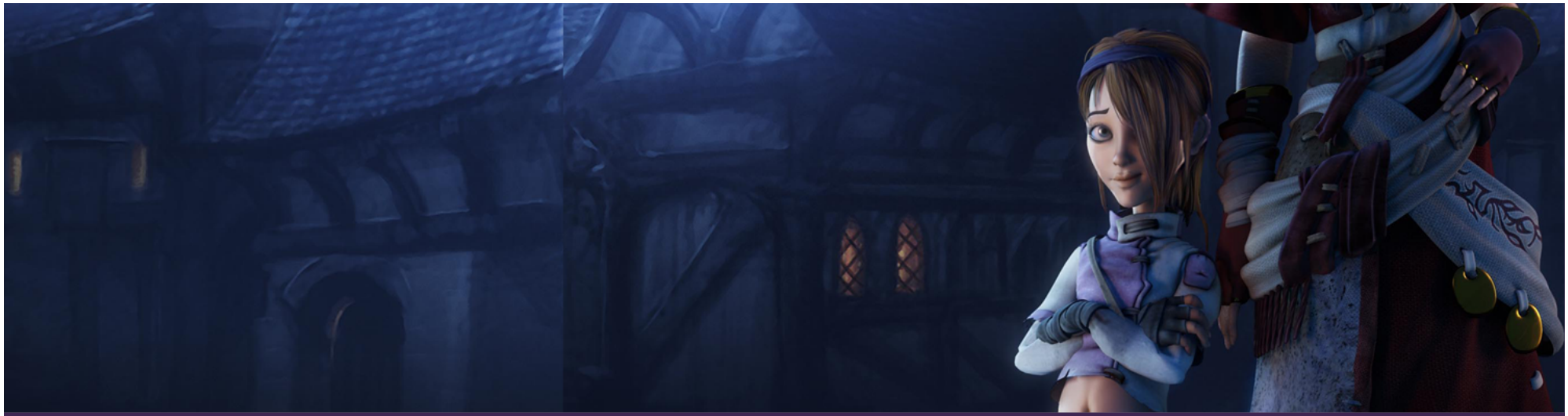


FALMOUTH
UNIVERSITY

Lecture 2: History & State of Cybersecurity

COMP280: Creative Computing
BSc(Hons) Computing for Games
BA(Hons) Game Development: Programming

FALMOUTH
UNIVERSITY

- Learning outcomes
  - **Understand** how developments in social, technical , legal and economic spheres created an environment for cybersecurity
  - **Define** the term ‘cybersecurity’
  - **Identify** common hacking and phishing approaches

- Understand how developments in social, technical , legal and economic spheres created an environment for cybersecurity

- History of cybersecurity
  - Cybersecurity is a complex subject even it's fairly short history
  - Makes sense to use analytical frameworks to help marshal our thinking

- History of cybersecurity
  - 5Ws & H (6Ws)
    - Who, where, why, what, when & how
    - 6 questions to think about complex situations from different perspectives
      - Take a complex problem
      - Break it down into smaller ones to understand it better
      - Combine them back together to demonstrate your mastery of the problem space

- History of cybersecurity
  - 3As (UML use case collaborations)
    - Actors (agents)
    - Activities
    - Artefacts (things that are produced and consumed by activities and agents)
    - Again, break complex problems down into things that make sense and re-combine in a way that makes sense to you
      - » https://app.pluralsight.com/library/courses/uml-introduction/table-of-contents

- History of cybersecurity
  - Macroeconomic analysis (STEP / PEST / PESTLE)
    - A way of looking at change through various lenses
      - Social (societal), technical, economic, political & (environmental & legal)
    - Again, take complex situations
      - split them into their parts to analyse
      - Rebuild the narrative so it makes sense

- History of cybersecurity

  – Once upon a time there was no ‘the internet’
    - Computers were standalone & single function
    - Users had dumb terminals
    - There was no inter- connectivity

- History of cybersecurity
  - Once upon a time there was no ‘the internet’
    - However, hacking and phishing did exist
      - Hacking (Enigma machine and other government ciphers)
      - Political espionage (Watergate scandal)
      - Industrial espionage (Operation Brunnhilde)
      - Dumpster diving (every PI ever)
      - Disgruntled employees (Shawshank Redemption)
    - ‘Information’ has value
      - Protected by laws
      - Legal protections can occur too late …

- History of cybersecurity
  - Growth of information technology over the last 50 years:
    - The internet
    - The WWW
    - Moore's Law
      - Number of transistors in a circuit doubles every two years
      - Massive growth of technology complexity
      - Massive reductions in prices
    - Reduction in barriers to entry for technology
      - Move towards software as a service (SaaS)
        - » Companies can rent rather than buy/build technology

    →Creation of technology—based companies

    →FANG companies (facebook, Apple, Netflix, Google)

- History of cybersecurity

https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

- Define the term ‘cybersecurity’

- Cybersecurity
  - We can see that cybersecurity relates to:
    - Unauthorised access to an organisation's information and/or systems
    - Making information and/or systems unavailable to an organisation
    - Tampering with an organisation's information and/or systems
  - I.e. systems and information suffering from some form of loss and/or harm

- Cybersecurity
  - We can define harm as:
    - Reputational damage
    - Financial loss
    - Regulatory
    - Operational
    - Loss of Intellectual Property (IP), trade secrets etc

- Cybersecurity
  - A definition of cyber security:
    - Cybersecurity is protecting the confidentiality, integrity & availability of an organisation's information assets from malicious actors and/or accidents.

- Cybersecurity
  - Who are these actors?
    - Depends on your organisation
    - Criminals, Competitors, Countries
    - Hackivists & Hackers

- Cybersecurity
  - Cyber Risk Assessments

- Use risk modelling to work out likelihood and impact
  - Then plan accordingly

- Cybersecurity
  - Cyber Risk Assessments

Scenario	Likely threat actors
I run a leading crypto currency wallet service. We have over a billion bitcoin hashes.	
I run the IT department for the world's leading soft drinks beverage with our famous, and secret, recipe	
I run a completely legitimate nuclear research facility in Iran	
I run a completely legitimate nationalist website	
I run the Apple Store	

- Cybersecurity
  - Cyber Risk Assessments

Scenario	Likely threat actors
I run a leading crypto currency wallet service. We have over a billion bitcoin hashes.	Criminals
I run the IT department for the world's leading soft drinks beverage with our famous, and secret, recipe	Competitors
I run a completely legitimate nuclear research facility in Iran	Countries
I run a completely legitimate nationalist website	Hacktivists
I run the Apple Store	Hackers

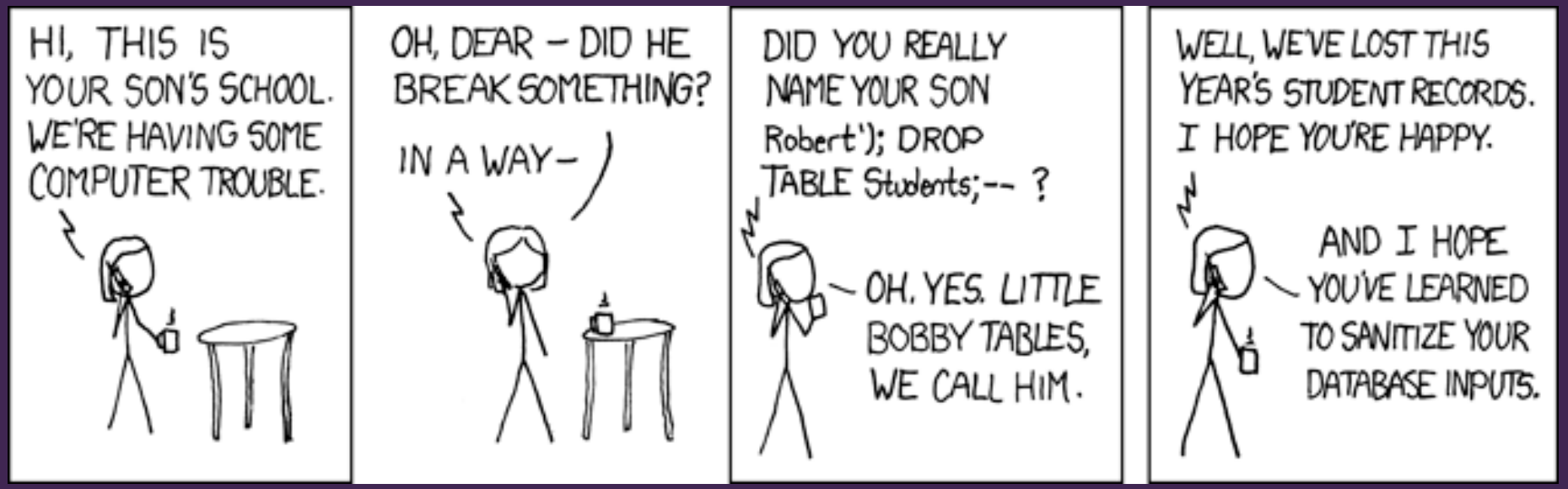
- Identify common hacking and phishing approaches

- Common hacking and phishing approaches
  - Let's define some terms
    - Hacking is 'attacking' a system through a computer
    - Phishing is 'attacking' a system through people (employers, employees, contractors, users etc)

- Common hacking and phishing approaches
  - Hacking
    - Exploits & Vulnerabilities
      - Relies on implicit weaknesses within hardware, operating systems, applications
        - » Admin / default accounts on switches / moderns, servers etc
        - » Buffer over-runs
        - » Backdoors in applications
        - » Known bugs in systems
      - See this a lot with video games, in particular with speed runs ;)
      - This is why we have so many patches and updates now

- Common hacking and phishing approaches
  - Hacking
    - Cross-site scripting
      - Inject client-side scripts into web pages
      - See this a lot with emails that have dubious links
      - Javascript in the links will attempt to copy user credentials in cookies
      - https://www.veracode.com/security/xss

- Common hacking and phishing approaches
  - Hacking
    - SQL Injections



- Common hacking and phishing approaches
  - Hacking
    - SQL Injections
      - Client server communications on HTTP will often encode data into urls
        - » You can see this with all the %whatever?stuff% you see in urls in the browser
        - » These are unpacked by the server and used to run server-side scripts
        - » Often, developers will send raw SQL commands that are not sanitised on the server
        - » DROP TABLE * will delete all the tables in a database
      - PySQL traps this behaviour ;)
        - » You should think about encrypting server bound data & commands

- Common hacking and phishing approaches
  - Hacking
    - Packet sniffing / Man in the middle
      - Network data follows a defined format (otherwise no-one would be able to read it)
      - You can sniff packets to see their contents
        - » Often, services will use raw text for data (see previous slide)
        - » This is v.bad if the service is sending raw passwords to the server (this is frighteningly common)
      - A man in the middle is a node that will read network packets before sending them on to their correct destination
        - » Daily Mail ‘Café Wifi’ concerns.
      - HTTPS is secure HTTP
        - » You can encrypt packet payloads and sequence them to stop replay attacks

- Common hacking and phishing approaches
  - Phishing
    - Email phishing
      - ‘Nigerian prince’ / assistance scams
      - Fake company log-on scams
        - » You need to log on to some service to for some reason
          - Bank, paypal, ebay, apple etc

- Common hacking and phishing approaches
  - Phishing
    - Voice phishing
      - Call up employees in a company asking for account details

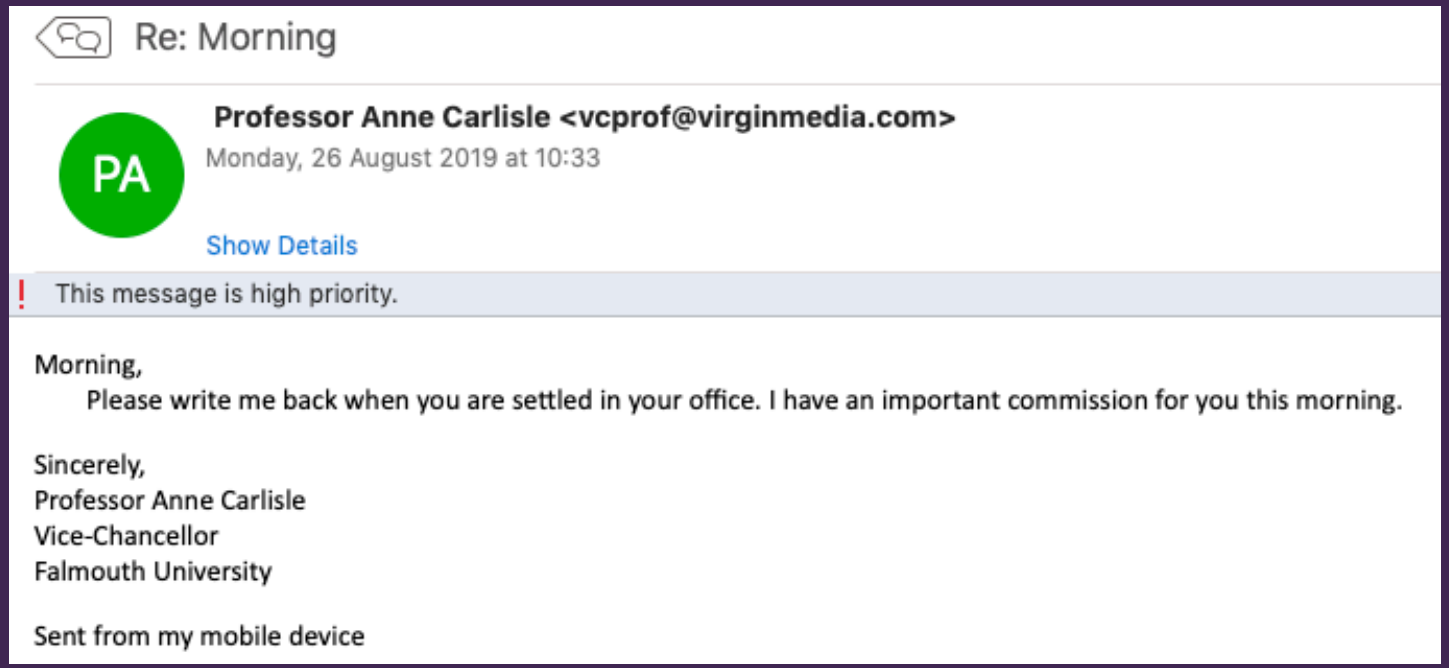
        'Hi this is Dave in accounts, we're having problems doing <some work> with your department's data, can you send over your finance account details so we can sort it out as we can't get through to IT and this needs to be done by the end of the day'

      - Can do it with email & spoofed addresses

      - It's a bit of a modern take on the old scam of sending companies bills for non-existent services
        - » Or the zoo parking warden

FALMOUTH UNIVERSITY

- Common hacking and phishing approaches
  - Phishing
    - Spear phishing
      - This is a derivative of phishing where the phishers look to target their victims using available company data



Re: Morning

PA

Professor Anne Carlisle <vcprof@virginmedia.com>

Monday, 26 August 2019 at 10:33

Show Details

! This message is high priority.

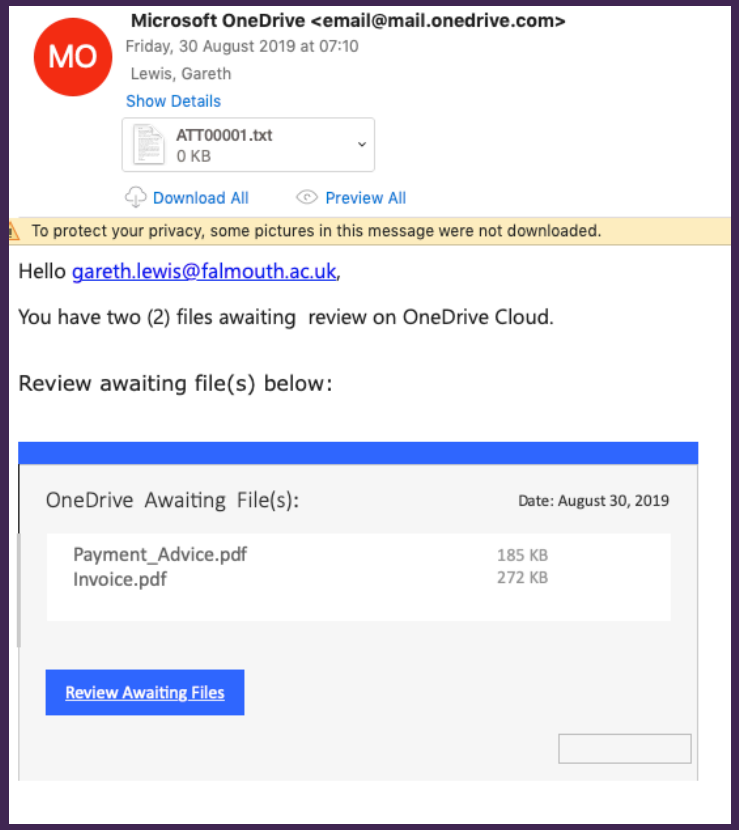
Morning,

Please write me back when you are settled in your office. I have an important commission for you this morning.

Sincerely,
Professor Anne Carlisle
Vice-Chancellor
Falmouth University

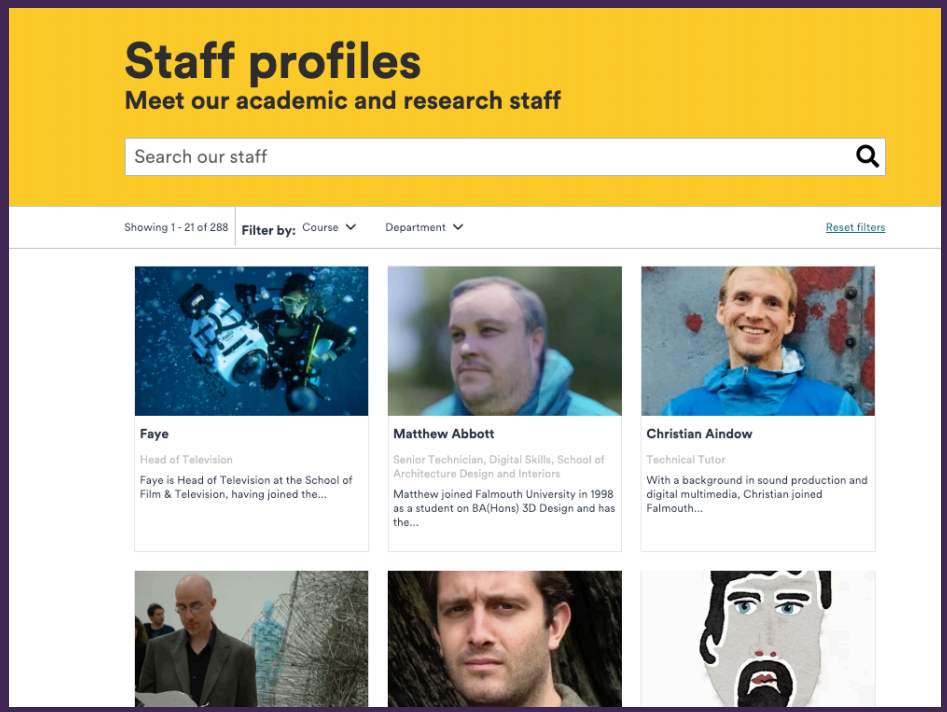
Sent from my mobile device

- Common hacking and phishing approaches
  - Phishing
    - Spear phishing
      - This is a derivative of phishing where the phishers look to target their victims using available company data



FALMOUTH UNIVERSITY

- Common hacking and phishing approaches
  - Phishing
    - Whaling
      - This is another derivative of phishing where the phishers look to target senior managers in a company.
      - These approaches can be easy when companies have fat websites with lots of social data on them



- Wrap-up
  - Data is the new oil, it is the world's most valuable resource
    - Therefore, there's value to be had in having it, especially if it's not yours
    - There's value to be had in keeping yours secure
  - Nothing changes in human nature, we just change the artefacts that we apply our activities to
    - Phishers will always phish
    - People will always want information
    - People and organisation will always want to keep their information private

- Wrap-up
  - **Understand** how developments in social, technical , legal and economic spheres created an environment for cybersecurity
    - Technology has created new ways to store, share and process data
    - This has created new industries and societal demands for data-centric businesses
    - Information always has value

- Wrap-up
  - **Define** the term ‘cybersecurity’
    - Cybersecurity is protecting the confidentiality, integrity & availability of an organisation’s information assets from malicious actors and/or accidents.
    - Breaches in cybersecurity will impact an organisation’s:
      - Reputation
      - Finances
      - Operational ability
      - Secrets (IP)
      - Position in within regulatory frameworks
    - Cyber criminals can be
      - Criminals, competitors, countries, hacktivists & hackers

- Wrap-up
  - **Identify** common hacking and phishing approaches
    - Hacking generally involves compromising computers
    - Phishing generally involves compromising people
    - Hacking
      - Exploits & vulnerabilities, cross-site scripting, SQL injections, man-in-the-middle
    - Phishing
      - Email, voice, spear & whaling

- Questions