MODULE 2

Cybersecurity & Troubleshooting

INTRODUCTION

This educational material is designed for participants aged 55+ who want to navigate the digital world safely. The course will teach you how to recognize risks, protect your data, and use modern technologies without fear.

During three modules, you will learn the basics of digital security, types of online threats, and how to protect your devices and data

In today's interconnected world, understanding digital security is paramount for everyone, especially for individuals aged 55+. While the digital realm offers vast opportunities, it also presents various risks that can impact personal data and financial well-being.

Equipping yourself with cybersecurity knowledge and effective troubleshooting skills empowers you to navigate this landscape confidently, protecting your valuable information and maintaining peace of mind.

You will explore how to:

- Identify common cyber threats such as scams, phishing, and malware.
- Create and manage strong, unique passwords and utilize two-factor authentication (2FA).
- Secure their devices and online accounts from unauthorized access.
- Perform basic troubleshooting steps for common software and internet issues.
- Safely browse the internet and make secure online transactions.

Through practical examples, etc. learners will gain the confidence to proactively safeguard their digital presence and effectively address technical challenges, ensuring a safer and more enjoyable online experience.

5 KEY WORDS

1. **Cybersecurity** - Protecting systems from cyber threats.
2. **Troubleshooting** - The process of identifying, diagnosing, and resolving problems.
3. **Password** - Secret access code.
4. **Backup** - A copy of data stored separately to restore information in case of data loss or system failure.
5. **Antivirus** - Software designed to detect, prevent, and remove malicious software and viruses from computers and systems.

5 MAIN GOALS

1. **Learn to recognize basic digital threats:** Understanding common dangers helps you stay safe online.
2. **Be able to create strong passwords:** Strong passwords and two-factor authentication protect your accounts.
3. **Gain awareness of malware and scams:** Knowing these risks helps you avoid falling victim.
4. **Know how to protect your devices** with antivirus and firewall: Security tools prevent unauthorized access and malware.
5. **Back up data securely and regularly:** Regular backups ensure your data is safe in case of problems.

CYBERSECURITY: AWARENESS, PROTECTION, CONFIDENCE

Digital life offers convenience, connection, and countless opportunities — but it also exposes individuals to a range of online risks that can affect personal data and everyday digital use. Building cybersecurity awareness is not about fear or technical expertise; it is about developing the confidence to recognise what is safe, what looks suspicious, and which simple habits provide solid protection.

The module begins by presenting the most common threats people encounter online, such as phishing attempts disguised as legitimate messages, fraudulent links that try to steal passwords or financial information, and malware that enters devices through unsafe downloads or outdated systems. These examples illustrate how cybercriminals rely more on deception than on technical complexity, and how understanding the signs — unexpected requests for action, unfamiliar senders, spelling mistakes, urgent language — already protects users from many risks.Alongside recognising threats, participants explore essential digital habits that strengthen everyday safety.

Cybersecurity also extends to protecting the device itself. The e-learning explains how antivirus software, firewalls, and regular updates strengthen the overall security of a system. These tools work quietly in the background to detect unwanted activity, prevent intrusion, and close vulnerabilities. Understanding their purpose helps demystify the idea of digital protection, turning abstract terminology into concrete safeguards. Data backup is another element highlighted in the module: a simple practice with enormous benefits.

Finally, safe online behaviour is addressed as the foundation of cybersecurity. We invite you to reflect on how you usually browse, which websites you trust, and how you approach online transactions. It offers practical recommendations on verifying website legitimacy, recognising secure connections, and avoiding unnecessary oversharing of personal details.

With these insights, cybersecurity becomes less about technical defence and more about informed, confident navigation of the digital world.

UNDERSTANDING TROUBLESHOOTING

Modern devices are sophisticated, yet most everyday problems follow simple patterns that users can learn to identify and resolve. Troubleshooting is not about technical expertise; it is about a calm, structured way of approaching a problem.

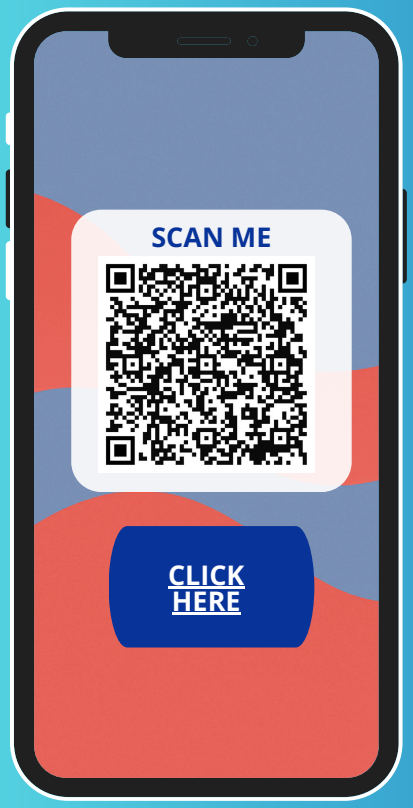
The module presents troubleshooting as a mindset rather than a set of isolated skills. It shows how devices often behave predictably: slow performance can stem from too many programs running at once, outdated software, insufficient storage, or an unstable internet connection; error messages often point to permissions, updates, or incompatible files; and connection issues usually have identifiable causes such as router problems or temporary network interruptions.

Participants are guided through the principle of “first steps first” — a reliable approach used even by IT professionals. Restarting a device, closing unnecessary programs, checking cables or Wi-Fi connections, updating software, and reviewing system notifications solve a large proportion of daily issues.

Throughout the module, participants are reminded that troubleshooting is not about perfection or technical mastery — it is about building confidence through familiarity, patience, and a clear sequence of actions. The more users understand how their devices operate, the more they realise that most difficulties are manageable. This perspective reframes troubleshooting from a stressful interruption into a practical life skill that supports independence in all digital activities.

E-LEARNING

ACCESS THE GENIALLY LEARNING UNIT



DESCRIPTION

This e-learning module is designed to empower participants with crucial knowledge and practical skills in cybersecurity and basic troubleshooting.

It covers essential topics from understanding online threats to securing personal devices and data, ensuring a safer and more confident digital journey.

KEY TOPICS

- Phishing & online scams
- Strong passwords & 2FA
- Malware prevention
- Basic troubleshooting
- Data privacy
- Safe online habits

> *"It's never too late to learn how to protect yourself and your data in the digital world."*

USER GUIDE

Navigate through this e-learning module at your own pace. Each section includes clear explanations, interactive activities, and practical tips. Click on icons and buttons to explore additional content, videos, or short quizzes to test your understanding.

Use the module step by step - start with short introductions, then continue to tasks and self-check questions. You can revisit any section as many times as you like. Throughout the module, you'll find examples and tips relevant to protecting your digital identity and devices.

Take notes, reflect on your own experiences, and apply what you learn to enhance your daily online safety and confidence.

WORKSHOP CONCEPT

PART 1: Cybersecurity

DURATION

1 hour and 30 minutes

MATERIALS

Laptops/tablets, projector, sample phishing scenarios, password-strength examples, device security checklist, markers & flipchart.

OBJECTIVE

To strengthen participants' ability to recognise digital risks, protect personal information, interpret suspicious situations, and make informed decisions using practical cybersecurity strategies.

DEBRIEFING

15 mins
Group reflection

What new cybersecurity risk did you learn about today?

How will you apply what you learned to better protect your devices and online accounts?

Facilitator summarizes key takeaways for improving personal digital security and confidence.

AGENDA

10 min – Warm-up: "Digital Risks We Have Seen"
Participants exchange personal experiences with suspicious messages or online threats.

15 min – Cyber Threat Patterns
Comparison of phishing vs. legitimate messages. Identifying warning signs.

20 min – Strong Digital Defences
Reflection on password habits, 2FA, and prioritising high-risk accounts.

20 min – Scenario Exercise: "Would You Trust This?"
Groups analyse real-life cybersecurity scenarios and decide safe next steps.

15 min – Personal Security Audit
Participants review their own digital habits and identify one improvement to implement.

WORKSHOP CONCEPT

PART 2: Troubleshooting

DURATION

1 hour and 30 minutes

MATERIALS

Laptop/tablet per participant, projector, troubleshooting flowchart, example error messages, checklist for “first steps,” post-its.

OBJECTIVE

To empower participants to approach digital issues calmly and strategically, understand what common device problems indicate.

DEBRIEFING

15 mins
Reflection & Feedback

What did you notice about how most technical problems develop?

Which troubleshooting step gives you the most confidence to try first on your own?

How can a structured approach reduce stress when something goes wrong?

Trainer reinforces calm, methodical problem-solving.

AGENDA

10 min – Warm-up: “How I Solve Problems”
Participants reflect on past troubleshooting successes and challenges.

15 min – Understanding Common Causes
Trainer explains typical issues (slow device, connection problems, app errors).

15 min – Troubleshooting Model
Introduction of a simple step-by-step logic for diagnosing issues.

20 min – Diagnostic Scenarios
Groups work through realistic cases and decide what they would check first.

15 min – Hands-On Micro-Practice
Participants perform basic diagnostic checks on their own device.

EVALUATION

1. What is the main purpose of two-factor authentication (2FA)?

a) To make your password longer.

b) To add an extra layer of security to your accounts. ✓

c) To automatically change your password daily.

2. What is considered a strong password?

a) Your birth date or your pet's name.

b) A combination of uppercase and lowercase letters, numbers, and symbols. ✓

c) A word found in the dictionary.

3. What is "phishing"?

a) A fun online game.

b) A type of malicious software.

c) A fraudulent attempt to get your personal information by pretending to be a trustworthy entity. ✓

4. Why is using public Wi-Fi without extra protection (like a VPN) risky?

a) It can slow down your internet speed.

b) Your personal data might be easily intercepted by others. ✓

c) You might accidentally download too many files.

5. What is "malware"?

a) A type of online advertising.

b) Software designed to harm or gain unauthorized access to your computer. ✓

c) A tool for speeding up your computer.

6. Why is it important to regularly update your operating system and applications?

a) To make your device look newer.

b) To fix bugs and improve security against new threats. ✓

c) To use up more storage space.

7. What is the main function of antivirus software?

a) To make your computer run faster.

b) To detect, prevent, and remove malicious software. ✓

c) To help you browse the internet anonymously.

8. What is a "firewall" primarily designed to do?

a) Display pretty backgrounds on your computer.

b) Control network traffic and protect your computer from unauthorized access. ✓

c) Store your photos online.

9. If your computer suddenly becomes very slow, shows unknown programs, or constantly displays ads, what could be the problem?

a) It's probably just old and needs replacing.

b) It might be infected with malware. ✓

c) You have too many tabs open in your web browser.

10. What is a key safe digital habit when working with IT?

a) Clicking on every link you receive in an email.

b) Regularly updating software, backing up data, and being cautious online. ✓

c) Sharing your passwords with trusted friends.

“Always protect yourself. The digital world needs you to be more awake”