**Unit 2: Principles of Evidence and Proof**

Welcome to Week 2.

This week’s learning introduces you to issues concerning proof. The burden of proof in the English legal system usually is usually borne by the prosecution. However, in some cases, the burden of proof might lie on the defendant. The standard of proof also varies depending on the law under which the alleged offence is committed. If the act is criminal, the standard of proof will need to be proved ‘beyond reasonable doubt’. If the act comes under civil law, the standard of proof will be ‘on the balance of probabilities’, that is, ‘more likely than not’. There is a whole doctrine of the admissibility of evidence but, in the case of cybercrime, the applicability of the normal rules is more problematic. This is because the evidence might not exist in a physical form. You will have the opportunity to explore further the nature of evidence in the forthcoming weeks. However, during this week, you will concentrate on issues concerning the standard and burden of proof.

**On completion of this unit you will be able to:**

* Explore the implications and limitations concerning evidence.
* Set the study of cyber forensic within the bigger context of law enforcement.
* Identify and evaluate information to build up a case analysis.

**Seminar 1**

#### Title: Cybercrime Case Analysis

Join the [**Seminar Session**](https://www.my-course.co.uk/course/view.php?id=8901&section=3) this week. Remember to bring the seminar questions and your attempted answers.

Visit the ‘Seminar 1 preparation’ below and attempt to complete the activities prior to the seminar session. As we will discuss these concepts in the seminar session, ensure you have completed the activities before this week’s Seminar session

## Seminar 1 preparation

#### Firstly, ensure you have completed the reflections from Unit 1 and come prepared to share your work.

Now, skim through the [**CPS (Cyber Physical Systems) guidance in: Cybercrime – prosecution guidance**](https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance), updated 26 September 2019.

Choose one of the cybercrimes in the guidance.

Write a brief (200-500 words) case analysis on the crime you have chosen.

The case analysis should provide:

* some description and explanation of the crime;
* identify its unique characteristics;
* evaluate the extent of which this cybercrime is different than its off-line version (if it lacks a direct comparison, assess whether this is a complete new offence or whether there could be any analogies with an even remotely similar offline offence);
* identify and assess issues concerning laws (you can focus on one jurisdiction or provide an international overview);
* identify and assess issues concerning burden of proof, standards of proof and admissibility.

You can draw upon the wider reading and carry out wider internet research.

Be prepared to share your case analysis in with the rest of the group (you can prepare a fact-sheet) and answer questions by tutor and fellow students.

**Remember**to also log your analysis in your e-portfolio.

#### Learning Outcomes

* Critically appraise the global legal and regulatory environment as it applies to cyberspace, and compliance requirements, including the GDPR and the obligations it imposes.