19 July 2016

Fake NHS website - Thatcher Memorial Hospital

We have been alerted to a fake NHS hospital website that is advertising nursing and consultant jobs and trying to gain personal information from other Trusts. Staff should be vigilant of any calls, emails or contact from this fake Trust. Both the police and NHS Protect have been made aware. The website is: http://thatchermemorial.nhs.yangarra.org/

Thatcher Memorial Hospital
Chatburn Road
Whalley,
Ribble Valley
BD7 6JZ

8 September 2016

IM&T asks staff to be vigilant against email viruses

The IM&T department is currently dealing with a Ransomware virus attack. Ransomware is a virus which encrypts the files on your computer to prevent you using applications or accessing your data. Ransomware is typically delivered via an email which asks you to open an attached file or a link to a web page. This then runs the Ransomware virus which infects your PC.

We are asking that you be **extremely vigilant** when opening emails and only open attachments if you are expecting one, even if it is from a known source. Remember that email addresses can be "spoofed" to disguise their true source, it may appear to come from your bank or even a "@pat.nhs.uk" account, so the email could look like it has been sent by someone you know. If there is anything suspicious or you are in any doubt about an email please do not open the attachment and do not click on any link contained within the email.

If you are suspicious or in any doubt of any email or if you think you have suffered an attack then please report it to the IM&T Service Desk via the IT support portal. This latest attack on the Trust's computers has been contained but this type of attack is increasing in regularity. We all need to assist in reducing the risk of these attacks by remaining aware of the dangers of emails in the distribution of viruses.

29 September 2016

Access to personal email accounts

An important message to staff has been circulated from Damien Finn, Director of Finance and the Trust's Senior Information Risk Owner (SIRO), reminding staff not to access or use personal email addresses from Trust computers and devices. The Trust has recently suffered Ransomware virus attacks that have originated from staff members' personal email accounts, which were accessed from Trust PCs. These attacks threaten the availability of key clinical systems and are becoming increasingly more sophisticated and difficult to prevent.

Options to reduce the likelihood of future attacks have been assessed and the removal of access to personal web email accounts (e.g. Hotmail, Gmail etc.) from Trust devices is now deemed necessary. This change will bring our Trust in line with Information Governance measures elsewhere in the NHS and help protect our systems from virus and cyber attack.

Access to NHSMail (@nhs.net) and Doctors.net.uk (@doctors.org.uk) will remain unaffected. Existing access to email via personal devices will remain available via the Trust's free Wifi facilities. Staff are reminded that personal email services must not be used to conduct Trust business.

9 November 2016

Be aware – Do NOT give out your IT username and password

The Trust has been made aware of recent incidents at neighbouring NHS Trusts where staff have received phone calls for someone claiming to be a Trust employee who works within the IT department and is investigating a clinical incident. The caller is then asking staff to disclose their user name and password. Please be aware that whilst IT may require your user name to assist you with a service call they wouldn't ask you to disclose your password. If you think your password has been compromised in any way please contact the IT service desk on 45678 for assistance.

Remember – please do not disclose your username and password.

18 November 2016

PASSWORDS – Why you must not share…

Many of you will hold bank accounts and credit cards which need a Password / PIN. You keep these private and confidential and don't share them, so that no one else can access your account without your authority and there are audit trails to show when and who has accessed your account. In the same way, your Trust passwords need to be kept private and confidential and not shared with others.

15 March 2017

Important reminder and guidance for staff around use of Social Media

Social media has the potential to be an excellent and effective communication tool. Health professionals are using social media technologies and platforms such as *Twitter, Facebook, LinkedIn and Instagram* in a variety of innovative ways - to build and improve social and professional networks and relationships, to share health-related information, as well as news about a service or organisation, and to engage with the public, patients and colleagues. Closed online groups are also used for education and peer support, as well as the use of health sector online community networks.

As Trust employees and health professionals we have a responsibility to adapt our behaviour and consider our use of social media at work and outside of work to ensure we use this technology safely, appropriately and responsibly. We must educate and remind ourselves in how to realise the benefits of social media, as well as how to manage its risks.

Potential Risks include:

- Potential loss of personal privacy
- Potential breaches of confidentiality of patients and/or colleagues and other staff
- Online behaviour and comments/content that might be perceived as unprofessional, offensive or inappropriate
- Risks of comments, posts or content being reported by the media or sent to employers (often out of context)
- Potential for personal social media comments/content that brings the Trust or any employer/org into disrepute

Staff are reminded that the use of social media is governed by two separate Trust policies; the Information Governance Policy and the Media Policy. Both policies are available on our intranet in Policies & Documents section.

In summary, staff must be aware of the following guidance when using social media:

- Confidential or business information related to the Trust must not be posted onto a personal social website.
- Staff should be aware that anything they share personally via social media (their own accounts) will be publicly available, perhaps for years to come. Care must be taken never to breach confidentiality or privacy rights of patients, staff and other members of the public.
- Trust staff must not post social media comments/content that contains person identifiable information of another Trust employee in relation to their employment including judgements of their performance/character.
- Trust staff must not post comments or content on social media that contains defamatory statements about the Trust, its services or contractors.
- Staff must not use their own personal social media channels to broadcast confidential, sensitive or inappropriate information about patients, visitors, staff or the organisation and its partners.
- The Trust's reputation must always be considered when joining a conversation/commenting via social media.
- Social media websites and channels should never be used to mount personal attacks on individuals or companies/organisations and heated/intense conversations should be avoided.
- No content posted on any website, online discussion forum or social media networking sites, blogs or "apps" must bring the Trust into disrepute.
- As a basic rule, if it would be inappropriate to make a comment verbally, then it is inappropriate to make the comment on social media. Staff must be aware of the potential that inappropriate comments might lead to investigation under the Trust's Conduct and Disciplinary Policy and may impact on professional registration.

29 June 2017

IM&T update - Global Cyber Attack – Be aware

Following this week's review of the global cyber threat to our email and IT systems, our IM&T department immediately applied the necessary controls to reduce the risk of an infection to our IT systems. [REDACTED SENSITIVE INFO]

Note that email restrictions may be re-enabled with no prior notice in the event of new email borne IT security threats.

Staff are reminded to:

- Be aware of emails from unknown sources. Never click on any web links or attachments: this is the simplest and most effective way to handle junk, phishing or malware emails.
- Where you consider the email suspect, highlight the message, hold down the shift key and press delete.
- Ignore and delete the spam message.
- Never reply to a spam message as this lets the sender know it is an active account.
- Never forward a spam/chain email message.
- If you receive e-mail attachments or links from a KNOWN SOURCEthat you are not expecting or the content seems unusual, contact the sender asking them to verify they actually sent the attachments/links before opening.
- If you are unsure, DO NOT click on any web links or open any attachments and contact the IM&T Service Desk on x45678, should you have any questions.

26 July 2017

Suspicious emails – Fake invoices

Some staff across the Trust are currently receiving scam emails where the sending address has been faked to look like it has come from staff within the Trust or someone that you have previously dealt with on behalf of the Trust. The subject line starts with the word "Your invoice notice number" and is followed by a random number. The body of the message suggests you have received an invoice which is in fact fake. If you receive one of these emails do not click any links or reply and then follow the instructions below:

[INSTRUCTIONS REDACTED]

28 March 2019

Email attachments with the potential to be a ransomeware or malicious malware/payload attack

It has come to the attention of our Lead Counter Fraud Specialist and the IM&T Security Manager that our staff have been receiving emails with attachments from senders pretending to originate from a PAT email account.

The email heading may look like this “CP00001283952” and be from an account using a random name at the start of @pat.nhs.uk which on checking the email address you will find is a fabricated /false email address.
An example of one such fabricated/false email address is Franklyn@pat.nhs.uk
If staff receive an email from a fabricated/false PAT email account, please do not respond to the email and follow the guidance on the Intranet at **[POSTER ATTACHED SEPARATELY]**

04 October 2018

Information assurance reminder
Staff are being reminded of their duty not to access patient data held on systems without a valid reason. Ipswich Hospital recently disciplined two staff for accessing the personal details of musician Ed Sheeran with no legitimate reason after he was treated there.
The NCA has high standards of safe and secure handling of patient data to support patient care.
 We are all required to sign an annual declaration of appropriate use as part of mandatory training
 Proactive audits are routinely carried out into appropriate access of electronic records
 Ad Hoc audits are completed, where there are concerns raised around access
 We all complete mandatory IG training programme

Potential inappropriate access (via paper, electronic or smartcard solutions) is reported to the individual’s manager and Human Resources for investigation and if proven will result in disciplinary action.
It is also important to realise that inappropriate access to personal data is also reported to the staff members professional body e.g. NMC, GMC if appropriate to the individual.
Remember:
 Never look at records without justification
 Never share passwords
 Always use strong passwords
 Ensure you maintain a clear working environment
 Always lock your screen when you leave a PC (Windows-L or Ctrl-Alt-Del)

21 February 2019

Recordings and photos taken on site by patients and visitors using mobile devices
Almost everyone has access to a camera on their mobile phone these days. It has become the norm for people to upload their life to social media, whether a photo of a meal they are about to enjoy at a new restaurant or a shaky video of their favourite singer live in concert.
Due to a number of Datix incidents reported that relate to patients using mobile phones to film other patients or staff on wards and in clinical areas, and to support staff who are confronted with patients/visitors making recordings on devices, a poster has been developed.
An advice poster has been created for wards to print and display in clinical areas. Download the poster here. **[POSTER ATTACHED SEPARATELY]**

09 May 2019

Use of personal devices for image capture – Message from Dr Prudham, Caldicott Guardian

Dear colleague,

I would like to remind you that it is Trust policy, in line with GDPR and good Information Governance practice, that the capture and storage of images or videos of patients on unsecure personal devices is not permitted. If you require images of any kind for clinical or research purposes then you must seek advice from Medical Illustration and also the appropriate written consent from patients.

I am happy to advise if a particular difficulty or scenario arises, but my view is that the capture and storage of patient images or data on personal non-secured devices creates a potentially serious Information Governance risk. This creates problems in terms of reputational risk, but also a financial risk, as the fines that may be imposed by the ICO are substantial. More importantly however, in my view, is that it may undermine trust between us and our patients.

To refresh aspects of Information Governance training you may access the mandatory training module here.

Regards,

Roger Prudham

Consultant Gastroenterologist, Caldicott Guardian and Clinical Director for Professional Standards

25 July 2019

NHS ESR scam alert

Please be aware that there is an active spear phishing attack where hackers have targeted Salford Royal resulting in members of staff's salaries being stolen. Spear phishing is a technique hackers use to trick people into providing them with sensitive information such as usernames and passwords.

How has this happened?

Users have received emails that claim to be from Human Resources (HR) but are sent from accounts outside the NHS. These emails typically say that the user's salary has been increased and invite them to click a link to access related documents. When the user clicks on the link, they are directed to a fake NHS ESR login page, which appears the same as the actual login page except that it does not offer smartcard login. Logging into this fake page gave the hackers the ESR username and password which is then used to log into the real ESR website. This access has then been used to change bank details that the salary is paid to.

The malicious emails are customised and typically contain the organisation's logo and the links include their website domain within the URL.

The current attack has been sent from the following email addresses; the square brackets are a safety measure and do **not** appear in the real addresses. If you have any emails from

any of these accounts they must be deleted immediately and IT Service Desk informed, **do not** click any of the links.

- karnishpuoma1@gmail[.]com
- belton@alwaysmoney[.]com
- lisa@belvito[.]com

How do we protect ourselves

The email address and fake website used by the hackers was blocked on the 19th July so the current campaign we are protected against. The problem is the hackers can just change the address and repeat the attack. This means we must be extra vigilant in ensuring any email that is asking you to click a link and/or provide usernames and passwords is legitimate, if there is any doubt at all you can contact the Service Desk on 45678 who will double check and advise on the safety; additionally if you receive something unexpected please contact the department who has supposedly sent the email and double check with them that it is legitimate.

IT Security

15 August 2019

Information assurance reminder - lock your computer screen
Staff are reminded that policy requires the **locking** of any screens if stepping away from your desk or
working area. This is to ensure confidential data and systems are kept protected and secure.

21 August 2019

Staff Alert - Beware of spoof emails purporting to be from the CEO or a Director requesting payment or bank changes

NHS Local Counter Fraud specialists and IM&T Security management have received a number of referrals in the last week again relating to "CEO or Director" spoof emails making fraud attempts. This is when members of the finance department or HR Managers or Trust secretaries receive phishing emails, which are purporting to be from the NCA CEO or a NCA Director or CO Director requesting an urgent transfer of funds or to make an urgent payment usually because it is purported by the sender they cannot access an account.

The criminals use an email address, which looks bona fide but is actually a fake or spoofed email address underneath the purported sender email. The fact that it is a different email address is not always possible to detect with the naked eye. However, if you hover over the sender email it will usually reveal the real sender email ID name or it may be the email address may have one letter or character changed or it could be more sophisticated again to make you think the email is from the CEO or a Director as fraudsters are evolving new techniques all the time.

However you will usually find the vocabulary and sentence structure used is not consistent with the language used by the CEO or Director and should immediately raise your concerns on receipt. There is always a sense of urgency in the request. E.g. usually seeking an urgent payment or bank account information.

It is obvious that criminals are researching publicly available information to identify who our CEO is and who his Director colleagues are and the relevant staff to send the emails to within the Health body Finance or the HR function or to a Corporate or Divisional secretary?

If you receive a suspect email do not respond to it or click on any links but please do not ignore it either by failing to report it.

We need all staff to help us to continue to block the criminals cyber-attacks using spoof email addresses. Please ensure you take these two actions. Firstly, ensure you report to the IM&T helpdesk and forward the email to spamreports@nhs.net for national intelligence. Secondly report it to Action Fraud www.actionfraud.police.uk using the on-line reporting tool or Tel: 0300 123 2040. Also, after taking both actions please delete the spoof email. Also, you can contact your Care Organisation fraud specialist named below:-

Alun Gordon

Lead Local Counter Fraud Specialist (PAHT)

0161 922 3549

AlunJames.Gordon@pat.nhs.uk