Cyber News

WORKING TOGETHER TO PROTECT OUR NETWORK

Think Random!

Wouldn't you love to find a way of creating a password that is easy to remember and really strong?

Well there is a very simple way to create strong and memorable passwords.

Strong passwords don't have to be a confusing array of special characters, numbers and letters that are virtually impossible to remember. The National Cyber Security Centre recommends using three random words to create a memorable password. To increase the strength and meet many password requirements you should also add at least one number and special character.

The three random words should not be anything someone else could easily guess such as the names of your partner, children or pets, or your favourite holiday destination.

You could pick three things you can see around you or three words about your favourite book, music group, sport, film, hobby, or even a memorable day, though we wouldn't recommend using your wedding day.

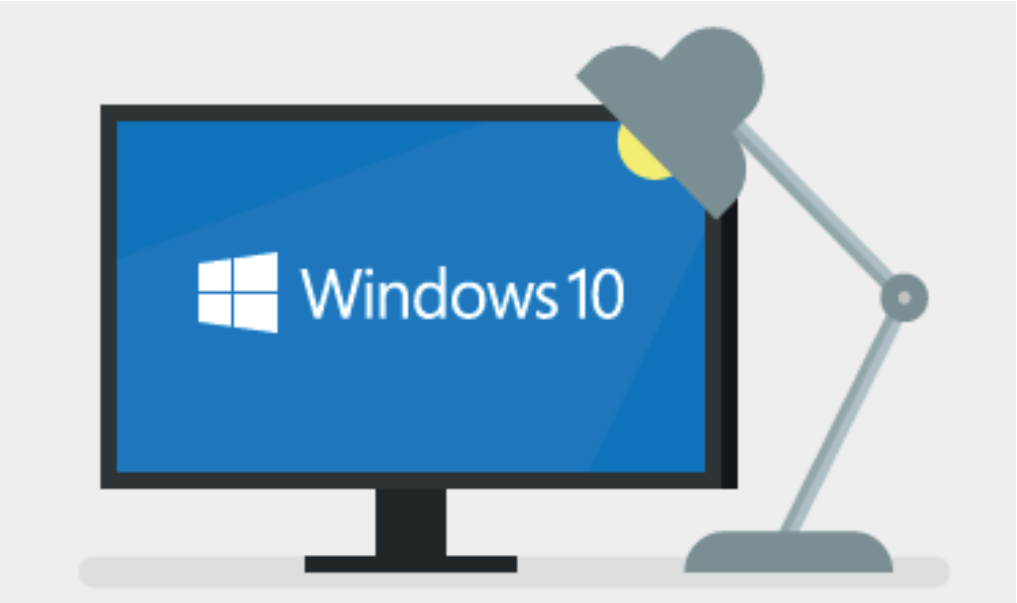
The three random words could be about anything, just make sure they are easy for you to remember but hard for anyone else to guess.

DO YOU HAVE THE LATEST UPDATES?

Make sure your iPhone has the latest iOS updates

To keep your Apple device secure it's important you regularly check for and accept any available software updates or select the automatic updates option.

Windows 10 is Coming



All NHS organisations are required to replace their Windows 7 operating system on all PCs and laptops by December 2019.

This deadline must be achieved as Microsoft are withdrawing all Windows 7 product support by the 14 January 2020, meaning the software will no longer receive security updates from Microsoft, increasing the likelihood that any future vulnerabilities will become known and exploited by cyber attackers.

Alongside this upgrade we will also be introducing Advanced Threat Protection (ATP) which offers an additional level of security to our network.

All compatible devices will be upgraded to Windows 10.

Applications are currently being tested to identify any which may be incompatible, this work will continue over the coming months due to the significant number of applications used across our networks.

The upgrade to Windows 10 commenced in January and will continue throughout 2019.

Sites and departments will be contacted over the coming months to schedule their upgrade.

Cyber Attack Saturday

1: FIREWALL ATTACKED BY FRENCH IP ADDRESS

On Saturday 3 November our external firewalls came under attack by a hacker using an IP address registered in France. To protect our network the firewall blocked the IP address.

2: THE ATTACKS MOVED TO BRITAIN

Then the hacker switched to using a British IP address. The methods used were the same as the previous attack, so it was clear the same person was behind both attacks.

3: 670 ATTACKS IN A FEW HOURS

In the space of just a couple of hours the hacker had launched 670 separate attacks to our networks!

4: HACKER MOVED TO NEXT TARGET

Hacking tools enable people to easily stage rapid attacks over a prolonged period. Whilst our firewalls can protect us from some of these attacks it is vitally important everyone uses strong passwords and remains vigilant.

Something 'ishy

Everyone is aware of phishing emails that are sent to many people asking for sensitive information but fraudsters don't just rely on email to try and trick you into sharing sensitive information such as passwords and bank details, they can also use social media, SMS text messages or phone you.

Phone phishing or vishing, is the criminal practice of using the telephone system to gain access to personal and financial information from customers for the purpose of committing fraud and smishing uses SMS text messages.

It is not unusual to receive these types of phone calls or text messages and it is usually only the most sophisticated ones that are likely to fool you.

Just like the phishing emails the fraudsters try to create a sense of urgency and voice of authority to gain your attention and build a sense of trust. They may suggest that they are working for a reputable organisation to create a sense of authority and try to persuade you to share information that you wouldn't normally share.

It is easy for these scams to slip through the net when you are busy and as this is the busiest time of the year for the NHS, the fraudsters may try and take advantage of this.

Phishing

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

Vishing

Phishing via phone calls: Making phone calls or leaving voice messages masquerading to be from reputable companies to gain sensitive information

How to protect yourself from Vishing and Smishing

- **Be wary of incoming calls** – before giving out any information to someone, call the company directly to verify the need for the information. Use the phone number displayed on their official website.
- **Don't call a number left in a voicemail or text message** – before calling a number verify the number is authentic by checking the company's website.
- **Do not reply to any emails or texts if you are unsure of the sender.**
- **Download apps through official channels** - always download applications from iTunes or Google Play store.
- **Don't click links from unverified senders in texts and emails.**

Smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Cyber Security Week

Sherwood Forest Hospitals NHS Foundation Trust held a cyber security week in December to raise awareness of a range of cyber security risks and help people to stay safe online.

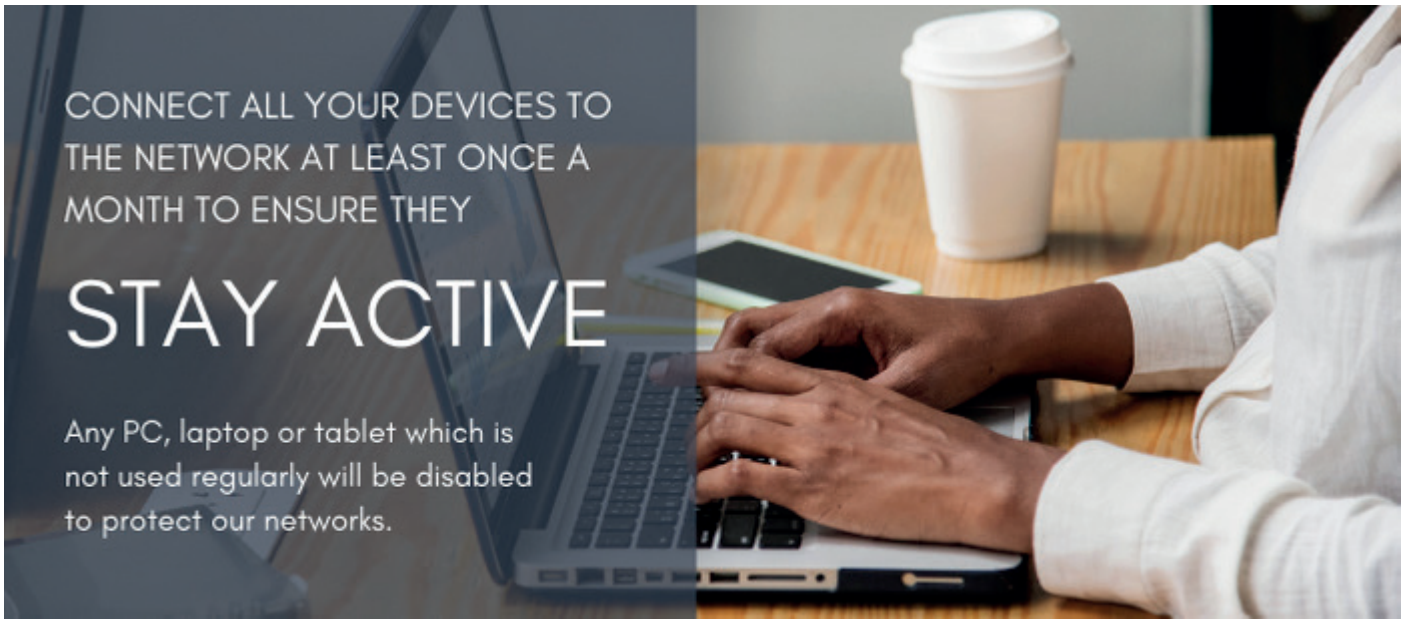
The Trust's Information Governance team, with support from the NHIS Cyber Security team, ran the week which included an information stall in the King's Treatment Centre at King's Mill Hospital.

The stall offered visitors and patients tips on how to stay safe online.

Advice and guidance included how to spot phishing emails, checking if email addresses had been compromised, the importance of strong passwords and tips on how to create strong but memorable passwords.

Visitors to the stall were able to use Kaspersky's password check website (https://password.kaspersky.com/) to see how easily a weak password such as 'Password1' can be cracked and comparing this to a password using three random words.

People who visited the stall found it useful and took away tips to improve their security online.



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

NHIS.Communications@notts-his.nhs.uk