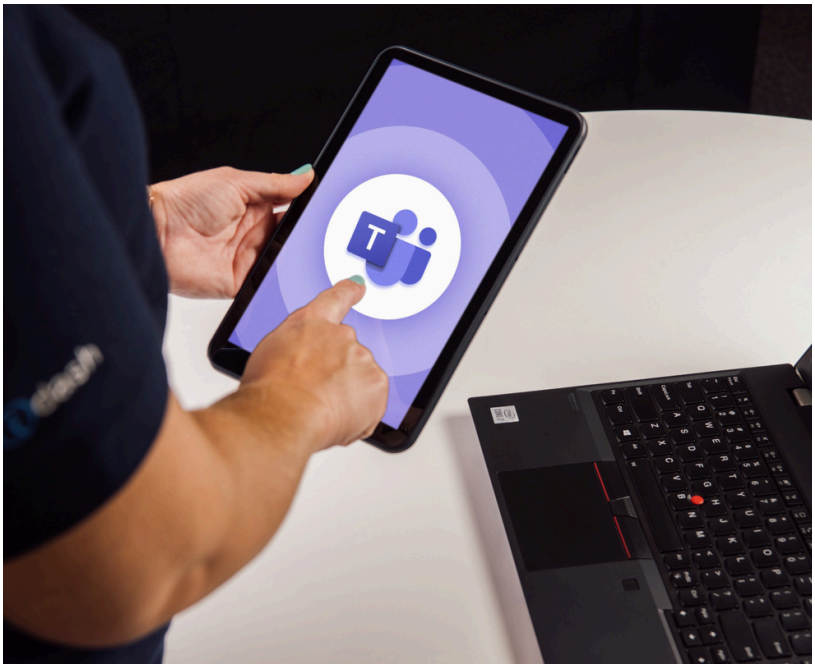
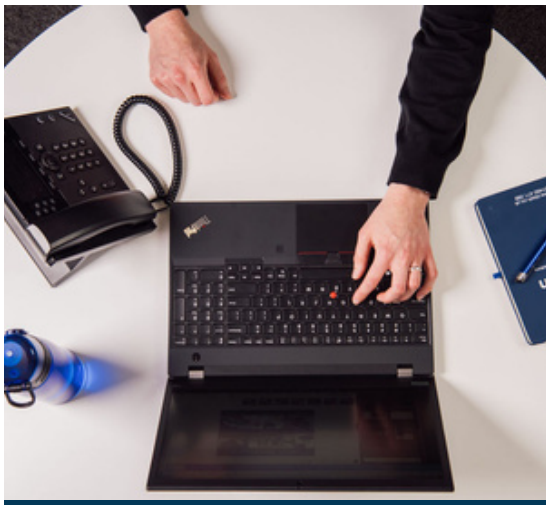
Outdated IT Systems Leave NHS at Risk of Further Cyber Attacks

In June, a devastating cyber attack led to the postponement of more than 6,000 appointments and procedures at major London hospitals. This incident highlighted the critical issues facing the NHS: outdated IT systems, vulnerable points, and the need for robust basic security practices.





NHS England has confirmed that data stolen during the 3 ransomware attacks in June on pathology services provider Synnovis has been published online. According to the BBC, Russian cyber gang Qilin shared almost 400GB of data on their darknet site and Telegram channel. This data included sensitive information such as patient names, dates of birth, NHS numbers, and descriptions of blood tests. However, NHS England has stated there is "no evidence" that the cyber criminals published an entire database, and it may take "some weeks" to determine which individuals were affected by the attack.

A leading cybersecurity expert has warned that the NHS remains vulnerable to further cyber attacks unless it updates its computer systems. The professionalisation of cybercrime has made significant progress, reaching a new level of maturity this year due to the emergence of AI and powerful new technologies. This development underscores the urgent need for organisations to invest in their security infrastructure. The advancements of recent years are just the beginning; cybercriminals are poised to develop even more sophisticated methods to achieve their goals.

Now more than ever, it is crucial for organisations to prioritise cybersecurity. Here are some practical tips on how to protect yourself from these threats:

Security Best Practices Checklist

1. **Regularly Update Software and Systems** Ensure that all software, including operating systems and applications, is up to date with the latest patches and security updates.
2. **Use Strong Passwords and Multi-Factor Authentication (MFA)** Implement strong, unique passwords for all accounts and use multi-factor authentication to add an extra layer of security.
3. **Conduct Regular Security Audits** Perform regular security assessments and audits to identify and address vulnerabilities in your systems.
4. **Educate and Train Employees** Provide ongoing cybersecurity training for employees to help them recognise and avoid potential threats such as phishing attacks.
5. **Backup Data Regularly** Regularly back up critical data and ensure that backups are stored securely and are easily accessible in case of a cyber attack.
6. **Implement Network Security Measures** Use firewalls, anti-virus software, and intrusion detection systems to protect your network from unauthorised access and malware.
7. **Develop and Test an Incident Response Plan** Create a comprehensive incident response plan and conduct regular drills to ensure your team is prepared to respond effectively to a cyber attack.

idash: Your Trusted Technology Partner

At idash, a local IT systems and services provider, our security team is ready to work with you to protect your data and business. We offer comprehensive cybersecurity solutions tailored to your specific needs, helping you stay one step ahead of cybercriminals. Investing in robust security measures today can safeguard your organisation from the evolving threats of tomorrow. Don't wait until it's too late—take proactive steps now to secure your IT infrastructure and protect your valuable data.

By following these best practices and partnering with experts like idash, you can significantly reduce the risk of cyber attacks and ensure the continuity of your operations. Together, we can build a more secure and resilient future.