Learning and Teaching Online:
A short MOOC in Cyber Security

Steve Riddle, Charles Morisset, Siamak Shahandashti
School of Computing Science
Newcastle University

HEA National Conference for Learning and Teaching in Cyber Security
6 April 2017
Overview

• MOOCs – what, why
• Designing a course in Cyber Security
• Activities – examples
• Course delivery (Sept 2016)
• Analysis and redesign
• Conclusions, observations and future directions
MOOCs – what, why

- Massive Open Online Course
- Unlimited numbers of student learners, open access, delivered online
- Growing in popularity in past 10 years
- Major providers: Coursera, edX, Udacity

In practice “Open” may mean anything from fully accessible, unlicensed content to open to fee-paying registered users, all rights reserved.

- Some MOOCs are credit-bearing and may form part of a degree qualification
MOOCs at Newcastle University

• Newcastle is a FutureLearn partner:
  • Owned by Open University
  • Launched Sept 2013
  • 120 global partners inc. UK and international universities

• All courses delivered via FutureLearn platform
  • Short articles, videos and exercises
  • Social learning: participants (learners) are encouraged to engage, interact, do exercises and discuss their results, argue

• Newcastle has several MOOCs established ...
DEMENTIA CARE: STAYING CONNECTED AND LIVING WELL
NEWCASTLE UNIVERSITY
A course for carers, to help you stay connected to loved ones, manage stress at home and defuse difficult situations.

AGEING WELL: FALLS
NEWCASTLE UNIVERSITY
Explore why people fall, discover practical methods to reduce the risk of falling and recognise when to seek expert help.

HADRIAN'S WALL: LIFE ON THE ROMAN FRONTIER
NEWCASTLE UNIVERSITY
Explore the archaeology of the most heavily fortified frontier in the Roman Empire, its people and their lives.

THE ENTERPRISE SHED: MAKING IDEAS HAPPEN
NEWCASTLE UNIVERSITY
Everyone is a thinker and a doer. Everyone is entrepreneurial. Turn your ideas into action with this free online course.
Why a Cyber MOOC?

• Current Newcastle MOOCs focussed on enterprise, medical and cultural topics – an opportunity to widen range of offered courses
• As one of 14 Centres of Excellence in Cyber Security Research, Newcastle well placed to develop a focussed MOOC in this area
• School of Computing Science keen to explore new ways to raise profile of research and teaching, increase PG student recruitment
• Work to increase opportunities to attract study and employment in cyber security
Aims of a Cyber MOOC

• To be complementary to existing courses
  • OU Introduction to Cyber Security – 8 weeks, in-depth introduction

• To play to strengths in research and teaching
  • Topics such as privacy, bank payments, access control, bitcoin

• To provide a taster for more advanced courses
  • “Traditional” MSc in Computer Security and Resilience
A MOOC is a team exercise...

- **Course team**: Charles Morisset, Kovila Coopamootoo, Martin Emms, Dylan Clarke, Siamak Shahandashti
- **Contributors/Editors/Reviewers**: Aad van Moorsel, Feng Hao, Paddy McCorry, Maryam Mehrnezhad, Ehsan Toreini, Mohammed Aamir Ali, Arthur Demanuele
- **Mentors**: David Yamoah, Peter Carmichael, Uchechi Nwadike
- **Learning and Teaching Development Service (LTDS) mooc team**: Nuala Davis, Suzanne Hardy, Ellie Lockhart
- **Digital media**: Steve Bradwel, Kevin Dick
- **PR**: Melanie Dunnett
Designing a Cyber MOOC

• Who is the audience? Initial thoughts about learners (personas):

  • Already done a MOOC on cybersecurity
  • Working in a company concerned with cybersecurity
  • Some background in IT
  • Interested in retraining to cybersecurity
  • General interest in subject

  • People concerned by high-profile incidents, wanting reassurance
Learning outcomes

• Explore the trade-offs between security and convenience in everyday life
• Explain key topics in cybersecurity
• Debate good practice in giving out data online
• Assess the value of personal data to commercial businesses
• Explore the evolving battle between payment fraud and fraud prevention
• Investigate the risks and mitigations in our use of "smart" devices
• Perspectives:
  • The general public, business, criminals, and experts
• Duration:
  • Three weeks (first run in September 2016)
• Crosscutting themes
  • Trade-off: security, privacy, usability
  • Balanced, informed decisions about risk
Planning and Project Management
Designing a Cyber MOOC: Topics

- Privacy
- Payments
- Smart devices (“The Future Home”)
Designing a Cyber MOOC: Topics

▼ Privacy
  • What is it?
  • Value of data for businesses
  • What information is tracked about you?
  • What do attackers aim to gain from your data?
  • How do the experts tackle risks?

▶ Payments

▶ Smart devices ("The Future Home")
Designing a Cyber MOOC: Topics

► Privacy

▼ Payments
  • The arms race of payment security
  • Fraud: who pays?
  • What is it like in your country?
  • The online retailer
  • Research: mobile and contactless payments
  • Reducing your risk
  • Bitcoin / cryptocurrencies

► Smart devices ("The Future Home")
Designing a Cyber MOOC: Topics

- Privacy
- Payments
- Smart devices (“The Future Home”)
  - How many connected devices do you have?
  - Case studies
  - STRIDE threat model
  - Security vs privacy
  - Research: Access control experiments
Course preparation: March – August 2017

• Hard work!
  • Writing articles, setting quizzes, recording videos
  • Planned, coordinated and directed by Newcastle MOOCs team (LTDS)
  • External review
  • Team effort
  • Technology (Trello, Slack) helpful
  • Writing days/half days even more helpful
Activities: Videos

• Typically 5 minute video with accompanying text
• Examples (week 1):
  • Privacy online and offline
  • Why would anyone want your data?
  • Preserving privacy in cloud storage

Why would anyone want your data?

It is easy to fall into the trap of thinking that adversaries simply wish to defeat our security systems. In reality they have a goal and are happy to achieve it by following the path of least resistance.

In this video Dr Dylan Clarke presents some examples of attacks and explores the motivations behind these.

How does being aware of these motivations help us protect ourselves?

© Newcastle University
Activities: Articles

• Around 500 word articles giving more in-depth information about a topic

• Examples (week 2):
  • How payments have changed
  • Usability vs security – who pays?
  • Motivations, methods and practical attacks by criminals
  • Is your mobile phone spying on you?
Activities: Quizzes

• 3-4 questions, formative tests not contributing to a course score
• Example (week 2):
  • What is the true cost of fraud in the UK?

Question 1

Does gender influence how much money is lost to fraud?

- It is about equal, men and women lose about the same amount of money.
- Men lose more money than women
- Women lose more money than men
Activities: Exercises

• A task taken individually. Learners then discuss their results with others.

• Example (week 3):
  • How many connected devices do you own?

  “Take part in our exercise below - a one question poll which asks about the number of connected devices you have at the moment, including in your home, in your car, etc.
  Once you have taken part, look at the results from other learners. What surprises you about the results? Why?”
Activities: Discussions

- More focussed discussion with specific questions to prompt debate
- Example (week 3):

  Issues raised by connected devices?

  Connected devices are becoming an important part of our everyday life. They are providing exciting new types of interaction, and they can be very helpful in many circumstances. However, there is limited control over the specification and the deployment of these devices, and a single flaw in one of them might open your home for attackers located anywhere in the world. Connected devices might create confidentiality issues, for instance by leaking personal information, integrity issues, for instance by allowing an attacker to enter your house, or even availability issues, for instance by preventing a legitimate user to use their connected home.

- What concrete risks can you associate with connected devices?
- Does the benefit they bring outweigh the risk?
- Or would you rather have an unconnected home?
Activities: Tests

• Summative tests
• Can only be taken once: 3 points per question
• Light approach: one single end of course test, 9 questions of average difficulty
• 70% or above on all tests entitles learner to purchase Certificate of Achievement
  • Change from March 2017: learner pays to take test (and maintain unlimited access to the course)
Mentoring

- During the course run, a small team of mentors (research students) has a rota for observing discussions
- Step in to answer direct questions or correct misunderstandings
- Sometimes needed to encourage most active learners to stay on topic
  - But mostly self-policing – this isn’t the Guardian comments section
- Learners appreciate a visible presence from mentors
Course run 1: September 2016

Enrolments, and the Huffington Post effect
Some learner statistics ...

- 14,000 enrolments, but only a fraction complete data about themselves
- 823 Male, 683 Female
Some learner statistics ...

- 995 out of 1516 enrolled educated at university level or above

Employment status:

- Full time student: 32%
- Looking for work: 16%
- Not working: 9%
- Retired: 16%
- Self employed: 7%
- Unemployed: 20%
A selection of comments

Thank you to the educators for giving me insight into cyber security and for your answers to my questions. Also to my fellow learners, I did learn a lot from you.

I'd disagree on writing passwords down, (assuming you have a secure place to store what you wrote them on). Password managers while making life easier do have a major flaw also, in protecting all your passwords with one password!

I protect my cards in RFID case. Why invite trouble?

Thank you team for a well put-together course, which has highlighted many of my shortcomings when I am using the internet ... I would like to wish everyone who took part in giving comments all the best with their future endeavours.

... The kind of technologies which Newcastle and other leading universities are developing could also be used ... to target civilians...

Do you consider the 'ethical' dimension when developing and deploying such technologies and how would you address it?
Review of Run 1

• Very high “joiner” numbers

• Low numbers of fully participating learners (around 2000) – typical for such courses

• Unusually low numbers of social learners:
  • Fears over privacy?
  • Novices intimidated by experts?

• Learners struggled with some advanced topics: bitcoin, psychology of behaviour, secure messaging
Changes for Run 2 (March/April 2017):

- Deal with privacy fears with additional activities on checking mobile app settings
- Rewrites/simplifications on some articles e.g. Bitcoin
- New video updating on recent Newcastle research
Conclusions and observations

• MOOCs are challenging to develop, require large team and buy-in from whole institution
  • Expertise from university MOOCs team essential
  • Good opportunities to involve research students in developing and delivering material
  • Easier to develop piecemeal than traditional lectures would be
• Development experience helps to reflect on teaching of traditional modules
• A good mentoring team is essential
  • Encourage and facilitate discussion
  • Steer some of the more “vocal” learners away from tangential topics which can disengage other learners
Future directions

• Several more Cyber-Security MOOCs now available (on FutureLearn and elsewhere)
  • Specific areas, e.g. android development
  • Online degree from Deakin University, Australia

• Future directions
  • Accreditation,
  • CPD
  • MSc courses
Not too late to sign up!

www.futurelearn.com/courses/cyber-security
Any Questions?