Cyber Awareness

1. Unlocked screens

Unlocked screens are a real threat to patient data - good cyber security is our shared responsibility and all staff across the NHS have a role to play.

2. Phishing

Suspicious emails could pose a threat to patient data - good cyber security is our shared responsibility and all staff across the NHS have a role to play.

Be aware of potential phishing scams and emails that try to trick you into providing information. Don't open attachments or click on links without establishing if they are legitimate.

3. Weak passwords

Weak passwords are a real threat to patient confidentiality - good cyber security is our shared responsibility and all staff across the NHS have a role to play.

Weak passwords are a cyber security risk. The longer and more complex your password, the more difficult it is to crack.

4. Tailgating

Letting tailgaters into restricted areas threatens patient confidentiality – good security is our shared responsibility, and all NHS staff have a role to play.

5. Sharing data?

Data breaches can lead to fines, disruption to services and reputational damage. Make sure you understand and follow the latest guidance around data sharing.

6. Messy files?

Disorganised filing leads to costly mistakes that can jeopardise patient confidentiality and legal compliance. Keep files organised, up to date and secure.

7. Be aware with who, what and where you share

Protect NHS data. Be aware with who, what and where you share.

8. Do you care about what you share?

Sharing NHS information in public spaces puts patient data at risk. Criminals know this and they are watching and listening. Keep your conversations and your screen time private.

Data is valuable to criminals. They’re watching and listening for any details that could help them access it. This puts data confidentiality at risk.

Be aware with who, what and where you share.

9. Who can you trust?

Sharing NHS information in public spaces puts patients data at risk. Criminals know this and they are watching and listening. Keep your conversations and your screen time private.

10. Who can you trust?

Criminals are always watching and listening for ways to access information. Be aware of what you share in public spaces and on social media.

11. Sharing your ID pass?

Stolen or fake NHS passes allow criminals to gain access to building and confidential data. Keep your pass safe and don't share it with others on social media.

12. Ransomware

Ransomware is a form of malicious software that makes data or systems unusable until the victim makes a payment. Reduce the risk by:

- choosing a strong and varied password
- being aware of potential phishing scams
- wearing your staff ID badge on-site

13. Unlocked screens

Unlocked screens are an open invitation. Keep your screens and devices locked when they’re not in use.