



---

# Functional Skills Certificate

## FUNCTIONAL ENGLISH

Component 1 Reading Level 2

---

### Insert

The three sources that follow are:

- Source A: a news report about computer hacking
- Source B: a webpage about Cyber Security Challenge UK
- Source C: an article about cybercrime.

**Please open the insert fully  
to see all three sources**

## Source A

**“I Was Lucky”: UK’s Youngest Hacker**

***“I started getting into the illegal side of hacking when I was 11 years old. I was first convicted under The Computer Misuse Act (1990) at the age of 12. I’m still the UK’s youngest convicted hacker.”***

10 years ago, Cal Leeming was convicted of using over 10 000 stolen identities to buy £750 000 worth of goods. Now a 29-year-old reformed character with jobs in cybersecurity and public speaking (on the topic), he’s keen to tell his story.

He suffered a number of challenges as a child. His single parent mother was dependent on Class A drugs and he would use stolen cards from the web to buy groceries for his family. But how did it spiral from ordering food to stealing much more valuable things, leading to his eventual conviction?

***“The people I was getting involved with and the crimes that were being committed got more and more serious,”*** he says. ***“I was breaking into company websites to steal data. It got to the point where I was buying like a thousand pounds’ worth of things and would get it sent to my house.”***

Once in prison, Leeming struggled with adjusting to a life without a computer. Plus, he didn’t find any other inmates who were fellow hackers.

The arresting officer in his case, Officer Clive Read, really helped Leeming after his release by introducing him to a bank and giving him a reference for his first job in London. ***“I got lucky,”*** he says. ***“You see schools constantly reporting children to the police for hacking into their systems, rather than dealing with it in-house and trying to mentor them. Trying to scare them away from hacking isn’t going to work for the majority. We shouldn’t make criminals out of them.”***

Some people believe that juveniles who find themselves convicted of hacking offences should be treated very severely. Others, however, will argue that everyone deserves another chance like the one that Leeming was given.

Leeming argues that, in a time where we are seeing an ever-increasing threat of cybercrime, it is far better for both society and offenders themselves to focus on helping hackers to use their skills for good.

And, in his case at least, it seems to be working out pretty well.



Source B


[Register to Play](#)
[Play Now](#)
[Competitions](#)
[Education](#)
[Sponsors](#)
[News & Events](#)
[Inside Cyber](#)

## UK's first cybercrime intervention workshop

Cyber Security Challenge UK has worked closely with the National Crime Agency (NCA) and industry partners to deliver a new scheme to rehabilitate young people who have committed low-level **cybercrimes**. The Intervention Day was held at PGI's Cyber Academy in Bristol. Its aim was to prevent them from re-offending and to encourage them to consider legal jobs in the cyber security sector. The cyber security industry estimates that 1.8 million more skilled workers will be needed by 2022.

These young people, aged 14–18, took part in workshops and training to highlight how talents could be used in legal and well-paid jobs, as well as hearing from a former hacker who transformed his life. It is believed that the rise in the number of young people committing **cybercrimes** results from a lack of education or a lack of a safe space to experiment. Debbie Tunstall, Head of Education said, "These young people often have the exact kind of abilities needed to plug the skills shortfall and we must support the Government in setting them on the right path."

There are currently no formal **cybercrime** rehabilitation programmes, as there are for crimes such as speeding, assaults or drugs. Early intervention is essential to ensure young people do not become involved in further offending with their career prospects being damaged. The average age of arrest by the NCA's National **Cyber Crime** Unit was just 17 years old in 2015, in contrast to the average age of 37 for those arrested in drugs cases, and 39 years old for economic based crimes.

Richard Jones, from the NCA said: "**Cybercrime** is increasingly easy to commit because there are so many easy-to-access tools, tutorials and online forums to share ideas. Even the most basic forms of **cybercrime** can have huge impacts and the NCA and police will arrest and prosecute offenders, which can ruin their future. That means there is great value in reaching young people before they ever become involved in **cybercrime**, when their skills can still be a force for good."

*"We want to demonstrate that a career in the industry can pay a lot more than cybercrime and can give them the sense of achievement and respect they are seeking."*



## Source C

### CYBERCRIME

You are now 20 times more likely to be robbed while at your computer by a criminal based overseas than mugged in the street.



The explosion in online fraud and cyber-crime saw almost 6 million offences committed in 2015. This means around one in ten adults in the population fell victim. Fraud has now become the most prevalent crime in the country with people ten times more likely to become a victim than they are to suffer a theft.

Unlike many traditional crimes, the victims of cyber offences are drawn from all ages, all social backgrounds and all areas of the country. Therefore, no-one who uses a computer regularly can feel safe.

Cyber-crime covers a wide range of offences including bank and credit card fraud. The unfortunate victims are sometimes not even aware they have been targeted until they realise their savings have been raided. By then it is often too late.

Then there are online shopping rip-offs and hacking. In many cases the perpetrators are based overseas, but are able to gain access to people's bank accounts remotely by conning them into revealing personal details and passwords.

With phishing, the aim is to trick people out of money or bank account details by getting them to click on a link in an email. There are even cruel "romance scams" where people are persuaded to part with thousands of pounds by someone posing as their lover online.

Around 1.4 million people suffered computer virus attacks, with almost 650 000 people reporting that their email or social media profile had been hacked. The number of victims of identity theft rose by 31% in the first 3 months of 2015.

A City of London police spokesman said, "Given the nature of this threat, victims must do everything they can to protect themselves; always being wary about who they are interacting with online and taking time to think before making any online transactions".

**END OF SOURCES**

**There are no sources printed on this page**

**Open out this page to see  
Source B and Source C**

**There are no sources printed on this page**

**Copyright information**

For confidentiality purposes, from the November 2015 examination series, acknowledgements of third party copyright material will be published in a separate booklet rather than including them on the examination paper or support materials. This booklet is published after each examination series and is available for free download from [www.aqa.org.uk](http://www.aqa.org.uk) after the live examination series.

Permission to reproduce all copyright material has been applied for. In some cases, efforts to contact copyright-holders may have been unsuccessful and AQA will be happy to rectify any omissions of acknowledgements. If you have any queries please contact the Copyright Team, AQA, Stag Hill House, Guildford, GU2 7XJ.

Copyright © 2018 AQA and its licensors. All rights reserved.