Cyber News

WORKING TOGETHER TO PROTECT OUR NETWORK

Introducing the Cyber Security Team

Our dedicated Cyber Security team brings together over 66 years of experience across different technical disciplines offering the best service to our users.

The Cyber Security team comprises of James Kay, Peter Fryer and Cyber Security Manager, Paul Richards.

James has worked on our Service Desk where he was the first point of contact for users and worked to resolve problems and fix any issues remotely.

Peter Fryer is an experienced service engineer who has supported Sherwood Forest Hospitals staff for many years and Paul Richards has worked in and then managed the team who maintain the Datacentres.

L-R Peter Fryer, James Kay and Paul Richards

The team work to prevent cyber-attacks and ensure security standards are monitored and maintained. They analyse cyber threats to determine the action required, implement improvements and work with other organisations to share best practice. Cyber threats are constantly evolving as cyber-criminals release new bugs and exploit new vulnerabilities, so the team are essential for ensuring our defences are constantly updated.

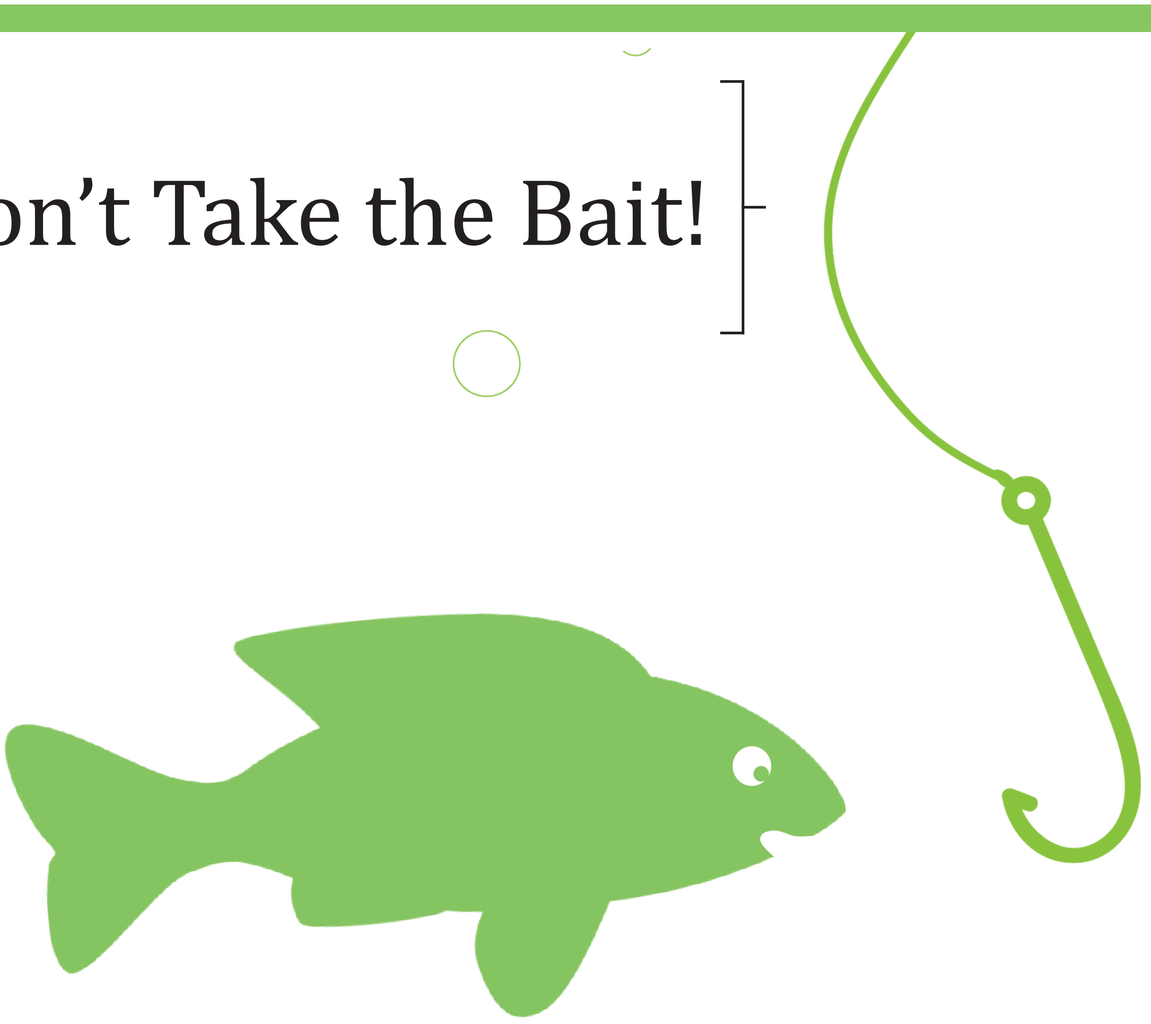
The team use tools which continually scan our networks. When the team see a threat they work quickly to close it. The main way malware enters our network is through users clicking links in spam emails that have slipped through the spam filters.

Paul Richards, Cyber Security Manager, offers the following advice: “Attackers are now mimicking accounts to make it look like their email is coming from a colleague or a trusted external organisation, such as HMRC.

“If you are unsure whether an email is genuine, hover over the sender’s details and any links in the email, they should match what you are expecting.

“If you are still unsure, do not open any attachments or click any links and report it to the Service Desk. If you do click on a link and then become suspicious, report it to the Service Desk straight away so that it can be investigated.”

Don’t Take the Bait!



We all know spam emails are annoying, but they can also be very dangerous.

Cyber criminals use spam emails for widespread phishing campaigns to spread malicious viruses or collect sensitive information.

The attacker wants to trick you into sharing sensitive information or download viruses to stage a cyber-attack.

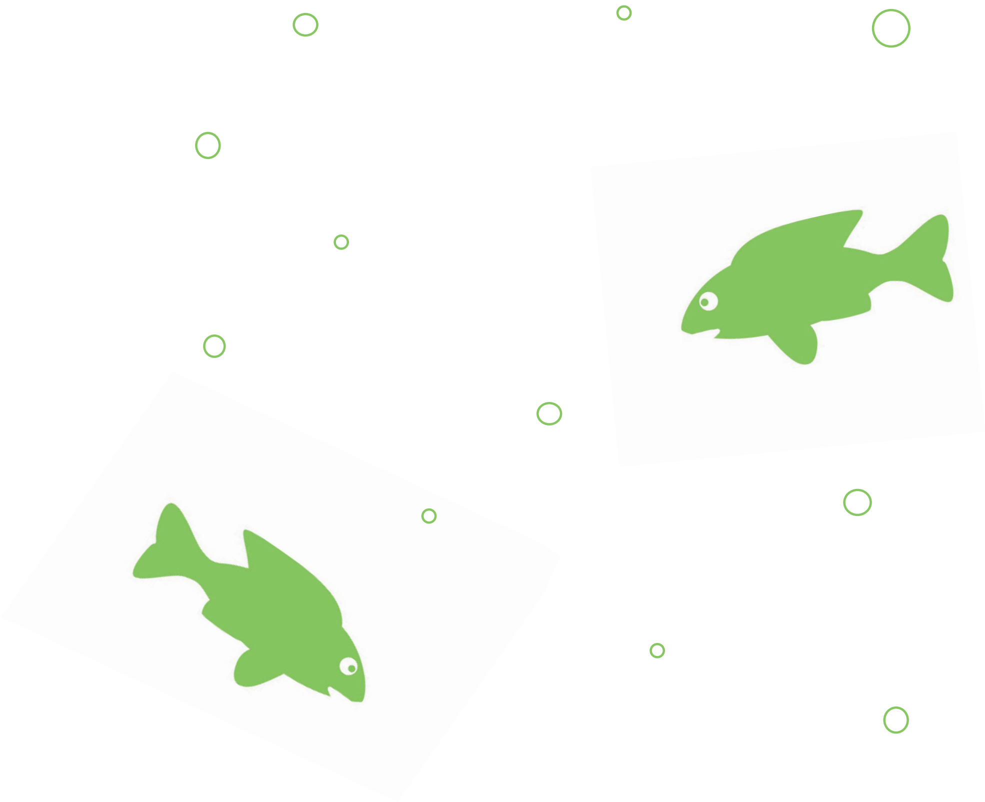
Phishing can be quite easy to spot. As people have become wary of emails promising to transfer millions of dollars into their accounts when they share their financial data, attackers are now using spear-phishing tactics more frequently.

Spear-phishing is more sophisticated and harder to spot. The email is targeted at you and may be designed to look like it’s coming from your own organisation or a company you use. The email might be something you would expect to receive, for instance an outstanding invoice, parcel delivery, a supplier meeting or a software licence and the emails are often sent during work hours to add authenticity.

Spear phishers may use an urgent deadline in the email to capture our attention and encourage you to respond.

The attacker wants to trick you into sharing sensitive information or download viruses to stage a cyber-attack.

There are a number of simple steps listed on the next page which you can take to avoid taking the bait and becoming a cyber criminal’s latest victim.



What can you do?

✓ **Think before you click.**
Were you expecting this email? Take the time to pause before responding.

✓ **Verify the communication is genuine without replying.**
If an email comes from a colleague but doesn't sound like them and isn't formatted in the way they would write – be suspicious. Call your colleague or email them directly to check or validate the details.

✓ **Check with a colleague – seek advice.**
If you are unsure use your mouse to hover over any links to check that it matches the URL (web address) that you were expecting. Check the 'reply to' email and address, does it match the 'from' address?

✓ **Don't panic if you do click and then become suspicious.**
Report it to spamreports@nhs.net. If you think your computer has become infected with a virus, unplug the network cable, turn off your Wi-Fi or power down your computer and immediately report the suspected infection to the NHIS Service Desk on extension 4040.

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Report any stolen IT equipment to the police and the NHIS Service Desk immediately.

The device's account will then be deleted to prevent any unauthorised access to the network. Any person who has used the device will be strongly advised to change their passwords.

Blocking Unencrypted Storage Devices

On the third of September 2018 unencrypted USB removable storage devices began to be blocked across our networks.

Blocking is being activated by organisation, on around 50-100 PCs and laptops per day. It is anticipated that all organisations will have blocking fully applied by early November.

A small number of unencrypted USB removable media devices will continue to be allowed on the network, this process is called 'whitelisting'. Whitelisted devices are those whereby an encrypted alternative is currently unavailable e.g. cameras, SD cards, clinical equipment. For a device to be added to the whitelist it must be approved by both the NHIS Cyber Security team and the Information Governance lead for the requesting organisation.

> Over the next few months encrypted USB removable media devices will be reviewed.

Encrypted USB removable media devices will remain unblocked; however, it is the intention over the coming months to risk assess these devices, along with devices that connect to PC's and laptops via Bluetooth and Wi-Fi. It is therefore important that any new devices that will connect to the network are approved prior to purchase as they may not be accessible via a corporate device.

For any queries in relation to USB removable media blocking please email sfh-tr.media.requests@nhs.net.

Filtering out Danger

To tighten network security web filtering will soon be expanded to cover all GP practices and the existing web filters used will be updated and aligned to one common approach across all NHIS supported organisations.

Web filtering plays an important role in protecting our network by categorising web sites and blocking access to those deemed high risk such as those associated with spam URLs, hacking, phishing and fraud. The filter also makes the web appropriate for business use by blocking any material considered to be illegal, racist, homophobic, immoral, offensive, obscene or pornographic.

Previously web filtering could not be applied to GP practices due to their native N3 connections. With the implementation of the new Community of Interest Network (CoIN) web filters can now be deployed to GP practices.

A full list of the categories of websites that will be allowed or available on a warn or quota basis is available in the Knowledge Base of the Customer Portal.

What is a web filter?

A web filter is a program that screens a web page to determine whether it should be displayed to the user.

Our cyber security provider Sophos reviews every website and categorises them. If a website is found to pose a high risk to the network it will be blocked, some less dangerous sites will warn you prior to accessing the site.

Security Clearance

As you will be aware, a joint Cyber Security Assurance Programme has been established by Nottinghamshire Health Informatics Service (NHIS), Mid-Notts CCGs, Greater Notts CCGs, Nottingham CityCare and Sherwood Forest Hospitals.

The focus of the programme is to further secure our networks, reducing the risk of the impact of a successful cyber-attack and ensuring that NHS patient data and systems are not compromised.

Globally there is an increasing cyber threat and it is critical that we work together to continue to monitor, review and implement additional security to protect our networks and information.

There is a programme of work underway to ensure that any third parties or suppliers that are connecting devices to the network (whether temporary or permanent) have provided the purchasing organisation and NHIS with the right security accreditations to add their devices to the network. This means that any device that is connecting to the network will need to be approved by NHIS before being installed on the network. Please ensure that you speak to someone in the NHIS Business Relationships Team before you purchase or install any equipment that has not been obtained through NHIS.

If you require further advice, please contact the NHIS Business Relationship Team at business.relationships@notts-his.nhs.uk or your NHIS account manager.

Beware of Freeware

Very rarely in life do you get something for free, there is usually a motive behind it and freeware is a prime example of this.

On the 30 August 2018 NHS Digital issued a Cyber Security Threat Notification after identifying suspicious activity on a computer on our network. The threat, which could easily have been avoided, took the Cyber Security team nearly 12 hours to resolve.

It all started so innocently…

Staff within the practice were downloading health videos from YouTube to display on their patient screens. The videos needed to be converted to MP4 files before they could be added to the screens, as they didn't have the software to do this, they searched the internet for something that could do this for them.

Choose wisely…

Unfortunately, this is where the problem which triggered the security threat notification began.

The internet search found an array of options many of which were free software.

Whilst free software, also known as freeware, can come from reputable sources, some freeware contains malware such as viruses, adware and spyware which can pose a significant security threat.

The freeware which was downloaded and used to convert the YouTube videos contained adware. This started to display pop up adverts which became increasingly offensive and replaced the browser homepage on the computers with another which contained links to high risk websites.

The clean-up operation…

Once the cyber threat notification was issued the NHIS Cyber Security Team contacted the user to gain a full understanding of the issue, how it arose and if other PCs were also affected. It became clear that a further two PCs had also been used to convert the videos using the same freeware. Luckily this malware hadn't been designed to spread or morph, so it was contained to three PCs which had downloaded the software.

Removing the adware and restoring the web settings was a time-consuming process, which took 12 hours to complete over a two-day period. Several products had to be used to remove the different elements of the adware before a full scan could be done to ensure the three computers were free of the offensive adware.

Once it was confirmed that all three PCs were clean, and their browser settings had been restored a full response was issued to the practice, the CCG and NHS Digital enabling the threat alert to be closed.

Remember…

- **Beware of Freeware** – it can contain malware. Luckily in this instance the type of malware had not been designed to morph or spread but it displayed offensive adverts and redirected web pages to dangerous sites.
- **Report anything strange** - If settings change on your PC or pop-ups start to appear contact the Service Desk immediately.
- **Ask for advice** - If you need a new piece of software contact the NHIS Cyber Security Team for advice.

Removing Adware

To clean the computers different products were used to target different elements:

- AdAware was used to remove the pop-up ads,
- Malwarebytes removed the malware,
- HitmanPro was used to remove all the cookies,
- Zemana performed a deep scan of each of the computers,
- Sophos performed a full scan to ensure the computers were clean.

Essential Cyber Security

The Nottinghamshire Health Informatics Service (NHIS) are pleased to have gained Cyber Essentials certification for a fourth year in September 2018.

Cyber Essentials is a government-backed, industry supported scheme designed to help UK organisations improve their defences and demonstrate their commitment to cyber security.

The Cyber Essentials scheme addresses the most common internet-based threats to cyber security, particularly attacks that use widely available tools and demand little skill such as hacking, phishing and password guessing.

The scheme helps organisations to protect the confidentiality, integrity and availability of data stored on devices which connect to the internet such as PCs, laptops, tablets, smartphones and servers.

By gaining the Cyber Essentials certification NHIS can demonstrate that it's taking the necessary precautions to protect itself and the users across their networks from general cyber-attacks.

Don't Forget to Connect

To ensure every PC and laptop you use receives essential security updates please ensure that they are connected to the network for at least three hours once a month.

Any device (PC, laptop, tablet) that hasn't connected to our network for at least 90 days will be deactivated as NHIS cannot confirm that all mandatory security updates have been applied.

If a device has been deactivated the user will receive an error message and will be unable to log on to the device. Users must contact the NHIS Service Desk (ext. 4040 or 01623 410310) to reactivate the device and apply all mandatory security updates.

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

✉ NHIS.Communications@notts-his.nhs.uk