Solgrid

The Solihull grid for learning

System security update – July 2019

There has been an increasing number of technology-related security issues reported in the media in the last few months. We have also seen more issues locally in schools than we have before. This update looks at what Solihull Council is doing for schools we support and what other schools should consider.

Threats

Ransomware attacks continue to be an issue, including schools and universities in the UK. Recently, one UK school lost GCSE coursework when a member of staff mistakenly opened an email containing ransomware.

Phishing attacks have heightened recently, leading to financial losses in some schools in the UK. The Education and Skills Funding Agency has guidance about particular threats and mitigating actions schools can take. [See **https://www.gov.uk/government/publications/esfa-update-26-june-2019/esfa-update-local-authorities-26-june-2019**.]

Email account hijacking has increased – we have seen a number of Solgrid accounts for school staff hijacked and we are aware that there are similar issues in schools that use other IT service providers. These attacks are harder to address with technology as they exploit weaknesses in user behaviours.

We have had an issue where a username and password to a school remote access system was offered for sale on a criminal forum. With those details, the system could have been accessed as it only relied on the username and password.

Our response and guidance

Schools need robust processes in place to protect themselves, such as firewalls, antivirus software and strong passwords.

- Solgrid schools already have industry-standard protection systems that are constantly updated and improved in response to emergent threats. We are proposing to enforce stronger passwords for school staff with regular changes in schools where we manage their networks. This minimum action will mitigate **some** of the risks.

The **National Cyber Security Centre** has issued guidance on passwords – see **https://www.ncsc.gov.uk/collection/passwords**.

Using multifactor authentication

The National Cyber Security Centre has also issued advice that people should use multi-factor authentication (MFA) for online services – both at work and at home. See **https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services**.

MFA strengthens access to online systems by requiring additional checks alongside a username and password. Typically, this double-checking can be done with a confirmation text message to the user's mobile phone, generated on an app on the user's smartphone or a with a small, dedicated, hardware token that the user carries. It is also possible to be automatically telephoned by the service to a known, secure, telephone number which is then confirmed.

A recent survey showed that around a quarter of secondary schools already use MFA for school staff. MFA is becoming used more widely and is becoming cheaper to implement. We think all schools should seriously consider adopting MFA for all staff. This will help mitigate many of the current risks that schools face..

- **We already have MFA** in place for all school staff that have remote access to school systems where they have their school networks supported by education ICT services.
- **We are proposing to offer MFA *as an option*** to all schools that directly use Solihull Council for Microsoft Office 365. We will give schools several choices about how this is done, allowing them to balance current working practices, staff goodwill, flexibility and cost.
- We will **offer MFA to school governors** (where they use Solgrid for Office 365) and also make it easier for them to change their passwords.

User education

We will continue providing school staff with guidance about safe working practices.

Getting more information

Name	**David Butt**
Email	**dbutt@solihull.gov.uk**
Telephone	**0121 704 6407**

Version control

Version	Date	Owner	Notes
V01b	11/07/2019	DB	Agreed version for *Head Lines*.

This document is consciously designed in black and white – to reduce printing costs.