The Scottish Parliament
Pàrlamaid na h-Alba

IT Security Update – Password Policy Changes
4 March 2021
Reference: SPCB(2021)Paper 16

Executive summary

1. This paper seeks SPCB endorsement of a proposed change to the password policy applicable to all users of the Parliament network.

2. A brief oral update will also be provided at the meeting on the current cyber threat landscape.

Issues and options

3. IT Industry experts such as Bill Gates predicted the death of the password around 15 years ago. Many assumed that alternative authentication methods would be adopted to control access to applications, services, data and IT infrastructure. In fact, over the years, password use has risen, and they remain the default method of authentication for a huge range of services that we all use, both at work and home.

4. The increase in password use is mostly due to the surge of online services, such as social media, home banking, online shopping, but also including those provided by government and the wider public sector. The growth in online services has also seen a massive growth in use of personal computers, smartphones and tablets both in the business and home settings thus introducing even more accounts and passwords which have to be managed.

5. Passwords are often seen as an easily-implemented, low-cost security measure as they do not require special hardware, with obvious attractions for online service provides and IT managers within enterprise systems. However, this proliferation of password use, and increasingly complex password requirements, places an unrealistic demand on users. Inevitably, users will devise their own coping mechanisms to cope with ‘password overload’. This includes re-using the same password across different systems, using simple and predictable password creation strategies, or writing passwords down where they can be easily found. Attackers exploit these well-known coping strategies, leaving people and organisation vulnerable.

6. At the start of the Covid Pandemic Lockdown in March 2020, it became clear that working from home with limited access to the Holyrood building would become the predominant way of working for the foreseeable future. At this point, BIT reviewed our remote working procedures and systems including our password policy, to see how we could best support homeworking.

7. At this point it was decided to pause the password expiry policy in operation for network accounts to ensure that remote users were not forced to change their passwords when operating remotely. The main reason for this was to try and reduce the possibility of account lockout during the password changing process whilst the IT helpdesk service was largely only contactable through voicemail and email. It was agreed that BIT would review the position before the end of 2020 or when the majority of SPCB staff, Members and their staff had returned to working at Holyrood and in Local Offices.

8. In making the decision to pause password expiry, it was recognised that there are several other technical mitigations in place to protect user accounts. The most important mitigation is multifactor authentication where the security of username and passwords is enhanced with another layer typically involving a code being sent to a predefined mobile number as a text message. Other mitigations in place include account locking where if the password is entered incorrectly several times then the account is locked out from trying again. During the pandemic we have also increased our monitoring capability.

9. Having undertaken a review of the current change to password policy, BIT have decided to continue with no automatic password expiry until the end of the session. This does not prevent individual users from changing their password at any time, however it does mean that they will not be automatically forced to change their passwords regular. BIT will continue to force a password change where there is evidence of a successful phishing attack where account credentials may have been compromised.

10. Looking forward, there are three permanent changes to network account password policy that will be introduced in session 6. The first is that we will remove password expiry permanently so that passwords never expire automatically. We will also increase the minimum password length (moving from 8 characters to 10 characters) and at the same time remove some of the required complexity (password currently must contain two of the following – a number, a capital letter, a special character). Finally we will utilise software to prevent the use of common (and therefore easily guessed) passwords.

    SPCB is asked to endorse the proposed changes to password policy which will come in to effect from the start of Session 6.

Governance

11. Although largely an operational matter, the proposed changes to password policy, if endorsed by SPCB, will apply to all users of the Parliament network and help safeguard against the risk of unauthorised access to our systems and data and cyberattack. The changes follow password good practice as recommended by the National Cyber Security Centre.

Resource implications

12. The resources required to make the technical changes to deliver the changes in password policy, are already in place and the work will be planned as part of normal operational duties for the BIT Office and become part of the account creation process.

Publication Scheme

13. This paper can be published.

Decision

14. SPCB is asked to endorse the proposed changes in password policy for Parliament network users.

Business IT Office
February 2021