Unit 3 - The Evolution of Threats to Digital Platforms and the Skills Required to Counter These Threats

Overview

The candidate can demonstrate a clear knowledge of the types and range of threats to online activity, systems to thwart or deter them, and recommendations for the future. Candidates will list and describe the main threats, both hardware and software based, as well as personnel based, that threaten online activity. They will begin to investigate mechanisms that deal with these threats and show practical skills of deploying some of the solutions as well as setting them up to be more effective and efficient. They will then show how they can evaluate these different tools and systems and what strengths and weaknesses they may show. At the end, they will be in a position to make some recommendations based on various situations that are exposed to threats.

A work activity will typically be 'non-routine or unfamiliar' because the task or context is likely to require some preparation, clarification or research to separate the components and to identify what factors need to be considered. For example, time available, audience needs, accessibility of source, types of content, message and meaning, before an approach can be planned; and the techniques required will involve a number of steps and at times be non-routine or unfamiliar.

Example of context – this unit can underpin other units. For example, if learners are working on a DTP poster and a presentation to pitch the poster to a local company, how do they know what applications to use? How do they know how much time it will take? How will they organise their files and understand how to solve problems that arise? All of these are part of this unit so as long as they start planning using IT tools from the beginning, they will be gathering information to use for the IPU unit. This unit should be the start, middle and end of the course as it is related to all other units.

Assessor's guide to interpreting the criteria

General Information

RQF general description for Level 2 qualifications

- Achievement at RQF level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straightforward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.
- Use understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems. Interpret relevant information and ideas. Be aware of the types of information that are relevant to the area of study or work.
- Complete well-defined, generally routine tasks and address straightforward problems. Select and use relevant skills and procedures. Identify, gather and use relevant information to inform actions. Identify how effective actions have been.

- Take responsibility for completing tasks and procedures subject to direction or guidance as needed.

Requirements

- Standards must be confirmed by a trained Gold Level Assessor or higher.
- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.
- The work in the unit is recommended in order for candidates to have covered enough depth and breadth in the topic to successfully carry out their controlled assessment and take the external exam.
- When the candidate has covered as much of ths material as necessary to complete the controlled assessment element, they may be introduced to the topic
- This unit should take an average level 2 learner 25 hours of work to complete.

Assessment Method

This unit will be assessed synoptically via a controlled assessment and also through an external examination.

Expansion of the assessment criteria

1. Candidates will understand the different risks associated with online digital material

1.1 I can understand that digital material is a valuable commodity
Learners will be able to demonstrate in their own words what makes something digital become valuable and sought after

Evidence: vlog or ePortfolio

Additional information and guidance
Learners will begin to appreciate the real value of digital material and the need to look after it.

Learners can investigate material presented to them about the value of data theft and fraud so that they can begin to appreciate the scale of the problem.
The government's current estimates for 2017 are that cybercrime costs the UK £27 billion per year.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/fil... [1]

Learners can discuss what the value of information about them might be as a starting point to their other investigations in this unit.

1.2 I can appreciate that digital material can be stolen if unprotected or badly managed
Learners will provide evidence from their own research of examples of data crime.

Evidence: assessor feedback

Additional information and guidance
Learners will show a range of different crime statistics to back up their understanding. They could look at the local news and newspapers to find out crime data for their area. There are also websites which list crimes, though they may not break these down
into digital crimes.

They might be lucky enough to have a local police officer who is specialised in digital crime who can come and talk to students.

1.3 I can describe the ways that digital material is threatened
Learners will comment on the material they have gathered and offer their own opinions and analysis to show a deeper understanding of
the issues.

Evidence: Written list, table or report

Additional information and guidance
Learners will describe the details of the crimes to show how the threats came about in terms of poor security. At this level they do
not need to go into a great deal of detail, just to show that they are aware of the way that people can get data for illegal activities.

This might be a good point to reinforce how easy the Internet has made crime possible. Many students will no doubt think it is
acceptable to listen to illegally streamed music and films, or be using pirated software, knowingly or otherwise. It is also a good time to
discuss plagiarism and copyright in terms of stealing IP (Intellectual Property).

1.4 I can detail the ways that digital material can be protected
Learners will research and present their understanding of some ways and means to prevent some of the crimes they have identified
earlier.

Evidence: Written report or vlog, assessor feedback

Additional information and guidance

Learners will list some of the protection mechanisms they have discovered and depending on the audience they can either present it
as a report, as a presentation or even as part of their extended project. Some areas they should show knowledge and understanding of will be:

- personal: training of workers
- software: https vs http, encryption, SSL
- hardware: firewall, IDS
- organisation: AUP, security protocols

What kind of training do people need in order to prevent fraud and crime happening to them. What knowledge of software and hardware is generally required to be safe online and are there simpleways to protect these elements. What can organisations do in order
to protect themselves.

It might be useful for students to have a talk from the network team on what is being done to protect their data and how the learners
themselves can help in that process, if it is not already covered in a school induction process.

1.5 I can explain the different types of threat currently in action
Learners can discuss a number of the main threats currently in the news.

Evidence: Written report, or table.

Additional information and guidance

Learners will discuss their understanding of how the threats operate and their main characteristics. Many of these are in the news every
day so there should be no shortage of source material, but they will need to summarise it in a form that others can understand and
appreciate.

- Online fraud
- Scareware
- Identity Theft
- IP Theft
- Espionage
- Loss of customer data
- Online theft from companies
- Extortion
- Fiscal Fraud

It might be useful for learners to put these into a table that they can use in other presentations and documents.

Name of Threat	Main Characteristics	Prevention Techniques	Potential Damage
Online fraud	Email or phone calls etc, or fake websites used to collect information such as bank details	Check where email comes from, not clicking on links, use only trusted websites, filter phone calls	Loss of money
Loss of customer data	Carelessness: leaving company laptop on train	More care Damage Auto switch off if no key pressed Training	Damage to company reputation, being fired from job

1.6 I can explain the threats to my personal safety from online activity
Learners will explain the key types of threat that affect them personally when they operate online.

Evidence: video material as report or assessor feedback

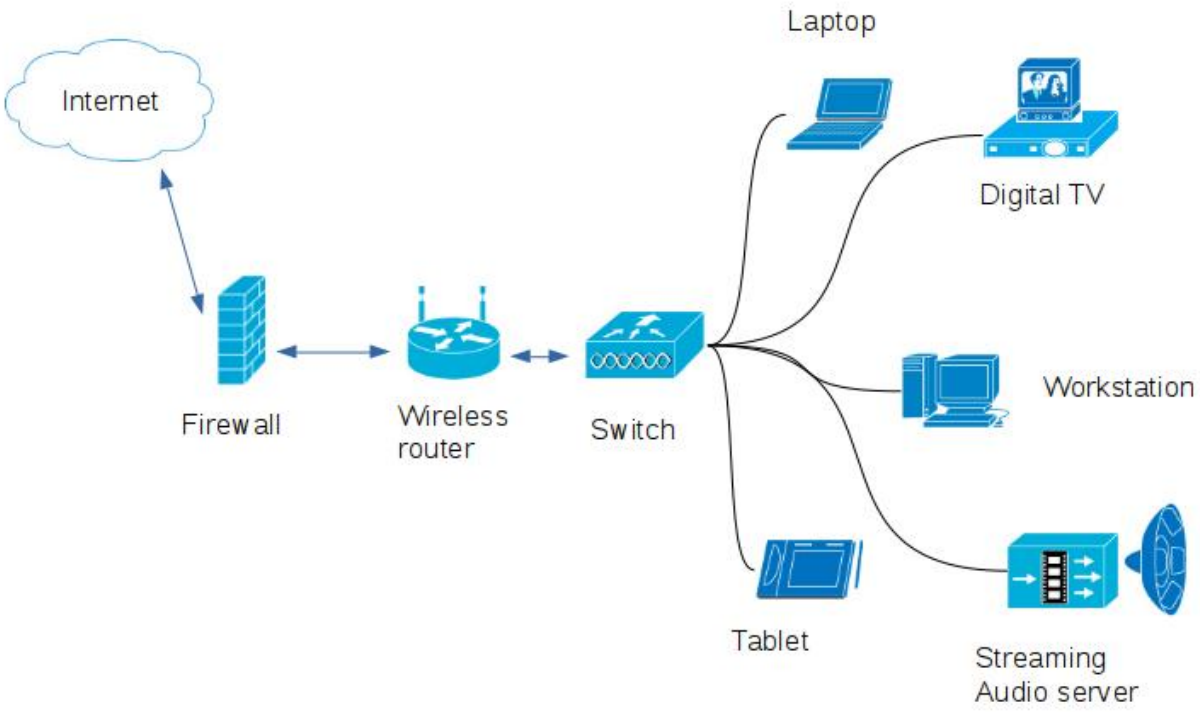
Additional information and guidance
Learners can reflect on these threats and rate them in terms of the likelihood of them occurring and what actions they will take to
minimise them. This could be as a report.

2. Candidates will plan, create and deploy systems and processes to minimise threats

2.1 I can detail the processes I use to protect my digital material
Learners will document and detail, with commentary, the actions they take to protect themselves online.

Evidence: diagrams, written reports.

Additional information and guidance
Learners will describe a situation that could occur in order to illustrate how their processes are effective at each point. They could
also diagram how they protect themselves at home from potential attacks.



You can add these types of network icons to LibreOffice by following the instructions here:

https://smacak.wordpress.com/2011/01/26/opensource-alternative-to-micros... [2]

2.2 I can describe the systems I use to protect my digital material
Learners will describe in detail the software they use to protect themselves from online threats.

Evidence: descriptions of their diagrams or video vlogs.

Additional information and guidance
Learners will know the vulnerabilities of different transmission protocols and be able to use this information to protect themselves.
Protocols they will have working knowledge of will include:

- Bluetooth
- SMS
- http and https
- wireless
- NFC

Learners will describe in detail the hardware they use to protect themselves from online threats. In most cases this will be some kind
of home based firewall. What are the attributes that make it work for them. What are the key features that protect their data from being
stolen and how would they know if it was?

2.3 I can describe the nature of different threats
Learners will pick a number of threats from 1.5 or their own research and describe in detail their attributes and strengths and weaknesses.

Evidence: Report or table of data

Additional information and guidance

Learners will illustrate their understanding with detailed examples and commentary. What makes something a threat rather than just
an annoyance? Do they have examples of threats that have occurred to them they can define and describe. Have they received
bogus emails asking them for money from a bank they don't have an account with. Why would anyone respond to these? What it is about
these that make them effective? What are some of the statistics about online fraud and threat that they can use to back up their
descriptions.

2.4 I can describe a working system that protects my digital material
Learners will give working examples of a system that will protect them from online harm.

Evidence: Written report or video based one, assessor feedback if class based project

Additional information and guidance

Learners can use the diagram they created for 2.1 and add in some detail about how each piece is protecting them or exposing them to
threats if not properly configured or maintained.

2.5 I can explore alternative methods to prevent future attacks on my digital material "a system is only as good as it's weakest link"

Having understood the vulnerabilities of a personal communication device (2.1) Learners can research and comment on different types
of software and hardware to the ones they currently use.

Evidence: ePortfolio and assessor feedback

Additional information and guidance
Learners will demonstrate an understanding of cost benefit and how more money may not deliver more security.

Learners will show an understanding that there is a trade off between security and flexibility. At what point does a system become
unworkable because it is too secure?

If they had unlimited amounts of money, how would they upgrade their home system to make it as secure as possible?

2.6 I can explain how different types of online activity bring with them a variety of risks to personal data and security
Learners will discuss a range of online activities and rate them in terms of their understanding of the risks associated.

Evidence: Own policy and procedure document

Additional information and guidance
Learners can create a blog or vlog to show the types of activity they undertake online and what types of risk are occurring at different stages of their activity. This is to collate all of their skills and understanding into a clear and concise form that can be either
presented in person or as a report. Candidates need to be aware that they may not even be aware of some threats like this [3].

3. Candidates will analyse and apply tools and systems to minimise threats to digital material

3.1 I can analyse the latest hardware technologies to prevent attacks on digital material
Learners will demonstrate a deeper understanding of the available hardware so that they can advise others on the suitability of choosing
equipment.

Evidence: assessor feedback and ePortfolio pages

Additional information and guidance
Having explored and researched various pieces of equipment in their research and practical exercises, learners can now make some
reasoned judgements, backed by their statements, about what kinds of technologies are the most appropriate. Are we at the point where
all home require hardware based firewall appliances? With more and more of our internal lives networked with IoT (Internet of Things)
devices like smart heating monitors and smart devices, are the simplistic firewalls that are part of home broadband routers enough
to protect our privacy? How do you know when someone is logged in to your Wi-Fi system and using it for other purposes. How well do
you understand the setup and use of a DMZ (Demilitarised Zone) on your home network. What ports are vulnerable and exploitable. If
large companies and banks struggle, what chance do we have at home?

Learners should gather some specifications on hardware and make reports about their features, perhaps comparing them in terms of
features and prices.

3.3 I can analyse the latest software technologies to prevent attacks on digital material
Learners will demonstrate a deeper understanding of the available software so that they can advise others on the suitability of choosing
equipment.

Evidence: Written or video report

Additional information and guidance

As above, what systems do they have in place to protect their own environment and how good are they at what they do. How do you
know they are working as well as they should. How do you keep track of the latest updates to software patches and exploits that have
been found.

As with the hardware, learners can compile a report to compare and contrast the different offerings in terms of suitability, features and
cost. What services are in place for software and hardware from your own ISP (Internet Service

Provider).

3.3 I can evaluate the current threats to my personal digital material and explain which offer the greatest risks

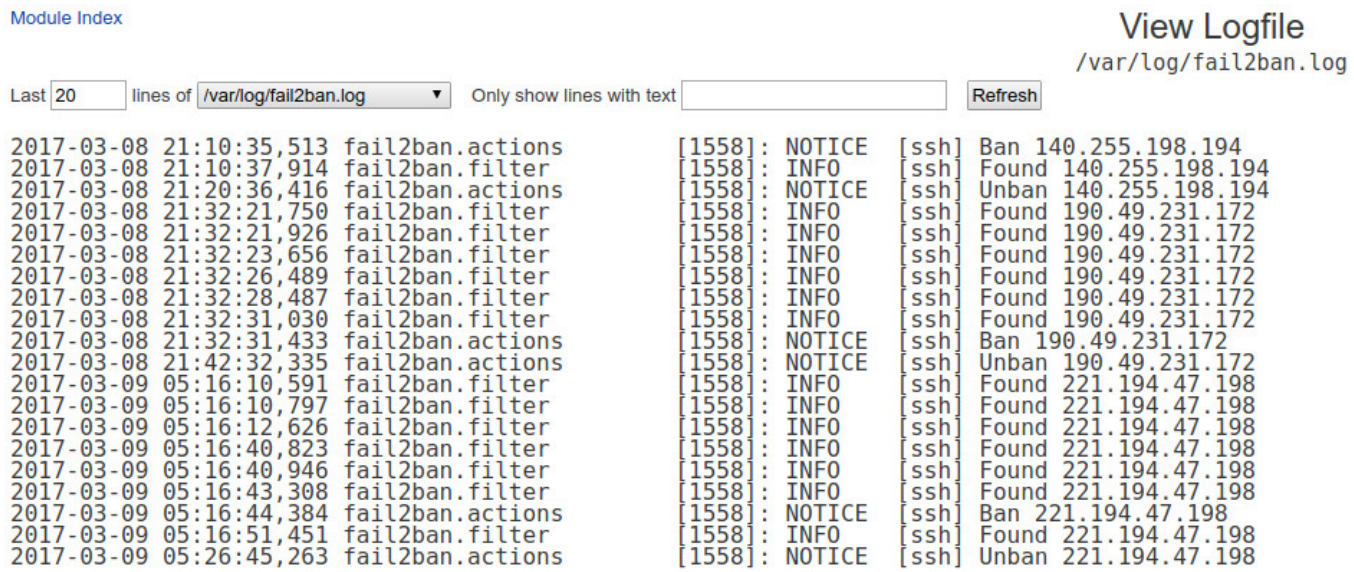
Learners will be able to demonstrate an understanding of software and hardware log files in order to fully understand what threats are
occurring.

Evidence: Forensic report on their systems or the school/college

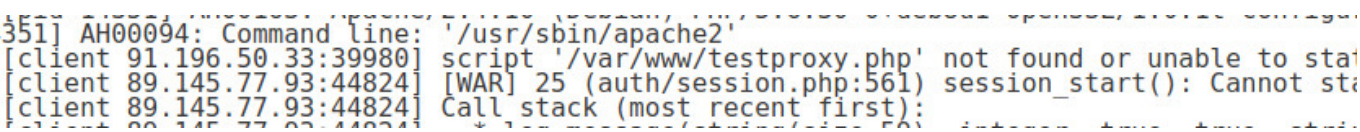
Additional information and guidance

Learners will comment on these findings to demonstrate their level of understanding and to inform their actions.

Operating systems have some of their own built in protection which can be used as a second way of understanding what is happening to
your network and therefore your digital material. The following is a log file from a software system on Linux called Fail2Ban which
detects unwanted attacks and bans them from trying for several minutes. When they try again later they will be ignored and
eventually go away.



This is on a home based server running a DMZ. On the router itself, most users should have some security logs which can be examined.
The following image is an attack on a web server software trying to run a script which might be there to exploit.



Learners should be able to give some examples of what threats they face from various areas, as well as threats created by bad habits
such as staying logged in on the school network, sharing passwords with friends or using public Wi-Fi systems.

3.4 I can evaluate the best methods of protection and recommend protocols to minimise the threat of attacks

Learners will explain some of the protocols used in their systems and link these to the identified

threats.

Evidence: Written report of protocols or video based.

Additional information and guidance

Learners will develop a working protocol for their own protection or recommend one for others.

A protocol is a set of rules that need to be followed to achieve a particular goal. In this case, it would be useful if learners could create a set of rules and guidelines to be followed. This could be for their own home, their school, or for a local company.

3.5 I can recommend systems to enhance security
Learners will be able to identify weaknesses in systems in order to recommend enhancements.

Evidence: Written or video based report, assessor feedback

Additional information and guidance

Learners will collect their findings in order to support these recommendations.

This material can be used as part of the presentation for 2.6. If they are working for a local company as a client, or as part of their
extended project they should have some specific details, though these may need to be anonymised to protect the company. This is a
collation of all their findings and understanding as well as practical demonstrations of what they have discovered and what constitutes
best practice.

3.6 I can provide cogent advice to other users about being safe online
Learners will generate a report to present to their peers on their advice and recommendations.

Evidence: Presentations and report to others

Additional information and guidance
Learners could create a questionnaire or survey to be used by local companies in order to evaluate their security protocols or services
and then to use this to report on improvements. They could also do this as a short video, perhaps loaded onto a video display system.

They should be able to demonstrate that they understand enough about the more common problems associated with online activity to
be able to help others, even if this is pointing them towards resources such as CEOP.

https://www.ceop.police.uk/safety-centre/ [4]

Perhaps they are part of a local club or organisation and they can offer them advice about online issues, or present as a group to in-coming Year 7 students.

Links
[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[2] https://smacak.wordpress.com/2011/01/26/opensource-alternative-to-microsoft-visio/

[3] http://www.bbc.co.uk/news/business-40324983
[4] https://www.ceop.police.uk/safety-centre/