Cyber News

April 2018

WORKING TOGETHER TO PROTECT OUR NETWORK

Welcome…

As our use and reliance on computers, emails and the internet increases so does the risk of cyber-crime.

Protecting our systems, equipment and patient information is critical which is why Nottingham CityCare Partnership, Sherwood Forest Hospitals, Mansfield and Ashfield, Newark and Sherwood, Nottingham North and East, Nottingham West, City and Rushcliffe CCGs and Nottinghamshire Health Informatics Service have formed a Cyber Security Assurance Programme. Together they are working to continually improve cyber security collectively across the local health community.

This newsletter, which will be published every two months, has been created to keep you up to date with the work being carried out.

Fighting against healthcare hackers

Hackers are targeting healthcare organisations globally. Just a few weeks ago an American hospital paid a $55,000 ransom to cyber criminals to regain control of their computer system and just days later, a US electronic health records company also suffered a ransomware attack. In January, Norway's largest health authority came under an advanced and persistent cyber-attack in what appears to have been a targeted attempt to access patient data.

As a health community we saw first-hand the disruption a cyber-attack causes, during the WannaCry virus in May 2017. That isn't the only attack made to our network. Locally our network is under daily attack from hackers in Russia, Ukraine and Asia but our security measures such as firewalls stop these attacks from accessing our networks.

> Our network is under daily attack from hackers in Russia, Ukraine and Asia

Cyber-criminals are constantly releasing new bugs and exploiting newly found vulnerabilities.

IT vendors release security updates to protect against these on a regular basis, for example Microsoft release their updates on the second Tuesday of every month. The Nottinghamshire Health Informatics Service (NHIS) receives these updates, tests them and then pushes the updates out across our network. Users must reboot their Windows based PC, laptop or tablet to ensure these critical updates are applied otherwise the device will automatically reboot after

seven days. To offer the highest level of protection across the local health community and reduce the risk of hacking it is vital all devices have the latest security updates applied to them.

All PCs and laptops used by Nottinghamshire GPs and CCGs, Sherwood Forest Hospitals and Nottingham CityCare have sophisticated anti-malware protection. The Sophos Endpoint protection proactively blocks malware (computer viruses, worms, trojans and spyware). It identifies and blocks known dangerous websites, apps, malicious code and malware as well as those that are not yet known to vendors or antivirus companies.

These are further supported by third-party vulnerability scanners which have been purchased by NHIS as part of their proactive cyber strategy. These independent scanners are used to discover any weak points across the network, allowing them to be strengthened.

New vulnerabilities are being discovered and published daily, so work to protect our systems and data will never be complete, but, by working together across the local health community we can reduce the risk posed by cyber-criminals.

> To reduce the risk of hacking it is vital all devices have the latest security updates applied to them.

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Cyber Security

The protection of devices, services and networks—and the information on them—from theft or damage.

Patching

Applying updates to firmware or software to improve security and/ or enhance functionality.

ISO and Cyber Essentials

Like all reputable IT organisations, the Nottinghamshire Health Informatics Service (NHIS) has both Cyber Essentials and ISO 27001:2013 certifications.

Cyber Essentials is managed by the Government's National Centre for Cyber Security. It focuses on controls that are needed to ensure an organisation is confident it's protecting its systems adequately.

ISO 27001:2013 is an internationally recognised certification which demonstrates an organisation keeps their information assets secure.

NHIS obtained the internationally recognised ISO 27001:2013 certification in March 2017. The certificate lasts for three years and is subject to an annual re-audit, which is taking place in April 2018. The standard supports an information security management system which is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

Cyber security is only as strong as the weakest link in the chain

Everyone plays an important part in protecting our IT systems and networks

Acceptable use of the Network

At times it is necessary for third parties to connect to our network, this can range from suppliers of clinical systems and patient call in screens to contractors .

To ensure that vulnerabilities are not introduced onto the network from external sources a procedure has been developed which check the security profiles of external organisations.

The Third Party Connection Agreement and the Acceptable use of the Network document have been approved by the Cyber Security Assurance Programme Board and have been shared for use by all NHIS supported organisations.

To access these documents please contact your organisation's Information Governance lead.

Deactivating Devices

To ensure all Windows based devices meet our minimum security standard, any device that hasn't connected to our network for at least 90 days will be deactivated.

This has been introduced as NHIS cannot confirm that essential security updates have been applied, therefore the device may be vulnerable to a cyber-attack and pose a risk to the entire network.

The WannaCry ransomware attack which happened in May 2017 exploited vulnerabilities and used a 'computer worm' to spread the virus quickly to other devices within that network.

If your device is deactivated you will not be able to log onto and use the device. You will need to contact the NHIS Service Desk (Mitel ext. 4040 or 01623 410310) to have the latest patches and anti-virus updates installed on the device before it can be reactivated.

To prevent your device from being deactivated it is recommended any Windows based PC, laptop or tablet is connected to the network for at least one hour every month to ensure it receives all the necessary security updates.

Removing Risks of Removable Media Devices

Over 584 unencrypted removable media devices connected to our network nearly 35,500 times over a three month period.

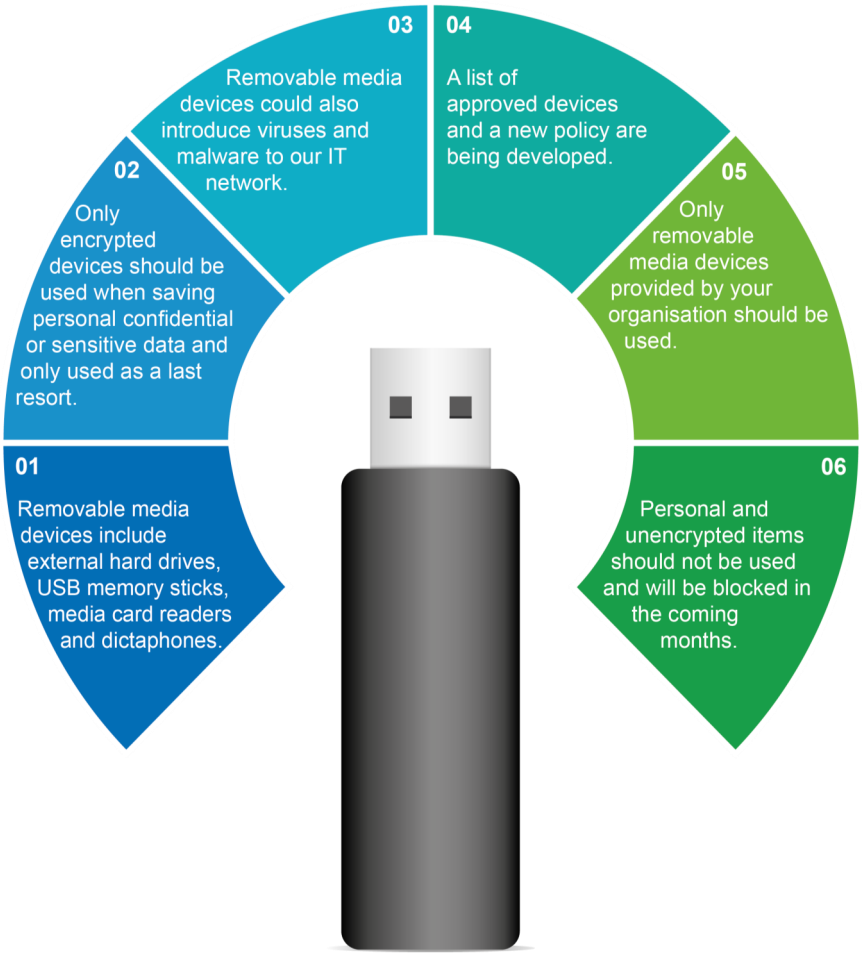
This high number of devices could pose IG and cyber risks. Data saved on unencrypted removable media devices could easily be accessed if the device was lost or stolen. Items such as USB sticks could also pose a cyber risk by potentially introducing viruses and malware to our network.

Members of the Cyber Security Assurance Project Group are working together to produce a new common policy that will be introduced across all CCGs, Nottingham CityCare Partnerships and Sherwood Forest Hospitals.

> Any removable media device not included on the list of approved devices

A list of devices that are allowed to connect to the network is also being agreed by the group. Each organisation will be reviewing the devices used and contacting users where necessary to understand if certain devices should be approved for business use. Any device not on this list will be blocked.

Further information will be shared over the coming weeks.



Cyber Security Assurance Project Group Members

CityCare - Mark Parry

Mid Notts CCGs - Ruth Lloyd

Greater Nottingham CCGs - Loretta Bradley

Sherwood Forest Hospitals - Mark Stone and Jacquie Widdowson

NHIS - Technical - James Berresford and Paul Richards

Project Management - Nigel Callahan and Martin Tooth

Business Relations - Stephen McCormick

Governance - Debbie Poznanski

Communications - Sophie Wragg

Produced by the Nottinghamshire Health Informatics Service on behalf of the Cyber Security Assurance Programme.

NHIS.Communications@notts-his.nhs.uk