

DefendEYourself: What Seniors Across Europe Told Us About Cybersecurity

Our Consolidated International Report is complete and it is shaping everything we build next.

After months of research and fieldwork across five countries, the DefendEYourself project has reached a significant milestone: the completion of our Consolidated International Report on cybersecurity awareness among older adults. In this blog post, we share what we found, what it means, and what comes next for the project.

About DefendEYourself

DefendEYourself is a cooperation partnership co-funded by the Erasmus+ programme of the European Union, bringing together partner organisations from Belgium, Greece, Italy, Lithuania, and Portugal. Our goal is straightforward: to develop practical, accessible, and culturally relevant cybersecurity education for adults aged 45 and above, a population that is increasingly active online yet consistently underserved by existing digital safety resources.

The project is led by Open Education Hub (Belgium) and the consortium consists of six organisations:

- Open Education Hub and ReadLab Brussels (Belgium)
- European Educational Association P.C. (Greece)
- ETS 7Hub (Italy)
- ART+INN / Menas ir inovacijos (Lithuania)
- Casa do Professor (Portugal)

The Research: 635 Participants Across Five Countries

Between late 2025 and early 2026, partners in all five participating countries conducted national surveys targeting adults aged 45 and above. A total of 635 people participated, sharing their digital habits, experiences with cybersecurity threats, confidence levels, and learning needs. The findings from each country were then brought together into a single Consolidated International Report, which now forms the empirical foundation for the training curriculum we are about to develop.

Data collection was deliberately inclusive. Partners reached beyond standard online channels to ensure that those least likely to self-select into a digital survey were still represented. In Greece, the team carried tablets into Citizen Service Centres to assist seniors on the spot. In Portugal, surveys were completed with residents of elderly care homes. In Belgium, the survey was made available in three languages to reach different linguistic communities. In Lithuania, the questionnaire was distributed through community networks across both urban and rural areas. In Italy, participants were reached through adult education networks and local community contacts. Every national team adapted their approach to ensure that the people who most needed to be heard were actually heard.

What We Found

Older adults are not digitally absent; they are digitally unprotected

One of the clearest findings across all five countries is that older adults are not disengaged from the internet. Across all five countries, the vast majority of respondents reported using the internet every day. They manage bank accounts, access healthcare, communicate with family, and interact with government services online. In many cases, they do this not by choice but by necessity: physical alternatives have disappeared. The problem is not that seniors avoid technology. The problem is that they have been pushed into the digital world without the tools to navigate it safely.

The informal support network is not enough

In all five countries, the main source of cybersecurity help for elderly adults is a younger family member, called upon after something has already gone wrong. In Portugal, most respondents rely on family or friends for digital support, and similar patterns were documented in Lithuania and Greece, with similar patterns of informal reliance documented in Belgium and Italy. This informal arrangement is reactive by nature, unavailable at the moment cybercriminals strike, and it prevents older users from ever developing the independent skills they need. Our research confirms what many have suspected: the family as a safety net is not a sustainable solution.

Each country has its own specific threat landscape

One of the most valuable findings of our cross-national approach is the level of detail it reveals about how cybercrime works differently in different countries. In Greece, the dominant threat is fraudulent SMS messages that convincingly mimic national banks and the government portal [Gov.gr](https://gov.gr). In Lithuania, password practices emerge as a significant vulnerability: a large proportion of participants reported reusing the same password across multiple accounts or applying inconsistent practices, meaning a single compromised account can put everything else at risk. In Italy, the key risk pathway runs through WhatsApp and Facebook, where users shift between socialising and sensitive financial interactions without any change in security mindset. In Portugal, many participants reported low confidence in identifying threats and heavy reliance on intuition rather than structured knowledge when assessing online risks. In Belgium, a recurring pattern was recognising that a communication seemed suspicious but not knowing how to respond to it.

This tells us something important for training design: a one-size-fits-all European cybersecurity course will not work. The examples, the platforms, the institutional names, and the scam types all need to reflect the actual digital environment of each country. Localisation is not a nice-to-have; it is a prerequisite for effectiveness.

The target population wants to learn

The research also contains genuinely encouraging news. Across all five countries, most participants indicated openness to learning and many expressed frustration that accessible, age-appropriate resources do not currently exist. In Greece, the majority of respondents expressed direct interest in cybersecurity training, and in Lithuania more than half indicated at least some interest in a dedicated course. In Belgium, Portugal and Italy, participants similarly demonstrated a clear demand for practical, accessible, and confidence-building learning formats. Older adults are not resistant to change. They are waiting for an offer that meets them where they are.

What Comes Next: The Training Curriculum

The next phase of the project will deliver the DefendEUself training course: a series of Micro-MOOCs covering the core domains of digital safety that the research identified as most urgent. The content will be practical, scenario-based, and entirely grounded in the findings of our research. No jargon, no abstract warnings, just clear and usable skills drawn from the real threat landscapes older adults face in their daily lives.

Beyond the training curriculum, the project will continue with further activities aimed at community building, knowledge sharing, and reaching a wider audience across all partner countries. More details will be shared as the project progresses.

We are proud of what the research has produced and grateful to every participant who gave their time to make it possible. The work ahead is **turning evidence into education, and education into safety.**

Co-funded by the European Union. Erasmus+ KA220-ADU. Project No. 2025-1-BE01-KA220-ADU-000350280

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.