Emerging Cyber Security Threats to the Integrity of UK Teaching and Learning

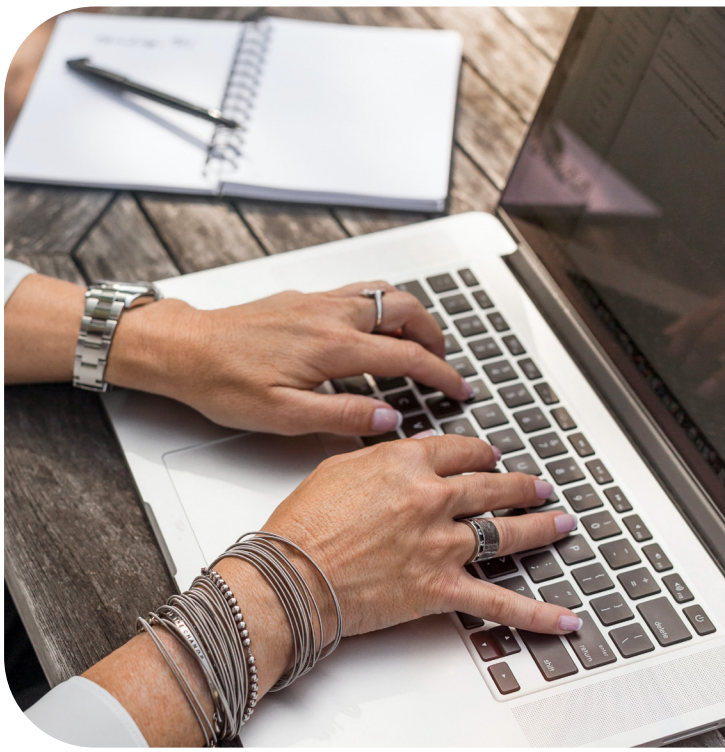
July 2021

Introduction

Over the last decade, a widespread online industry of professional contract cheating services has developed. These companies have become known as 'essay mills', although many supply a range of services in addition to essay writing. Research published by Swansea University in August 2018 indicated that as many as one in seven recent graduates internationally may have paid someone to undertake their assignment for them.

Academic misconduct presents a threat to the world-class reputation of UK higher education. However, the implications go far wider than higher education; students who cheat can enter the workforce without the necessary skills, knowledge and competency, with potential public health and safety implications. Extortion and blackmail are also becoming greater threats to people who use essay mills. Personal data may be stored online with minimal if any security, exposing customers to identity theft and bank fraud.[1]

In 2020, QAA guidance identified that essay mills have been seeking to take advantage of the COVID-19 pandemic to target students. QAA has been working with international partners to identify emerging threats and in April 2021 notified all UK higher education institutions to inform them that Australia's Tertiary Education Quality and Standards Agency (TEQSA) had identified a new cyber security threat.



TEQSA's research found that essay mills had been compromising websites of Australian higher education providers through inserting malicious code that redirected students to contract cheating websites. It is recommended that providers conduct an investigation of their websites for infiltration or vulnerability, and this document is intended as practical guidance that institutions may wish to draw upon in order to address these cyber security threats and others.

[1] Sutherland-Smith, W and Dullaghan, K (2019), You don't always get what you pay for: User experiences of engaging with contract cheating sites, Assessment & Evaluation in Higher Education, 44:8, 1148-1162, DOI: 10.1080/02602938.2019.1576028

Jisc's advice on emerging cyber security threats

In addition to significant changes in tactics around ransomware targeting organisations, there is growing evidence of a change in criminal activity targeting students in connection with essay mills services. This is in support of a growing international economy in the sale and purchase of essays and course related material. Whilst the sale or purchase of such material is not currently illegal in the UK, claiming this material as your own in support of a formal academic qualification is fraudulent.

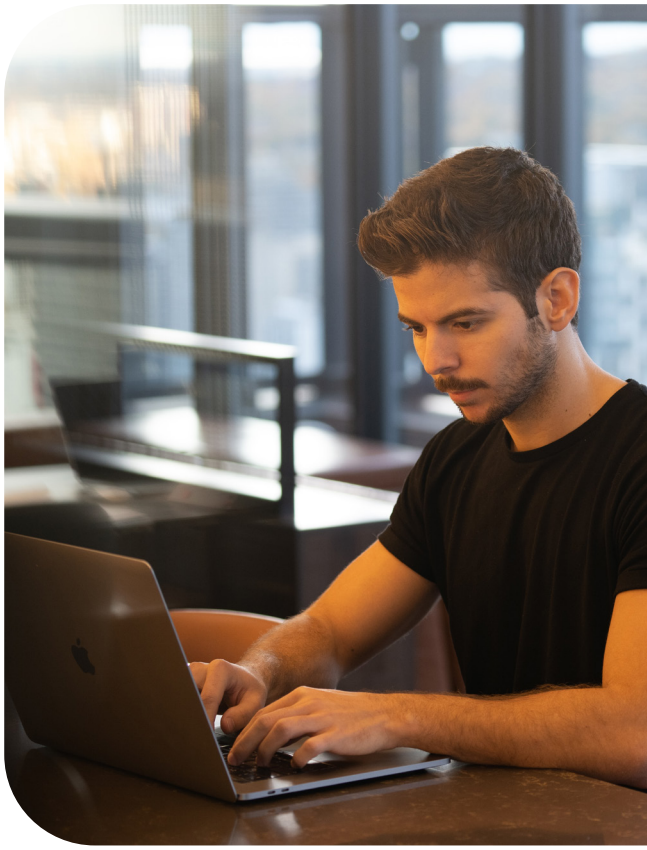
In the same way as for ransomware, the starting point for this activity is gaining unauthorised access to computer systems. A ransomware attack seeks to exfiltrate data, encrypt and disable digital infrastructure with the object of placing maximum pressure on an organisation to pay a ransom. In these emerging attacks, criminals are seeking to hijack legitimate student-facing websites to promote essay mills services via re-direction and other means.

Types of malicious code

TEQSA identified four key types of malicious code in Australian university domains:

- code inserted into a provider's website to redirect students to a cheating service website from specific URLs
- links to a contract cheating website being embedded within a provider's website
- comments inserted to propagate or provide links to contract cheating services in discussion forums (especially in WordPress)
- fake scholarship/essay contests inserted into provider websites, designed to harvest original student work that the commercial academic cheating companies then sell on.

The existing guidance provided by Jisc and NCSC on defending against ransomware attacks applies equally to mitigating the impact of these new attacks. However, whilst ransomware seeks to be hugely disruptive, these attackers are seeking to remain undetected and persistent for as long as possible. This necessitates awareness and vigilance on behalf of staff and students, so early detection and mitigation can be undertaken.



Jisc provides cyber security services that can block known malicious content in the context of sites hosting command and control software or known malware, helping mitigate phishing and other forms of attacks against UK education and research. This is provided to members via the Janet Network Resolver Service (JNRS) on an opt-in basis. Jisc is currently consulting on changes to the Janet Security Policy to deliver some services on an opt-out basis.

In seeking to take a proactive stance against these evolving threats, Jisc will be working with universities, colleges, representative bodies and regulators to help coordinate a policy-based approach to blocking a greater range of cyber security threats.

Practical guidance and useful resources

Colleges and universities must remain vigilant to the evolving threat landscape. Many of the controls that can be deployed to help improve cyber resilience in relation to one of the biggest current threats - ransomware - also provide wider protective benefits to users and organisations. This is important because students remain an active target for cyber criminals.

Students have long been a target of student loan payments fraud via phishing attacks, but there are growing threats from services sold to students, including from contract cheating sites or essay mills. Students need to be aware of the increased risk they face by using contract cheating services. QAA's Contracting to Cheat guidance includes case studies on raising awareness with students.

In addition to raising awareness, organisations should implement effective protective measures against website defacement and hijacking, as well as the ongoing ransomware threat. These include:

- securing all services using strong passwords and multi-factor authentication
- maintaining effective vulnerability and patch management policies
- maintaining vigilance and awareness that criminals are seeking to legitimise their services by embedding content into student-facing systems.

If a college or university does suffer a cyber attack, there are recommended recovery measures to take. These include:

- effective and timely recovery of systems from offline backups
- exercise and rehearse your incident response plan for a range of cyber security incidents.

Any Jisc member needing support to prevent cyber security incidents or recover from attacks should contact the Janet Network computer security incident response team (CSIRT) via irt@csirt.ja.net or 0300 999 2340.