51.7%).

5.2 Overlapped Results

In our study, we offered two versions of the survey: Chinese and English. Participants selected their preferred language based on their individual needs. In Hong Kong, we encountered participants who could not understand Chinese as well as those who could speak Chinese but could not read simplified Chinese. These participants opted for the English survey. This portion of the data overlaps with both Chinese and English survey participants; however, we later distinguished them based on their locations.

5.3 Quality of Default Settings

Accepting default settings may carry varying implications across regions or vendors. Users could be genuinely satisfied with them, or be agnostic to them. Generally, default settings can vary significantly by brand, with certain brands being more localized. Prior work showed that default settings of home routers could be unsafe [34]. In our study, we did not establish a baseline for default settings across different regions. Further research into the acceptability of default settings should clarify the quality and perception of default settings.

5.4 Impact of Option Order

In the online questionnaire, the order of options for each question is fixed, which may lead users to choose the top option if they are not sure about their own judgment. For example, when we ask participants about their attitude towards the initial setup, the first option is *"I read the questions and settings shown to me and make configuration changes as I consider appropriate"*, which means the

user understands how to configure a router properly. The second option *"I mostly accept the default settings because I want to use my equipment quickly and I will change the configuration later if necessary"* and third option *"I mostly accept the default settings because I think they are good enough"* means that the user keeps default settings but can understand them. These three options may confuse participants, leading them to tend to choose the first option. *"I do not understand the technical jargon and tend to accept/proceed"* may be the case of most non-IT users, but it is the last option and can be ignored by participants. This is one of the factors that introduces noisy data, which may be mitigated by pilot testing.

5.5 Credibility of Online Participants

To spread the questionnaire on a large scale, we try to keep it as short as possible to save participants' time and improve their willingness to complete, which makes it difficult for us to assess the participants' knowledge level in detail and ensure that they fully understand the questions and options. Participants may subjectively choose options that match their true situation, but the results may not necessarily be trustworthy. For example, elderly people over 60 years old may think they can read the guidance and configure routers correctly, but in reality, they do not understand what the correct configuration is.

Although age, IT background, and education background can help us understand participants, they cannot objectively reflect their level of professional knowledge. Adding professional knowledge test questions to the questionnaire can be a method to evaluate the real knowledge level of participants, but it may cause non-IT user dissatisfaction and make it difficult for the questionnaire to spread.

Additionally, small-scale interviews can serve as a supplementary method for our survey, as during interviews, we can gain a deeper and more comprehensive understanding of the interviewees' thoughts through dialogue, which will be our future work.

6 Summary and Conclusion

We conducted a user survey on configuration habits and attitudes of home router users by spreading an online questionnaire in several countries and regions and collecting responses from 392 participants. Noteworthy opposite trends were sometimes found between the English and Chinese surveys. We identified important issues and trends that are worthy of consideration by router manufacturers and other security practitioners in the design of initial configurations. First, technical jargon during router configuration hinders effort by the non-IT population to change the default configuration. Second, certain demographic factors play a key role in router configuration and password selection. Third, considering all scenarios, we estimate that the home router of 91% of our survey participants is configured with default settings only. This finding must fuel effort towards safe defaults; however, prior work has shown security issues with them [34]. Fourth, there is a category of users who do not perform an initial firmware update when asked and their router does not automatically update, resulting in permanently outdated devices. Trends for manual firmware updates are promising but insufficient. Automatic updates should become the norm to palliate this issue.

Our study highlights the importance of the router initial configuration assistant (setup wizard), the need for clarity of options offered to users, and emphasizes getting default settings right regardless of whether the router is "plug-and-plug" or not. Moreover, plug-and-play routers reduce the involvement of users in the configuration of the devices. As a result, special care must be given to the default settings of such routers. We made several observations relevant to manufacturers, and suggested legal cybersecurity frameworks and pointed to baseline requirements as a way forward for the future of home router security. Meanwhile, users may also benefit from an increased awareness about the importance of configuring their routers, given that default settings are, so far, not always safe.

Acknowledgments

The work was partly supported by the National Natural Science Foundation of China (No. U23B2002), the European Union (EU) under Horizon Europe grant n. 101120393 (Sec4AI4Sec), and by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) under grant n. NWA.1215.18.006 (Theseus). We thank Katja Tuma, Hala Assal, and anonymous reviewers for their helpful feedback. We are also especially grateful to the initial participants, who not only contributed their perspectives but also played a crucial role in sharing our survey with a wider audience.

References

[1] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L Mazurek. 2021. Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms. In *Symposium on Usable Privacy and Security (SOUPS'21)*. USENIX Association, Vancouver, BC, Canada, 139–158.

[2] Charles Arthur. 2012. DNSChanger may Take 300,000 Offline. https://www.theguardian.com/technology/2012/jul/09/dnschanger-malware.

[3] Avast. 2020. Avast Analyzes GhostDNS Exploit Kit Source Code Used to Attack Brazilian Routers. https://press.avast.com/avast-analyzes-ghostdns-exploit-kit-source-code-used-to-attack-brazilian-routers.

[4] Beacon. 2023. Wi-Fi® by the numbers: Technology momentum in 2023. https://www.wi-fi.org/beacon/the-beacon/wi-fi-by-the-numbers-technology-momentum-in-2023.

[5] George Chalhoub and Martin J. Kraemer. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *International Conference on Human Factors in Computing Systems (CHI'21)*. ACM, Virtual Event/Yokohama, Japan, 555:1–555:16.

[6] Daming D. Chen, Manuel Egele, Maverick Woo, and David Brumley. 2016. Towards Automated Dynamic Analysis for Linux-based Embedded Firmware. In *Network and Distributed System Security Symposium (NDSS'16)*. The Internet Society, San Diego, California, USA, 1–16.

[7] Cisco. 2023. Networking Basics: What You Need to Know. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html.

[8] ETSI. 2020. Cyber Security for Consumer Internet of Things: Baseline Requirements. ETSI EN 303 645 V2.1.1.

[9] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *International Conference on Human Factors in Computing Systems (CHI'22)*. ACM, New Orleans, LA, USA, 407:1–407:24.

[10] fyy0r. 2015. NetgearKiller.dict - my Netgear WPA dict. Hashcat forum post (June 21, 2015). https://hashcat.net/forum/thread-4463.html.

[11] Justin T. Ho, David Dearman, and Khai N. Truong. 2010. Improving Users' Security Choices on Home Wireless Networks. In *Symposium on Usable Privacy and Security (SOUPS'10)*. ACM, Redmond, Washington, USA, 1–12.

[12] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(es) with Smart Home: Experiences of a Living Lab Field Study. In *International Conference on Human Factors in Computing Systems (CHI'17)*. ACM, Denver, CO, USA, 1620–1633.

[13] Adam D. G. Jenkins, Linsen Liu, Maria K. Wolters, and Kami Vaniea. 2024. Not as easy as just update: Survey of System Administrators and Patching Behaviours. In *International Conference on Human Factors in Computing Systems (CHI'24)*. ACM, Honolulu, HI, USA, 972:1–972:17.

[14] Kaspersky. 2021. 87 Critical Vulnerabilities Discovered in Routers in 2021. https://www.kaspersky.com/about/press-releases/2022_87-critical-vulnerabilities-discovered-in-routers-in-2021.
[15] Mingeun Kim, Dongkwan Kim, Eunsoo Kim, Suryeon Kim, Yeongjin Jang, and Yongdae Kim. 2020. FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis. In *Annual Computer Security Applications Conference (ACSAC'20)*. ACM, Virtual Event/Austin, TX, USA, 733–745.
[16] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In *International Conference on Human Factors in Computing Systems (CHI'11)*. ACM, Vancouver, BC, Canada, 2595–2604.
[17] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. 2019. Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines. In *Symposium on Usable Privacy and Security (SOUPS'19)*, Heather Richter Lipford (Ed.). USENIX Association, Santa Clara, CA, USA, 273–288.
[18] Eduardo Novella Lorente, Carlo Meijer, and Roel Verdult. 2015. Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers. In *USENIX Workshop on Offensive Technologies (WOOT'15)*. USENIX Association, Washington, DC, USA, 1–13.
[19] Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. 2017. Understanding the Mirai Botnet. In *USENIX Security'17*. USENIX Association, Vancouver, BC, Canada, 1093–1110.
[20] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. 2022. "As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication. In *Symposium on Usable Privacy and Security (SOUPS'22)*. USENIX Association, Boston, MA, USA, 483–501.
[21] Charlie Parker, Sam Scott, and Alistair Geddes. 2019. Snowball sampling. *SAGE research methods foundations* (2019), 1–13.
[22] Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure Settings Are Quick and Easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *International Conference on Advanced Visual Interfaces (AVI'22)*. ACM, Frascati, Rome, Italy, 20:1–20:9.
[23] RouterNetwork. 2023. Default Router Username and Password List. https://router-network.com/default-router-passwords-list.
[24] Franziska Schwarz, Klaus Schwarz, Daniel Fuchs, Reiner Creutzburg, and David Akopian. 2021. Firmware Vulnerability Analysis of Widely Used Low-Budget TP-Link Routers. In *Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications (MOBMU'21)*. Society for Imaging Science and Technology, Online, 1–11.
[25] Rohit Shewale. 2023. Internet User Statistics In 2023 — (Global Demographics). https://www.demandsage.com/internet-user-statistics/.
[26] European Union. 2024. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 March 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 Accessed: 12 Feb. 2025.
[27] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *USENIX Security'12*, Tadayoshi Kohno (Ed.). USENIX Association, Bellevue, WA, USA, 65–80.
[28] Mathy Vanhoef and Frank Piessens. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In *ACM SIGSAC Conference on Computer and Communications Security (CCS'17)*. ACM, Dallas, TX, USA, 1313–1328.
[29] Mathy Vanhoef and Frank Piessens. 2018. Release the Kraken: New KRACKs in the 802.11 Standard. In *ACM SIGSAC Conference on Computer and Communications Security (CCS'18)*. ACM, Toronto, ON, Canada, 299–314.
[30] Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. 2022. A Large-Scale Analysis of Wi-Fi Passwords. *Journal of Information Security and Applications (JISA)* 67 (2022), 103190.
[31] Swaathi Vetrivel, Veerle van Harten, Carlos H Gañán, Michel van Eeten, and Simon Parkin. 2023. Examining Consumer Reviews to Understand Security and Privacy Issues in the Market of Smart Home Devices. In *USENIX Security'23*. USENIX Association, Anaheim, CA, USA, 1523–1540.
[32] Vasaka Visoottiviseth, Pongnapat Jutadhammakorn, Natthamon Pongchanchai, and Pongjarun Kosolyudhthasarn. 2018. Firmaster: Analysis Tool for Home Router Firmware. In *International Joint Conference on Computer Science and Software Engineering (JCSSE'18)*. IEEE, Nakhonpathom, Thailand, 1–6.
[33] Ding Wang, Ping Wang, Debiao He, and Yuan Tian. 2019. Birthday, Name and Bifacial-security: Understanding Passwords of Chinese Web Users. In *USENIX Security'19*, Nadia Heninger and Patrick Traynor (Eds.). USENIX Association, Santa Clara, CA, USA, 1537–1555.
[34] Junjian Ye, Xavier de Carné de Carnavalet, Lianying Zhao, Mengyuan Zhang, Lifa Wu, and Wei Zhang. 2024. Exposed by Default: A Security Analysis of Home Router Default Settings. In *ACM Asia Conference on Computer and Communications Security (ASIACCS'24)*. ACM, Singapore, 63–79.
[35] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security, SOUPS'17*. USENIX Association, Santa Clara, CA, USA, 65–80.
[36] Eric Zeng, Shrirang Mare, Franziska Roesner, Santa Clara, Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS'17)*. USENIX Association, Santa Clara, CA, USA, 65–80.
[37] Serena Zheng, Noah J. Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *ACM Human-Computer Interaction* 2, CSCW (2018), 200:1–200:20.

A Online Survey Questions

Q1: Select the age category you belong to:
- 18-29
- 30-39
- 40-49
- 50-59
- 60+
- I prefer not to say

Q2: You are a:
- Male
- Female
- Other

Q3: What is your highest level of education?
- High school or equivalent
- College (pre-university)
- Bachelor in _____
- Master / Diploma in _____
- Doctorate in _____

Q4: What is your occupation?
- Student
- Worker
- Retiree

Q5: Select the region you live in:
- China (Mainland)
- China (Hong Kong, Macao, or Taiwan)
- North America
- Other

Q6: Is your education background or job related to information technologies (IT)?
- Yes
- No

Q7: Did you subscribe to a home Internet plan (DSL, cable, fiber) with an Internet Service Provider?
- Yes
- No, I have Internet access at home by other means (e.g., residential Wi-Fi, mobile data plan)

Q8: (If Q7 is Yes) Are you using your own network equipment such as a Wi-Fi router (a device that allows you to connect laptops and phones wirelessly)?
- Yes, I use my own router
- No, my Internet Service Provider lends/rents/sold me a modem and/or a router and I do not use other equipment
- I don't remember/don't know

Q9: (If Q7 is Yes) Is your Wi-Fi router configured by a technician from your Internet Service Provider?
- Yes, everything worked after the technician came
- No, I configured it myself
- No, it did not require any configuration, I just plugged it and it worked
- I don't remember

Q10: (If Q7 is Yes) Did you set up or change your router's Wi-Fi passphrase?
- Yes
- No
- I don't know

Q11: (If Q7 is Yes) Did you set up or change your router's admin password (used to login to the management page)?

- Yes
- No
- I don't know

Q12: Suppose you are installing a new router for your home. During the setup procedure, you get prompted with this screen. What is the action you will likely take?

Fig. 1a is displayed here

- I would set a simple password that meets minimum password strength requirements (e.g., "password", "12345678")
- I would set a simple password that can make the meter display "very strong" (e.g., "!Aa12345")
- I would use my privacy information (such as birthday, name) to generate a password that meets minimum password strength requirements
- I would use my privacy information (such as birthday, name) to generate a password that can make the meter display "very strong"
- I would set a random password that meets minimum password strength requirements
- I would set a random password that can make the meter display "very strong"

Q13: Suppose you are installing a new router for your home. During the setup procedure, you get prompted with this screen. What is the action you will likely take?

Fig. 1b is displayed here

- I would click Cancel
- I would click Firmware Upgrade
- I would close the page

Q14: (If Q7 is Yes) Do you perform firmware updates on your router?

- My router keeps updated automatically
- I perform firmware updates upon receiving a notification
- I regularly check for the availability of firmware updates
- I do not perform firmware updates or do not know what it is or how to do it

Q15: In general, when you configure new IT equipment such as a router, which of the following best describes your approach:

- I read the questions and settings shown to me and make configuration changes as I consider appropriate
- I mostly accept the default settings because I want to use my equipment quickly and I will change the configuration later if necessary
- I mostly accept the default settings because I think they are good enough
- I do not understand the technical jargon and tend to accept/proceed