
Tutorial
LIVING SAFELY WITH COMPUTERS

Agenda

1. COMPUTER-INDUCED MEDICAL PROBLEMS
2. GOOD HEALTH AND SAFETY PRACTICE
3. PASSWORDS AND SOCIAL ENGINEERING

WHAT MEDICAL PROBLEMS ARE COMPUTER-INDUCED?

- Computer Vision Syndrome
- A range of vision issues can be caused by prolonged viewing of computer screens including:
- Dry Eye - itchy sore eyes
- to the more serious Glaucoma - pressure in the eyeball damaging the optic nerve

WHAT MEDICAL PROBLEMS ARE COMPUTER-INDUCED?

- Musculoskeletal problems
- Crouching over a computer keyboard for long periods can cause:
- Back problems
- Severe and acute pain in the neck and shoulder regions
- Carpal Tunnel Syndrome: Acute pain caused by repetitive movement of the joints (Repetitive Strain Injury), particularly the wrist

WHAT MEDICAL PROBLEMS ARE COMPUTER-INDUCED?

- Sleep Disorders
- There is growing evidence that viewing computer screens late at night disrupts sleep patterns. Computer screens emit more light from the blue end of the spectrum than occurs in natural daylight, and this affects the body's melatonin production, which in turn disrupts our normal wake/sleep cycles

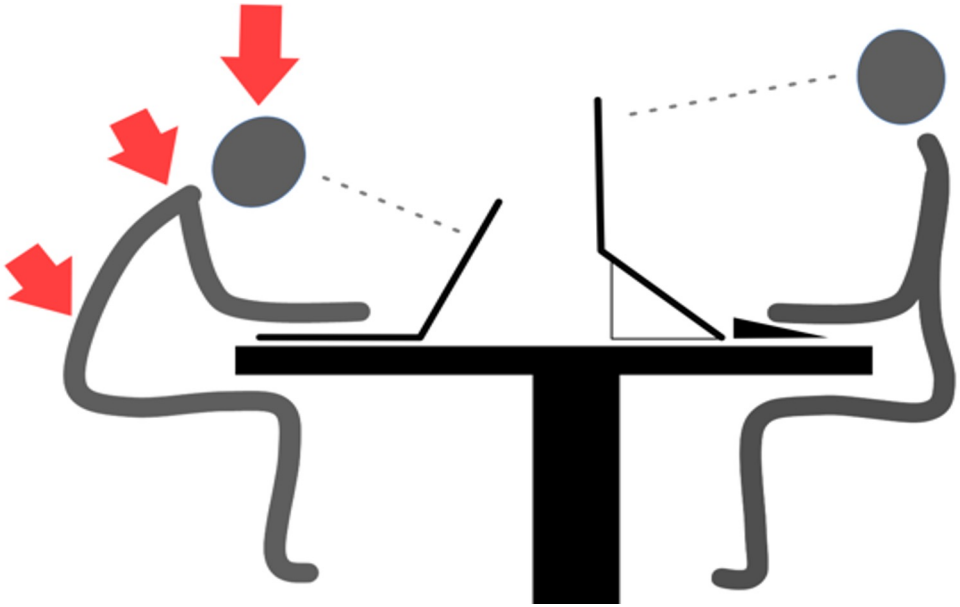

Assisted Living
BET
WHAT CAN I DO?

Take regular breaks - do not work for more than one hour without a break. Take at least a five-minute break every hour. Stand up and walk around, so that you're not sat in the same position all day

Look away from the screen into the distance for a few moments to relax your eyes; focus on something 30 metres away for 30 seconds every 30 minutes

Adjust lighting to be comfortable, for example using window blinds to reduce glare. Try to avoid the computer screen being the only light source in darkened room

Use a display adjustment settings on your computer ('night mode' or similar) or an app such as f.lux to reduce blue light emissions in the evening



- Exercise your back, shoulders, neck, wrists and legs
- Ensure your posture is correct to reduce risk of repetitive strain injury. Consider using a laptop stand and keyboard to raise the screen at your eye level, taking the strain off your shoulders and lower back.

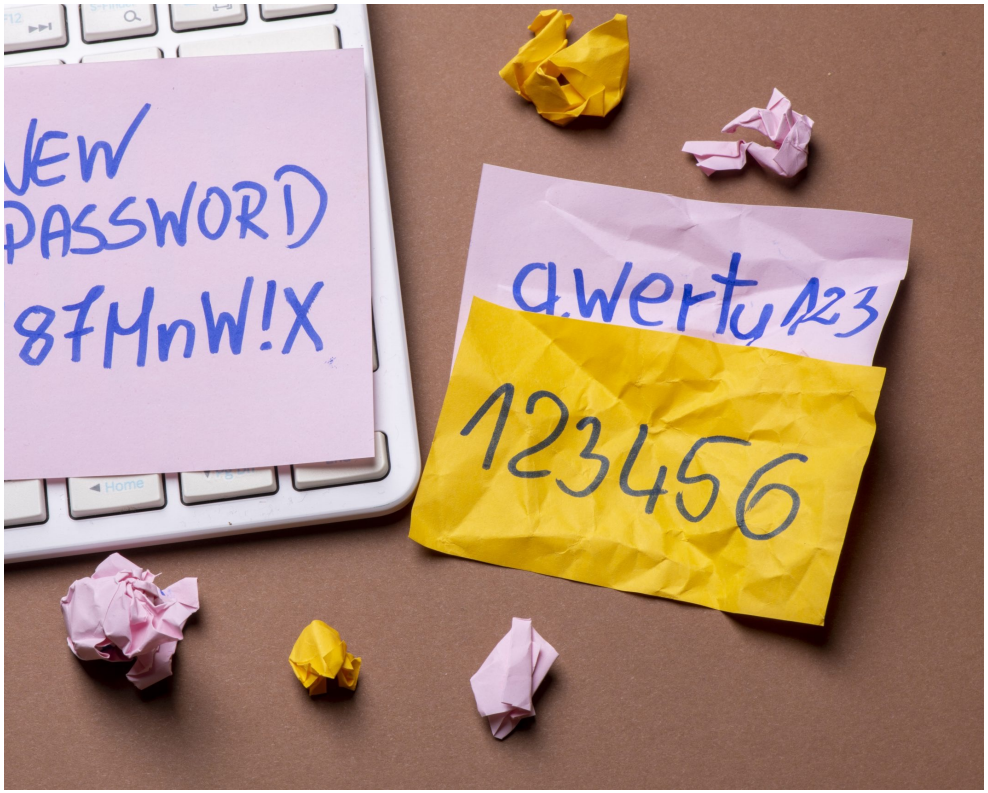
Stop using your computer one hour before you go to sleep


Password:
****

HOW CAN PASSWORDS BE CRACKED?

- Dictionary attacks: These are simple passwords, e.g. arsenalaregreat, that can be cracked by trying words, and combinations of words from a dictionary
- Brute force attacks: More complex passwords, e.g. Ars5Tot0, can be broken by trying different combinations of words, letters, numbers and symbols
- Rainbow Table Attacks: These involve looking up a stolen encrypted password hash value in pre-compiled tables to find an equivalent plaintext password value

HOW CAN I ENSURE MY PASSWORD IS SAFE?



- Create unique passwords that use a combination of words, numbers, symbols, and both upper and lower-case letters
- Do not use your network username, email address, website login etc. as your password
- Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, phone number, or names of family members

HOW CAN I ENSURE MY PASSWORD IS SAFE?

- Avoid words that can be found in the dictionary
- Complexity is nice, but length is key
- Avoid using the same password for multiple sources

- PASSWORD DOS AND DON'TS
- BETTER PASSWORD PRACTICE
- VISUALIZING COMMON PASSWORDS

HOW CAN I SAFELY BACK UP MY WORK?

- If you have a Mac, Apple's built in Time Machine does the job well
- For Windows, this review of options
- For Linux, see this list of options

EXTERNAL HARD DEVICES

- Pros: Easy to use; large capacity; works well with backup software; don't need to be online
- Cons: Device can be broken, lost or stolen

MEMORY STICK

- Pros: Convenient and portable
- Cons: Smaller capacity than hard drives. Very easy to lose or put in the washing machine

CLOUD-BASED STORAGE (E.G. MICROSOFT ONEDRIVE, GOOGLE DRIVE, DROPBOX ETC.)

- Pros: Limited free storage capacity
- Cons: You can't lose it, but it's only as safe as your password

VERSION CONTROL SYSTEMS WITH 'REMOTE' STORAGE

- Pros: Especially useful for code and for sharing with others. Has the advantage of keeping a record of incremental changes which can be 'rolled back' if you wish to revert to older versions
- Cons: Not generally suitable for confidential information

EMAIL AN ATTACHMENT TO YOURSELF

- Pros: Quick. Easy. Handy when other backup storage is not available
- Cons: Size limit of a few MB per email. Useful only as a short-term measure

HOW OFTEN SHOULD I BACK UP MY WORK?

- Ask yourself, how inconvenient would it be to lose everything since your last backup?
- Then adjust your backup frequency accordingly
- Establish a balance between the effort required to backup and the effort required to reproduce the content you'd lose without backing up.
- Backup really important content to more than one place

SOCIAL ENGINEERING

- ... a process that cyber criminals use to psychologically manipulate an unsuspecting person into divulging sensitive details
- Also known as "The art of hacking humans"

The internet containing a wealth of information about you

You are a kind and honest person

You reveal more about you than you think

Your mind easily jumps to conclusions

You are inclined to believe others are like you

SOME ONLINE SOCIAL ENGINEERING TECHNIQUES

- Phishing: shortened or misleading links redirect users to suspicious websites with the aim of obtaining personal information such as names and addresses
- Pretexting: attackers use an invented scenario (the pretext) to try and steal their victims' personal information. It often involves research to create an elaborate lie, and then use this information for impersonation (e.g. date of birth) and to establish legitimacy in the mind of the target
- Baiting: the promise of an item or good that malicious actors use to entice victims. Baiters may leverage the offer of free music or movie downloads, for example, to trick users into handing their login credentials
- Quid Pro Quo: Promises a service in exchange for information. E.g. an attacker calls random numbers at a company, claiming to be calling back from technical support. A naive user with a legitimate problem gives the attacker access in exchange for helping solve the problem
- Tailgating: The tailgating attack, also known as "piggybacking," involves an attacker seeking entry to a restricted area that lacks the proper authentication

HOW TO AVOID IT

- Slow down
- Do the research before clicking their links
- Delete any message asking directly for personal or financial information
- Be cautious of requests/offers of help, particularly from overseas
- Beware of any download

NEXT STEPS

- You need to take the Safety Quiz in Moodle
- It opens on 27th January and closes on the 15th of June at 5pm.
- You can take the test as many times as you like
- Passing this is a requirement as part of accreditation from the British Computing Society (BCS), and therefore you will need to achieve 100% in order to progress to stage 2 of your degree
- If you don't have a chance to complete it successfully by the deadline, you will have another opportunity for a resit