



# Cyber News

WORKING TOGETHER TO PROTECT OUR NETWORK

## [ Deactivating User Accounts ]

The Nottinghamshire Health Informatics Service is constantly striving to enhance the security of our networks, so they will now be deactivating any user accounts that haven't been used in over 90 days.

The National Cyber Security Centre recommends that any account which is used to log on to a computer should be deactivated if it is not used for a prolonged period.

By deactivating the AD accounts which are used to log on to our networks, we reduce the risk to our network.

### RETURNING TO WORK?

Anyone who has been away from work for over 90 days will need to contact the NHIS Service Desk to reactivate their AD account.



Deactivating any account which hasn't been used in over 90 days lowers the total number of accounts on our network that could potentially be hacked and prevents the inactive accounts becoming compromised.

If anyone is away from work for over 90 days, they will need to contact the NHIS Service Desk (01623 410310 or ext. 4040) on their return to have their account reinstated.

## [ What is an AD Account? ]

**AD stands for Active Directory. It is a directory service that Microsoft developed for Windows operating systems.**

It authenticates and authorises all users and computers in a network

Everyone who uses a computer on our networks has their own username and password to log into the computer – this is your AD account.

When you enter your username and password AD

authenticates your details and authorises your access to our network – it lets you log in.

To keep our networks and data secure it is important that you use a strong password and never share it with others.

# [ Cyber Associates Network ]

NHS England and NHS Digital have established a network of cyber security expertise across the health and care system.

The Cyber Associates Network enables members to benefit from professional development, enhanced knowledge-sharing and networking opportunities

in order to secure their organisation's resilience and embrace technological change while ensuring patient safety.

The network is being developed to provide a health and care industry-specialist 'resource' where NHS Digital's Data Security Centre and NHS England's cyber security teams



can get direct and relevant support to test, review and deploy cyber-related products and services as well as build relationships and better understand local priorities around data security.

There will be numerous benefits for network members to shape and influence the

health-specific cyber security landscape as a critical friend and advocate.

More information about the Cyber Associates Network is available here:

<https://digital.nhs.uk/services/data-security-centre/cyber-associates-network>.

## Industries Most Targeted by Cyber Criminals in 2018



Healthcare  
41%



Financial Institutions  
20%



Education  
10%



Professional Services  
7%

Healthcare is the most targeted industry so it is vital we all take steps to protect our network and data

Based on information from investigations into more than 3,300 data incidents in 2018.  
Data Source: Beazley.

# [WhatsApp Hack]

**WhatsApp users are being urged to update the app on their phones immediately because of a security flaw that allows hackers to take over the phone by simply calling it, whether or not you answer.**

The vulnerability allowed hackers to install spyware on their targets' smartphone which is capable of searching through calls, texts and other data, switching on the phone's camera, microphone and performing other malicious activities.

WhatsApp believe only a "select number of users were targeted



through this vulnerability" but the full extent of the hack and the number of users infected is unknown.

WhatsApp have fixed the vulnerability in their latest

version of the app and users should manually check for updates through their app store.

All WhatsApp users are advised to upgrade to the latest version of the app immediately.



## Breach

An incident in which data, computer systems or networks are accessed or affected in a non-authorized way.



## Hacker

In mainstream use as someone with some computer skills who uses them to break into computers, systems and networks.



## Vulnerability

A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorized access to a system.

## [ Have you been Pwned? ]



**Did you know you can quickly check if your email address has been compromised or “pwned” in a data breach?**

HavelBeenPwned.com is a free resource which allows you to check whether your email address has been compromised in a data breach, if it has it will give you details of the breach.

As many apps and online accounts require your email address when creating an account it can easily become compromised if their databases are hacked. Unfortunately, data breaches are widespread and many people don't appreciate the scale or frequency with which they occur. For example, in May 2016 LinkedIn had 164 million email addresses and passwords exposed and sadly this is just one example of many.

If your email has been compromised, you should change your password immediately where ever your email is used.

Use [HavelBeenPwned.com](https://haveibeenpwned.com) to check your work and personal emails haven't been compromised and always use strong passwords.

## The feeling of creating a secure and memorable password!

Use 3 random words for a secure password

#thinkrandom



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



NHIS.Communications@notts-his.nhs.uk