



Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	SERIOUS GAMES FOR CYBERSECURITY	
Corso di studio	COMPUTER SCIENCE	
Anno Accademico	AA 2023/24	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU	
Settore Scientifico Disciplinare	INF/01	
Lingua di erogazione	English	
Anno di corso	Second	
Periodo di erogazione	1 [^] semester, the exact dates are shown in the poster/regulations	
Obbligo di frequenza	Attendance is strongly recommended	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/computer-science/computer-science	

Docente/i

Nome e cognome	VERONICA ROSSANO
Indirizzo mail	veronica.rossano@uniba.it
Telefono	080 5442477
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.771, 7 [^] piano.
Sede virtuale	https://elearning.uniba.it/course/view.php?id=2105
Sito web del docente	https://www.uniba.it/it/docenti/rossano-veronica
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Mon 9-12 – in other days teacher is available on appointment

Syllabus



Obiettivi formativi	There are several risk factors for system security, one of the weakest links being the human factor. Lack of knowledge about the threats one is exposed to and the lack of training of individuals can amplify the damage of cyber attacks. The course aims to illustrate the processes of designing and implementing serious games in order to gain solid knowledge of system security and limit vulnerabilities caused by users.
Prerequisiti	The following background knowledge facilitates and accelerates understanding of the teaching topics: <ul style="list-style-type: none">• from Project Management for Security: knowing and knowing how to manage the life cycle of a complex project• from Human-Computer Interaction: techniques for designing a good user interface and evaluating the usability of a software product• Programming experience in object-oriented languages, or in languages for the web or mobile development environments
Didactic contents	<p>Part I: Serious games fundamentals</p> <ol style="list-style-type: none">1. Designing Learning Experience (10 ore)<ol style="list-style-type: none">1.1. Learning element: motivation, engagement, and experience1.2. Building experiences with games1.3. Intrinsically experiences in a game2. What is a Serious game (5 ore)<ol style="list-style-type: none">2.1. Play and game2.2. Play as indispensable element of learning2.3. Games definition2.4. Making game design choices that support learning3. Pedagogy and games (3 ore)<ol style="list-style-type: none">3.1. The impact of pedagogic approaches on educational game3.2. Learning theories <p>Part II: Design Serious games for cyber-security</p> <ol style="list-style-type: none">4. Designing a game (4 ore)<ol style="list-style-type: none">4.1. Learning objectives and gaming essence4.2. Gamification in educational context4.3. Game aspects4.4. Designing tips: brainstorming, prototypes, iterative approach4.5. Game elements5. The creation process (2 ore)<ol style="list-style-type: none">5.1. The game space5.2. The rules6. Game Mechanics and Aesthetics (6 ore)<ol style="list-style-type: none">6.1. The flow state6.2. Decision making6.3. Chance6.4. Skills6.5. Collaboration and competition6.6. Linking fun to learning6.7. Linking game mechanics to learning6.8. Aesthetics7. The target audience (4 ore)<ol style="list-style-type: none">7.1. Player taxonomies7.2. Player learning styles <p>Part III: Serious games LAB</p>



	<p>8. International research in serious games for cybersecurity (5 ore) 9. Serious games for cybersecurity examples (7 ore) 10. The creative process to create a serious game (5 ore) 11. Describe a document to plan and design a serious game for cybersecurity (3 ore)</p>		
Books	<p>Kalmpourtzis, G. (2018). Educational Game Design Fundamentals: A journey to creating intrinsically motivating learning experiences. AK Peters/CRC Press.</p> <p>Students who wish can borrow texts from the Library. Is it convenient to check availability via the University Library System https://opac.uniba.it/easyweb/w8018/index.php? and contact the library to arrange the loan</p>		
Note ai testi di riferimento	<p>During the lessons, the teacher will illustrate the concepts with the help of slides that summarize (and sometimes integrate) the contents of the reference text and report exercises carried out in the classroom. The slides will be made available at the end of each lesson on the department's e-learning platform (see 'virtual venue' above).</p> <p>Also available on the ADA platform are all the instructions for creating the case study, some examples of case study documentation from previous academic years and the template for creating the design document.</p>		
Organizzazione della didattica			
Ore			
Totali	Didattica frontale	Pratica (progetto)	Studio individuale
150 ore	24 ore	30 ore	96 ore
CFU/ETCS			
3+2+1P CFU	3 CFU	2 CFU	

Metodi didattici	
	<p>The course is organised in lectures with the aid of slides and specific seminars that may be organised during the course of the course.</p>



	During the teaching some laboratory lessons will be dedicated to support the development of the final case study.
--	---

Expected Learning Results	
Knowledge and Understanding	<ul style="list-style-type: none">• Acquire knowledge regarding methods for designing learning experiences using the game approach• Acquire knowledge regarding the integration of game elements (mechanics, dynamics, rules and aesthetics) to effectively convey the cybersecurity theme• Acquire knowledge regarding the design and production of a serious game as a multimedia product
Applied Knowledge and Understanding	<ul style="list-style-type: none">• Know how to design and develop a serious game for cybersecurity• Know how to combine the game element and cybersecurity knowledge transfer
Metacognitive Skills	<p>Autonomy of judgement</p> <p>An important objective of the course is that the student achieve the ability to integrate knowledge, manage complexity and make decisions during the design, development and evaluation of a serious game. Case studies are a means of training students to make decisions. This ability will be assessed by the lecturer and contributes to the final grade, which also takes into account the student's active participation in class discussions and case study presentations.</p> <p>Communication skills</p> <p>Ability to communicate the results obtained to specialist and non-specialist interlocutors, as well as the development of collaborative skills indispensable for teamwork.</p> <p>Ability to learn autonomously</p> <p>Achieve autonomy in studying and identifying and defining games to support learning in cybersecurity. Know how to apply the serious game in contexts other than cybersecurity.</p>

Evaluation	
Learning assessment methods	The Assessment of the training results achieved takes place through:



	<p>- Case study Students organised in small groups (2 to 4 members) must design and implement a serious game using the methodologies illustrated in the lesson. The case study must be accompanied by a document illustrating all the typical elements of a serious game. The case study must be submitted via the ADA e-learning platform and within 10 days of the date set for each call. The evaluation of the case study, in thirtieths, will take into account the skills acquired by the students and their ability to apply them to real cases. The grade obtained for the case study will be valid for all appeals of the academic year. If the case study is graded insufficient, students will not be allowed to take the oral examination.</p> <p>- Oral examination. Oral discussion of the case study in which students must demonstrate their ability to illustrate the case study and link it to the theoretical knowledge presented during the lectures. The oral examination is single but it is preferable for the group of students to take the oral examination in the same roll call. The oral examination will be marked in 30s and is considered passed if the mark is higher than 18.</p> <p>For students attending lectures, the projects/case studies are carried out during the semester of lectures. Students who do not intend to attend class should contact the teacher at the beginning of the semester so that they can organise discussion and implementation of the projects/case studies.</p>
<p>Evaluation Criteria</p>	<p>Knowledge and understanding:</p> <ul style="list-style-type: none">• To ascertain the knowledge acquired by the student, the oral test will be assessed by verifying the correctness of the answers given by the student.• The project carried out (in a group) will be assessed by taking into account the depth of the actual domain, the appropriateness of the techniques used, the originality of the solutions, the clarity and ability to synthesise resulting from the documentation produced <p>Applied knowledge and understanding:</p> <ul style="list-style-type: none">• The student will have to demonstrate the ability to design and produce a serious game for the effective communication of cybersecurity issues• The student will have to demonstrate the ability to use multimedia design techniques in real contexts <p>Autonomy of judgement:</p> <ul style="list-style-type: none">• Ability to assess the quality of a serious game as a whole and the appropriate use of individual elements characterising a game <p>Communication skills:</p> <ul style="list-style-type: none">• The student must demonstrate the ability to appropriately illustrate the solution created using correct technical language.



	<p>Learning skills:</p> <ul style="list-style-type: none"> Capacity for abstraction, reasoning by analogy and demonstration of creativity in the realisation of multimedia applications in other real contexts 																
<p>Criteria di misurazione dell'apprendimento e di attribuzione del voto finale</p>	<table border="1"> <thead> <tr> <th>Voto</th> <th>Descrittori</th> </tr> </thead> <tbody> <tr> <td>< 18 insufficiente</td> <td>Fragmentary and superficial knowledge of content, errors in applying concepts, poor description.</td> </tr> <tr> <td>18 - 20</td> <td>Sufficient but general knowledge of content, simple description, uncertainties in the application of theoretical concepts.</td> </tr> <tr> <td>21 - 23</td> <td>Appropriate but not in-depth knowledge of content, ability to apply theoretical concepts, ability to present content in a simple manner.</td> </tr> <tr> <td>24 - 25</td> <td>Appropriate and broad knowledge of content, fair ability to apply knowledge, ability to present content in an articulate manner.</td> </tr> <tr> <td>26 - 27</td> <td>Accurate and complete knowledge of content, good ability to apply knowledge, ability to analyse, clear and correct description.</td> </tr> <tr> <td>28 - 29</td> <td>Extensive, complete and thorough knowledge of content, good application of content, good analytical and summarising skills, secure and correct description.</td> </tr> <tr> <td>30 30 e lode</td> <td>Very broad, complete and thorough knowledge of content, well-established ability to apply content, excellent ability to analyse, synthesise and make interdisciplinary connections, mastery of description.</td> </tr> </tbody> </table>	Voto	Descrittori	< 18 insufficiente	Fragmentary and superficial knowledge of content, errors in applying concepts, poor description.	18 - 20	Sufficient but general knowledge of content, simple description, uncertainties in the application of theoretical concepts.	21 - 23	Appropriate but not in-depth knowledge of content, ability to apply theoretical concepts, ability to present content in a simple manner.	24 - 25	Appropriate and broad knowledge of content, fair ability to apply knowledge, ability to present content in an articulate manner.	26 - 27	Accurate and complete knowledge of content, good ability to apply knowledge, ability to analyse, clear and correct description.	28 - 29	Extensive, complete and thorough knowledge of content, good application of content, good analytical and summarising skills, secure and correct description.	30 30 e lode	Very broad, complete and thorough knowledge of content, well-established ability to apply content, excellent ability to analyse, synthesise and make interdisciplinary connections, mastery of description.
Voto	Descrittori																
< 18 insufficiente	Fragmentary and superficial knowledge of content, errors in applying concepts, poor description.																
18 - 20	Sufficient but general knowledge of content, simple description, uncertainties in the application of theoretical concepts.																
21 - 23	Appropriate but not in-depth knowledge of content, ability to apply theoretical concepts, ability to present content in a simple manner.																
24 - 25	Appropriate and broad knowledge of content, fair ability to apply knowledge, ability to present content in an articulate manner.																
26 - 27	Accurate and complete knowledge of content, good ability to apply knowledge, ability to analyse, clear and correct description.																
28 - 29	Extensive, complete and thorough knowledge of content, good application of content, good analytical and summarising skills, secure and correct description.																
30 30 e lode	Very broad, complete and thorough knowledge of content, well-established ability to apply content, excellent ability to analyse, synthesise and make interdisciplinary connections, mastery of description.																
<p>Altro</p>	<p>Students are advised to rely exclusively on the information/communication provided on the official websites of the Department of Computer Science, namely on social groups only if they are set up and administered exclusively by the lecturers of the relevant subjects:</p> <ul style="list-style-type: none"> https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea https://www.uniba.it/it/ricerca/dipartimenti/informatica https://elearning.di.uniba.it/ <p>The teaching programmes are available here:</p> <ul style="list-style-type: none"> https://programmi.di.uniba.it/ <p>Information that all students should be aware of is written in the teaching regulations and study manifestos available on the website:</p> <ul style="list-style-type: none"> https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea <p>Students are advised to be wary of information and materials circulating on unofficial websites or social groups, as they are often found to be unreliable, incorrect or incomplete. If you have any doubts, please ask the lecturer for a meeting in accordance with the reception arrangements.</p>																



Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	SERIOUS GAMES FOR CYBERSECURITY	
Corso di studio	COMPUTER SCIENCE	
Anno Accademico	AA 2023/24 per i corsi del I sem	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU (totali; l'indicazione della distribuzione è prevista più avanti)	
Settore Scientifico Disciplinare	INF/01	
Lingua di erogazione	Inglese	
Anno di corso	Secondo	
Periodo di erogazione	1^ semestre, le date esatte sono riportate nel manifesto/regolamento	
Obbligo di frequenza	La frequenza è fortemente raccomandata	
Sito web del corso di studio	https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/computer-science/computer-science	

Docente/i

Nome e cognome	VERONICA ROSSANO
Indirizzo mail	Veronica.rossano@gmail.com
Telefono	080 5442477
Sede	Dipartimento di Informatica, Via Orabona 4, 70125, Bari. Stanza n.771, 7^ piano.
Sede virtuale	Piattaforma ADA - https://elearning.di.uniba.it/
Sito web del docente	https://www.uniba.it/it/docenti/rossano-veronica
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Lunedì, 9-12. Negli altri giorni previo appuntamento via mail.

Syllabus

Obiettivi formativi	Esistono diversi fattori di rischio per la sicurezza dei sistemi, uno degli anelli più deboli è il fattore umano. La scarsa conoscenza delle minacce a cui si è esposti e la
----------------------------	--



	<p>mancata formazione degli individui può amplificare i danni degli attacchi informatici. Il corso ha l'obiettivo di illustrare i processi di progettazione e realizzazione di serious game per acquisire solide conoscenze relative alla sicurezza dei sistemi e limitare le vulnerabilità causate dagli utenti.</p>
Prerequisiti	<p>Le seguenti conoscenze preliminari facilitano ed accelerano la comprensione degli argomenti dell'insegnamento:</p> <ul style="list-style-type: none">• da Project Management for Security: conoscere e saper gestire il ciclo di vita di un progetto complesso• da Human-Computer Interaction: le tecniche per la progettazione di una buona interfaccia utente e la valutazione dell'usabilità di un prodotto software• Esperienze di programmazione in linguaggi object oriented, o in linguaggi per il web o in ambienti di sviluppo mobile
Contenuti di insegnamento (Programma)	<p>Part I: Serious games fundamentals</p> <p>12. Designing Learning Experience (10 ore)</p> <p>12.1. Learning element: motivation, engagement, and experience</p> <p>12.2. Building experiences with games</p> <p>12.3. Intrinsically experiences in a game</p> <p>13. What is a Serious game (5 ore)</p> <p>13.1. Play and game</p> <p>13.2. Play as indispensable element of learning</p> <p>13.3. Games definition</p> <p>13.4. Making game design choices that support learning</p> <p>14. Pedagogy and games (3 ore)</p> <p>14.1. The impact of pedagogic approaches on educational game</p> <p>14.2. Learning theories</p> <p>Part II: Design Serious games for cyber-security</p> <p>15. Designing a game (4 ore)</p> <p>15.1. Learning objectives and gaming essence</p> <p>15.2. Gamification in educational context</p> <p>15.3. Game aspects</p> <p>15.4. Designing tips: brainstorming, prototypes, iterative approach</p> <p>15.5. Game elements</p> <p>16. The creation process (2 ore)</p> <p>16.1. The game space</p> <p>16.2. The rules</p> <p>17. Game Mechanics and Aesthetics (6 ore)</p> <p>17.1. The flow state</p> <p>17.2. Decision making</p> <p>17.3. Chance</p> <p>17.4. Skills</p> <p>17.5. Collaboration and competition</p> <p>17.6. Linking fun to learning</p> <p>17.7. Linking game mechanics to learning</p> <p>17.8. Aesthetics</p> <p>18. The target audience (4 ore)</p>



	<p>18.1. Player taxonomies 18.2. Player learning styles</p> <p>Part III: Serious games LAB</p> <p>19. International research in serious games for cybersecurity (5 ore) 20. Serious games for cybersecurity examples (7 ore) 21. The creative process to create a serious game (5 ore) 22. Describe a document to plan and design a serious game for cybersecurity (3 ore)</p>		
Testi di riferimento	<p>Kalmpourtzis, G. (2018). Educational Game Design Fundamentals: A journey to creating intrinsically motivating learning experiences. AK Peters/CRC Press.</p> <p>Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.</p>		
Note ai testi di riferimento	<p>Nel corso delle lezioni il docente illustrerà i concetti con l'ausilio di slide che sintetizzano i contenuti del corso. Le slide saranno rese disponibili al termine di ogni lezione sulla piattaforma ADA del dipartimento (v. sopra 'sede virtuale').</p> <p>Sulla piattaforma ADA sono disponibili, inoltre, tutte le indicazioni per realizzare il caso di studio, alcuni esempi di documentazione di casi di studio degli a.a. precedenti e il template per la realizzazione del documento di progettazione.</p>		
Organizzazione della didattica			
Ore			
Totali	Didattica frontale	Pratica (progetto)	Studio individuale
150 ore	24 ore	30 ore	96 ore
CFU/ETCS			
3+2+1P CFU	3 CFU	2 CFU	

Metodi didattici	
	<p>Il corso è organizzato in lezioni frontali svolte con l'ausilio di slide e seminari specifici che potranno essere organizzati durante il corso dell'insegnamento.</p>



	Durante l'insegnamento alcune lezioni laboratoriali saranno dedicate al supporto nello sviluppo del caso di studio finale.
--	--

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	<ul style="list-style-type: none">• Acquisire conoscenza relativamente ai metodi per progettare esperienze di apprendimento usando l'approccio del gioco• Acquisire conoscenza riguardo all'integrazione degli elementi del gioco (meccaniche, dinamiche, regole e estetica) per veicolare in maniera efficace il tema della cybersecurity• Acquisire conoscenza relativamente alla progettazione e produzione di un serious game come prodotto multimediale
Conoscenza e capacità di comprensione applicate	<ul style="list-style-type: none">• Saper progettare e sviluppare un serious game per la cybersecurity• Saper combinare l'elemento di gioco e il trasferimento di conoscenza relativo alla cybersecurity
Competenze trasversali	<p>Autonomia di giudizio</p> <p>Un importante obiettivo del corso è che lo studente raggiunga la capacità di integrare la conoscenza, gestire la complessità e prendere decisioni durante la progettazione, lo sviluppo e la valutazione di un gioco serio. I casi di studio sono un mezzo per allenare gli studenti a prendere decisioni. Questa capacità sarà valutata dal docente e contribuisce al voto finale, che tiene conto anche della partecipazione attiva dello studente alle discussioni in classe e alla presentazione dei casi studio.</p> <p>Abilità comunicative</p> <p>Capacità di comunicare i risultati ottenuti a interlocutori specialisti e non, così come lo sviluppo di capacità collaborative indispensabili per il lavoro di gruppo.</p> <p>Capacità di apprendere in modo autonomo</p> <p>Raggiungere l'autonomia nello studio e nell'identificazione e definizione di giochi per sostenere l'apprendimento nella cybersecurity. Saper applicare il serious game in contesti diversi dalla cybersecurity.</p>



Valutazione	
Modalità di verifica dell'apprendimento	<p>La verifica dei risultati formativi raggiunti avviene tramite:</p> <ul style="list-style-type: none">- Caso di studio Gli studenti organizzati in piccoli gruppi (da 2 a 4 componenti) dovranno progettare e realizzare un serious game utilizzando le metodologie illustrate a lezione. Il caso di studio, inoltre, deve essere accompagnato da un documento che illustri tutti gli elementi tipici di un serious game. La consegna del caso di studio deve avvenire tramite la piattaforma di e-learning ADA e entro 10 giorni dalla data fissata per ogni singolo appello. La valutazione del caso di studio, in trentesimi, terrà conto delle competenze acquisite dagli studenti e dalla loro capacità di applicarle a casi reali. Il voto acquisito per il caso di studio valido per tutti gli appelli dell'a.a. Se il caso di studio è valutato insufficiente gli studenti non potranno accedere alla prova orale.- Prova orale. Discussione orale del caso di studio in cui gli studenti dovranno dimostrare di saper illustrare il caso di studio e collegarlo alle conoscenze teoriche illustrate durante le lezioni frontali. La prova orale è singola ma è preferibile che il gruppo di studenti sostenga l'esame orale nello stesso appello. La prova orale sarà valutata in 30simi e si considera superata se il voto è maggiore di 18. <p>Per gli studenti che frequentano le lezioni, i progetti/studi di casi sono svolti durante il semestre di lezione. Gli studenti che non intendono frequentare le lezioni devono contattare l'insegnante all'inizio del semestre in modo che possano organizzare la discussione e realizzazione dei progetti/casi di studio.</p>
Criteri di valutazione	<p>Conoscenza e capacità di comprensione:</p> <ul style="list-style-type: none">• Per accertare la conoscenza acquisita dallo studente si valuta la prova orale verificando la correttezza delle risposte fornite dallo studente.• Il progetto svolto (in gruppo) sarà valutato tenendo conto di come è stato approfondito il dominio reale, dell'appropriatezza delle tecniche usate, dell'originalità delle soluzioni, della chiarezza e della capacità di sintesi che risultano dalla documentazione prodotta <p>Conoscenza e capacità di comprensione applicate:</p> <ul style="list-style-type: none">• Lo studente dovrà dimostrare di saper progettare e produrre un serious game per la comunicazione efficace di tematiche riguardanti la cybersecurity• Lo studente dovrà dimostrare di saper utilizzare tecniche di progettazione multimediale in contesti reali <p>Autonomia di giudizio:</p> <ul style="list-style-type: none">• Abilità di valutazione della qualità di un serious game nel suo complesso e dell'uso appropriato dei singoli elementi caratterizzanti un gioco <p>Abilità comunicative:</p> <ul style="list-style-type: none">• Lo studente dovrà dimostrare di saper illustrare in modo appropriato la soluzione creata utilizzando un linguaggio tecnico corretto. <p>Capacità di apprendere:</p> <ul style="list-style-type: none">• Capacità di astrazione, di ragionamento per analogia e dimostrazione di creatività nella realizzazione di applicazioni multimediali in altri contesti reali



Criteria di misurazione dell'apprendimento e di attribuzione del voto finale

Voto	Descrittori
< 18 insufficiente	Conoscenze frammentarie e superficiali dei contenuti, errori nell'applicare i concetti, descrizione carente.
18 - 20	Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell'applicazione di concetti teorici.
21 - 23	Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.
24 - 25	Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.
26 - 27	Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.
28 - 29	Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.
30 30 e lode	Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.

Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>
- <https://www.uniba.it/it/ricerca/dipartimenti/informatica>
- <https://elearning.di.uniba.it/>

I programmi degli insegnamenti sono disponibili qui:

- <https://programmi.di.uniba.it/>

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:

- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.