Authentication security advice is given with the goal of guiding users and organisations towards secure actions and practices. In this article, a taxonomy of 270 pieces of authentication advice is created, and a survey is conducted to gather information on the costs associated with following or enforcing the advice. Our findings indicate that security advice can be ambiguous and contradictory, with 41% of the advice collected being contradicted by another source. Additionally, users reported high levels of frustration with the advice and identified high usability costs. The study also found that end-users disagreed with each other 71% of the time about whether a piece of advice was valuable or not. We define a formal approach to identifying security benefits of advice. Our research suggests that cost-benefit analysis is essential in understanding the value of enforcing security policies. Furthermore, we find that organisation investment in security seems to have better payoffs than mechanisms with high costs to users.

CCS Concepts: • Security and privacy → Authentication; Economics of security and privacy; Usability in security and privacy;

Additional Key Words and Phrases: Passwords, cybersecurity, costs versus benefits, password advice, security policies

ACM Reference format:
Hazel Murray and David Malone. 2023. Costs and Benefits of Authentication Advice. ACM Trans. Priv. Sec. 26, 3, Article 30 (May 2023), 35 pages.
https://doi.org/10.1145/3588031

1 INTRODUCTION

Passwords are an integral part of our online security, yet the rules and restrictions placed on passwords have become a source of considerable frustration for users [1]. Many security policies and procedures are imposed without proper research and their security objectives can be unclear [50]. In his book "Beyond Fear," Bruce Schneier explains that almost every security measure requires tradeoffs. These tradeoffs might be worse usability of a system, additional financial costs, or a decrease of security in another place [6]. In this article, we aim to delve deeper into the tradeoffs and effects of security policies and discover whether decreases in usability are justified by increases in security.

This publication was supported in part by the CyberSkills HCI Pillar 3 Project 18364682. This publication was also supported in part by a research grant from Science Foundation Ireland (SFI) and is co-funded under the European Regional Development Fund under Grant 13/RC/2077_P2.

Authors’ addresses: H. Murray, Munster Technological University, Bishopstown, Co. Cork, Ireland, T12 P928; email: hazel.murray@mtu.ie; D. Malone, Maynooth University, Maynooth, Co. Kildare, Ireland, W23A3HY; email: david.malone@mu.ie.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2023 Copyright held by the owner/author(s).
2471-2566/2023/05-ART30 $15.00
https://doi.org/10.1145/3588031
To achieve this goal, we collected 270 pieces of authentication security advice from security specialists, multinational companies, and public bodies. We noticed significant variations in the advice given, with 41% of all the advice we collected being contradicted by advice from another source. To learn more about the usability and implementation costs of this advice, we surveyed administrators and users about the costs associated with adhering to it. The results of this study are tabulated and discussed in Section 5. We found that humans were impacted by 87% of all the costs identified. In the user survey, we witnessed strong emotional responses towards the advice we asked users to consider: e.g. “I hate this!” As part of the user survey, we also asked both end-users and administrators whether they approved of each advice statement or not. Strikingly, we found that end-users disagreed with each other 71% of the time about whether a piece of advice was valuable. Determining whether advice is “worthwhile” seems to be a difficult task and one that is not well understood even by those giving the advice.

In addition to analysing the costs and benefits of the collected advice, we developed a methodology for assessing the security benefits of following security advice. Applying this methodology, we found that most authentication advice focused on improving password strength rather than back-end processes. This is an example of organisations placing the security burden on the user, rather than implementing security measures that would carry the cost for the organisation. Comparing the costs and benefits of the advice, we found that the most security-beneficial advice overlapped with the advice that had high organisational costs. This shows that if organisations are willing to invest in security, then they can implement advice that results in strong security benefits. However, the same is not true for user advice: An increase in costs does not imply an increase in benefits for user advice.

Throughout the survey, many users showed a willingness to follow advice provided it seemed to have a benefit: “Undoubtedly sensible, undoubtedly annoying.” There is substantial evidence that user education has been effective. Users echoed the advice that was given in historic security documents [7]. However, few users and administrators showed awareness of new recommendations that have superseded the legacy advice [19]. Understanding users’ approval of advice is a valuable stepping stone to improved user education and mutual respect between users and policy enforcers.

Our research highlights the challenges of determining the value of security advice and the difficulty of balancing the costs and benefits of security measures. We found that quick assessments of whether advice is valuable are not always possible, as evidenced by contradictions in the advice given by different sources and the differing opinions of end-users. Our study emphasises the need for a more nuanced approach to evaluating the effectiveness of security measures rather than end-users or administrators relying on preconceived notions of what should be secure. We provide a methodology for organisations to assess which authentication advice to follow, and we provide an assessment of current advice that demonstrates to end-users which advice is worthwhile.

2 RELATED WORK

The concept of usability in relation to security has gained significant attention in recent years, with researchers and practitioners recognising the need for security systems that are not only effective but also easy to use. The field of usable security has its roots in the publication of the paper “Users are not the enemy,” by Adams and Sasse in 1999 [1]. In this paper, Adams and Sasse highlighted the fact that users often employ workarounds for security policies that do not align with their work procedures. This, they argued, is because security systems are often designed without taking usability into consideration, leading to mechanisms that might look secure on paper, but fail in practice.

Following this, in 2005, Cranor and Garfinkel published their book Security and Usability: Designing Secure Systems that People Can Use [11]. This book covered pivotal topics in the usable security discussion. The chapter “Evaluating Authentication Mechanisms,” by Karen Renaud, is of
particular relevance to this article [38]. Renaud [37–39] quantified the quality of web authentication mechanisms by evaluating a selection of alternative password mechanisms with respect to accessibility, memorability, security, and vulnerability. This was one of the first works to quantify authentication security versus usability. However, Renaud’s work only compares four password methods and does not expand to two-factor authentication or biometrics. In 2007, Braz et al. [5] proposed a method to compare the security problem to the usability criteria for online tasks such as: authenticate yourself, transfer funds, or buy a concert ticket. In 2009, Lampson argued that we need to measure the time users spend on security, as this can have a significant impact on usability [29]. In 2009, Shay and Bertino [41] and in 2012 Arnell et al. [3] built simulations to model the costs versus the benefits of a password policy with complexity rules, throttling, and regular expiry. They aimed to help organisations to determine the tradeoffs between the user and organisation costs and the security improvements of password complexity rules.

In the aptly titled paper “The true cost of unusable password policies: Password use in the wild,” Inglesant and Sasse [25] find that users are generally concerned with maintaining security, but that while an organisation or user may want to enforce strong security if the time and monetary constraints are too high, then it might not be feasible. Beaumont et al. find that bypassing security policies is a widely employed practice [4]. They introduce the idea of a compliance budget, which formalises the understanding that users and organisations do not have unlimited capacity to follow new instructions and advice. Herley [23] argues that a user’s rejection of security advice is rational from an economic perspective. Herley quantifies the costs versus benefits for three specific authentication guidelines: password rules, phishing site identification advice, and SSL certificate warnings. Redmiles et al. show that when participants are explicitly aware of security risks and costs they will likely make a rational security choice [34]. This provided evidence that if a user perceives the policy to be beneficial to them, then they will be more likely to follow it.

In their 2015 paper, Ion et al. surveyed experts and non-experts about their self-reported security habits [26]. They find that experts and non-experts had different security practices and that while experts’ practices were rated as good by other experts, those employed by non-experts received mixed ratings. This means the non-experts are known to be wasting time and energy on security practices that are not considered good, for example, deleting cookies and visiting only known websites. In 2017, Reeder et al. asked 200 experts for their top three pieces of security advice [36]. They found that while each piece of advice given had merit, the set of advice across all experts lacked consensus. In 2020, Redmiles et al. conducted a large-scale automated survey, scraping advice from 1,264 online documents [35]. Redmiles found that the quantity of advice results in a crisis of prioritisation. Experts perceived 89% of the 394 advice statements to be effective and the 41 experts chose 118 pieces of advice to be among their top 5. This emphasises the importance of methodologically evaluating the costs and benefits of advice so we can give consistent ordinal advice to users and not overwhelm them. The first part of our work complements Redmiles’ paper, as we find that in addition to a large quantity of advice being available, this advice is often inconsistent.

3 COLLECTION AND CATEGORISATION OF AUTHENTICATION ADVICE

We collected 270 pieces of authentication advice from 20 different sources. We primarily used Internet searches to collect advice but also looked at the advice given by standards agencies and multinational companies. We attempted to recreate the actions an individual or organisation might take when seeking to inform themselves about proper authentication practices.

The advice was coded using an iterative coding methodology. One researcher examined the advice and for each piece of advice added it to an existing category or created a new category. Once all the advice was analysed in this way, the categories were evaluated by both researchers to identify overlapping or superfluous categories. All advice was then re-categorised into the finalised
categories allowing any category gaps to be identified. In total, we identified 27 categories shown in Table 1. The categories are listed in two columns—one showing categories containing advice aimed at users and the second showing advice aimed primarily towards organisations. Also included is the amount of advice in each category. We collected 179 pieces of advice aimed towards users and 91 pieces aimed towards organisations.

To extract insight into the views and opinions on the advice, we created over-arching statements to describe advice with the same goal but with different wording. For example, we consider “Change your password regularly” and “Passwords should be changed periodically” to both be summarised by the statement: Change your password regularly. Each category will contain a small number of advice statements summarising the advice within that category. For example, the category “Expiry” contains 27 pieces of advice. Five encourage organisations to store previous user passwords to prevent cycling through previous passwords; 12 relate to periodic password changes; and 10 tell users and organisations to change passwords if they suspect compromise. Therefore, the category “Expiry” contains three advice statements: (1) Store password history to eliminate reuse, (2) Change your password regularly, (3) Change password if compromise is suspected. Note that rather than separately coding contradicting advice, we include it within the advice statement. For example, below are the 12 pieces of advice under the statement Change your password regularly:

(1) “Passwords should be changed periodically.”
(2) “Enforce a Maximum Password Age, users should change passwords regularly.”
(3) “Change your password regularly.”
(4) “Have a minimum Password Age.”
(5) “Password expiration should be enforced on all accounts.”
(6) “Change your passwords regularly (every 45 to 90 days).”
(7) “All user-level passwords must be changed at least every six months.”
(8) “All system-level passwords must be changed on at least a quarterly basis.”
(1*) “The routine changing of passwords is not recommended.”
(2*) “Don’t change your passwords, unless you suspect they’ve been compromised.”
(3*) “Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).”

Table 1. Categories and the Quantity of Advice They Contain

| Users                          | #    | Organisations | #    |
|-------------------------------|------|---------------|------|
| Phrases                       | 39   | Expiry        | 27   |
| Composition                   | 28   | Storage       | 16   |
| Personal Information          | 21   | Generated passwords | 7   |
| Reuse                         | 17   | Individual accounts | 7   |
| Personal password storage     | 17   | Throttling guesses | 6   |
| Length                        | 17   | Keeping system safe | 6   |
| Sharing                       | 13   | Default passwords | 4   |
| Keep your account safe        | 10   | Administrator accounts | 4   |
| Backup password options       | 8    | Input         | 3    |
| Password managers             | 4    | Shoulder surfing | 3    |
| Two factor authentication     | 3    | Policies       | 2    |
| Username requirements         | 2    | Transmitting passwords | 2   |
|                               |      | SNMP strings  | 2    |
|                               |      | Password auditing | 1   |
|                               |      | Back up work  | 1    |
| **Total**                     | **179** | **Total**   | **91** |
(4*) “Normally, there should be no reason to change your password or PIN.”

We can see the first 8 pieces of advice fit under this category, because they encourage users or organisations to enforce periodic password changes. The last 4 pieces of advice also belong in this category, because they disagree with periodic password changes. We chose to display it in this way, as it highlights the contradictions in the advice circulated. All the collected and categorised advice is shown in Table 2. The first column in the table shows the 27 categories and the 79 advice statements related to them. In the second and third columns, we show how many pieces of advice contradict the advice statement and how many pieces of advice support the advice statement, respectively. We use an asterisk, *, to denote a statement that is contradicted by a separate statement in the category. For example, “Never reuse a password” does not have advice within the statement that contradicts it. However, the third statement, “Don’t reuse certain passwords,” is a contradiction of never reusing passwords.

4 ADVICE DISCUSSION
Looking through Table 2, we can see that for many categories, we collected advice that was given by one source and contradicted by another. 41% of all the advice we collected was contradicting. In this section, we will discuss some observations that we made for four chosen categories of advice.

For our insights on all the advice categories, see the supplementary material in Reference [31].

4.1 Phrases
Advice regarding password phrases was the most commonly given advice we encountered. This implies that advice is mostly concerned with making passwords “strong.” While this is important for some attacks, for attacks such as phishing and keylogging the strength of the password is irrelevant [16, 52]. Within the category Phrases, the statements: Don’t use published phrases and Substitute symbols for letters had contradictions. For don’t use published phrases, the advice given was:

1) “Don’t use song lyrics, quotes or anything else that has been published.”
2) “Do not choose names from popular culture.”
1*) “Choose a line of a song that other people would not associate with you.”

The last piece of advice directly contradicts the first. This inconsistency makes it no surprise that users seem disinclined to follow security advice [1, 25]. The advice statement Substitute symbols for letters is proposed by two sources but is advised against by a third. We know from Warner [48] that passwords with simple character substitutions are weak. Yet, 2 of 3 pieces of advice recommend it. This could stem from the attitude that it is “better than nothing.”

4.2 Reuse
We collected six pieces of advice telling users to never reuse passwords and three pieces telling users to not reuse passwords for certain sites. In addition, we found three pieces of advice encouraging users to alter and reuse their passwords and three pieces telling users to not alter and reuse their passwords. There is little agreement among the password reuse advice.

Das et al. estimate that 43%–51% of users reuse passwords across sites [12]. They also provide algorithms that improve an attacker’s ability to exploit this fact. Florêncio, Herley, and Van Oorschot [15] declare that “far from being unallowable, password reuse is a necessary and sensible tool in managing a portfolio” of credentials. They recommend grouping passwords according to their importance and reusing passwords only within those groups. Interestingly, the advice we collected in the category Don’t reuse certain passwords gave a slightly different take on this advice. The advice mostly asked users to not use the password used for their site anywhere else, e.g,
Table 2. Advice Collected

| Back-up password options | #x | #✓ | #✓ |
|--------------------------|----|----|----|
| Email up-to-date and secure. | 0 | 1 | 0 |
| Security answers difficult to guess. | 0 | 1 | 0 |
| Do not store hints. | 0 | 2 | 0 |
| Composition | #x | #✓ | #✓ |
| Must include special characters. | 5 | 2 | 2 |
| Don’t repeat characters. | 0 | 1 | 0 |
| Enforce restrictions on characters | 0 | 1 | 12 |
| Keep your account safe | #x | #✓ | #✓ |
| Check web pages for SSL. | 0 | 1 | 0 |
| Manually type URLs. | 0 | 1 | 0 |
| Don’t open emails from strangers. | 0 | 1 | 0 |
| Keep software updated. | 0 | 2 | 0 |
| Keep anti-virus updated. | 0 | 2 | 0 |
| Log out of public computers. | 0 | 2 | 0 |
| Password protect your phone. | 0 | 1 | 1 |
| Length | #x | #✓ | #✓ |
| Minimum password length. | 0 | 13 | 0 |
| Enforce maximum length (+40). | 0 | 1 | 1 |
| Password Managers | #x | #✓ | #✓ |
| Use a password manager. | 0 | 1 | 1 |
| Create long random password. | 0 | 1 | 1 |
| Personal Information | #x | #✓ | #✓ |
| Don’t include personal information. | 0 | 1 | 1 |
| Must not match account details. | 0 | 8 | 0 |
| Do not include names. | 0 | 16 | 0 |
| Personal password storage | #x | #✓ | #✓ |
| Don’t leave in plain sight. | 0 | 1 | 2 |
| Don’t store in a computer file. | 0 | 1 | 1 |
| Write down safely. | 1 | 0 | 1 |
| Don’t choose “remember me.” | 0 | 1 | 3 |
| Phrases | #x | #✓ | #✓ |
| Don’t use patterns. | 0 | 6 | 0 |
| Take initials of a phrase. | 0 | 4 | 0 |
| Don’t use published phrases. | 0 | 1 | 2 |
| Substitute symbols for letters. | 0 | 1 | 1 |
| Blocklist common passwords. | 0 | 2 | 0 |
| Don’t use words. | 0 | 16 | 0 |
| Insert random numbers and symbols. | 0 | 1 | 4 |
| Reuse | #x | #✓ | #✓ |
| Never reuse a password. | 5 | 6 | 6 |
| Alter and reuse passwords. | 3 | 5 | 3 |
| Don’t reuse certain passwords. | 3 | 0 | 5 |
| Sharing | #x | #✓ | #✓ |
| Never share your password. | 0 | 9 | 0 |
| Don’t send passwords by email. | 0 | 9 | 0 |
| Don’t give passwords over phone. | 0 | 0 | 0 |
| Two-factor authentication | #x | #✓ | #✓ |
| Use for remote accounts. | 0 | 1 | 0 |
| Two-factor authentication using phone. | 0 | 1 | 0 |
| Username | #x | #✓ | #✓ |
| Enforce composition restrictions. | 0 | 1 | 0 |
| Don’t reuse username. | 0 | 1 | 0 |

LHS table: advice aimed at end-users, RHS table: advice aimed at organisations. #x = number of sources contradicting the statement. #✓ = number of sources supporting the statement. An asterisk (*) represents the unusual case where an entire statement in a category contradicts another.
“Never use your Apple ID password for other online accounts.” Most organisations gave advice prioritising their own accounts. Only one piece of advice suggested using a unique password for any important accounts [17].

An alternative to grouping accounts for reuse is to alter and then reuse a password. This advice was given by three sources and rejected by three sources. Alterations to passwords are often predictable. Using a cross-site password-guessing algorithm, Das et al. [12] were able to guess approximately 10% of non-identical password pairs in less than 10 attempts and approximately 30% in less than 100 attempts.

4.3 Composition
Composition restrictions are regularly enforced by websites, but the advice given is not consistent from site to site. It is interesting to note that Herley [23] hypothesises that different websites may deliberately have policies that are restrictive to different degrees, as this can help ensure that users do not share passwords between sites. We collected 12 pieces of advice encouraging Enforce restrictions on characters and only 1 piece of advice against it. The source rejecting character restrictions was the NIST 2017 authentication guidelines [19]. These guidelines have received praise from the authentication research community [10] and specifically considered usability issues, which is why they moved away from some of the more burdensome, less effective advice still popular in the security community at that time. This raises the question of whether organisations will begin to disseminate these new security practices or continue to enforce their stringent password restrictions.

Kelley et al. show that strict composition rules do increase the security of passwords [27]. However, similar security can be offered by password blocklists or mandating minimum of 16-character passwords. In a related study, Komanduri et al. [28] showed that the 16-character password restriction was less annoying and less difficult for users. In addition, when composition rules are enforced, the probability of a user including a “1” as their number and an “!” as their symbol is high [46]. So, an attacker who knows the composition restriction in place could potentially tailor their attacks to suit it. Tan et al. also echo this finding, stating that requiring passwords to have multiple character classes has at most minor benefits to password strength and can even reduce effective security [45].

4.4 Expiry
We found 5 pieces of advice telling organisations to Store password history to eliminate reuse, 1 encouraged organisations to Enforce a minimum password age, and 10 were in favour of Changing passwords if compromise is suspected. If organisations do store their users’ password history, then this creates an additional security hole, as the company needs to allocate resources to protect this file. Also, even though users can no longer reuse prior passwords, alterations are still possible [42]. Zhang, Monrose, and Reiter [51] identify that we can easily predict new passwords from old ones when password ageing policies force updates.

The reason given for introducing a minimum password age is to prevent users from bypassing the password expiry system by entering a new password and then changing it right back to the old one [30]. However, if an attacker gains access to a user’s account and changes their password, then the user will be unable to change it again until the required number of days have elapsed, or with an administrator’s help. Ten pieces of advice recommended changing passwords if a compromise is suspected. This can be inconvenient for users not affected by the compromise, and also for those who are. If there is a breach at the server, then the users were not at fault, yet still they must choose a new password.

From anecdotal evidence, we know the advice to change your password regularly is widely hated by users [20]. Seven pieces of the advice we collected encouraged the use of password expiry,
Table 3. Finalised Cost Categories

| Organisation Costs                  |
|-------------------------------------|
| Increased help desk/user support time |
| User education required             |
| Organisation needs extra resources  |
| Takes organisation time to implement|
| Increases the organisation’s computing power needed |

| User Costs                          |
|-------------------------------------|
| Makes it more difficult to create a password |
| Makes it less easy to remember       |
| Requires extra resources             |
| Requires the creation of a new password |
| Increases the computing power needed |
| Requires other extra time or effort  |

while only four pieces of advice discouraged it. This is despite research suggesting that the security benefits are minimal [9, 51]. This implies the inconvenience to users is worth less to organisations than the minimal security benefits. Or, do organisations want to be seen to be enforcing strong security practices, and forcing expiry is just one way of doing this?

More discussions of the advice collected can be found in Reference [31]. However, the circulation of contradictory advice could give an insight into why organisations and users might have trouble following proper authentication recommendations.

5 COSTS MODEL

In this section, we describe the methodology for the creation of our costs model. We began with a brainstorming exercise. At the heart of it was a conscious consideration for the usability costs: costs that are often overlooked when security policies are implemented [11]. We viewed costs as any burdens on the user who must follow the advice or any burdens on the organisation who must either follow or enforce the advice.

5.1 Cost Categories

The finalised set of costs was reached through an iterative process that involved assigning costs to each of our 79 advice statements and adapting the cost-categories until we reached a set of cost-categories that made it possible to describe the range of advice impacts. This finalised list of cost types, as shown in Table 3, was then presented to user and administrator participants in our study for feedback.

User versus organisation costs. We wished to differentiate between costs borne by the user and costs borne by the organisation. We believe it will be interesting to know who bears most of the costs: the user or the organisation. In addition, what might be a small cost for an organisation could be a large cost for a user. We, therefore, separated cost categories to be user- and organisation-specific, e.g., user computing power separate from organisation computing power.

Minor costs. In our analysis, we acknowledged the need to distinguish the extent to which a cost occurs. For example, both Enforce restrictions on characters and Make digital and physical back-ups require organisation time. But little organisation time is needed to enforce a composition restriction, and a lot of effort is needed to digitally and physically back up work. It is not within the scope of this model to have a full grading of the costs, but we do acknowledge a difference between small
or partially felt costs and more substantial costs. In our tables, a minor cost is identified as ○ and a more substantial cost is identified as ●.

Periodic costs. We also notice that advice such as Make digital and physical back-ups and Keep email up-to-date and secure require continued action. This significantly increases the costs. We acknowledge three types of costs: one-off costs usually relating to setup or account creation, costs that occur at every login, and periodic costs that occur repeatedly over different time frames. To identify these costs, we use a super-scripted symbol. Costs at login are denoted by an at symbol: ○ @ and periodic costs are denoted by a sun: ● ☀.

Positive costs. Finally, some pieces of advice reduced the burden on the organisation or user. These pieces of advice we acknowledge as “positive costs” and, as such, they are represented with the positive symbol: +.

5.2 User and Administrator Surveys

Once satisfied that we had a provisional set of cost categories for users and organisations, we began our user study. We created five surveys aimed at administrators and five surveys aimed at end-users. Both survey types used a multiple-choice format where participants were asked to identify the costs they associated with a selection of advice statements. We randomly directed participants to one of the five relevant surveys, each containing questions about a subset of advice. This allowed us to ask about the large number of advice statements we had collected without overburdening participants. However, to ensure that even with a low number of sample participants we would still receive some meaningful analysis, we did include some overlap in the end-user surveys. Every end-user was asked to identify costs for the following advice statements:

- Composition - “include specific character types in your password.”
- Expiry - “change your password regularly”
- Reuse - “never reuse a password”
- Sharing - “never share your password”
- Paste “you should not be able to paste your password when logging in”
- Password manager - “you should use a password manager to store your passwords”
- Two-factor authentication - “you should use 2-factor authentication when logging into accounts (e.g., a code from an app or a special device)”

We chose these as representative of typical current advice. Note that the advice “Do not allow users to paste passwords” was not collected as part of our research yet we include it here. We chose to add it to our survey as a “canary.” This advice has been discussed online as a piece of bad advice that, unfortunately, became common practice, but has no discernible security ramifications [24]. This advice will act as a test case for our methods.

While we might have liked to include overlap in the administrator surveys, too, the breadth of advice related to administrators was too great to allow redundancy. In fact, we were forced to remove some advice from the administrator survey to keep the estimated completion time within 10 minutes. Neither users nor administrators were remunerated for completing the survey, so keeping it within a shorter time frame was important for encouraging meaningful responses.

Example survey question. In the survey, participants were asked to indicate the severity and frequency with which they experience costs and inconveniences as a result of authentication advice. We also asked for comments about whether they approved of the given piece of advice. Figure 1 shows a graphic providing users with an explanation of how to complete a survey question. Users were also given the following example to help them understand the survey:
Fig. 1. Infographic with instructions for users for the survey. For each advice statement, participants were asked to identify the frequency and severity of any costs they perceived.

For example: for the advice "Change your password regularly" you might consider the following costs:
- Makes it less easy to remember (periodically - every time I need to change it)
- Need to pick a new password (periodically - every time I need to change it)
- Takes extra time (periodically - sometimes I can’t start work until I change the password)

You could complete the question for this advice as shown in Figure 1. Note these costs are individual and may differ for you and you are not required to offer explanations.

Administrators were given a similar description but were asked to assess which of the organisation cost categories the advice affected. Full versions of the questions and answers for both the user survey and the administrator survey are available on GitHub [31].

5.3 Sampling and Ethics
Participants were chosen using a snowball sampling technique. For the administrator survey, we reached out directly to our contacts in systems administration or security management roles. We asked these people to take part in the survey and encouraged them to recruit future subjects from among their acquaintances. Similarly, we reached out to a selection of non-technical acquaintances, asking them to complete the user survey and encouraging them to circulate it to others. Both surveys were circulated to the general population via social media.

The study was approved by our university Ethics Review Board and no personal identifying information was collected about participants. The only demographic information collected asked end-users to rate themselves on their internet security knowledge. This was to ensure that our sampling techniques did not skew our end-user results towards highly technical or security-aware individuals. We received 44 participants for our end-user survey and 37 participants for our administrator survey. In Figure 2, we plot the number of users who assigned themselves to each Internet security rank. Users were told to "Select a rank on the below scale from 1 (very poor) to 5 (very knowledgeable) to describe your internet security knowledge." No users described their knowledge as very poor but after that, we seem to have a reasonable spread across the remaining ranks with an expected lower number of people selecting 5 (very knowledgeable).
5.4 Representation of Survey Responses

When collecting the survey results, we use the following rules for identifying what costs the participants agreed exist for each piece of advice (i.e., did participants believe a cost major, minor, positive, or non-applicable):

- If one answer option was chosen by more participants than any other, then it is the majority answer.
- If two answer options were chosen with equal frequency, then we report the option with the largest cost but note with an underline that there was variability in the responses, e.g., \( \text{ } \). This means we are choosing to overestimate rather than underestimate costs.
- If “Doesn’t apply” is outweighed or equaled by minor and major combined, then we assign it as minor.\(^1\) We again indicate that there is variability. For example, if 40% of the users said non-applicable but 30% said it was a major cost and 30% said it was a minor cost, then we would mark it as a minor cost, as the sum of minor and major is greater than “Doesn’t apply.”

Users and administrators were also asked about their approval of the advice statements. The results of this are represented in the table for both users and administrators. A ✔ represents that the majority of respondents approved of the advice. ✗ indicates that the majority disapproved, and ■ represents that the majority of respondents were neutral about the advice. Occasionally, respondents were split between different approval ratings. This is also indicated in the table. For example, if users were split between approve and neutral, then we represent this as ✔/■.

In Table 4, we present the costs that users and/or administrators associated with each piece of advice. As mentioned, we could not include every piece of advice in the surveys in an attempt to reduce the size of the survey. In the table below, we highlight the corresponding row in the table in blue (see the organisation side of the row “Enforce maximum length”) to show that this advice was not included in the survey. At times, even when the advice was not directly included in the survey, we indicate obvious costs that exist. For example, for the “Enforce maximum length” advice, the administrative costs could be extrapolated from the “Minimum password length” costs.

6 COSTS SURVEY: RESULTS

We received 44 participants for our end-user survey and 37 participants for our administrator survey. We received insightful comments about the costs from both a user and administrator perspective. A minimum of eight end-users indicated the costs they associated with each piece of advice, and a minimum of six administrators indicated the organisation costs they perceived, again for each piece of advice. Table 4 details the costs that users and administrators identified for each advice statement. In this section, we highlight the following: 6.1, the feedback we received from users and administrators on our suggested cost-categories; 6.2, the costs participants assigned to the advice; and 6.3, participants’ approval of the advice.

6.1 Cost Category Comments

6.1.1 User Cost Categories. After users had attempted to assign cost categories to the advice statements, they were asked at the end of the survey whether they agree with the cost categories that were used in the survey.

For the user survey, the prevailing answer was between “Somewhat” and “Yes”: 21 end-users said Somewhat, 18 said Yes, and 1 said No. The user who chose “No” said: “In most cases the categories seemed not applicable to the points, so most were of no cost to me.” This is a valid point, for many advice statements there was only one cost category that users deemed to apply and for

\(^1\)Note that “Doesn’t apply” was the default response for the survey questions.
### Table 4. Costs of Implementing Password Advice

| Advice to Users | Organisation | User costs |
|-----------------|--------------|------------|
| **Backup password options** | | |
| Email up-to-date and secure | | | |
| Security answers difficult to guess | | | |
| Do not store hints | | | |
| **Composition** | | |
| Must include special characters | | | |
| Don’t repeat characters | | | |
| Enforce restrictions on characters | | | |
| **Keep your accounts safe** | | |
| Check web pages for TLS | | | |
| Manually type URLs | | | |
| Don’t open emails from strangers | | | |
| Keep software updated | | | |
| Keep anti-virus updated | | | |
| Log out of public computers | | | |
| Password protect your phone | | | |
| **Length** | | |
| Minimum password length | | | |
| Enforce maximum length (>40) | | | |
| **Password managers** | | |
| Use a password manager | | | |
| Create long random password | | | |
| **Personal information** | | |
| Don’t include personal information | | | |
| Must not match account details | | | |
| Do not include names | | | |
| **Personal password storage** | | |
| Don’t leave in plain sight | | | |
| Don’t store in a computer file | | | |
| Write down safely | | | |
| Don’t choose “remember me” | | | |
| **Phrases** | | |
| Don’t use patterns | | | |
| Blocklist common password | | | |
| Take initials of a phrase | | | |
| Don’t use published phrases | | | |
| Substitute symbols for the letters | | | |
| Don’t use dictionary words | | | |
| Insert random numbers and symbols | | | |
| **Reuse** | | |
| Never reuse a password | | | |
| Alter and reuse passwords | | | |
| Don’t reuse certain passwords | | | |

(continued)
Table 4. Continued

| Source contributing to costs and benefits of authentication advice | Organisation | User costs |
|---|---|---|
| | Increased help desk user support time needed | User education required | Increased support from peers needed | Administrator approval | Makes it more difficult to reset a password | Makes it less easy to remember | Requires extra resources | Requires the creation of a new password | Requires extra resources for computing power needed | Requires other extra time or effort | User approval |
| **Sharing** | | | | | | | | | | | |
| Never share a password | 0 | 9 | | | | | | | | | |
| Don’t send passwords by email | 0 | 3 | | | | | | | | | |
| Don’t give passwords over phone | 0 | 1 | | | | | | | | | |
| **Two-factor authentication (2FA)** | | | | | | | | | | | |
| Use 2FA using app or special device | 0 | 1 | | | | | | | | | |
| Use 2FA on phone | 0 | 1 | | | | | | | | | |
| Use 2FA for remote accounts | 0 | 1 | | | | | | | | | |
| **Username** | | | | | | | | | | | |
| Enforce restrictions on characters | 0 | 1 | | | | | | | | | |
| Don’t reuse username | 0 | 1 | | | | | | | | | |
| **Advice to organisations** | | | | | | | | | | | |
| **Administrator Accounts** | | | | | | | | | | | |
| Not for everyday use | 0 | 1 | | | | | | | | | |
| Must have its own password | 0 | 2 | | | | | | | | | |
| Should have extra protection | 0 | 2 | | | | | | | | | |
| **Back-up work** | | | | | | | | | | | |
| Make digital & physical back-ups | 0 | 1 | | | | | | | | | |
| **Default passwords** | | | | | | | | | | | |
| Change all default passwords | 0 | 4 | | | | | | | | | |
| **Expiry** | | | | | | | | | | | |
| Store history to eliminate reuse | 0 | 5 | | | | | | | | | |
| Change your password regularly | 4 | 8 | | | | | | | | | |
| Change if suspect compromise | 0 | 10 | | | | | | | | | |
| **Generate passwords** | | | | | | | | | | | |
| Use random bit generator | ‘2’ | 2 | | | | | | | | | |
| Must aid memory retention | 0 | 2 | | | | | | | | | |
| Must be issued immediately | 0 | 1 | | | | | | | | | |
| Distribute in a sealed envelope | 0 | 1 | | | | | | | | | |
| Only valid for first login | 0 | 1 | | | | | | | | | |
| **Individual accounts** | | | | | | | | | | | |
| One account per user | 0 | 4 | | | | | | | | | |
| Each account password protected | 0 | 3 | | | | | | | | | |
| **Input** | | | | | | | | | | | |
| Don’t perform truncation | 0 | 1 | | | | | | | | | |
| Accept all ASCII characters | 1 | 1 | | | | | | | | | |
| **Keep system safe** | | | | | | | | | | | |
| Implement Defense in Depth | 0 | 2 | | | | | | | | | |
| Implement Technical Defenses | 0 | 1 | | | | | | | | | |
| Apply access control systems | 0 | 1 | | | | | | | | | |
| Monitor and analyse intrusions | 0 | 1 | | | | | | | | | |
| Regularly apply security patches | 0 | 1 | | | | | | | | | |

(continued)
Table 4. Continued

| Network: SNMP community strings | Organisation | User costs |
|---------------------------------|--------------|------------|
| Don’t define as standard defaults | 0 | ○ | ○ |
| Different to login password | 0 | ○ | ○ |

| Password auditing | | |
|-------------------|------------------|------------------|------------------|------------------|
| Attempt to crack passwords | 0 | ○ | ○ | ○ | ○ | ○ | ○ |

| Policies | |
|----------------------------------|---------------|------------------|------------------|
| Establish clear policies | 0 | ○ | ○ | ○ | ○ |

| Shoulder surfing | |
|-------------------|------------------|------------------|------------------|
| Offer to display password | 0 | ○ | ○ | ○ | ○ | ○ | ○ |
| Enter your password discretely | 0 | ○ | ○ | ○ | ○ | ○ | ○ |

| Storage | |
|----------------------------------|---------------|------------------|------------------|------------------|
| Encrypt password files | 0 | ○ | ○ | ○ | ○ | ○ | ○ |
| Restrict access to password files | 0 | ○ | ○ | ○ | ○ | ○ | ○ |
| Hash and salt passwords | 0 | ○ | ○ | ○ | ○ | ○ | ○ |
| Encrypt passwords | *4 | 7 | ○ | ○ | ○ | ○ | ○ |
| Don’t hardcode passwords | 0 | 1 | ○ | ○ | ○ | ○ | ○ |

| Throttling | |
|-------------------|------------------|------------------|------------------|
| Throttle password guesses | 0 | 6 | ○ | ○ | ○ | ○ | ○ |

| Transmitting passwords | |
|--------------------------|------------------|------------------|------------------|
| Don’t transmit in cleartext | 0 | 4 | ○ | ○ | ○ | ○ | ○ |
| Request over a protected channel | 0 | 2 | ○ | ○ | ○ | ○ | ○ |

| Don’t allow users to paste passwords | |
|----------------------------------|------------------|------------------|------------------|
| | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

○, filled circle: major cost. ○, empty circle: minor cost. +, plus: positive cost. ★, superscript @: cost occurs at each login. ☽, superscript ☽: cost occurs periodically. ☐, underline: implies that variance existed in the costs that respondents indicated. ✓: approval split between Yes and Neutral. The shaded blue background indicates that this advice was not included in the survey.

some advice such as “Every user in an organisation must have their own account,” the majority of participants decided that there were no associated user costs.

After asking participants whether they agreed with the cost categories, we asked whether there were any cost categories that they think should be added or removed. We received the following suggestions: One person said we could remove computing power. One person said a cost could be that the advice “decreases sense of security in passwords.” Another participant suggested maybe including the cost category “makes it harder to follow other advice.” They gave the example that needing to have long passwords would make it more difficult to not write them down somewhere. One participant suggested that there is a “cost to personal stress related to constantly interacting with devices that require various different logins and passwords and eat up time and energy!!” All 34 other participants suggested no changes to the cost categories.

We did consider removing the user computing power cost but, in the end, decided that in some areas it might be relevant. For example, for the pieces of advice “Keep anti-virus updated” and “Keep software updated,” the majority of users said that computing power was a minor cost. This can relate to a slowdown of computing processes during an installation or waiting for restarts during updates. The ability of a participant to follow multiple pieces of advice simultaneously
is important to consider. For example, Florêncio et al. show that never reusing a password and also random password choice is an impossible task outside the bounds of human memory [15]. In fact, many respondents in our survey made the point that the advice “Never reuse a password” is impossible to uphold unless it is coupled with the use of a password manager. For this reason, to really get a sense of the value or effect of a piece of advice, it is important to consider it in light of a complete security policy.

A yes/no answer system would have made the survey easier for participants to understand and simplify the completion. We were eager to get information about severity and frequency but in retrospect, a simplified version of the survey should have been considered. We did also notice that there was misunderstanding among participants about the meaning of the “Positive costs.” We think a different term should have been used to describe these that was more self-descriptive. Based on the answers, we believe some participants indicated “positive” when they were “positive” there was a cost there. These participants were always the minority, so largely did not affect the results.

Finally, the stress associated with current password systems is exemplified by the respondents’ encouragement for “costs to personal health” to be included as a category. When we consider a security system and speak about usability, it is mitigating this stress and pressure that users are burdened by that we want to achieve. We believe this stress is a result of the human effort and mental strain that is encompassed within the existing categories.

6.1.2 Organisation Cost Categories. As with users, after administrators had attempted to assign organisation costs to the advice statements, they were asked at the end of the survey whether they agree with the cost categories that were used in the survey. Most administrators agreed with the five cost categories that were used to denote organisation/administration costs in this survey. However, nearly as many said they “Somewhat” agreed. Thirteen administrators said Yes, 12 said Somewhat, and 4 said No.

The most common comment we received was that user burdens were not included as a cost category. It is likely that administrators were not aware that a second survey existed aimed at users and the burdens they experience. However, the fact that many administrators insisted that user burdens must be considered is reassuring. It shows a change in the ethos within security development and indicates that there could exist a changing perspective that is no longer viewing users as the enemy.

One respondent commented that the “resources” cost was not specific enough. From feedback we received during the survey, we acknowledged that a misunderstanding existed with the term “additional resources needed.” Some respondents viewed resources as additional personnel needed, whereas we were referring to resources as physical purchases required. We categorised a need for additional personnel under increased help desk/user support time and/or time taken to implement. We did include a clarification for this partway through the study, stating that “Resources refers to physical resources that may need to be acquired or purchased.” After this clarification, the responses seemed more aligned with this definition. For this reason, though, a resource cost is sometimes identified where it does not seem clear to us why it should be. We do leave it in, as significant increases in necessary personnel and other forms of resources are valid forms of burdens for an organisation.

One administrator participant mentioned that “Everything has a cost sometimes it is small, but in many areas questioned in this survey, the benefit outweighs the cost.” This indicates that this comparison of costs versus benefits of security advice is something that security administrators are required to do mentally for each policy consideration.

Two participants mentioned other costs. One said that “Some things need more than just help desk resources—development time, administration, auditing.” The second participant said, “There
is more than just training and help support in terms of cost. [There] is also engineering cost, audit cost, risk assessment cost, employee quality costs (not all employees can implement the policies discussed here in an enterprise environment). Technology cost. Enforcement cost. Incident response cost (for policy violations). These are all interesting areas for consideration. We would have viewed all of these as “organisation time taken to implement the policy,” though employee quality costs are not something we considered.

Finally, one respondent mentioned that the extent of costs can depend strongly on the ethos of a company. They state that “Having a business leadership team that fully supports IT Security and is prepared to champion it will for example make the initial and ongoing “cost” in terms of resource much easier. Many of the things here will depend not just on technology but the culture and maturity of the organisation.” This alludes to feedback we received throughout the survey and directly from some respondents: The costs experienced differ for each organisation. While the general costs felt might be similar, the extent to which they are felt, and the difficulty involved in implementing advice, will strongly depend on the ethos, size, and sector or services of the company. In our application of our cost model, we can only consider generalised costs felt by the majority. However, if an organisation is utilising this methodology to determine which advice to implement, then they can tailor the costs selected based on their own context.

6.2 Cost of Security Advice

The costs associated with implementing and following advice are shown in Table 4. The most selected user cost category was increased risk of forgetting, and the most selected organisation cost category was user education required. It is important to note that while organisation time is required to develop and run user education, user time is also necessary. Therefore, each time we see a user education cost, we recall that this also involves a burden for users.

There were 200 costs identified across all the pieces of advice for the organisation and 109 costs identified for users. Of these, the users identified that 28% of them were major costs. Administrators identified that 16% of the costs to the organisation were major. 37.5% of these major organisation costs were attributed to user education. Of the 200 organisation costs, 44% were repeating costs, i.e., they were felt at each login or periodically. Of the users’ 109 costs, 46% were repeating. However, nearly half (49%) of the repeating organisation costs were attributed to user education, a cost that will be felt by users as well. Similarly, of the user repeating costs, 40% were related to the cost of forgetting, as many attributed this as occurring at login. The cost of forgetting is a cost that is felt by the organisation as well, since the users’ only solution is often to contact the organisation’s help desk.

Of our 11 cost categories, help desk time, time to implement, user education, and all the user costs excluding computing power, involve a human directly. In these categories, advice is adding to the emotional burden or workload of the individuals involved. Humans are impacted by 87% of all the costs identified. In the user survey, we witness strong emotional responses towards the advice we asked users to analyse. We received responses such as “I am sick of passwords and logins and they are making me less productive as I have to look up the passwords so often!!” Users only agreed on three pieces of advice that have a positive impact on a cost category. These are: “You should use a password manager to store your passwords,” “Write your password down safely,” and “You should alter your password and then reuse it on other websites or computers.” All three of these had a positive impact on memorability.

6.3 Approval of Advice

For each piece of advice, we asked users and administrators to indicate whether they approved of the advice, felt neutral about it, or disagreed with it. In the 6th and 13th columns of Table 4,
Table 5. Differing Opinions among User Respondents and among Administrator Respondents

| Decision | #Approve | #Neutral | #Disagree | #Approve | #Neutral | #Disagree | #Approve | #Neutral | #Disagree | Acceptance |
|----------|----------|----------|-----------|-----------|----------|-----------|-----------|----------|-----------|-----------|------------|
| ✓        | 6        | 1        | 0         | 19        | 9        | 13        | ✓         |          |           |           |            |
| x        | 2        | 0        | 6         | 14        | 10       | 17        | x         |          |           |           |            |
| ✓        | 5        | 2        | 1         | 3         | 2        | 4         | x         |          |           |           |            |
| x        | 0        | 2        | 5         | 2         | 4        | 2         |           |          |           |           |            |
| ✓        | 7        | 0        | 0         | 3         | 4        | 2         |           |          |           |           |            |
| ✓/ x     | 3        | 3        | 1         | 32        | 15       | 13        | ✓         |          |           |           |            |
| ✓        | 6        | 1        | 0         | 19        | 9        | 13        | ✓         |          |           |           |            |
| ✓        | 4        | 0        | 3         | 7         | 2        | 1         | ✓         |          |           |           |            |
| ✓        | 3        | 2        | 2         | 0         | 2        | 6         | x         |          |           |           |            |
| ✓        | 4        | 2        | 2         | 2         | 5        | 1         |           |          |           |           |            |
| x        | 2        | 1        | 4         | 10        | 10       | 20        | x         |          |           |           |            |
| ✓        | 4        | 1        | 1         | 2         | 2        | 5         |           |          |           |           |            |

The majority opinion for each group is highlighted and indicated in the decision column.

While we took the majority answer as the mutual consensus for Table 4, it is important to note that opinions on advice were divided. We found that for 32% of the advice, there was at least one administrator respondent who disagreed with others on whether advice was valuable. More starkly, for 71% of the advice considered by end-users, there was at least one user-respondent with a different opinion from others. While a 32% difference could be put down to differences of opinion on practice or different interpretations of the advice statement, the 71% disagreement among end-users shows a significant lack of consensus.

Table 5 shows examples where a lack of consensus was prominent. For both administrators and end-users, we indicate how many respondents agreed with the given advice statement, were neutral about it, and disagreed with it. For example, 6 administrators agreed with the advice “Never reuse passwords” and 1 was neutral about it. However, for the same piece of advice, 19 users approved of “Never reusing passwords,” but 9 were neutral and 13 disapproved. One user said, “I experience regular frustration and lose valuable time at work trying to login to numerous platforms with different passwords.” The majority opinion for each group is highlighted and indicated in the decision column. Notice that in some places, the users and administrators come to a different consensus about whether a piece of advice is valuable. For example, users believe they should be allowed to store password hints, but administrators disagree.

Throughout Table 5, we see evidence of differences in opinion between users and administrators. Users were conflicted about whether typing URLs was good advice, however, administrators unanimously (excluding neutral responses) disapproved of it. Administrator respondents said “It might be nice in theory, but impossible to implement and enforce in practice” and “There may be occasions when this is relevant but typo-squatting also poses a risk besides phishing.” This advice might have security benefits, but it introduces a new attack vector and also results in a significant time loss for anyone who follows it.

The advice “Include specific characters in your username” divided administrator opinions and users strongly disagreed with it. In a 2007 research paper [14], Florêncio et al. determined that rather than making the secret password more complex, complexity could instead be added to the username. Users can choose and record a long username and this will likely offer effective
protection from a bulk guessing attack; the same attack that a complex or long password is hoping to combat. One administrator disapproving of this advice said, “good for passwords, over complicates usernames as password should be secure, usernames are often generated based on firstname.lastname etc.” One end-user respondent commenting on the advice said, “Stupid and pointless” and another said, “Can’t see a good reason for this, but with a password manager it wouldn’t be too painful.” If this policy was being implemented in an organisation, then these responses emphasise the need for it to be coupled with effective user education and validation.

Administrators were generally in favour of altering a password before reusing it at another site. But most users surveyed did not approve of the advice. One user who disagreed with the advice said, “Impossible to remember what password goes with what site.” A different user who disagreed said, “Any method to your password creation makes it less secure.” One administrator commented that ensuring alterations before password reuse should be a strict policy that is reinforced by user education.

End-users were torn on the advice, stating that it should not be possible to paste your password when logging in. The comments given emphasise the differing opinions. One user said: “If someone is trying to copy/paste a password, they’re probably beyond help.” While another user said: “This is horrendous advice that leads to problems using password managers. It encourages using crappy passwords.”

Many users were willing to follow advice if it seemed beneficial. For example, for the advice “regularly change passwords,” one user commented: “Undoubtedly sensible, undoubtedly annoying.” There is substantial evidence in the responses [31] that user education has been effective. Generally, users’ responses echoed the advice that was given in historic security documents [7]. However, few users and administrators showed an awareness of new recommendations that have superseded the legacy advice [19]. For example, the 2017 NIST advice recommends not introducing restrictions on the characters allowed in passwords. Yet, most users and administrators indicated that they agreed with forcing the use of certain characters in passwords. Note that this new NIST advice has been available and circulating since 2017, and our user survey was completed in October 2020.

Overall, understanding users’ approval of advice is a valuable stepping stone to improved user education and mutual respect between users and policy enforcers. As Adams and Sasse show, users will simply employ less secure workarounds if security policies do not allow them to do their job effectively [1].

7 BENEFITS MODEL

Now, we ask the question: What are the benefits of this advice? From our analysis of costs, it is evident that advice is generally not attempting to make authentication more usable. Instead, the goal of the advice must be to guide the creation of robust authentication systems that will prevent unauthorised access to an account or data [3, 13, 23, 41]. Therefore, the “benefit” of a piece of advice is the effect it has towards achieving this goal. In this section, we provide a methodology for identifying what benefits a single piece of advice can bring.

7.1 Benefit Categories

Unauthorised access has many avenues, and one piece of advice is unlikely to protect against them all. For example, requiring passwords of length 12 might help against a password-guessing attack but will do nothing to protect against a phishing attack. To represent how “beneficial” a piece of advice is, we would like to know in which ways the piece of advice protects against unauthorised access, if at all. To this end, we require a concise list of the different methods an adversary could use to gain access to a protected account. The NIST 2017 Digital Identity Guidelines [19] includes a table of “Authenticator Threats.” Given that this NIST 2017 authentication document has been a
### Table 6. Attack Types on Authentication

| Attack type                  | Description                                                                                     | Examples                                                                                     |
|-----------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| **Assertion**               | The assertion is used to communicate the result of the authentication process from the verifier to the Relying Party (RP). The verifier and the RP may be the same entity or separate entities. | Use of assertion replay to impersonate a valid user or leakage of assertion information through the browser [44]. |
| **Physical theft**          | A physical authenticator or a physical device used in the authentication process is stolen by an attacker. | A hardware cryptographic key (e.g., a USB authenticator), a phone, computer or one-time-password device is stolen. |
| **Duplication**             | The subscriber’s authenticator has been copied with or without their knowledge.                  | Passwords or private keys written on paper or stored in an electronic file are copied. A counterfeit biometric authenticator is manufactured. |
| **Eavesdropping**           | The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating. | Passwords are physically observed during keyboard entry or intercepted by keystroke logging software or recorded during transmission or via network packet sniffing. |
| **Offline Cracking**        | An offline guessing attack is an analytical guessing attack by an attacker, it requires little to no communication with the system under attack. | A dataset of passwords or keys that are hashed & salted or encrypted are made available to an attacker (leaked). Using a dictionary or brute force guessing method the attacker attempts to guess the plaintext values of these protected secrets. |
| **Side Channel Attack**     | This attack leverages an aspect of the implementation of the computer system or security device. | An attacker exploits information about a cryptographic key gathered from power, timing, or audio data. |
| **Phishing or Pharming**    | Fooling the subscriber into thinking the attacker is a verifier. Phishing: electronic communication masquerading as the verifier. Pharming: directing a website’s traffic to a masquerading fake site. | Phishing: A password is revealed by a bank subscriber in response to an email inquiry from a phisher pretending to represent the bank. Pharming: a password is revealed by the subscriber at a fake verifier website reached through DNS spoofing [2, 8] |
| **Social Engineering**      | The attacker establishes a level of trust with a subscriber to convince the subscriber to reveal their authenticator secret or authenticator output. | An attacker masquerading as a system administrator makes a telephone inquiry requesting the victim’s password. |
| **Online Guessing**        | The attacker connects to the online server of the verifier and attempts to guess the valid authenticator output for one or multiple users. | An attacker who knows the usernames for all the accounts guesses the top 10 most popular passwords to try to access them. An attacker who knows neither the username nor password guesses combination of both to try to unlock the account. |
| **Endpoint Compromise**     | Malicious code on the endpoint authenticates without the victim’s consent, compromises the authenticator, or causes authentication to other than the intended verifier. | Malicious code can steal data from the user’s device. Malicious code can be used to conduct man-in-the-middle attacks on all connections. New trusted certificates can be installed on the user’s device. |
| **Unauthorised binding**    | An attacker can cause an authenticator under their control to be bound to a subscriber’s account. | Forcing a password reset to change the password to one the attacker knows; or creation of a USB authenticator and linking it to a user’s account. |

highly regarded [10] and thoroughly researched document, we accept these as a concise list of the attack vectors against authentication. Below, in our Table 6, we list the attacks that NIST identified (Table 8-1 in Reference [19]). Included are the name, details, and example for each different attack type. In places, we diverge slightly from the official text provided by the NIST document to simplify the descriptions and examples.
7.2 Representation of Advice Benefits
As with costs, which could be larger or smaller, the benefits provided by different advice also vary. The benefits of advice, therefore, should reflect the probability of each attack being successful. Given some baseline chance of each attack, we reflect on whether a piece of advice increases or decreases the chance that an attack is successful. We show the result of this analysis for the 79 advice statements in Table 7. We use the symbols ↑ and ↓ to indicate an increase or decrease, respectively, in the probability of success for the attack type. ↑ and ↓ indicate less significant increases or decreases in the probability of success for the attacks. An underline, _, indicates that the improvement is not directly enforceable. This could be because the advice is too vague and therefore there is ambiguity on how an organisation or user might follow it. Or simply that an organisation cannot bind their users to follow the advice. In supplementary material, we include all explanations for why we believe the chances of certain attacks are impacted by the advice [31]. When determining this assignment of benefits, we took input from stakeholders and experts, including giving presentations at specialist conferences/workshops [21, 22, 32, 47], statistics from our university IT department, and insights from our university’s information security manager.

7.3 Baseline for Comparison
Throughout Table 7, we mark each piece of advice as either increasing or decreasing the chance of compromise. However, there is an interesting question about what baseline the advice increases or decreases the chance of compromise relative to. We first thought of the baseline as being a passive version of the advice. For example, if the advice is: “Email up-to-date and secure” or “Encrypt passwords,” then the baseline we measure the improvements from is doing nothing. This made sense for a lot of the advice statements, but not all. For example, the advice “Do not store hints” is already a passive action, but we do not want to measure its effects against itself. Our second consideration for the baseline was the opposite of what the advice stated. For example, for the advice “do not store hints,” we consider the difference in attack threat between this and “do store hints.” Or maybe less strictly, “you are allowed to store hints.” This appears to be a logical comparison for most pieces of advice. The downside is that the opposite can, in a few cases, be too “strict.” For example, the opposite of “do not include names” and “don’t repeat characters” are “include names” and “repeat characters,” respectively, both unnatural pieces of advice. Two pieces of advice had ambiguous opposites. The opposite of “write down safely” could either be “don’t write down” or “write down, but not safely.” In this case, we chose to consider the opposite as “don’t write down.” Similarly, we choose the opposite of “alter and reuse passwords” to be that reuse is allowed even without altering. For our purposes, we choose to identify the increase or decrease in the chance of attack by comparing it to the opposite of the specific piece of advice. However, in a real-world situation, a proposed policy could simply be compared in light of the current/previous policy in place. No matter what baseline method is chosen, the discussions provided in our supplementary material [31] should be relevant when assessing benefits.

8 Benefits: Results
Table 7 shows the benefits of implementing each of the 79 advice statements that we collected and the extra “canary” statement that we added in (don’t allow users to paste passwords). In this section, we will discuss the results of this assignment of benefits. First, we highlight an example assignment of benefits for the piece of advice on “Password managers.” Then, we discuss statistics on the types of attacks the advice we collected protects against.
Table 7. Benefits of Implementing Authentication Advice

| Advice to users | Physical Theft | Eavesdropping | Offline Guessing Attacks | Side-Channel Attack | Phishing or Pharming | Social Engineering | Online Guessing | Endpoint Compromise | Unauthorized browsing |
|-----------------|----------------|---------------|-------------------------|--------------------|---------------------|-------------------|----------------|---------------------|-----------------------|
| Backup password options | # sources contradicting | # sources advising | | | | | | | |
| Email up-to-date and secure | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Security answers difficult to guess | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Do not store hints | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Composition | 7 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Must include special characters | 7 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t repeat characters | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Enforce restrictions on characters | 12 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Keep your account safe | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Check web pages for SSL/TLS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Manually type URLs | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t open emails from strangers | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Keep software updated | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Keep anti-virus updated | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Log out of public computers | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Password protect your phone. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Length | 13 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Minimum password length | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Enforce maximum length (<40) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Password managers | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Use a password manager | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Create long random passwords | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Personal Information | 5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t include personal information | 8 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Must not match account details | 6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Do not include names | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Personal password storage | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t leave in plain sight | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t store in a computer file | 6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Write down safely | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Don’t choose “remember me” | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

(continued)
**Table 7. Continued**

| Phrases                                      | Attack Types                          |
|----------------------------------------------|---------------------------------------|
| Don’t use patterns                          |                                       |
| 0                                            | ✶ ✶ ✶ ✶                                |
| Blocklist common passwords                   |                                       |
| 0                                            | ✶ ✶ ✶ ✶                                |
| Take initials of a phrase                    |                                       |
| 0                                            | ✶ ✶ ✶ ✶                                |
| Don’t use published phrases                  |                                       |
| 1                                            | ✶ ✶ ✶ ✶                                |
| Substitute symbols for letters               |                                       |
| 1                                            | ✶ ✶ ✶ ✶                                |
| Don’t use words                              |                                       |
| 0                                            | ✶ ✶ ✶ ✶                                |
| Insert random numbers and symbols            |                                       |
| 1                                            | ✶ ✶ ✶ ✶                                |

**Reuse**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Never reuse a password                        |                                       |
| *5                                            | ✶ ✶ ✶ ✶                                |
| Alter and reuse passwords                     |                                       |
| 3                                              | ✶ ✶ ✶ ✶                                |
| Don’t reuse certain passwords                 |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

**Sharing**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Never share your password                     |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Don’t send passwords by email                  |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Don’t give passwords over phone                |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

**Two factor authentication (2FA)**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Use 2FA using app or special device           |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Use 2FA on phone                              |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Use 2FA for remote accounts                   |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

**Username**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Enforce composition restrictions              |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Don’t reuse username                           |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

**Advice to organisations**

**Administrator accounts**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Not for everyday use                           |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Must have its own password                     |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |
| Should have extra protection                   |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

**Back-up work**

|                                               |                                       |
|------------------------------------------------|---------------------------------------|
| Make digital & physical back-ups.             |                                       |
| 0                                              | ✶ ✶ ✶ ✶                                |

(continued)
### Table 7. Continued

| Default passwords | Attack Types |
|-------------------|-------------|
| Change all default passwords. | 0 4 | |
| Expiry | |
| Store history to eliminate reuse | 0 5 | ⬆ |
| Change your password regularly | 4 8 | ➩ |
| Change if suspect compromise | 0 10 | ➩ |
| Generated passwords | |
| Use random bit generator | *2 2 | ⬇ |
| Must aid memory retention | 0 2 | ⬆ |
| Must be issued immediately | 0 1 | ⬇ |
| Distribute in a sealed envelope | 0 1 | ⬆ |
| Only valid for first login | 0 1 | ⬇ |
| Individual accounts | |
| One account per user | 0 4 | ⬇ |
| Each account password protected | 0 3 | ➩ |
| Input | |
| Don’t perform truncation | 0 1 | ➩ |
| Accept all characters | 1 1 | ➩ |
| Keep system safe | |
| Implement Defense in Depth | 0 2 | ⬇ |
| Implement Technical Defenses | 0 1 | ⬆ |
| Apply access control systems | 0 1 | ⬆ |
| Monitor and analyse intrusions | 0 1 | ⬆ |
| Regularly apply security patches | 0 1 | ⬆ |
| Network: Community strings | |
| Don’t define as standard default | 0 1 | ➩ |
| Different to login password | 0 1 | ➩ |
| Password auditing | |
| Attempt to crack passwords | 0 1 | ➩ |
| Policies | |
| Establish clear policies | 0 2 | |

(continued)
## Table 7. Continued

| # sources contradicting | # sources advising | Attack Types |
|-------------------------|-------------------|--------------|
|                          |                   | Shoulder surfing |
|                          |                   | Offer to display password | 0 | 1 | ↑ |
|                          |                   | Enter your password discreetly | 0 | 2 | ↓ |
|                          |                   | Storage |
|                          |                   | Encrypt password files | 0 | 1 | ↓ |
|                          |                   | Restrict access to password files | 0 | 2 | ↓ |
|                          |                   | Hash and salt passwords | 0 | 4 | ↓ |
|                          |                   | Encrypt passwords | *4 | 7 | ↓ |
|                          |                   | Don’t hardcore passwords | 0 | 1 | ↓ |
|                          |                   | Throttling |
|                          |                   | Throttle password guesses | 0 | 8 | ↓ |
|                          |                   | Transmitting passwords |
|                          |                   | Don’t transmit in cleartext | 0 | 4 | ↓ |
|                          |                   | Request over a protected channel | 0 | 2 | ↓ |

| Underline: advice is impossible to enforce, it must be followed voluntarily or in a certain way. |

### 8.1 Example Allocation of Benefits

Below, we take two advice categories and provide our discussion describing the benefits that were identified for each advice statement in that category. The two categories are password managers and generated passwords. For a discussion of all other advice statements in Table 7, see Reference [31].

#### 8.1.1 Security Benefits of Password Manager Advice

The security benefits of a password manager will depend heavily on both how it is utilised by the user and on the capabilities of the specific software that users are using. For this reason, all benefits are dependent on the implementation. A password manager greatly reduces the users’ memory load and, by extension, a user can then use passwords that are as long, random, and complex as they wish. Thus, this act will increase security. A password manager does mean that the user is relying on an external agent to store their passwords and therefore if this agent is compromised or if the user’s password for this particular account is compromised, then the passwords of all the user’s accounts are compromised. Therefore, we consider this to be a new way in which the users’ passwords can be duplicated. Password managers that automatically fill in the users’ credentials with no user interaction do
have some corner-case vulnerabilities [43]; though, this same paper shows that a password manager can provide more security than the normal manual typing of the password. For example, password managers can be effective against phishing and pharming attacks. One piece of advice related to password managers was “Configure your password manager to create 30–50 random characters with a mixture of upper- and lower-case letters, numbers, and symbols.” This has the same benefits as creating a complex long password but without the user memory costs.

8.1.2 Security Benefits of Generated Passwords Advice. One piece of advice relating to generated passwords was “Must be issued immediately.” This decreases the chance that generated passwords are stolen before they are given to the user. If passwords were created in advance, then they would likely be recorded, as administrators could not remember multiple generated passwords. Therefore, these passwords could be duplicated while in storage. Another piece of generated passwords advice was “Distribute in a sealed envelope.” This advice increases the chance that the password is physically stolen, as the envelope could be taken. The password could also be duplicated, since it has been recorded. If an adversary opens the envelope and duplicates the password, then it will go undiscovered if the adversary places the password page in a new envelope and reseals it. The benefit of the sealed envelope is that an observational, audible, or network eavesdropping attack is less likely. Finally, because generated passwords are often issued and created by administrators, the user has no confidence in the security of their password up until the point they receive it. Maintaining a rule that “passwords must be changed at first login” means that the user can now have complete control over the security of this new password. This advice then protects against previous duplication of the password.

8.2 Benefits of Advice

Overall, we identified 177 positive benefits (decreasing the chance of attack) and 26 negative benefits (increasing the chance of attack). 69% of the negative benefits related to the user advice and 31% of the negative benefits related to the organisation advice. A more even split of 43% to 57%, respectively, exists for the positive benefits.

8.2.1 Ambiguous Advice. We mentioned that an underline, in Table 7 indicated that the advice is not directly enforceable. We find that over half (52%) of the advice we collected was either un-enforceable or too vague. This unenforceable advice was split evenly between the organisation and user advice statements. For example, “Implement defense in depth” can be divided into three categories: physical controls, technical controls, and administrative controls. The security defense in depth can provide depends on exactly what strategies are deployed. They have the potential to mitigate any of the 11 attack types, but without knowing what is implemented, we cannot say exactly what the security advantages or disadvantages are.

8.2.2 Negative Benefits. Observe that, overall, the advice does seem to decrease the chance of compromise (most arrows point down, indicating a decrease in the chance of compromise). This should be unsurprising, as this is, after all, the aim of authentication advice. However, there are some areas where there are increases in the chance of attacks. Eight advice statements have major negative benefits, and six pieces of advice have minor negative benefits. That is, in some areas, these pieces of advice can increase the probability of compromise. The remaining 65 advice statements all show improvements for security.

8.2.3 Frequency of Attack Protection. In the current model framework, it might not always be meaningful to compare the security impact of one piece of advice against another. Take, for example, one piece of advice that decreases the probability of compromise against one attack type, and a piece of advice that decreases the probability of compromise against three attack types. It
is likely that the latter piece of advice is “better,” but in reality, different attacks occur with higher frequency than others and therefore protecting against one attack that occurs regularly might be more effective than protecting against three rare attack types. This leads us to an interesting question on the frequency with which the different types of attacks are successful and whether there is more advice against the more frequent attack types. Phishing, for example, occurs continuously, from targeted spear phishing attacks to mass phishing emails [2]. Whereas side-channel attacks, while they attract interest from researchers, appear to have a small real-world chance of occurring.

Figure 3 shows the number of times an attack was affected by a piece of advice. Green bars show the number of pieces of advice that decrease the chance of this attack occurring. The red-boxed bars show the number of pieces of advice that increase the chance of the given attack occurring. This figure shows that the advice does not equally consider all the attack types. Most of the advice is focused on online guessing and offline guessing. This reflects the quantity of advice that focused on how a password should be created. Eavesdropping is the third most protected against attack type. Eavesdropping refers to both online eavesdroppers, which encrypted communications protect against, and shoulder surfing eavesdroppers who attempt to view a password as it is typed. One interesting insight is that the amount of advice given does not necessarily seem to correspond to the severity or regularity of the attack type. Only 7 pieces of advice protect against phishing or pharming attacks. This is in comparison to the 34 pieces of advice that protect against online guessing. In fact, 6 pieces of advice protect against social engineering and 4 against side-channel attacks. Both of these are less common attacks than phishing. Physical theft had the least amount of advice that helped protect against it and was also the attack that advice most commonly led to increased exposure. This is because advice such as “use 2-factor authentication using a phone” introduces an additional physical object into the authentication procedure and therefore opens up new potential for a physical theft attack.

9 COSTS VERSUS BENEFITS
As we have now reviewed the costs and benefits independently, in this section, we will compare costs versus benefits for each piece of advice that we collected. We use an elementary scoring system that assigns positive scores for each benefit a piece of advice provides and subtracts points
9.1 Scoring Costs

We begin by assigning points to each cost type using an ordinal scale. We assign 2 points to a major cost that reoccurs at each login, 1.5 to a major periodic cost, and 1 to a major one-time cost. A minor login cost is assigned 1, a minor periodic cost 0.75, and a minor one-time cost is 0.5. A positive cost can account for $-2$. Though this is a crude scoring system, it provides insight into both the most costly and least costly advice. Figures 4(a) and 4(b) depict the 12 most costly pieces of advice for the organisation and the end-user.

In Figure 4(a), most of the least costly pieces of advice to the organisation relate to the composition of passwords. For example, “Take initials of a phrase and use this as your password.” Advising this does not bring any costs to the organisation. Many of the most costly pieces of advice for the organisation involve back-end processes; for example, “Implement Defense in Depth,” “Monitor and Analyse intrusions,” and “apply access controls.” Introducing two-factor authentication shows up in both the user and the administrator’s most costly advice. Similarly, the advice to change passwords regularly occurs in both top 12 lists. Whereas, the advice “Don’t choose remember me on your computer” has high costs for users but low costs for the organisation. Most of the most difficult pieces of advice for users relate to password creation, memorising, and changing. For example, “Don’t use dictionary words in your password.” This last piece of advice specifically relates to when regular password changes are enforced. It ensures a user does not choose a previous password. The piece of advice “Don’t use dictionary words in your password” is particularly interesting. The advice was given by 16 different sources, yet we know from leaked password databases that users primarily choose word-based passwords [49]. This depicts how impotent giving advice can be if the costs appear to not outweigh the benefits from a user’s point of view. Shay et al. find that the “use of dictionary words and names are still the most common strategies for creating passwords” [42]. Notice that the last piece of advice in the user chart Figure 4(b) has a negative cost. This is because allowing users to use any ASCII characters actually makes their life easier. Of course, most security policies and rules will come at a cost. What will be interesting is to see whether the benefits outweigh these costs.
“Security beneficial” is a simple indication of whether the advice protects against the different attacks listed in Table 6.

9.2 Scoring Benefits

For benefits, we use a similar ordinal scale: a large decrease in attack risk (⇓) counts for 2 points, a minor decrease to attack risk (↓) is 1 point. A small increase to risk (↑) is −1 point, and a large increase of risk (⇑) is −2 points. Note that a comparison of benefits alone can only provide limited meaning. Some attacks are more important to protect against than others, and advice can protect against attacks to varying degrees. However, for this analysis, a simple comparison of how many attacks a piece of advice protects against and whether it offers minor or major protection could be interesting. We, therefore, attempt a loose ranking of the advice according to the assigned benefits. “Security beneficial” is a simple indication of whether the advice protects against the different attacks from Table 6.

Using the above scoring methodology, Figure 5 shows the 12 most security-beneficial pieces of advice and the 6 least security-beneficial pieces of advice. The advice that this classification identifies as the most beneficial seems to be in line with what we might imagine. Also, notice that there is an overlap between the 12 most beneficial pieces of advice and the 12 pieces of advice that had high organisation costs. For example, “Apply access controls,” “Implement defense in depth,” and “Monitor and analyse intrusions” appear in both lists.

The 6 least beneficial pieces of advice actually result in negative benefits. This means they increase the likelihood of an attack occurring. Looking through the 6 pieces of advice, we can understand why. For three of these advice statements, rather than increasing security, their goal seems to be to create a better user experience. For example, “write [your password] down safely,” “offer to display password,” and “generated passwords must aid memory retention.” The other three pieces of advice have negative benefits, because they create a new attack vector or make an attack more likely. Distributing passwords by envelope means they can be physically intercepted. Enforcing a maximum length puts an upper bound on the length of passwords and makes guessing attacks easier. Finally, though storing backups is an important secure practice, it rarely actually protects against attacks, instead, it mitigates the harm done if an attack takes place. Therefore, purely in terms of protection from attacks, this ranks poorly. In addition, having both physical and digital copies creates extra data that must now be protected, and physical protection is now a factor. This is a good example of how our simple points system does not give the whole picture of whether a security practice should be employed.
9.3 Costs versus Benefits Tradeoff

We are interested in the tradeoffs between the costs and the benefits. Is high-cost advice balanced by high benefits? Or are users paying high usability costs for small increases to security? To analyse costs versus benefits, we plot each piece of advice on a graph. This allows us to visualise how benefits compare to costs. The benefit score is shown on the x-axis, and the cost score is on the y-axis. Advice that falls in the bottom right quadrant (green area) is high-benefit and low-cost advice. Similarly, the advice that falls in the upper left quadrant (red area) is low-benefit and high-cost advice. The worst advice will have low benefits and high costs. Figure 6 shows the results of this plot for a selection of advice.

High-cost and low-benefit advice. Let us look first at the high-cost and low-benefit advice. Reassuringly there is not too much advice in this quadrant. The only piece of advice that falls in the red area is “change your passwords regularly.” This was high-cost advice for both the end-user and the organisation. Research has also shown that regular password changes have few security benefits and that they can do more harm than good [9, 51]. The NIST advice explicitly states that regular password changes should not be enforced [19]. One user in our user study wrote “I hate this! The only solution I’ve come up with is to increment a number in the password each time. So inconvenient and frustrating, especially when combined with other bad password advice.”

The next piece of advice closest to the top left (high-cost and low-benefit) quadrant is the advice “Use SMS or call-based 2-factor authentication.” While we have generally come to accept that two factor authentication (2FA) offers security benefits, SMS text and call-based authentication have security flaws. Text and phone calls are not protected by encryption, and phone numbers can be easily spoofed. In the initial version of the NIST Digital Guidelines, SMS-based two-factor authentication was to be deprecated [18]. However, this decision was overturned [19]. Susceptibility to spoofing explains why this advice receives a lower security ranking than 2FA using an app or specialised device in our plot. However, the low ranking of 2FA in general reflects a limitation of our model. Despite offering major decreases in attack probability in the important areas of phishing and online guessing, 2FA using a phone introduces four new attack vectors: physical...

---

Fig. 6. Scatter plot comparing costs versus benefits for a selection of password advice. The red (upper left) quadrant shows high-cost low-benefit advice. The green (bottom right) quadrant shows low-cost high-benefit advice. The plot and data for all advice are available [31].

2It would be too crowded to show all the advice, as most of it falls in the centre of the graph. However, if the reader is interested, then we have provided the data and the graph in GitHub for a more detailed perusal [31].
Table 8. Evaluating Authentication Advice

| Good advice                                      | Benefits | Costs |
|--------------------------------------------------|----------|-------|
| Apply access control systems                     | 12       | 4     |
| Administrator accounts should have extra protection | 11       | 0.5   |
| Implement technical defenses                     | 11       | 2     |
| Every user in an organisation must have their own account | 10       | 2     |
| Restrict access to password files                | 6        | 1     |
| Don’t perform truncation                         | 6        | 1     |
| Encrypt password files                           | 6        | 1.5   |
| Each user account must be password protected     | 5        | 1.5   |
| Don’t send passwords by email                    | 4        | 0.75  |
| All email must be kept up-to-date and secure     | 4        | 0.75  |
| Accept all ASCII characters                      | 3        | 0     |

| Bad advice                                       | Benefits | Costs |
|--------------------------------------------------|----------|-------|
| Enforce maximum password length (<40)            | –6       | 2     |
| Change your password regularly                   | 2        | 10    |

theft, eavesdropping, side channel attack, and endpoint compromise. Since our model does not have probabilities or more graded weightings, it thinks that these new attack vectors outweigh the benefits. This is only an issue for the 10 pieces of advice that have both positive and negative security impacts, however, it is important to keep in mind.

**Low-cost and low-benefit advice.** In the bottom left quadrant, we can see low-cost and low-benefit advice. Enforcing a maximum password length falls directly into this category. This advice had no positive security value. It is an example of advice that compromises usability for no increase in security. Unfortunately, this practice is still enforced by organisations. In 2014, Saini assessed the policies of 23 different websites and 8 enforced maximum lengths of 40 characters or less on passwords [40]. Three of these limited the length to just 16 characters and one limited it at 12 characters. In the course of our study, we found that some websites only reveal their limit on password length after the user had attempted to use a longer password [33].

**High-benefit advice.** “Administrator accounts should have extra protection,” “Every user in an organisation must have their own account,” and “Implement technical defenses” all fall solidly within the bottom right quadrant. “Apply access control systems” comes at a higher cost but offers the strongest benefits of any advice. All the advice in this quadrant is shown in Table 8 under Good advice. Notice that most of the high-benefit advice is under the control of the organisation and not the end-user. It seems that if an organisation can put proper controls and secure systems in place, then they can ensure a much higher level of security more effectively than placing the burden on the user.

**Some benefit and some cost advice.** The advice in the blue diagonal is more difficult for us to form conclusions about. Anything on the positive x-axis offers security benefits but inevitably comes at a cost. For this advice, a more detailed quantitative analysis would be necessary to determine whether the benefits outweigh the costs.

For example, one expensive piece of advice is “Use 2-factor authentication using an app or special device.” However, it offers increases in security against online guessing and phishing attacks, two of the most common attack types. It is likely that ensuring the benefits outweigh the costs will depend on its implementation and the needs of the specific organisation and users. These nuances are something our current model ca not uncover. Similarly, the piece of advice “Use a Password
manager” lies at \((\text{benefits}=4, \text{costs}=2)\). It was well-regarded by users in our study. It can protect against three attack types, and most of the costs it incurs are to the organisation. A password manager greatly reduces the users’ memory load and by extension, a user can use as long, random, and complex a password as they wish. However, as with many of the pieces of advice, the value of a password manager will lie in how users utilise it. If a user uses a password manager and continues to reuse a common password choice across multiple sites, then many of the potential benefits will not materialise.

In summary, we see that, in many cases, it is difficult to distinguish whether the costs outweigh the benefits of security advice at a glance. Most advice had some negative impact on users or the organisation. This difficulty in assessing the tradeoff could be evidence of one reason why users and organisations often follow advice that researchers have shown ineffective. It seems, an “at a glance” observation, even by a security professional, might not always be possible for many of the pieces of advice we collected. Interestingly, we would have expected the high-benefit advice to correlate with high costs. However, when we plotted a trend line for the full scatter plot of advice, this was not the case. The trend line had a negative slope of \(m = -0.0373\). The fact that the high-cost advice does not map to high benefits implies that the advice we force users and organisations to follow does not necessarily result in positive returns for their effort. Interestingly, if we restrict to organisation costs, then the trend line has a positive slope, while restricting to user costs gives a negative slope. This reinforces our earlier observation that organisational efforts seem to result in a better cost/benefit tradeoff.

10 RESEARCH LIMITATIONS

Using our taxonomy of 270 pieces of authentication advice, we develop a model to determine the costs associated with enforcing and following security advice. We asked 73 end-users and administrators to assign a severity (major, minor, positive) and frequency (one-off, periodic, at login) to each cost category for each piece of advice. Costs could be positive or negative, e.g., advice can reduce the number of resources or time needed. While users and administrators largely agreed that our model was an accurate way of differentiating costs, it made for a convoluted user study. Some participants misunderstood the ranking, in particular the concept of a “positive cost” being one that has a positive impact on their authentication process. We added in clarification part way through and removed three answers where users clearly used “positive cost” to indicate that they were positive there was a cost. If repeating this survey, then we would simplify the general questionnaire and potentially conduct detailed interviews with a smaller cohort of participants where we can learn about the finer details. On the whole, we still received meaningful feedback from our participants.

We defined a crude points system to employ an ordinal scaling to the costs of authentication advice. However, as one administrator in our survey mentioned, the costs experienced differ for each organisation. While the general costs felt might be similar, the extent to which they are felt and the difficulty involved in implementing advice will strongly depend on the ethos, size, sector, or services of the company. Similarly, different end-users may feel different costs to a greater or lesser extent. For example, some people find it easier to memorise letters and numbers than others. While it is useful for us to map perceived costs to an ordinal scale and to generalise costs felt, it is important to note the highly subjective nature of a usability cost. It will always depend on the person and the context.

Once we had identified the costs of the security advice, we sought to qualify what benefits this advice offered. We defined the benefits as the change in security risk. Like costs, benefits can also be positive or negative, i.e., advice can increase or decrease the risk of an attack. We used the NIST 2017 Digital Identity Guidelines list of authenticator threats as our set of possible
attacks. For each attack, we indicated whether each piece of advice increased or decreased the likelihood of the attack occurring. We validated this assignment of security benefits by gathering input from specialists within our university and at specialist conferences [21, 22, 32, 47]. Despite this, this is inherently a subjective assessment based on our knowledge and available research. More sophisticated threat and vulnerability assessment of risk reduction could have provided more concise assessments of security benefits. However, such a detailed qualification comes with its own problems and is beyond the scope of our simple assessment structure.

11 SUMMARY OF RESULTS

The survey highlighted that most of the security advice collected places a large burden on humans, both system administrators and end-users. Humans are impacted by 87% of all the costs identified, and 44% of these were repeating costs, for example, at every login it adds on extra time. In the user survey, we witnessed strong emotional responses towards the advice we asked users to analyse. We received responses such as “I am sick of passwords and logins and they are making me less productive as I have to look up the passwords so often!”

As part of the user survey, we also asked both groups whether they approved of each advice statement or not. Strikingly, we found end-users disagreed with each other 71% of the time about whether a piece of advice was valuable or not. Along with the contradiction in the advice that is circulated by organisations, this shows serious cohesion issues within user education and professionals’ security understanding.

Our analysis of the advice benefits revealed that the majority of the advice focused on defending against online and offline guessing attacks, but less emphasis was placed on phishing, pharming, or keylogging attacks despite their prevalence. Additionally, most of the offline guessing protection strategies emphasised enhancing password strength instead of addressing back-end processes. This highlights the tendency of organisations to shift the security responsibility to the user rather than implementing proper security measures themselves.

We compared the costs to the benefits for each piece of security advice. We identified what advice was most costly to users and found that it was different to the advice that was most costly to the organisation. We also found that the most security-beneficial advice overlapped with the advice that was costly to the organisation. This shows that if organisations are willing to invest in security, then they can implement advice that can result in strong security benefits. The same is not true for user advice.

While we could identify a selection of advice that seemed valuable (high-benefit and low-cost) and one piece of advice that was not worthwhile (low-benefit and high-cost), for the majority of the advice it was unclear whether benefits did outweigh costs. We conclude that quick assessments of whether advice is valuable are not always possible. This is emphasised throughout the article. We found contradictions in the advice websites and organisations circulate and enforce. We found that end-users found it difficult to agree on what advice they approved of. Clearly, it is a difficult challenge for organisations and users to determine the nuances of whether security benefits outweigh the costs of advice. This difficulty in assessing whether security advice is valuable could help explain the incongruity of advice and opinions in the wild.

Finally, we note that our “canary” worked: We included the advice “Don’t allow users to paste passwords” knowing that it had been determined by the security community to have no security value [24]. In our user study, both users and administrators identified it as a piece of advice that they disapprove of (users with slightly more uncertainty). We also could not identify any security benefits.

In supplementary material, we include all our explanations for why particular security benefits were aligned to each piece of advice [31].
benefits for the advice under our attack categories and yet both users and administrators saw it as coming with costs \((\text{benefits}=0, \text{costs}=4.75)\). There was a debate at the time about whether this was good or bad advice; we have shown that we can use a systematic methodology to help us determine whether advice has value rather than relying on instinct.

12 CONCLUSION

In this article, we collected 270 pieces of authentication security advice that were given by security specialists, multinational companies, and public bodies. This collection highlighted stark variations between the advice given by different sources. 41% of the recommendations we collected were contradicted by recommendations given by another source. We surveyed administrators and users about the costs associated with following this advice. The results of this study are tabulated and illustrate the costs and perceptions that accompany password advice. Our research exposed the disconnect that exists between the recommendation of security research and the advice given by organisations and believed by users. Finally, we qualify which attack vectors each piece of advice offered protection against. We find that most advice was concerned with protecting against online and offline guessing attacks, with little emphasis on the security of back-end processes. We also find that some advice that is circulated has no discernible security value and also hinders usability. This research highlights the need for organisations to follow best practice guidelines when giving advice rather than preconceived notions of what should be secure.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. Commun. ACM 42, 12 (1999), 40–46.
[2] APWG. 2018. Phishing Activity Trends Report 1st Quarter 2018. Technical Report. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf.
[3] Simon Arnell, Adam Beaumont, Philip Inglesant, Brian Monahan, David Pym, and Martina Angela Sasse. 2012. Systematic decision making in security management modelling password usage and support. In International Workshop on Quantitative Aspects in Security Assurance. Citeseer.
[4] Adam Beaumont, Martina Angela Sasse, and Mike Wonham. 2009. The compliance budget: Managing security behaviour in organisations. In Workshop on New Security Paradigms. ACM, 47–58.
[5] Christina Braz, Ahmed Seffah, and David M’Raihi. 2007. Designing a trade-off between usability and security: A metrics based-model. In IFIP Conference on Human-Computer Interaction. Springer, 114–126.
[6] Schneier Bruce. 2003. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Springer-Verlag New York, Inc.
[7] Dodson Burr and Polk. 2003. NIST Special Publication 800-63: Electronic Authentication Guidelines. Retrieved from https://csrc.nist.gov/csrc/media/publications/sp/800-63-ver-10/archive/2004-06-30/documents/sp800-63-v1-0.pdf.
[8] Junaid Ahsenali Chaudhry, Shaﬁque Ahmad Chaudhry, and Robert G. Rittenhouse. 2016. Phishing attacks and defenses. Int. J. Secur. Applic. 10, 1 (2016), 247–256.
[9] Sonia Chiasson and Paul C. Van Oorschot. 2015. Quantifying the security advantage of password expiration policies. Des. Codes Cryptogr. 77, 2-3 (2015), 401–408.
[10] Philip Cox. 2016. Password Sanity: Thank You NIST. Retrieved from https://www.linkedin.com/pulse/password-sanity-thank-you-nist-philip-cox.
[11] Lorrie Faith Cranor and Simson Garfinkel. 2005. Security and Usability: Designing Secure Systems that People Can Use. O’Reilly Media Inc.
[12] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The tangled web of password reuse. In Network and Distributed Security Symposium, Vol. 14. 23–26.
[13] Dinei Florêncio and Cormac Herley. 2010. Where do security policies come from? In 6th Symposium on Usable Privacy and Security. ACM, 10.
[14] Dinei Florêncio, Cormac Herley, and Baris Coskun. 2007. Do strong web passwords accomplish anything? HotSec 7, 6 (2007).
[15] Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. 2014. Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In 23rd USENIX Security Symposium. 575–590.
[16] Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. 2016. Pushing on string: The “don’t care” region of password strength. Commun. ACM 59, 11 (2016), 66–74.

ACM Transactions on Privacy and Security, Vol. 26, No. 3, Article 30. Publication date: May 2023.
Costs and Benefits of Authentication Advice 30:35

[44] Juraj Somorovsky, Andreas Mayer, Jörg Schwenk, Marco Kampmann, and Meiko Jensen. 2012. On breaking SAML: Be whoever you want to be. In 21st USENIX Security Symposium. 397–412.

[45] Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2020. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In ACM SIGSAC Computer and Communications Security Conference. 1407–1426.

[46] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. “I added ‘!’ at the end to make it secure”: Observing password creation in the lab. In Symposium On Usable Privacy and Security (SOUPS).

[47] USENIX Security 2017. Poster Session. Retrieved from https://www.usenix.org/conference/usenixsecurity17/poster-session.

[48] Chad Warner. 2010. Passwords with Simple Character Substitution Are Weak. Retrieved from https://optimwise.com/passwords-with-simple-character-substitution-are-weak/.

[49] Matt Weir. 2009. The RockYou 32 Million Password List Top 100. Retrieved from https://reusablesec.blogspot.com/2009/12/rockyou-32-million-password-list-top.html.

[50] XKCD. 2011. Password Strength. Retrieved from https://xkcd.com/936/.

[51] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. 2010. The security of modern password expiration: An algorithmic framework and empirical analysis. In 17th ACM Computer and Communications Security Conference. ACM, 176–186.

[52] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. 2016. Revisiting password rules: Facilitating human management of passwords. In APWG Symposium on Electronic Crime Research (eCrime). IEEE, 1–10.

Received 22 June 2022; revised 13 January 2023; accepted 12 March 2023