# Developing a Junior Cycle Short Course in Cyber Security

## PHASE 1 REPORT

21st October 2022

www.cyberwise.ie

School of Education
College of Computer Science

RISING TO THE FUTURE
UCD Strategy 2020-2024

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

# CONTENTS

# EXECUTIVE SUMMARY

On 14 May 2021, the Health Service Executive (HSE) of Ireland suffered a major ransomware cyberattack which caused most of its IT systems nationwide to shut down. It was the most significant cybercrime attack on an Irish state agency and the largest known effective attack against a health service computer system. This coupled with the move towards remote working and learning using digital technologies in response to the COVID-19 global health emergency has further rendered individuals and society as a whole extremely vulnerable to cybercrime. This increasing reliance on digital technologies that are cyber secure has led to calls for the education system to address cybersecurity so that our young people are prepared for the modern world.

To facilitate the development of cyber resilience education, the current National Cyber Security Strategy (GOI, 2019-2024) seeks to "support the development of a Junior Cycle short course in cyber security, which will provide for the inclusion of cyber security education in second level" (Ibid, Measure 12:4, p. 39). Following consultations with the National Council for Curriculum and Assessment (NCCA), the Department of the Environment, Climate and Communications (DECC) facilitated the establishment of a cross-sectoral multi-disciplinary working group to develop the Junior Cycle Short Course and pilot its implementation. The working group was educational stakeholder led, under the chair of Prof. Joe Carty of University College Dublin and comprised representatives from the Computers in Education Society of Ireland (CESI), the NCCA, Cyber Ireland, the National Cyber Security Centre (NCSC) and the DECC. A representative of the Department of Education was invited to attend meetings of the working group as an observer. The working group was also supported by a team of teacher educators and researchers from UCD School of Education to implement the project. The UCD project team developed the short course specification, arranged webinars and developed units of learning to support teachers, piloted the short course in a diverse range of 10 post-primary schools nationally in 2021/22, developed a course website and organised a shared learning day in UCD in May 2022 (see appendix for details).

A bespoke website **www.cyberwise.ie** has been created where the short course specification and associated lesson ideas, units of learning and sample student-centred resources are freely available to the wider community. In addition, this website also serves as a digital hub for teacher professional development and an interactive online forum and community of practice for participating schools and teachers.

The short course was developed on a modest budget (i.e. less than € 15,000) along with contributions in kind from the UCD School of Education. The pilot implementation with schools has only taken place to date over 1 year of the 3-year Junior Cycle timeframe. It is recommended that the pilot implementation be extended by a further 2-years to enable it to become embedded in participating schools and to provide for extensive feedback for more effective evaluation of the impacts of the short course. The extended pilot will also give space to address the sustainability question. Furthermore, while this report will be a key input to the midterm review of the current National Cyber Security Strategy in Autumn 2022, the extended pilot to the end of the current Strategy in 2024 will facilitate the opening up of broader questions regarding how cybersecurity is being accommodated in education curricula at first, second and third levels.

# INTRODUCTION

Arising from stakeholder consultations that took place in 2019 in the compilation of the current National Cyber Security Strategy, the need to address the skills shortage in cyber security was emphasised by many industry commentators. While this was largely manifested in the need for more educational courses involving upskilling and apprenticeships after the Leaving Certificate, an earlier stage intervention akin to the experience with the Junior Cycle Short Course on Coding was suggested. The resultant was a commitment to support the development of a Junior Cycle Short Course in cyber security in the National Cyber Security Strategy 2019-2024.

This report is intended to take stock of the development of the Short Course in cyber security and provide some guidance as the next steps on sustaining this initiative. It recognises the extensive work of the UCD project team from the School of Education in realising this initiative under the guidance of the cross-sectoral multi-disciplinary working group of representative stakeholders.

In particular, this report outlines the background to the development of the working group and the design and implementation team, resourcing to date, details of the short course development and associated activities, details of the state of the deployment of the course and the key learning, recommendations and next steps.


Minister Smyth pictured with participating teachers and students at the shared learning day in UCD in May 2022

# BACKGROUND

DECC is the lead Government Department for cyber security in the State. It oversees the implementation of the National Cyber Security Strategy 2019-2024. A key theme of the Strategy centres on developing the capacity of the State, research institutions, businesses, the public sector and of the people to both better understand and manage the nature of the challenges we face in this space. ln particular, measures 12 of the Strategy include actions on developing cyber security education in second level education as outlined in table 1. below.

| **Measure 12: Government will continue to ensure that second and third level training in computer science and cyber security is developed and deployed, including by supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.** | | | |
|---|---|---|---|
| Actions for Delivery | Timeline by Quarter | Lead | Key Stakeholders |
| Support the development of a Junior Cycle short course in cyber security, which will provide for the inclusion of cyber security education in second level. | Q4 2020 | NCSC | NCCA |

In Spring and early Summer of 2020, discussions took place with the NCCA on how to realise this objective of a developed Short Course in Cyber Security. The resultant was an agreed scoping document that recognised the primacy of an education stakeholder led approach.

In establishing a consultative working group of stakeholders in July 2020, it was stated that the underlying objective of the Short Course was to provide for broadly based cyber security education with a multidisciplinary approach encompassing aspects of psychology, law, ethics, communications and crisis management as well as computer science. In the context of digitalisation of society, all students, regardless of gender and not just those with STEM aptitudes need to be familiar with resilience and security in the online world. The course should also influence the content of and could lead to greater uptake of the curriculum subject Computer Science in Senior Cycle. The course needs to be sufficiently appealing to schools and distinct from alternative short courses

# WORKING GROUP

DECC facilitated the establishment of a consultative working group comprising an interdisciplinary team chaired by Professor Joe Carthy from UCD School of Computer Science. Members from the NCSC, Cyber Ireland, the NCCA, and CESI provided technical, industry, educational and curriculum development insights respectively. The Department of Education was also invited to join the working group in an observer capacity. The full working group is listed below with full biographies in the appendix.

## WORKING GROUP MEMBERS

| | |
|---|---|
| James Caffrey | Department of Environment, Climate and Communications (DECC) |
| Professor Joe Carthy | School of Computer Science, UCD |
| Ruaidhri Fernandes | National Cyber Security Centre, (NCSC) |
| Pat Seaver | Computers in Education Society of Ireland (CESI) |
| Neil Butler | Computers in Education Society of Ireland (CESI) |
| John Hegarty | Computers in Education Society if Ireland (CESI) |
| Paul Behan | National Council for Curriculum and Assessment (NCCA) |
| Carmel Somers | Technology Ireland ICT Skillnet, Cyber Ireland Representative |

The working group was tasked with:

1. Developing the short course specification using the template provided by the NCCA and in accordance with the scoping document. The course specification should be flexible and adaptable enabling as wide a range as possible of schools, teachers and students to take up the course;

2. Identifying the essential resource requirements for schools undertaking this course, including training supports and providing practical solutions on how such requirements could be met for a pilot implementation in a small, yet diverse number of secondary schools;

3. Overseeing the pilot implementation of the short course, monitoring developments and providing high level support where necessary and appropriate;

4. Evaluating the short course pilot implementation in schools and providing for feedback with lessons learnt regarding course content and delivery, and;

5. Reviewing implementation of the short course by mid-2022 and making recommendations regarding the further development of a cyber security course at Junior Cycle that can be made available to schools.

It was agreed that a project team would be needed to implement the Short Course development project under the guidance of the consultative working group. The working group approached UCD School of Education in Autumn 2020 to support the design and implementation of the short course.

## DESIGN AND IMPLEMENTATION TEAM

UCD School of Education has a proven track record in Democratic Pedagogical Partnerships (Farrell, 2021) and is at the forefront of technology enhanced learning in Initial Teacher Education. The multi-disciplinary UCD design and implementation team is outlined below with full biographies in the appendix.

| | |
|---|---|
| Dr Rachel Farrell | PME Programme Director |
| Karen Maye | School Placement Lead and Head of PME Outreach Initiatives |
| Liam Fogarty | Technology Enhanced Learning Manager in the College of Social Science and Law at UCD |
| Marelle Rice | Philosophy for Children Expert |
| James Doyle | PME Digital Technology Lecturer |
| Declan Qualter | LOETB Schools' Support Coordinator |
| Seamus Knox | Maths and Physics PME Lecturer |
| Mark Baldwin | Web Developer |


Minister Smyth pictured with the working group and project implementation team at the shared learning day in UCD in May 2022

# SHORT COURSE DEVELOPMENT

## AIMS OF THE SHORT COURSE

The working group and design and implementation team first met in October 2020 bringing together expertise from the worlds of cyber security and education and this allowed for the following aims of the course to be clearly identified that would not only engage teachers and learners but would allow for a specification that had the flexibility to respond to future developments in the world of cyber security including:

- Design learning outcomes that build on the key skills of Junior Cycle and will appeal to a broad spectrum of students and teachers.
- Design a course that can respond to changes in the world of cyber security.
- Encourage students to solve problems directly related to their own life.
- Develop the student voice so students can actively contribute to and support the development of school policies around cyber safety.
- Foster critical reflection
- Assessment that allows for choice and encourages students to reflect on new learning and see the implications for their own lives, schools, or for society as a whole.

## APPEALING TO A BROAD SPECTRUM OF LEARNERS

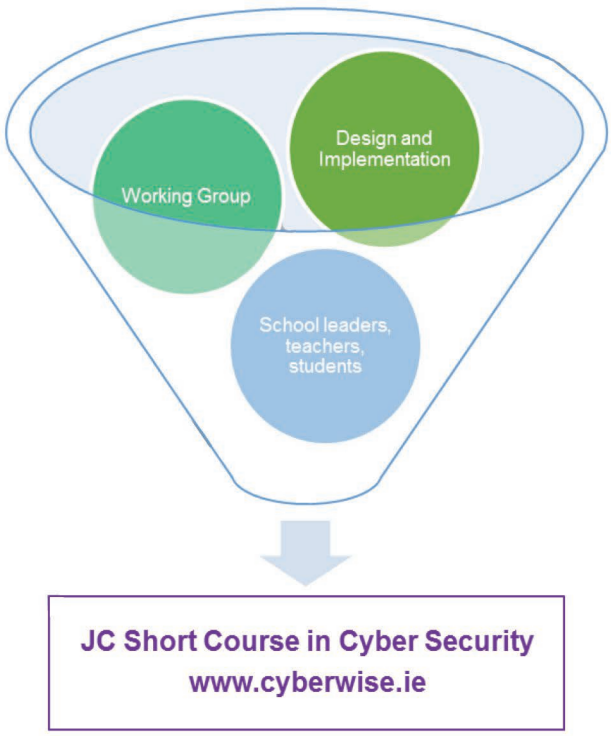
One of the initial directives for this initiative was to design a course that would incorporate the key skills of junior cycle and would appeal to a broad spectrum of students and teachers. As such the working group and design and implementation team do not view this short course as a niche course designed for those teachers and students who already have a keen interest in computer science or digital technology. The specification has been designed so that any teacher, regardless of their subject specialism, can facilitate the delivery of this course. This creates opportunities for the course to be adapted and developed as teachers use the lens of their own subjects such as history, economics, politics, science, maths etc. to develop cross-curricular links to plan lessons that will engage and challenge learners in an interesting and non-threatening manner.

## DEVELOPMENT OF SPECIFICATION

Having established the aims of the course the design and implementation team carried out a review of national and international policies and guidelines on cybersecurity education that informed the design of the course. This allowed for the design and implementation team to identify key themes and develop them as “strands” of the course. These initial iterations of the course were presented to the working group for feedback and discussion. Inputs from all members of both groups were also facilitated via the forum of a shared document where members could suggest learning outcomes, possible learning intentions, classroom activities, stimuli, and websites that were relevant to the cyber security in Ireland. This allowed for the various elements to be expanded or refined and, importantly, for the course to be viewed from the unique context of cyber security as an Irish citizen as well as international perspectives.

Teachers from a range of subject specialisms and schools then developed trial lesson plans detailing learning intentions, assessments, and student activities in response to the learning outcomes on the specification that appealed most to them. This allowed the design and implementation team to tease out what the course might

look like in the Irish classroom and see how the teachers would connect the strands together. The potential for a learning outcome to engage students in active learning and provide opportunities for students to engage in their own research on topics and make connections to their own lived experiences was assessed and this allowed the team to further refine the specification and ensure it was addressing the aims of this initiative.




## RECRUITMENT OF SCHOOLS TO THE PILOT PHASE (SEPTEMBER 2021 - MAY 2022)

10 post-primary schools were recruited to trial this course with junior cycle students for the academic year 2021 to 2022. A purposive sample of schools was selected so that a diverse range of school patronage bodies and contexts were represented see appendix for full details. This included interventions to seek to address the policy challenge of insufficient female participation in cyber security.

## SUPPORT FOR TEACHERS

The design and implementation team were responsible for planning and delivering a programme of professional development and support for teachers participating in the pilot phase of the project. This took the form of blended learning with resources and documents being made available to teachers via a shared online web resource. The team also facilitated a series of live webinars that would allow teachers to collaborate on lesson plans and units of learning together and learn from the experiences of each other and ultimately uild a professional learning community (PLC) together.

| Support for Teachers | | |
|---|---|---|
| **Materials** | **Professional Development** | **Shared Resources** |
| Lesson planning tools - long term and short term<br><br>Unpacking learning outcomes, linking to other specifications<br><br>Stimuli for class discussion and debate<br><br>Resources designed to foster inquiry based learning | 6 x Webinars<br><br>Philosophy for Children training | Maintained and updated consistently<br><br>Library of resources and relevant literature<br><br>Units of Learning<br><br>Artefacts of Learning |

## TEACHERS' NEEDS INFORMING DESIGN

Initially it was envisaged teachers would agree to plan lessons around particular learning outcomes from the specification and then share their work and their experience with the rest of the group. In this way the teachers would "jigsaw" together a series of lessons and resources. However, the impact of the Covid-19 pandemic during the winter of the pilot phase on teachers' workloads and wellbeing proved challenging. Teachers struggled to attend webinars consistently and many reported feeling overwhelmed by the prospect of planning a new course, the content of which many were not familiar with.

The UCD team responded to this by developing units of learning that would be easy for teachers to navigate as well as being easy to adapt and mix and match with other units of learning so the teacher could tailor lessons for the specific needs of their own classroom. These units of learning then acted as a blueprint for teachers to design their own units of learning. This established a consistent format so that when teachers did share units of learning they were easily understood by their peers.

## UNITS OF LEARNING

Mindful of the time pressures on teachers, accessibility and coherency were identified as key features in the design of the units of learning. The team were also cognisant that teachers readily refine and adapt any resource they use for the needs of their own learners so developing resources that would be overly prescriptive would undermine this.

All of the units of learning follow the same format; a single document with a series of activities that act like "stepping stones" that navigate the learning outcomes. All resources are embedded in the document to make it easy for teachers to scan and the documents can be edited when downloaded so teachers can mix and match different elements and create their own lesson plans and schemes of work. These units of learning were "road-tested" by teachers in their classrooms who then shared their reflections on it with the pilot group of teachers

during online webinars. This helped form a shared understanding of how the units of learning were designed and their potential to be adapted for different year groups and abilities and the following features were identified as core elements for each unit of learning.

- Teacher as facilitator
- Student led enquiry-based
- Stimuli to prompt questions and debate.
- Project work
- Group work with roles and responsibilities for all students
- Creativity in problem solving and presentation skills.
- Teacher and peer assessment that focuses on identifying how the student's thinking has changed and how that learning will influence the next unit of learning.
- Student reflection to connect learning to their own lived experiences.

The following Units of learning that have been developed and "road tested"

- Case studies of cyber events/cyber crimes
- Social engineering - modern day con artists
- Data is the new oil - could your life online help design a new product? bring down a government?
- Black Hats and White Hats - careers in cyber security
- Women in cybersecurity

The Units of learning below are currently in development:

- Securing your online world - passcodes, firewalls, backing up
- Cyber Incident Response/Crisis Management
- What is the economic cost of cybercrime?
- Cyber psychology
- Cyber security in film study
- What if scenarios e.g. if Explosive Ordinance Disposal robots are sabotaged etc.

An extension in the pilot would enable the further development of Units of Learning.

## ASSESSMENT

Assessment strategies are informed by the NCCA Toolkit for Assessment. Students will be required to complete one classroom-based assessment (CBA). It is envisaged that the CBA should encourage students to reflect on new learning and see the implications for their own lives, schools, or for society as a whole. As such, it should promote and reward the following elements.

- Project based.
- Inquiry-based learning
- Cross-curricular links to other Junior Cycle subjects.
- Allow for students to choose the most appropriate means of communicating their project.
- Identification of an action (or actions) they have taken as a consequence of their learning.

- Connections to the students' own lived experience and the context of cyber security in Ireland.
- Features of quality identified and used to create a rubric for deciding on the level of achievement.

## WEBSITE DEVELOPMENT - *www.cyberwise.ie*

The Cyberwise.ie was officially launched at the shared learning day in May 2022 and now acts as the online platform for the resources and support for teachers developed during the pilot phase of this initiative. In addition, the website serves as a repository of artefacts of students' learning that demonstrate the potential of the course to engage and challenge students with a diverse range of interests and aptitudes.

## TEACHER COLLABORATION

The emphasis placed on collaboration and sharing learning during the pilot phase of this initiative enabled the cross-pollination of these ideas and indeed the potential of pedagogies such as inquiry-based learning, philosophy for children, and cooperative learning to foster student engagement to be explored. It is hoped that this ethos of sharing learning and examples of good practice will be sustained through the model of the shared learning day held in May 2022 and the forum on the website www.cyberwise.ie where teachers and students can not only access resources for lessons and view artefacts of learning but can also continue to contribute to the development of resources and artefacts as an ongoing endeavour.

## SHARED LEARNING DAY

In May 2022, 300 students and their teachers who had participated in the pilot phase of this initiative came to the O'Brien Centre for Science in UCD for a shared learning day. This day also allowed the team to launch the website www.cyberwise.ie. Students exhibited their projects, attended talks and learned about the diverse range of careers that exist in cyber security from experts working in the field in Ireland. Moreover, the students and teachers addressed the audience and shared their learning from the project and the impact their participation in the pilot phase had on their own learning and mindsets. See appendix for further details.

## TIMETABLING FOR A SHORT COURSE: THE COVID-19 PANDEMIC

The pilot was initiated in schools in September 2021. The subsequent months coincided with the Irish education system trying to meet extraordinary challenges as a result of the Covid-19 pandemic. High levels of staff and student absenteeism as a result of rising levels of infection meant teachers and school leaders were under enormous pressure to cover for absent colleagues. Teachers' workloads increased as they strived to ensure students who had to self-isolate or were unwell and unable to attend school could follow lessons online or "catch up '' with their peers when they returned to school. Guidelines for social distancing meant that pedagogies, such as group work and cooperative learning, that were being advocated as means of delivering the course were hampered and alternative ways for students to work together in groups using digital technology had to be identified. Teachers reported high levels of exhaustion as a result of these challenges and indeed many were dealing with the impact of the pandemic on their own families and on themselves personally. Many

teachers participating in the study were often unable to attend the webinars as a result of these demands. In response to this we recorded webinars and shared recordings with all participants. Those teachers that did attend the webinars expressed that they simply did not have the capacity to start designing lesson plans and units of learning from scratch and that they needed more support and guidance in this regard. This prompted the UCD project team to develop units of learning that would be easy for teachers to navigate as well as being easy to adapt and mix and match with other units of learning so the teacher could tailor lessons for the specific needs of their own classroom.

Minister Smyth speaking to Ciara Molloy and pupils from St. Colman's National School, Mucklagh, Offaly (LHS) and students from Stepaside Educate Together (RHS)


Arushi Doshi, senior cybersecurity consultant at Deloitte Ireland

# KEY LEARNINGS FROM THE PILOT

The importance of listening to and accommodating the needs of students, teachers and schools was a central theme. In particular the following was of particular relevance:

- **Getting "buy-in".** Schools need to believe in the potential for initiatives to address needs in their own school. Demonstrating that a short course can form cross-curricular links thereby supporting other subjects and appeal to a diverse range of learner interests and promoting a more inclusive classroom were key selling points for schools.

- **Teachers' needs informing design.** Actively listening to teachers when they spoke of the challenges they anticipated or had experience with this implementation of this course in their classroom was a key element of their continued participation and the continued participation of their students and ultimately the success of the pilot phase of this project.

- **"At a glance" documents.** Designing resources that were consistent in their format and easy to scan made them more coherent and accessible for teachers and students alike. The units of learning developed during the pilot were formatted consistently. Rather than each unit of learning consisting of a series of folders of lesson plans and resources, each unit consists of one document that included all the templates and worksheets as well as links to video clips and relevant websites and no unit of learning consisted of more than two pages. See appendix for examples.

- **Importance of fostering collaboration.** Acknowledging the challenges facing teachers and responding to them built strong collaborative relationships that allowed for robust debate and a rigorous review of the specification and associated resources as it was piloted.

- **"Out of the mouths of babes…"**. Student voice be it through artefacts of learning, exhibits, or presentations is a persuasive tool for convincing school leaders, teachers, and parents of the value of an initiative. Investing in a forum such as the shared learning day held in UCD is a valuable means of bringing the experiences of students together to not only celebrate them but to learn from them and promote an initiative.

# RECOMMENDATIONS: NEXT STEPS

This report on the pilot implementation of the Short Course is timely given the imminent review of the National Cyber Security Strategy. A key recommendation emerging from this pilot is that there is a need to address other aspects of cybersecurity education that the Department of Education could engage with. This could include the role of cybersecurity awareness and problem solving in senior classes of primary education and senior cycle of second level education. Further to this a list of recommendations and next steps are listed below.

Recommendations for the phased scaling up of the implementation of the junior cycle short course are outlined below according the three broad themes 1. School engagement 2. Teacher Support and 3. Awareness Raising.

1. **School Engagement**

- Strategic **recruitment of schools** in clusters in collaboration with Education & Training Boards and other school patronage bodies
- Work with a sample of schools and the Dept. of Education Inspectorate to see how this Short Course can be implemented as part of the suite of wellbeing support in schools currently being implemented via a school self-evaluation (SSE) approach from 2023 to 2028

2. **Teacher Supports**

- Further development of a blended programme of continuing professional development for teachers in collaboration with teacher support services, Education & Training Board of Ireland and Education Support Centres Ireland.
- Cascade model of teacher professional development and shared learning whereby teachers are supported to lead local communities of practice.

3. **Awareness Raising**

- Collaboration with the NCCA to have the specification visible on the NCCA list of JC short courses
- Strategic alliances with school management bodies such as National Association of Principals and Deputy Principals to provide information and support to school leaders to implement the short course
- Capitalise on Cyber Security Month1 by developing standalone activities for projects during this period.
- Awareness campaign - aided by the Adventures in Cyberland initiative funded by Public Service Innovation Fund - peaking during Cyber Security Month.

Furthermore, there are a number of synergies with existing initiatives that can be further explored for the promotion and further development of the Junior Cycle Short Course, namely:

- The Public Service Innovation Funded initiative, Cyber Resilience Education for Primary & Post-Primary Schools (CREPS): A Collaborative and Innovative Cyber Security Outreach Programme. Details are set out in the appendices.
- Initiatives by Cyber Ireland
- Science Foundation Ireland discover projects on equality, diversity and inclusion in cybersecurity.

[1] Generally October each year

# FUNDING AND MODEL OF SUPPORT FOR THE EXPANSION OF THE PROGRAMME

The development of the Junior Cycle short course to date has been funded by €5,000 from DECC and €10,000 from the School of Computer Science and by cash and in-kind contributions from UCD School of Education to the value of €20,000. A further € 20,000 is being provided by DECC to facilitate an extension of the pilot implementation for a further 2 years to mid-2024.

The establishment the UCD Centre for Cyber Resilience Education in Primary and Post-Primary Schools (CREPS) funded by Public Service Innovation Fund (PSIF) will ensure that the future development of this junior cycle short course will be enhanced in a sustainable way. This involves an infrastructure that will include technical, educational and research supports through an interdisciplinary advisory board and relevant admin and academic staff. The PSIF is not directed at JC but is bringing some of the learning from the JC to a wider audience and in doing so generating interest, creating awareness, building skills and capacity and creating resources that can be adapted to JC so that there is a learning loop and some synergy but not duplication.

The UCD design and implementation team have applied for SFI funding for an initiative entitled: Enquiry, Diversity and Inclusion: Busting the Bias in STEM careers and part of this initiative will look at the role of women in cybersecurity and computer science which aligns with the goals of this initiative.



Marelle Rice and Ciara Molloy pictured at Féilte 2022

# CONCLUSION

The pilot implementation of the Junior Cycle Short Course appears to have been very successful. However, a longer period of time is needed to enable the pilot to be fully embedded with participating schools and for quantitative and qualitative feedback on the impacts. Furthermore, the sustainability question needs to be addressed as any short course in cyber security needs to be regularly updated, with schools and teachers supported on an ongoing basis.

A sustainable funding model for this future development and maintenance of the Junior Cycle Short Course would need to include contributions from a number of sources, namely industry as well as from the public sector. A shared resourcing or collective sponsorship from a group of industry players to contribute to this education driven initiative would be preferable to promotion of particular platforms and technologies by specific large corporates. A capital grant-based model, which may include the option of EU co-funding, could be explored for the public sector contribution.

The short course was developed on a tiny budget (i.e. less than € 15,000) along with contributions in kind from the UCD School of Education. The pilot implementation with schools has only taken place to date over 1 year of the 3 year Junior Cycle timeframe. It is recommended that the pilot implementation be extended by a further 2 years to enable it to become embedded in participating schools and to provide for extensive feedback for more effective evaluation of the impacts of the short course. The extended pilot will also give space to address the sustainability question. Furthermore, while this report will be a key input to the midterm review of the current National Cyber Security Strategy in Autumn 2022, the extended pilot to the end of the current Strategy in 2024 will facilitate the opening up of broader questions on how cybersecurity is being accommodated in education curricula at first, second and third levels.


Karen Maye pictured at Féilte 2022

# APPENDICES

## APPENDIX A: PARTICIPATING SCHOOLS

Coláiste Choilm, Tullamore, Co. Offaly.

Killina Presentation Secondary School, Rahan, Co. Offaly.

Presentation College, Co. Carlow.

Sacred Heart School Tullamore, Co. Offaly.

St. Oliver's Community College, Drogheda, Co. Louth.

Oaklands Community College, Edenderry, Co. Offaly

Gort Community School, Co. Galway

Clarin College, Athenry, Co. Galway

Clongowes Wood College, Co. Kildare

Coláiste Éamann Rís, Co. Cork

# APPENDIX B: SCHOOL THAT HAVE BEEN RECRUITED TO EXTEND THE PILOT IN 2022/23

St. Andrew's College, Co. Dublin.

Blackrock College, Dublin.

St. Colman's NS, Mucklagh, Co. Offaly.

Stepaside Educate Together Secondary School, Co. Dublin.

St. Fergal's College Rathdowney, Co. Laois.

Woodbrook College, Bray, Co. Wicklow

St. Fergal's College, Rathdowney, Co. Laois.

Tullamore College, Co. Offaly

Portlaoise College, Co. Laois

Ard Scoil Chiaráin Naofa, Clara, Co. Offaly

Bannagher College, Co. Offaly

# APPENDIX C: TIMELINE FOR INITIAL PILOT PHASE

October 2021: Initial meeting with DECC, School of Computer Science, UCD, and the School of Education, UCD.

November 2021- December 2021: School of Education, UCD team develop outline of specification for the short course in cyber security and potential strands and learning outcomes.

January 2021: Big picture overview of the specification with learning outcomes for 2 of 3 strands presented by the School of Education, UCD for review by the working group.

February 2021: Begin recruitment and selection of schools for the pilot phase.

June 2021: All strands of the specification presented for review by the working group.

September 2021: Pilot schools begin to implement the short course in the classroom.

September 2021 - May 2022: Ongoing support offered to participating schools through webinars facilitated by the School of Education in UCD.

January 2021 - May 2022: Website development

May 2022: Shared Learning Day held in UCD.

May - June 2022: Review of pilot and report submitted.

# APPENDIX D: INITIAL DRAFT OF THE SPECIFICATION FOR THE JUNIOR CYCLE SHORT COURSE IN CYBER SECURITY

| *Unifying Strand* | **Ethics** | | |
|---|---|---|---|
| | 1. Identify/Refine/Create Ten Commandments of Cyber Ethics **Understanding the landscape of Cyber Security** | 2. Ethical Dilemma, grey areas | 3. Discuss ethical behaviour in online context |
| Strands | Cyber Security Fundamentals | Cyber Crime (Political Gain/ Financial Gain) | Opportunities & Challenges of Cyber Security |
| Elements | How do we define cyber security?<br>Passwords – what constitute strong password<br><br>They understand that things need to be secured | Discuss historical cyber crimes<br>Freedom fighter or criminal?<br>Hacktavisit<br>Nation State | Role of regulation<br>i.e. role of unbreakable encryption |
| | Keeping email safe | Explain rationale for a cyber attack | Voluntary Vs Mandatory Regulation |
| | Safe use of social media<br>Cyber hygiene<br>Multi Factor authentication<br>How your data is processed by social media | Communication and Crisis Management | School Policies |
| | Psychology | Psychology | Psychology |
| | Legislation | Legislation | Legislation |
| Assessment | CBA<br>4 inquiries? Resources Share the learning<br>Examples that inspire rather than prescribe. Risk assessment/Audit of own device/audit of cyber risk in home/ or Parents device<br>Career investigation | | |

# APPENDIX E: WORKING GROUP MEMBERS' BIOGRAPHIES

**Professor Joe Carthy, School of Computer Science, UCD, Chair of Working Group**

Joe Carthy is a professor of Computer Science at UCD. He was Dean of Science for 10 years until 2021. He was the founding Director of the UCD Centre for Cybersecurity and Cybercrime Investigation which has established strong links with Europol, Interpol, UNODC, and the Irish Banking Federation. Professor Carthy has a strong record in winning funding for research. He has also supervised/co-supervised 14 PhD and 19 MSc Research students to completion. He also leads the UCD in the Community initiative which mobilises UCD staff and students in volunteering activities in communities in Ireland.

**James Caffrey, Department of Environment, Climate and Communications (DECC)**

James Caffrey, Staff Engineer has been in the Department of the Environment, Climate & Communications working on cybersecurity since 2012. Originally seconded into the NCSC, he has since led on policy development work with the NIS Directive and more recently with EU negotiations on the forthcoming NIS2 Directive. After 3 years in Brussels with the European Commission on cybersecurity policy development, he returned in 2020 to assist with coordination and implementation of the National Cyber Security Strategy 2019-2024. In that regard he is focused on delivery of skills development, gender diversity, enterprise engagement and realisation of research and educational initiatives.

**Ruaidhri Fernandes, National Cyber Security Centre, (NCSC)**

Higher Executive Officer in the NCSC within the Department of Environment, Climate & Communications since 2018. Working between the NIS Directive compliance and Engagement teams. Assigned to support James Caffrey on the development of a Junior Cycle short course in cyber security. Co-ordinator for European Cyber Security Month.

**Neil Butler, Professional Development Service for Teachers (PDST)**

Neil Butler is a maths and SEN teacher currently seconded (from North Wicklow Educate Together Secondary School) to the PDST as an advisor for Leaving Certificate Computer Science. In his time at North Wicklow Educate Together Secondary School he was the head of Maths, SEN Coordinator, and IT Coordinator. Neil's interests include the use of data to inform practice in schools, citizenship through empowerment via technology, creative coding, gamification of learning, and computational thinking in the classroom.

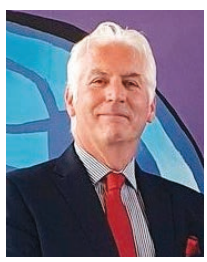
### Carmel Somers, Technology Ireland ICT Skillnet

Carmel is an Organisational Psychologist and is Technology Ireland ICT Skillnet's Human Capital Strategist supporting organisations in Ireland develop and implement their future of work strategies. Prior to joining ICT Skillnet, Carmel held a number of senior roles in research & development, consulting services, operations and "technology for good" at IBM. Carmel is chair of Technology Ireland ICT Skillnet's Cybersecurity Skills Initiative (CSI), and a member of the board of Cyber Ireland where she leads the Talent & Skills working group. In addition, she is a member of the Education and Skills working group of Blockchain Ireland and a member of the External Advisory Board of the Irish Institute of Digital Business (DCU).

### John Hegarty, Computers in Education Society if Ireland (CESI)

John Hegarty has been teaching computing and ICT for over 30 years at second level. He is a member of CESI and promotes the use of open source software in education. He was involved in phase one of the rollout of Leaving Certificate Computer Science and teaches the Junior Certificate Coding short course.

### Pat Seaver, Computers in Education Society of Ireland (CESI)



Pat Seaver has over thirty years experience in teaching, curriculum innovation and teacher professional development.  His main area of interest is leveraging technology to promote more effective learning.

### Paul Behan, National Council for Curriculum and Assessment (NCCA)

# APPENDIX F: DESIGN AND IMPLEMENTATION TEAM BIOGRAPHIES

### Dr Rachel Farrell, School of Education, UCD

Dr Rachel Farrell is Assistant Professor of Initial Teacher Education (ITE) and the Director of the Professional Master of Education Programme (PME) in the School of Education at University College Dublin. Rachel's main research interest is in the area of Democratic Pedagogical Partnerships and Expansive Learning in Initial Teacher Education (ITE). Rachel has led many collaborative initiatives including: effective use of immersive technology in post-primary education with SchooVR, an evaluation of digital portfolios in ITE with MS Education Ireland, cyber resilience education with the Department of the Environment Climate and Communications (DECC), Equity, Diversity and Inclusion: Changing Mindsets/Impacting Futures in STEM funded by SFI and supported by the Professional Development Services for Teachers and the PDST Young Economist of the Year national awards for post-primary students in association with member universities of the Irish Economics Association (IEA), Central Bank of Ireland, Irish Economic and Evaluation Service (IGEES), and Business Studies Teachers' Association of Ireland (BSTAI). Rachel is also involved in a number of Erasmus + Teacher Academy Projects including Supporting Teachers who Support Student Transitions - https://supportingstart.eu/ and Teaching Sustainability - https://tu-dresden.de/zlsb/forschung-und-projekte/tap-ts?set_language=en

### Karen Maye, School of Education, UCD

Karen Maye is the School Placement Lead and Head of PME Outreach initiatives in the School of Education of UCD and is the project manager of the design and implementation of the Short Course in Cyber Security for Junior Cycle Initiative. Karen is passionate about education and its ability to transform the lives of students. Informed by her belief in the principles of social justice and equity, this passion has been her motivation in her role as a classroom teacher, a leader of professional development nationally with the National Induction Programme for Teachers, and in her roles as a tutor, supervisor, and lecturer in ITE in UCD and the Professional Diploma in School Leadership in UL. Karen's research interests include mentoring and coaching, gender in STEM, and teacher professional development.

### Marelle Rice, School of Education, UCD

Marelle has worked in the UK as Head of Religion, Philosophy and Ethics in both the state and independent sectors and has also been active in teacher professional development and was a SAPERE accredited Philosophy for/with Children (P4C) teacher trainer in the UK for many years. Co-founder and Director of Philosophy Ireland and Director of The Thinker's Midwife, her work with the NCCA on the Philosophy Short Course brought her back to Ireland in 2017 and she wears a number of hats as she supports the development of Philosophical Inquiry and IBL in all areas of the Irish education system. She is a PME lecturer at UCD, Co-Project Manager on the SFI funded project; 'Girls in DEIS Schools: Changing Attitudes, Impacting Futures in STEM', which was shortlisted by the Teaching Council for their Teachers Inspire Award for Teacher Collaboration in September 2019. In her role as a JCT Associate, Marelle is responsible for the design and delivery of the Philosophy Short Course CPD. As a freelance consultant, Marelle works with a wide range of educational institutions and organisations to bring philosophy and P4C to a wide range of curricular areas at primary, post primary and third level.

### Mark Baldwin, School of Education, UCD

Mark Baldwin is an immersive technology in education expert and works on the PME programme supporting the implementation of VR/AR in schools. He is the cyberwise.ie web designer.

### Liam Fogarty, School of Education, UCD

Liam is the Technology Enhanced Learning Manager in the College of Social Science and Law at UCD, providing support and guidance on the design and delivery of online and blended learning for the School of Education. A qualified teacher, Liam has a pedagogy-first approach to educational technology. As one of the project leads for the School of Education's National Online Training Programme for SNAs, Liam received a Teaching and Learning Award for outstanding contribution to student success.

### Declan Qualter, LOETB

Declan Qualter is the Schools' Support Coordinator working with Laois and Offaly Education and Training Board (LOETB). He is on secondment from his role as Guidance Counsellor and teacher of Business Studies in Portlaoise College. He is a former seconded advisor with the PDST and associate with JCT and NIPT. His current role involves creating opportunities for collaborative professional learning and supporting schools with initiatives and programmes related to teaching, learning, and assessment. Declan also is the project coordinator for two Erasmus+ Small Scale Partnerships which focus on supporting teachers and school leaders to address digital transformation. Declan is also a PhD candidate in the UCD School of Education. His area of research is on assessing the impact of an intervention programme for parents in supporting their children with digital learning.

### James Doyle, School of Education, UCD

James is a teacher of Business, Maths, and Economics at St. Andrews College Dublin and is a Digital Technology and Economics Methodologies Lecturer in the School of Education in UCD.

# APPENDIX G: THE JUNIOR CYCLE SHORT COURSE FOR CYBER SECURITY "AT A GLANCE" DOCUMENT

| Unifying Elements | Strand 1 Exploring Cyberspace | Strand 2 Cybersecurity Solutions | Strand 3 Cybersecurity in a Global Village |
|---|---|---|---|
| **Philosophy of Cyber Security**<br>Recognise the interdisciplinary and complex nature of cyberspace and the personal, local, national and global role it has in our lives.<br><br>Critically engage, evaluate and reflect on the implications cyberspace has for privacy, security and freedom.<br><br>Collaboratively create, inquire and reflect upon philosophical questions that arise when exploring cyberspace and cyber security.<br>**Careers in Cyber Security**<br>Investigate career opportunities in cyber security.<br><br>Identify qualities, skills, and qualifications that are suitable for a career in cyber security.<br><br>Evaluate if a career in cyber security is of interest to you.<br><br>Examine the portrayal of people in cyber security<br>**The Psychology of Cyber Security**<br>Internet psychology<br>Cyberpsychology<br><br>How has society changed after an event?<br><br>Why do people engage in threatening behaviour in cyberspace? | **Making Sense of Cyberspace**<br>Consider the variety of uses of digital technologies for individuals, communities, businesses and governments that make up cyberspace.<br><br>Discuss the core functions of cyber security and appreciate its importance in society.<br><br>Understand the concept of cyber hygiene and the key steps for good cyber hygiene<br><br>Explore the role of codes in cyber security (data compression, cryptography, error detection and correction, data transmission and data storage) | **Who goes my way?**<br>Explore the historical role of passwords and encryption to secure valuable information.<br><br>Develop an understanding of the properties of codes<br>Identify the factors needed to make a successful encryption<br><br>Appreciate why passwords should be managed well and kept safe.<br><br>Understand the features of a strong password or passphrase and the common errors made when creating or maintaining them.<br><br>Understand how to improve personal online account security by enabling screen locks, changing default passwords, using passphrases and using multi-function authentication (mfa) and password managers | **Communication and Crisis Management**<br>Understand what the NCSC's role is during a major cyber security incident.<br><br>Describe some of the high-profile cyber security crises in modern times.<br><br>Evaluate the risks to cyber security during a crisis<br>Explain how to plan and respond to a cyber security attack as an individual.<br><br>Explain how an organisation can plan and respond to a cyber security attack - i.e Local level, corporate level, policies, response plans, communication plans, simulation exercises<br><br>List examples of how the Irish Government communicates cyber security threats during a crisis |
| | **Data is the new oil**<br>Consider what data is, and what makes data politically, economically and personally valuable.<br><br>Investigate the ways data is legally collected.<br><br>Reflect on the concept of privacy and the value they place on their own privacy.<br><br>Access and amend privacy settings appropriately on a variety of relevant digital media platforms and software apps. | **Building Security**<br>Describe and evaluate different ways to back-up data.<br><br>Outline the role of the Firewall in cybersecurity and know how to implement and maintain a firewall.<br><br>Explain how to improve your home router security against malicious cyber activity by taking some simple steps<br><br>Evaluate the benefits and risks of using public wifi systems and consider cybersecurity methods that could be used to protect their data, such as a VPN | **Regulation and Legislation**<br>Investigate the role of regulation in cybersecurity.<br><br>Examine the distinctions between voluntary versus mandatory regulation, and ethical versus government regulation.<br><br>Describe the positive and negative implications of regulation around cybersecurity.<br><br>Understand the principles of cyber security legislation<br>investigate and evaluate national, european and international cyber security legislation |
| | **Cyber Events**<br>Describe the types of cyber events, including attacks, identifying who the victim is, and who benefits.<br><br>Examine examples of political, economic, social and personal cyber-attacks.<br><br>Investigate how cyber security breaches occur for individuals, institutions and businesses. | **Spotting Cyber Attacks**<br>Investigate the impact of different types of malware used to attack individuals, businesses, organisations and governments.<br>Discern the difference between fake profiles and messages and authentic online communications.<br><br>Know how to authenticate data before sharing and how to block and report unwanted communication.<br><br>Explore current methods used by cybercriminals to access sensitive data such as PINS and passwords | **Reporting breaches of Cyber Security**<br>Recognise when something is a threat and should be reported<br>Identify who or what organisation you should contact and how to contact them.<br><br>How to report online crime or threats<br>-illegal content<br>-financial transaction<br>-fraud<br>-a leak of personal information<br>-extortion |

# APPENDIX F: EXAMPLE OF A UNIT OF LEARNING DEVELOPED BY THE IMPLEMENTATION TEAM AND AVAILABLE AT www.cyberwise.ie

**Lesson 1 : What is social engineering?**

**Task 1: Watch the video "Watch how a social engineering hack works"**
https://edition.cnn.com/videos/business/2019/10/17/hacked-tech-reporter-social-engineer-orig.cnn-business
CNN tech reporter Donie O'Sullivan thought he was being safe on social media. Watch social engineer & Social Proof Security CEO Rachel Tobac prove him very, very wrong.

**Task 2: Discuss the video**
Identify 3 things that the hackers took advantage of to hack Donnie.
Identify 3 things Donnie could have done to protect himself from being hacked?
More advanced and detailed Video: Interview with hacker Kevin Mitnick on all things Social Engineering who now runs a business doing ethical hacking.
https://www.knowbe4.com/what-is-social-engineering/

**Task 3: Think/Pair/Share: Develop a definition of Social Engineering**
Having watched the video students can develop their own definition of social engineering individually and then compare it to their partner's definition.
Which one do you prefer? Why? How could it be improved?
Pairs can then move to larger groups and repeat the process.

**Task 4: Relating to real-life examples**
What is social engineering? https://youtu.be/5ZqNX6YeH6c
Can you think of any examples of social engineering that you have experienced? How did it try to get you to give away information? Is social engineering new? Can you think of examples of social engineering that existed before the internet existed? (prompt: are Séances, fortune tellers examples of social engineers?) What do you think are the traits you would need to be a good hacker using social engineering?

**Task 6/HW task: Identify 5 types of social engineering and write a sentence in your own words explaining how it works.**
Extension: Watch the movie Catch Me If You Can (PG-13) or read the article
https://www.businessinsider.com/frank-abagnale-crimes-2012-4?r=US&IR=T#he-forged-his-own-pilots-id-and-faa-license-3
How does this movie/article relate to social engineering? Can you identify tricks that Frank Abagnale uses that modern hackers might also use?

### Lesson 2 : Project - set up

**Task 1**

Each group selects one of the following topics - the topics they covered as their HW for lesson one here can be helpful to form groups and get them started.

- Phishing
- Vishing
- Smishing
- Pretexting
- Baiting
- Tailgating
- Piggybacking
- Quid Pro Quo
- Blagging
- Pharming
- Shouldering

**Task 2 Planning Tool for Project**

Students read through the headings, plan first steps, decide who work will be presented and assign roles using the table below.

Headings in yellow are discussed and answered as a group. Sections in green can be assigned as individual topics within the group. They can decide how many headings each person should take.

| Heading | Who | Agreed next steps/actions |
|---|---|---|
| What is it? | | |
| How does it work? | | |
| Examples | | |
| Who benefits? | | |
| Countermeasures businesses/government | | |
| Countermeasures Personal | | |
| Media Coverage | | |
| What do you think should be done about it? | | |
| Other questions you have | | |

### Lesson 4 : Project development

Project development and coordination of presentation of project. Students continue to use the project planning tool to record learning, ensure everyone has a role, and plan next steps.
Students choose and plan how they wish to present their project e.g. posters, slides, digital storytelling, a dramatic retelling, but it addresses all the headings in the planning table.

### Lesson 5/6 Project presentations and viewing

Students

- Identify what makes each form of social engineering different
- Identify what they all have in common
- Identify common personal countermeasures
- Rate the different types of social engineering in terms of the threat they pose.

### Lesson 7/HW Reflection

Design a poster/write a blog/ create a video/TikTok/Reel advising people (or a specific audience) how to avoid one of these attacks
Or
Write a letter to the Minister of the Department of Environment, Climate, Communications outlining what steps you think the government should take to protect people from such attacks.

Suggested Resources:
https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance_for_Organisations_on_Phishing_and_Social_Engineering_Attacks_Oct19.pdf
https://www.itgovernance.eu/en-ie/phishing-penetration-test-ie
https://www.bbc.co.uk/bitesize/guides/znnny4j/revision/2
https://www.knowbe4.com/

# APPENDIX G:
# SCREENSHOTS FROM www.cyberwise.ie


# APPENDIX H:
# CYBER RESILIENCE FOR PRIMARY SCHOOLS

Work on the primary version of the junior cycle specification is underway and it is expected that a draft of this will be available to showcase at the shared learning event in November. The primary school teacher that we have commissioned to do the work has commenced adapting the Junior Cycle short course to the primary context by dividing up the "3 strand course on a page" learning outcomes into 6 sections which are more age and stage appropriate for the primary context as follows:

1. Staying Secure Online - creating strong passwords
2. Cyber Hygiene - protecting my data
3. Cyber Events & Cyber Careers
4. Fake vs Real - spotting an attack
5. Codes, Ciphers, Encryption - the techie stuff in cyber security

The curricular area that it fits best under is SPHE (strand myself and the wider world).

My hope is that each section will have the following:

- Presentation with interactive content and tasks (oral, reading and written)
- A digital game
- A quiz
- Videos with questions
- Guiding conversations for teachers

The teacher leading this is also in the process of creating an immersive digital escape room under the theme of cyber security.

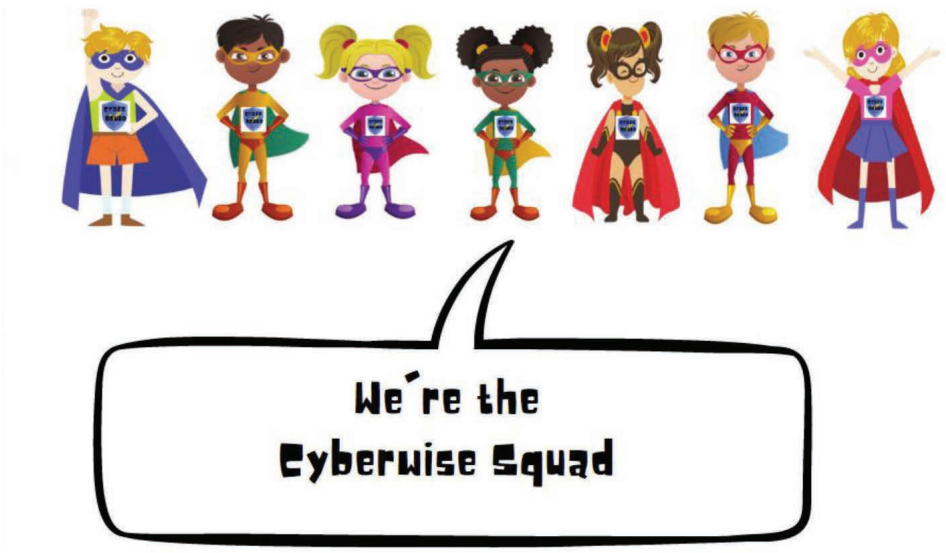
This teacher is attempting to make the content animated as you will see in the canva link below.

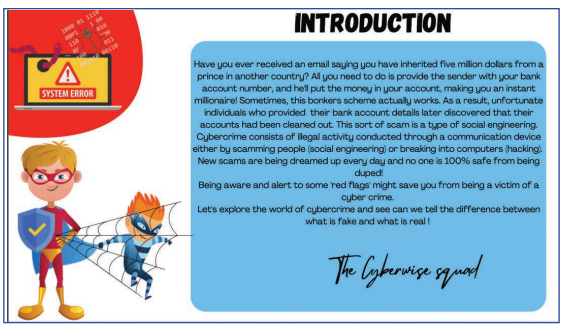
https://www.canva.com/design/DAFFi9ynqp8/BAOGgkdxu-7Tw-Pt_GTQEA/view?utm_content=DAFFi9ynqp8&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

The primary school Cyber Security short course will be hosted on www.scoilnet.ie the national education resource repository

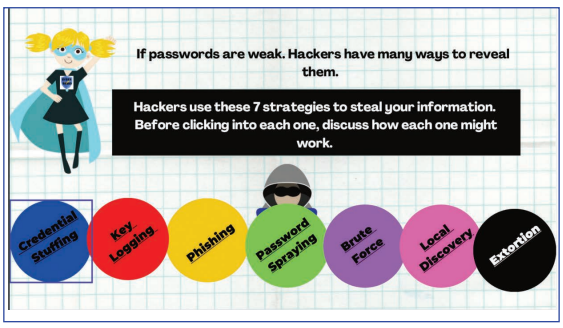
scoilnet

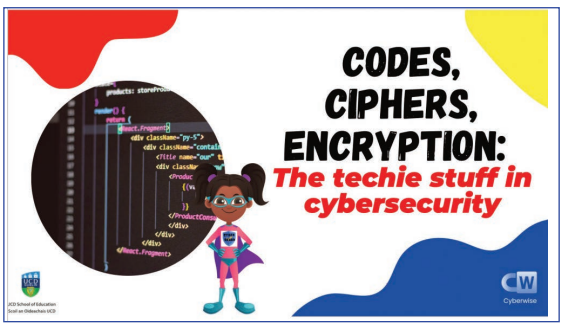
The Cyberwise Squad will feature in all of the materials for targeted at the primary school audience. All materials will be available under the CC share and share alike attribution where the teacher will be acknowledged at the source with the support of UCD School of Education and funded by OPS PSIF

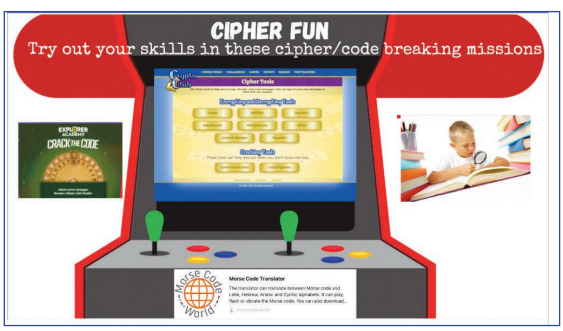






www.cyberwise.ie





Please cite as: Farrell, R. & Maye, K. (2022). Developing a Junior Cycle Short Course on Cyber Security: Phase 1 Report October 2022. University College Dublin.