Costs - supplementary material

Hazel Murray

December 2021

This document contains a description of the costs associated with each advice category and statement. The costs correspond to those indicated by users and administrators in our user study. For each category, we provide further impressions, characteristics and notable respondent comments.

1 User advice

We begin by discussing the advice associated with users.

For some pieces of advice in this section, administrators were not asked about the costs to an organisation as these costs could largely be extrapolated based on related advice statements.

1.1 Backup password options

Email up-to-date and secure Most organization can not practically check that each user has kept their email up-to-date and secure. For a compliant user, this is a continuous process and will cost the user their time. In the survey users were divided about whether this has no cost or a minor periodic cost. We suspect that for most users their email client will automatically update the email software. However, we do mark it as a minor periodic cost. Administrators also marked this as advice as having no cost. This reinforces the automated nature of email updates which will often be handled by the external email client.

Security answers difficult to guess Making security answers difficult to guess is a challenging task for an organisation. Administrators noted a large number of costs associated with the advice. Most notable is major user education periodically.

In reality, it is unlikely an organization can verify that security answers are difficult to guess. One option could be to employ guessing and require users to change their answers if they have been guessed. But in reality a practice such as this would have its own additional costs and privacy concerns associated with it. Respondent to our user survey indicated that security answers which are difficult to guess will likely be difficult to remember and will also take time for the user to create.

Do not store hints This statement represents two pieces of advice. One of the pieces of advice tells organizations to not allow users to store a hint, and one tells a user to not store a hint. Administrators in our survey were asked "Users should not set password hints on websites" and end-users were asked "Do not store hints about your password". The major cost for users was that their password would be less easy to remember and that it would require extra time or effort. For the organisation the major cost is periodic user education.

One administrator survey respondent noted in the comments that they did not understand the question and the interpretation they provided spoke of password reset practices. We therefore removed their response for this question.

1.2 Composition

In our user survey we asked about the composition advice "Include specific character types in your password. E.g. your password must include uppercase, lowercase, digit, symbol".

Both users and administrators indicated a number of minor costs associated with this advice.

1.3 Keep your account safe

The advice "Check web pages for TLS"and "Manually type URLs" take user time. Users interpreted the check webpages for TLS to be only at login. They marked it as advice they approved of. As with a lot of the advice circulates, this advice would be very difficult for an organisation to enforce. One administrator said "Not sure how to implement this, users often ignore instructions".

User identified no costs with "Don't open emails from strangers". We would have thought it could interfere with daily life or work but a 2012 study by Böhme and Moore found that as a result of concerns over cybercrime 42% of participants say they do not open email from strangers [1].

Both "A user's anti-virus software should be kept up to date " and "All users should keep software updated" require user *additional computing power* and *additional resources*for the users. Respondents to the user study also said that it "required extra time". Though in the case of anti-virus software, respondents disagreed about whether it was a minor or major cost. "Log out of public computers" has a small extra effort cost for users. The focus on administrators is user education.

"Password protect your phone" introduces an increased password memory burden on users. For administrators, there were varying views on whether there was a help desk/user support cost associated with this advice. It likely depends on how much oversight the organisation has. For example, given the user forgets their password, is it the organisation they go to or their personal phone provider?

1.4 Length

Minimum password length This advice has a major affect on the users' *risk of forgetting*. It also *inconveniences the users' password creation* and can mean that a user needs to choose a new password.

Enforce maximum length (<40) This advice *inconveniences the users' personal system for password generation* as a user may wish to choose a longer password. In fact one of the pieces of advice we collected, told the organization to limit the password length to less than 15 characters.

Administrators were not asked directly about the costs to the organisation associated with enforcing a maximum length. The assumption is that it will bear similar costs for an organisation as enforce a minimum length.

1.5 Password managers

Use a password manager A password manager helps a user by remembering their passwords and saves the user the time of typing the password at each site. Users indicated that using a password manager has a positive impact on remembering passwords. Some organizations will be able to force all their users to use a password manger but most organizations will not have this capability. This requires additional resources for the user as the user may need to purchase and/or download and maintain a password manager.

Respondents in the administrator survey indicated that encouraging users to use a password manager would result in a minor increase in help/desk user support time. They marked this as either a once off or periodic cost. We suspect that this relates to support user may need setting up their password manager and they may also need ongoing support.

Organisation requires extra resources if they are supplying the password management software for their employees/users.

Throughout the user studies we saw very positive responses in favour of password managers. One respondent said "Would almost consider it essential for modern Internet usage. Some additional setup and potentially cost, but absolutely worth it". However, others had comments such as "Haven't seriously considered using them before" and "I've never been recommended one or used one".

Create long random passwords when using a password manager One of the advantages of a password manager is that, because a user no longer needs to recall their passwords, the password can be as long and complex as a user wishes. If the password created is different to the users' general structure and is random, the user may never be able to remember it. One administrator mentioned that this "assumes that the user will always have access to their password manager. SaaS on off site work may limit this".[1]

[1] SaaS: Software as a service [2].

1.6 Personal Information

Don't include personal information This is a difficult thing for an organization to enforce. In fact, there is no reasonable way for an organization to eliminate all personal information from passwords. We did not ask administrators about this information as user education is the only method they have for enforcing the advice.

Users identified an *Increased risk of forgetting* as personal details could have made the password more memorable.

Must not match account details Users were asked about the inclusion of both personal information and account details in their passwords in the single statement: "Don't include personal information, account details or names in your password".

Because on organisation can restrict the inclusion of account information in passwords, administrators were also asked about this advice.

1.7 Personal Password Storage

Don't leave in plain sight If the users are internal to the organization and work areas are monitored then it could be possible for an organization to enforce this advice. However in many situations it will be impossible. Administrators saw user education as the only organisation cost for this piece of advice.

If the user follows the advice they have two options. They can memorize the password in which case there is a chance it is forgotten. Or they can store it in a hidden location which will require extra user effort or time to retrieve. Users indicated an *increased risk of forgetting* as the cost associated with this advice.

Don't store your passwords in a computer file Unusually, for this piece of advice, administrators were split between the *help desk/user support time* being either a major cost or non-applicable.

This that marked it as a major cost indicated that it would be periodic. We suspect they are envisioning an increase in help desk call as a result of users forgetting their passwords over time. As a compromise between those who consider it a major cost and those who saw no cost, we mark it as a minor periodic cost and indicate variability.

Administrators were generally not in favour of users storing their passwords in a computer file. However, many people noted that provided the file was encrypted by the user then it was fine.

Write down safely We did not include this in the advice administrators were asked about as they can have little impact on the practice except for user education.

Three out of the seven respondents marked this as having a positive impact on "Makes it less likely to forget". Four said it was non-applicable. Perhaps

because a user could still forge their password but it will save them the inconvenience of a reset when they do as they will simply need to locate the recorded password. We do mark it as a positive cost for forgettability since writing it down means the cost of forgetting won't exist.

Two users disagreed with this advice and 4 agreed. One person was neutral.

Don't choose "remember me" The user will now need to remember their password instead of it being saved in the browser. In addition, at each login the user will need to physically type their password.

1.8 Phrases

There exists a PAM module called 'cracklib' which automates blocklisting [3]. User education is required to explain the risks of choosing a common password and which types of passwords are likely to be common. One administrator made the point that blocklists that are not transparent lead to a lot of user support.

Contrary to the NIST 2017 advice, one administrator responded to this advice by saying "Force the password complexity, then this is not needed".

We did not ask administrators about the advice "Don't use patterns in a password", "Don't use published phrases as your password" and "Substitute symbols for the letters in your password". The first two would come under the remit of a blocklist. The third seems impossible for an organisation to enforce and therefore would only require user education costs.

In the user study, respondents said that "Don't use published phrases" makes password creation more difficult, makes a password less easy to remember, and requires a minor amount of extra time or effort on top of this. When asked how frequently this extra time or effort was required, the prevailing answer was N/A. The next most popular was periodic so this is how we recorded it.

1.9 Reuse

Never reuse a password If users never reuse a password they must create a new password when they open an account.

Password reuse could be within an organization or across organizations. It is very hard to enforce a no reuse policy across organizations. Administrators marked this advice as having a major user education cost.

Alter and reuse passwords Respondents to our user study asked about the affect this advice has on ease of password creation were split between it being a positive and negative cost (See Figure 1). Three users said it was a positive cost, i.e. the advice made it easier to create a password. We suspect this was in relation to needing to create a completely new password at every site which was the previous piece of advice that users were asked about. Antithetically, one user said it was a major cost when creating a password and three users said it was a minor cost. We choose to mark it as a minor cost as more people said major and minor combined than said positive.

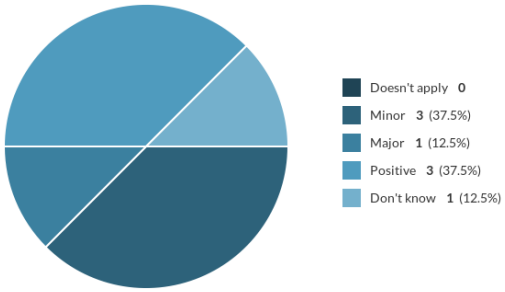

Figure 1: Alter and reuse passwords. Results from user study for the cost category *Makes it more difficult to create a password*

There was similar discrepancy in determining whether the advice *made the password less easy to remember* was positive or negative. In this case the major and minor votes combined equaled positive. Most users typically use the exact same password for multiple websites. Therefore, we see the baseline as keeping all passwords the same, rather than having all random. For this reason, and to keep with the same narrative as above, we mark it as a minor cost.

1.10 Sharing

Sharing All user surveys include the advice "Never share your password" and 36 out of 40 users agrred with it.

User comments did vary though. One user said "This feel obvious and not something a website needs to point out". While other pointed out that exceptions apply and sometimes a system is not capable of dealing with it: "Sometimes it makes sense to share an account with close collaborators or family (if the underlying system doesn't otherwise support collaborative use). Sharing passwords may be a justifiable risk".

1.11 Two-factor authentication

Use multi-factor authentication All users were asked about implementing two factor authentication. The phrasing they were given was: "When you want to log in, you should have to enter an additional code from an app or a special device ".

A subset of these users were also asked specifically about two factor authentication using their phone: "When you want to log in, you should have to enter an additional code that is sent to you by text message (or phone call)".

In both cases users agreed that an extra resource was required at login. Using a specific app or device also incurred an additional time cost.

Administrators were asked about "Users should have to use some form of 2-factor authentication" and "Some form of 2-factor authentication should be available to users". The distinct difference being the option of choice for the

user. There was little difference in the costs to the organisation between the two pieces of advice. Though it is important to note that different groups of administrators answered each question with 6 answering the first version and a different seven answering the second. The major difference was that 5 of 6 (83%) agreed that some form of 2-factor authentication should be available to users, whereas only 4 of 7 (57%) agreed that users should have to use some form of 2 factor authentication. In the Table in the paper we show the costs that administrators related to users *having* to use 2-factor authentication.

One participant gave the strong opinion that 2-factor authentication "should be completely mandatory. Be it a push notification to their phone or some randomly generated OTP or both. Some form of MFA should be used".[2]

If a phone is not used then it is likely that either the user or the organization will have to provide the *additional resource needed* for authentication, for example a USB device.

Setting up 2-factor authentication using texts to phones will also require extra resources for the organisation as they will need the ability to initiate authentication texts or phone calls of app alerts.

Additional user time is needed to complete the authentication process since multiple factors are needed at each login. Some devices do offer a "remember me on this device option" which would ease the burden on the users. But this will have it's own security trade-offs.

If the user is using 'something you have' to authenticate and loses it, this will also have an impact for *user time and inconvenience*. Also, the user must remember to bring the device with them.

Colnago et al. found that [5] implementing two factor authentication (2FA) in their university increased the help desk calls by 10%. In particular, as the deadline for implementation approached, 2FA related tickets represented 24% of all support that was provided by their help desk.

Use for remote accounts The costs for this piece of advice are similar to those for "Use multi-factor authentication". The difference is that the costs only need to apply to remote accounts. In the user study, users were unsure whether this advice *required an additional resource*. This could be because users maybe already have a phone on their person which will simply be used as the second factor. Three respondents said it did not apply, two said it was a minor cost and two said it was major. We therefore mark the severity as minor. Also, respondents were split between the extra user time being needed periodically or at login. Assuming the two factors are required at every login, we mark it as a login cost.

The exact advice statement given in the user study was phrased as: "You should use 2-factor authentication (e.g. an extra PIN) when logging into accounts remotely". Some respondents marked it as *requiring the creation of a new password*. Maybe it was unclear to users whether they had to create this

[2]OTP: One time password [4], MFA: Multi-factor authentication.

additional PIN or not. Because we envision it as being a PIN sent to a device and created automatically, we do not include this cost.

1.12 Username

Enforce restrictions on characters The majority of users in our study assigned no cost to needing to include specific character types in their username. Some said it might require a minor amount of extra time. Interestingly, despite this, 6 respondents said they did not approve of the advice, none said they approved and two were neutral. One participant commented to say it was "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".

2 Organization advice

In this section we discuss advice that was directed towards the organisation. It relates to back-end security such as storage of passwords and other security decisions that the organisation has control over. For some pieces of advice in this section end-users were not consulted about the costs as we deemed them not to be overly relevant to them in terms of costs.

2.1 Administrator Accounts

Not for everyday use The main cost here is to the administrator who must switch between accounts for different tasks. This burden is lessened by the implementation of programs such as su and sudo which allow users to easily run programs which require extra security privileges. The organization must also have the resources to create two accounts for the one user.

Must have its own password This requires the organization to set up password protection on the administrator account. The administrator must create a new password and enter it in some way at each login. Multiple users with privileged access may all need to know the same administrator password. This is the disadvantage of using su protocols over sudo.

Should have extra protection In relation to not using admin accounts for everyday use, one respondent commented that "standard admin accounts are common vectors of attack". Another respondent mentioned using two factor authentication for admin accounts. All administrators agreed with additional security for administrator accounts. The only cost noted was a minor implementation cost. However, the advice does not specify what extra protection are recommended. If it is two factor authentication that is recommended, then this would come with its own costs for the administrator and organisation.

2.2 Backup work

We asked both users and administrators about the costs of needing to digitally and physically backing up work. From a user point of view it was their own work. From an organisation point of view it is the organisation's files and data. For both it requires time and resources. For the organisation there is also a need for user education and help desk support if a back-up policy is in place.

2.3 Default passwords

Change all default passwords This requires changing from default passwords but does not require that each password is unique and they often may be recorded, thus not requiring much additional burden on users. Users marked the only cost as a need to create a new password. Though admittedly, we would see figuring out how to change the default password as another major time cost. Often administrator accounts exist on devices and have associated default passwords that the user of the device may know nothing about.

2.4 Expiry

Store history to eliminate reuse The organization must store all previous passwords, requiring memory. The user will need to pick a new password as old passwords cannot be reused. There is also an *Increased risk of forgetting* as the user may forget which passwords have been expired and which is the current password in use.

Change your password regularly Regularly needing to change passwords have an impact on users' memory load as well as taking time out of their day. Users will repeatedly *need to create a new password*.

Only 50% of the 40 end-users surveyed disagreed with regular password expiry. 25% were neutral and 25% agreed with it. For administrators we have a much smaller number of responses. However, 3 administrator respondents disagreed with expiry, 1 was neutral and 1 agreed.

Change if suspect compromise An organization can internally monitor breaches or link with a breach application. For example receiving notifications about their users' credentials from `https://haveibeenpwned.com` [6]. The notifications to users will require organization time, and user education and support.

All users and administrators agreed with this advice.

2.5 Generated passwords

The assumption by users for most of the advice related to generated passwords is that they will create their own password afterwards. This is evidenced by the inclusion of a costs for the user of creating a new password for most of the

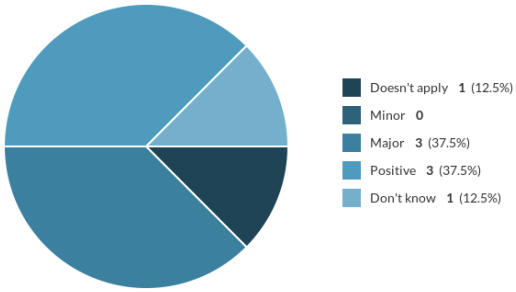

Figure 2: Generated passwords must aid memory retention. Results for cost category *makes it less easy to remember*.

related advice. One user said "Should also be replaced hence the added cost to create."

One issue an administrator flagged with generated passwords is that it is difficult to distribute them safely when off-site.

Must aid memory retention Interestingly, the eight respondents who answered this question were split according to Figure 2. Notice that 3 said it was a major cost and 3 said it was a positive cost. This is interesting as it depends on the interpretation. In comparison to choosing their own password, any generated password will be more difficult to remember. But in terms of a generated password that is randomly generated, it is easier to remember. We mark it as a minor *inconvenience to remembering a password* as the status quo of creating their own password would be easier to remember.

Must be issued immediately Uses users time as the user must be available to receive the newly created password. Takes administrator time to distribute.

2.6 Distributed in a sealed envelope

Respondents to the user survey disagreed with whether this advice *required extra resources*. Two said does not apply, two said minor and two said major. We suspect that though the organization may need the extra resources of envelopes, the end-users shouldn't need any extra resources.

Only valid for first login Requires the user to generate their own password as well as administrators to generate the initial generated password. Most users said it had no costs but some said *requires the creation of a new password*, which we mark in.

2.7 Individual accounts

One account per user This will require organization time to set up. The cost can be high in an environment where there are shared computers. However, in our user study the majority of users assigned no cost to this piece of advice.

Each user account must be password protected User study respondents assigned very few costs to this advice. Three of eight answering the question said that it brought a major cost to *easy memorability* and one respondent said it was a minor cost. This cost was presumably assigned because it requires another pair of account details to be remembered. However, four of the eight respondents marked N/A for it's affect on memorability. Therefore we mark it as a minor variable cost.

Surprisingly, half respondents said that *need to create a new password* was a non-applicable cost. This could be because, even though a new password needs to be set, they don't necessarily need to create a new one as potentially an existing password could be used. However, we mark it as yes as it does require a new password to be set.

For the administrator survey, the only cost marked was for help desk/user support time. The majority of administrators said there was no cost for implementation. We expect this is because it is considered standard on most systems. In fact, one administrators commented to say "I haven't awarded severity/frequency costs because this should be mandatory and the cost is unimportant".

2.8 Input

Don't performed truncation Users often will not notice if their password has been truncated. One administrator gives a reason for truncation as "compatibility with legacy systems". It takes organisation time to be able to implement this advice and also requires extra resources.

Accept all ASCII characters The organization must create a system which has the ability to accept all ASCII characters in a consistent way. Accepting all characters should reduce the likelihood that the policy will inconvenience a user's password choice.

2.9 Keep accounts safe

Implement Defense in Depth Because we do not know what defense in depth strategies would be deployed, it is very difficult for administrators to assess what costs will incur. One administrator said "Its context specific based on the burden of costs associated with it".

Implement Technical Defenses Similar to above, this advice is not specific enough. It shows the importance of describing exactly what systems are intended to be put in place when giving security advice. Some respondents suggested technical defence that should be in place. For example, "..MFA should be mandatory, any company resources should have to be accessed over a VPN and the access policy on that VPN should have you running some sort of company approved anti-virus". Others said that it is "not specific or meaningful enough to be useful advice".

Apply access control systems This advice was worded for administrators as: access controls should be applied to access particular features or systems. One respondent commented to say that the advice statement was not clear. There was disparity in responses about the cost to organisation time for implementing these access controls. Two said that implementation costs were non-applicable, 1 said minor, 1 positive, and 2 major. We marked it as major as we believe implementing a fully access controlled system will take time for an organisation. However we mark it as having variability in the responses. All except those that marked it as non-applicable indicated that it is a periodic cost.

Access control can cause problems for end-users. One user survey respondent noted that "The problem is that someone has to decide which parts of the system are relevant for everyone else, and it's easy to err on the 'safe' side, which can create lots of friction."

Intrusions should be monitored and analysed One respondent mentions that in order to follow this advice it is "Assuming you know the attack vector". This could mean working with users of the system and also engaging in user education so that users can recognise compromises. Computing power is also important for identifying and monitoring and analysing breaches. It is a major organisation cost to implement.

Regularly apply security patches In order for security patches to be applied across an organisation, users must be compliant. Administrators assigned *user education* and *user support time* to this advice. Administrator survey respondents also mentioned the difficultly of this task. One said that it "requires a lot of additional management to be done properly and audited." Another respondent mentioned that some patches can break existing functionality and a third emphasised that it is a big but necessary job.

2.10 Network: SNMP community strings

An SNMP community strings can be compared to a username or password, knowing the string provides access to a device's statistics.

As one respondent pointed out, community strings are only used in devices supporting the SNMPv1 and SNMPv2c protocols. The newer SNMPv3 uses an

encryption key along with a username and password for authentication.

2.11 Password auditing

Attempt to crack passwords Both administrators and end-users were asked about this advice. There are a large number of costs for both users and administrators. One administrator commented to say "Don't let it run forever or using spare cycles on your nearby supercomputer or you'll start cracking relatively strong passwords too!".

2.12 Establish clear policies

The exact wording of this question for administrators was: "Clear policies should be established (e.g what passwords will be accepted or security advice for use of IT systems)". Users were not asked about this advice.

An administrator commented to say "Most questions of info sec come down to good user education, good policy and effective "policing" (and that does not necessarily mean punishment for non compliance)".

2.13 Shoulder surfing

Offer to display password Administrators were asked "When logging in there should be an option to view a password after it is typed". Users were asked "You should have an option to view your password after you have typed it".

Users saw no costs for them regarding this advice. One user commented to say "There's a trade-off to be made. Context matters. If you're in a public space, it is riskier. If you're at home or otherwise alone, it can be helpful. Suitable for low security applications (meme generator account?). Not suitable for high security applications (bank?)."

Enter your password discretely Administrators were not asked about this advice as all they can so is provide user education. One user said "Absolutely! All password boxes should be starred or invisible to type".

When a user is logging in it may take some *extra time or inconvenience* for them to verify that they are entering their password discretely. Users also marked it as impacting the *ease of creating their password.*

2.14 Storage

Encrypt password files For the organization, at each system start up the password needs to be provided. This can be done manually, which would require periodic organization time. Or it could be automated in which case the password is accessible to the computer system, which would bear security risks, by reducing the effective secrecy provided by the encryption. One administrator

noted that "It's common practice to ensure password files are encrypted.. To me this is a no brainer".

Access to password files should be restricted Administrators disagreed about whether *help desk support* and *user education* was necessary for this piece of advice. For both, half the administrators said non-applicable, while the other half were split between it being a minor and major cost. We mark it as a minor cost.

One administrator commented to say that "It is dependent on the type of organisation". We would be curious to know which organisations would prefer to not have access controls in place for their password files.

Hash and salt passwords In the authentication advice we collected we found four pieces of advice recommending storing passwords as hashes. However, of these, only two also recommended including a salt. Because a hashed password should always be salted, we asked administrators about hashing and salting together.

Administrator said it would require extra resources, organisation computing power and time to implement. We did not ask users about this advice as many would not be familiar with the terms. However, we do know that if the hash of the password is stored, then if the user forgets their password, the password cannot be recovered from the hash. Therefore, the user will need to create a new password.

Encrypt passwords One respondent said "Usually you would hash, but encryption can be used too". Another mentioned the "Minor cost to help desk, as passwords cannot be retrieved, only reset. Could be offset with self-service reset, at additional overhead cost". Another respondent said "Assume by encrypted you mean hashed".

Passwords should not be hardcoded One respondent did not understand the question. They commented to ask if this meant using certificates instead of passwords or MFA only. We removed this response as we believe the hard-coding is referring to the storage of the password on the organisation's system.

Another administrator gave the comment "Users should be allowed set their own password. Orgs should not keep lists of unencrypted passwords that have been hardcoded". This is more in line with our interpretation of the advice.

2.15 Throttling

Throttle password guesses Throttling involves limiting the number of wrong guesses that can be made against an account. The cost of this is that a legitimate user could accidentally be locked out if they mistype or forget their password a certain number of times. For example, Brostoff and Sasse [7] find that with a three strike system 31% of users are unfairly locked out is. With ten strikes

it is 7%. Smart systems can help to minimize the risk for real users [8]. Users noted that this has a cost associated with time and effort and forgetting.

One user said "means you want to be extra sure of your password, either having it linked to the site/service or else stored somewhere that you can be sure of getting it correct". Another said "Depends on the value of what is being protected and there are better ways of providing extra security".

All administrators agreed with this advice (7/7) whereas users were less sure. One user said they disagreed and one was neutral. Four (4/7) users did agree with the advice.

One administrator emphasised the need to "let the user know that this can happen, to reduce confusion". Another administrator respondent mentioned that depending on the system in use, setting up throttling can range from a very simple 'tick box' task to a complete system overhaul.

2.16 Transmitting passwords

Different subsets of administrators were asked about "Don't transmit in cleartext" and "Request over a protected channel". Users were not asked about this advice.

The costs administrators noted for the two are very similar. Except for the transmission of passwords which involved *increased computing power* as well.

Both involve user education and help desk time. This is to ensure users or employees are not sending and asking for passwords using unencrypted means.

One administrator said "Passwords should not be transmitted in clear text - having a policy that states that is one thing (with little cost), educating the userbase to the risks of not adhering to the policy is more involved from a cost perspective and technically policing the policy can be quite expensive. So in effect you can have a range of answers here. I agree with going all the way to the technical policing (systems in place to discover clear text passwords)". Another said that mandating that passwords should be requested over protected channels is "Good in theory, in practise my experience is that users start to work around it".

2.17 Additional advice

Don't allow users to paste passwords Administrators and users disagreed with this advice. One administrators said: "Terrible idea. Increased help desk costs and user frustration. Makes it impossible to use password managers".

One user said "This is horrendous advice that leads to problems using password managers. It encourages using crappy passwords." But some 14/31 agreed with not allowing passwords to be pasted. One user said: "auto-fill is okay, paste is not".

References

[1] R. Böhme and T. Moore, "How do consumers react to cybercrime?," in *2012 eCrime researchers summit*, pp. 1–12, IEEE, 2012.

[2] "Software as a service (SaaS)." `https://en.wikipedia.org/wiki/Software_as_a_service`.

[3] A. Muffet, "Cracklib: a proactive password sanity library," *Dec*, vol. 14, pp. 1–5, 1997.

[4] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: time-based one-time password algorithm." `https://tools.ietf.org/html/rfc6238`, 2011.

[5] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, ""it's not actually that horrible" exploring adoption of two-factor authentication at a university," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–11, 2018.

[6] T. Hunt, "Have I Been Pwned." `https://haveibeenpwned.com/`.

[7] S. Brostoff and M. A. Sasse, ""Ten strikes and you're out": Increasing the number of login attempts can improve password usability," *Presented at: CHI 2003 Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale, Florida.*, 2003.

[8] H. Lockhart, D. Nicholas, and S. Roberts, "Demystifying password hash sync." `https://www.microsoft.com/security/blog/2019/05/30/demystifying-password-hash-sync/`, 2019.