LESSON 27

Staying Safe Online: Phishing, Scams, Malware, and the Digital Age of Consent

60 minutes | ICT1: Introduction to the computer and word processing | Outcome M1.U3.1

WHAT THIS LESSON DOES

This lesson helps students recognise phishing and scams in daily messages. It covers malware risks, better passwords, and Ireland's digital age of consent at 16. You will use scenarios to identify what makes messages suspicious.

CURRICULUM OUTCOMES

Outcome	What the specification asks for
M1.U3.1	Understand the concepts and associated risks of the internet and the World Wide Web.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Recognise common scam and phishing patterns students actually meet
- Explain malware risk in plain terms and name one safer password or two-factor habit
- State the Irish digital age of consent (16) and who to tell first if a message or sign-up feels wrong
- Identify three scam examples and write what gives each one away

BEFORE THE BELL

- Print the key concepts table and full red-flag list as the default handout for mixed-ability readers.
- Have img_phishing_red_flags and img_scam_spotter_layout ready to project.
- Check that students can reach the Project Portfolio. Be ready to create 02_research with anyone who still lacks it.
- Decide before class whether 02_scam_spotter also feeds a named Key Assignment this term, and prepare the one-sentence announcement.
- No software demo needed yet. Have img_phishing_red_flags ready to project on the welcome slide. Optional: one printed or on-screen sample scam text for the warm-up if the class is quiet. Know your school's reporting route for online incidents.
- Print the key-concepts table and full red-flag list for the class. Read three or four red flags so you can restate them in plain language with one example each.
- Project the scenario-cards interactive. Protect create-file and portfolio time: core two cards first; extras only if the clock allows. Plan the two must-bank spoken lines for malware and password/2FA.
- Know your school's reporting route for online incidents before class. Support signposts already appear in the intro; this step only reinforces the two most common stuck points.
- First circulate check: who is missing 02_research. Demo New → Folder and New document on Word Online and Google Docs if the room is mixed. Board machine signed into cloud storage before class. Have the courier-fee worked example ready to type live as the first row.
- Students should already have 02_scam_spotter open from the create-file step. Decide KA banking before class and announce it in the first minute. Project layout image, worked example, and success criteria only.
- Optional 2-minute pair share; skip if time is tight after the portfolio build.
- Quick visual check that 02_scam_spotter exists for as many students as possible before pack-up.

Staying Safe Online: Phishing, Scams, Malware, and the Digital Age of Consent

HOW THE LESSON RUNS

5 min	introduction	Introduction
8 min	content	Key concepts
14 min	activity	Scam scenarios
3 min	content	Common issues
5 min	activity	Create your Scam Spotter file
15 min	activity	Portfolio build
5 min	content	Reflection
5 min	summary	Lesson summary

TEACHING MOVES

- Talk key-concept rows aloud as five short beats; split Lock the account and Digital age of consent.
- Speak only three or four red flags with one example each; full list stays on the handout.
- Run delivery text and placement DM whole-class; bank spoken malware and password/2FA lines in those debriefs even if optional cards are cut.
- Mandatory live-model: name Word Online or Google Docs, hand up if 02_research is missing, New → Folder, new document, rename to 02_scam_spotter only, type title plus one model example row.
- Do not teach table insert; numbered list only.
- Announce KA status in the first minute of portfolio time.
- Project success criteria, worked example, and layout image; keep the example bank off the main screen if possible.
- Minimum viable artefact: two example/giveaway rows + login habit + age-16 line.

WHAT TO WATCH FOR

- Using vague terms like 'urgent' without details; prompt for exact indicators such as unknown short links.
- Clicking links in suspicious messages; reinforce always using official trusted channels instead.
- Leaving password/2FA and age 16 off the portfolio page; both are required for everyone.
- Inconsistent file names; insist on exactly 02_scam_spotter inside 02_research.
- Starting the full portfolio checklist before the file exists; finish create-file for the whole class first.

DIFFERENTIATION

- Support: Sentence starter "This message is suspicious because…" and the printed simplified table.
- Support: Pair weaker tech users with a peer for the create-file clicks only.
- Support: Minimum viable artefact (two rows + login + age 16) as the floor; live-model row counts as the first example.
- Extension: Third example, second personal rule, or a creator/small-seller scam row.
- Support: Allow paired talk on scenarios before whole-class share.