



A User Guide to Cyber Security

What is Cyber Security? Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access.

What's the biggest risk to me? Whilst there are many security systems in place, both national and local, the vast majority of Cyber Security incidents start with someone opening an e-mail that has a virus attached or by leaving their mobile device unlocked and easy to look at or steal. The FBI's former Head of Computer Intrusion Prevention stated 'there is no patch for careless, greed or stupid', highlighting that one of the greatest threats to security comes from user's actions.

What do I need to do to protect myself? There are some very simple steps that you need to follow to ensure that you protect yourself, your system and your data. Don't forget that if it is found during any formal incident investigation that you are the source of the incident through negligence you could be liable.

- 1) **Never share your password with anyone:** No one should ever ask you for your password, even from a supporting organisation such as NHS Mail or the service desk, so you should never give your password to anyone else, even your colleagues
- 2) **Never leave your computer logged in if unattended:** If you walk away from your desk, lock your device by pressing the Windows key and L, or CTRL+ALT+Del and selecting Lock this Computer.
- 3) **Never open unexpected e-mails:** If you receive an e-mail from someone you don't know with an attachment, it could easily be a phishing e-mail looking to trick you into opening it or clicking on a link.
- 4) **Beware 'shoulder surfers':** If you are using your machine in a public place, or even just in your office, always be aware of people around you who can see your screen and read the data on it.
- 5) **Have complex passwords:** It's important that your passwords are complex (i.e. they have numbers and symbols as well as letters) to make them difficult to crack. An 8 character password all in lower case will be easily cracked using available 'brute-force' technology (much less if a proper word is used), whereas with numbers, capitals and symbols your password quickly becomes a very effective protection for your system and data.

Bad Password:	welcoming	(no capitals, no symbols, known word)
Good Password:	Welc0m1ng	(capitals, numbers replace letters, spells a word)
Better Password:	G1c0We\$lm	(capitals, numbers, symbols, not a word)

IG helpdesk: embed.infogov@nhs.net