

Connecting devices, health, environment and authentication

Printable handout — what plugs into what, what to do when it is not recognised, how to work at a machine for years without damage, where old equipment goes, and how you prove who you are.

The most practical lesson in the course

Four subjects, and every one of them is something you will use outside this room. The last one — authentication — is the only subject in this course that is getting more important every year rather than less.

Objectives

1. Identify the common ports and say what each carries: USB, HDMI, Ethernet, audio, power.
2. Diagnose why a connected device is not recognised, and name the usual culprit.
3. Describe four ergonomic and health measures for extended computer use.
4. Explain why e-waste cannot go in a household bin, and what to do before disposal.
5. Compare three authentication methods and state one weakness of each.
6. Explain what two-factor authentication adds, and why a password alone no longer suffices.

1 · What holds it all together

Part or port	What it does — and what it carries
Motherboard	The main circuit board. Every other component plugs into it so they can exchange data.
Power supply	Converts mains electricity into the low voltages components need — which is why you cannot plug a component straight into a wall.
USB	The general-purpose connector: data <i>and</i> power. Keyboards, drives, phones, charging.
HDMI	High-definition video and audio, down one cable.
Ethernet / wireless	Data to and from other computers.
Audio jack	Sound, to headphones or from a microphone.
Power socket	No data at all — which is why a device can charge perfectly and still never appear on the machine.

2 · When a device is not recognised

There are four usual suspects — the port, the cable, the driver and the power. This section is not about the order. It is about how to find out.

Habit	Why it works
-------	--------------

One at a time	Swap the cable, or the port, or the machine — never two at once. Change two things and the result tells you nothing.
Split it in half	That device on another machine; another device in that port. Two tests say which side the fault is on.
What changed?	Working yesterday, broken today means something changed — an update, a new cable, a move. Hardware rarely fails just as software changed.
Cheapest test first	Free and instant before slow and expensive. Look at the plug before you buy a cable.
The usual answer	Power but no recognition? The driver is the most common cause — software, not the socket.

Write down what you tried and what happened. The list is what stops you going round the same circle three times.

3 · Working safely at a computer

Bad habits build up quietly over years of screen time, and the damage does not reverse.

Measure	What to do
Screen at eye level	The top of the screen level with your eyes, about an arm's length away, so your neck stays neutral.
Feet flat, back supported	Both feet on the floor, lower back against the chair, elbows at roughly a right angle.
Break the stare	Blink deliberately and look into the distance regularly — screens cut your blink rate by half.
Move every hour	Stand, walk, stretch hands and wrists. Sitting still is the part that does the damage, not the computer.

The 20-20-20 rule: every 20 minutes, look at something 20 metres away for 20 seconds.

4 · Looking after it, and letting it go

Practice	Why
Keep it cool and clean	Blocked vents cook a machine slowly, over months, and the damage is permanent.
Shut down properly	Pulling the power mid-write is how files and whole drives get corrupted.
Handle cables gently	Pull the plug, never the wire, and never force a connector the wrong way round.

Wipe it first	Sign out, remove the accounts, then erase the drive — in that order. A discarded phone with your accounts still on it is worth more to a stranger than the phone was to you.
E-waste, never the bin	Batteries and circuit boards contain lead, mercury and cadmium, which leach into groundwater. Old devices go to an e-waste collection point.

Green computing is also the boring daily version: sleep settings, double-sided printing, and keeping a working machine for another two years instead of replacing it.

5 • Three ways to prove who you are

Every authentication method in existence is one of these three — and every one of them has a weakness.

Factor	Examples	Weakness
Something you know	Password, PIN, security question	Guessed, reused across sites, phished out of you, or written on a note under the keyboard. Reuse is the real problem: one leaked password becomes a key to eleven other accounts.
Something you have	Phone, bank card, swipe card, hardware key	Lost, stolen or borrowed — and then it works perfectly for whoever is holding it.
Something you are	Fingerprint, face, iris, voice	You cannot change it. A stolen password is replaced in a minute; a copied fingerprint is yours for life. Readers also reject the legitimate person often enough that people switch them off.

6 • Two-factor authentication

	One factor	Two factors
What it is	A password alone.	A password <i>plus</i> something from a different category.
What an attacker needs	One stolen thing, from anywhere in the world, silently.	Two things, one of which is usually in your pocket.

- **Why a password stopped being enough.** Billions of real passwords have leaked in breaches, and most people reuse them. Attackers do not guess any more; they look you up.
- **Two of the same category is not two factors.** A password and a security question are both things you know, and one convincing phone call takes both.

- **Not all second factors are equal.** An app code or a hardware key beats an SMS, because a phone number can be moved to somebody else's SIM.
- **Keep the recovery codes.** The commonest two-factor disaster is not an attacker — it is you, with a new phone and no way back in.

A second factor does not make an account unbreakable. It makes a stolen password worthless on its own, which stops almost every attack that happens at scale.

7 · Check yourself

1. A phone charges from a laptop but never appears on it. What does that tell you immediately, and what would you test next?
2. Why is a fingerprint the hardest factor to recover from once it is compromised?
3. A bank asks for a password and your mother's maiden name. Is that two-factor authentication? Explain.
4. Name the four ergonomic measures, and state the 20-20-20 rule.
5. Why can a laptop battery not go in a household bin?

Activities for this lesson

Activity 1 — The unrecognised device. A device is plugged in and does nothing. Work through port, cable, driver and power in order, and say which step you would try first and why. There is more than one defensible order; the reasoning is the answer.

Activity 2 — Password post-mortem. Four real-world breach scenarios. For each, identify which authentication factor failed and what would have prevented it. Be precise: "they got hacked" is not an answer.

Neither activity carries marks. The marks for this topic are in the Checkpoint, which assesses Lessons 1–3 together.

Glossary

Port	A socket on a machine through which a device connects.
Ergonomics	Designing the workstation around the body, so long use does no damage.
E-waste	Discarded electronic equipment, which contains material that must not reach landfill.
Authentication	Proving to a system that you are who you claim to be.
Two-factor authentication	Using two factors from two different categories to authenticate.