VB2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

THE HISTORY AND TACTICS OF VISA-CENTRIC SCAMS IN SEARCH, SPAM, AND SOCIAL APPS

Chris Boyd

Malwarebytes, UK

cboyd@malwarebytes.com

ABSTRACT

Immigration and visa scams are big business, leading to large profits for some and misery for others. These attacks have evolved over the years to target everyone from workers to students and family members, often with potentially devastating results for those affected. Recent developments have even seen people working in the legal profession and crisis/emergency visa groups targeted in the drive to obtain both funds and data.

This paper explores a variety of historical and current attacks in this realm, and how said attacks have evolved over time alongside some of the tactics used to shut them down.

From dubious ESTA search engine results and bogus visa offers via *WhatsApp* to stolen laptops leading to blackmail, the chosen targets are ideal for fraudsters. We have people with insecure immigration status, who may not understand complex and ever-changing rules. Workers without the funds to fight what they believe to be genuine threats to their residency permits. Students who often arrive with their digital documents on laptops, ripe for the taking and using the data contained within against them.

Spam and social engineering attacks via email, social networks and IM services will be explored and explained, including the risks to those handling client data and how some United Kingdom Visas and Immigration (UKVI) processes have given me some cause for concern in my own dealings with the British Home Office.

With so much immigration work being handled remotely, convenient forms of digital communication are being restricted from use by immigration firms due to increasing amounts of imitation and fraud. Add scams into the mix, targeting crucial aspects of the economy like health and care visas, and we have a recipe for disaster.

This presentation will highlight the most significant aspects of this realm of security and give attendees a hopefully new insight into a not commonly explored area of information security.

INTRODUCTION

The British immigration system, managed by UKVI (United Kingdom Visas and Immigration, a division of The Home Office), is one of the most expensive [1] and arduous visa systems in the world. A combination of tough rules and harsh punishments for potential violations have created an environment where migrants are prime targets for fraudsters.

Attacks also target holiday makers and long-term residents in other countries too. The more money is sunk into a system, the bigger the risk for applicants. The UK system is particularly attractive as scammers know the majority of applicants able to apply potentially have a high income and/or large savings. This is partly as a result of how costly the fees are.

The current UKVI transparency index highlights the discrepancy between the actual admin cost of processing an application and the cost to the applicant [2]. An application for permanent residency with an admin fee of £491 may cost the applicant £2,404. If a Government was going to be incredibly overt about which pool of applicants are prime targets for having some money in the bank, this would be the way to do it.

Over the years, specific forms of fraud have evolved to target certain groups of visa holders. These attacks take note of the current immigration rules and tailor their methods appropriately. If a need exists for healthcare workers, groups will target said sector and offer to cover certain fees. When international student numbers increase, fraudsters will use data theft and blackmail to make money.

Even refugees and people working in immigration law are targeted. These attacks can have devastating effects on the victims. Loss of funds can mean no money to pay for expensive visa renewals and loss of residency. Becoming embroiled in a scam can have serious legal consequences for the victim, as we'll see below.

PAID ESTA RESULTS IN GOOGLE ADS

The US Department for Homeland Security began charging British applicants to use the Electronic System for Travel Authorization (ESTA) in 2010. This allowed successful applicants to fly to the US on a visa waiver.

Search results began appearing in *Google*, offering 'assistance' to fill in the reasonably straightforward ESTA online forms. These sites typically charge a much higher fee than you'd pay doing it yourself directly on the official ESTA portal (£10.70 in 2018, now roughly £16.96 in 2023). Images and text would frequently be copied directly from official sites, with little indication of the qualifications for immigration advice on display.

Using sites like these potentially puts your data at risk, or leaves you open to social engineering attacks at a later date. These types of portals are not limited to ESTA scams, and in 2018 *BBC* reporters found portals targeting Australian and Canadian visit visa services too [3]. One of my own relatives lost money to a site offering similar visa assistance services to travel to Egypt, via a site found close to the top of search engine results.

Google's policy at the time forbade this type of activity [4]:

> '*Charging for products or services where the primary offering is available from a government or public source for free or at a lower price.*'

A follow-up investigation in 2020 discovered assistance sites still appearing in paid search results charging more than they should be [5], despite *Google* taking a firmer stance on said advertising [6]:

> '*New policy for government documents and official services.*
>
> *Google will no longer allow ads for documents and/or services that can be obtained directly from a government or a delegated provider. This includes offers of assistance to obtain these products or services.*'

Unlike the examples given by *Google* on their 2018 page, some of the (non-exhaustive) examples now explicitly highlight visa and Electronic Travel Authorization assistance. There has been no apparent change to this policy since 2020, and yet sites offering ESTA assistance at a higher price than official government portals are still appearing in search results.

In what may be a tactic to evade accusations of offering services at higher fees than are standard, sites in sponsored slots now offer very little in the way of upfront information regarding cost. In practically all cases I've observed, sites want you to submit a wealth of personal data before seeing any mention of fees. Specific costs aren't listed in terms and conditions, and the first direct mention of payment tends to be listed close to (or at the end) of a list of personal data entry forms.

Remember that, under the 2020 advertising rules, whether fees are listed or not should now make no difference ('*this includes offers of assistance to obtain these products and services*'). Despite this, a simple search for 'ESTA form' will routinely return a maximum of four sponsored ESTA assistance sites above the official Homeland Security application page.

PERMANENT RESIDENCY SCAMS

People looking to start a new life somewhere else can have their plans destroyed before they get started. Depending on the country, some paths to permanent residency (PR) are via direct application for the initial entry visa, and portions of others are tied to a so-called 'lottery system'. This is where applicants register for the chance to be randomly drawn from a candidate pool. In the US, the lottery system (officially known as the Diversity Immigrant Visa) selects 100,000 applicants annually to potentially obtain one of 55,000 visas [7].

Regions, not countries, are granted allocations of visa places determined by whether the region is considered a high or low admission region. Millions of people apply, and so scammers claim to offer services to grant an edge to applications. The lottery application period is October through November, and it is free to submit an application.

Despite this, the assistance sites will charge fees regardless of whether or not an application is successful. It's worth noting that, although applying through the lottery system is free, a successful green card allocation will require payment as normal so it's possible that the actual green card fees may have been wasted on a needless assistance website [8].

Scams in this realm are rife, with a specific warning from the FTC on what to look out for when considering submitting an application [9]. In 2018 we found a site claiming to be the 'Official website to apply since 1996', despite being wholly unofficial and openly admitting [10]: 'we are not a law firm, we do not provide legal advice, and are not a substitute for an attorney. This site provides a review and submission service that requires a fee.' Paying people with zero legal background for immigration assistance is a terrible idea.

In the example above, the basic fee was £104. In a call with a sales rep, they tried to hard sell us an 'upgrade' package which would grant multiple chances to 'win'. This is not how the diversity visa program works. No information was given to our researcher as to how the actual process works, nor did they reveal what giving them money would actually accomplish.

As we observed at the time, the sheer convoluted business of immigration services coupled with austere design may make it more likely that someone will turn to a scam site. The genuine lottery page was sparse, lacked informative and easy to understand descriptions, and provided no way to obtain additional information.

By contrast, the previously mentioned fake 'official' site appears to go out of its way to help. It looks friendly, offers FAQs, and appears to strip the uncertainty from the process. You'll notice a similar trend when looking at ESTA assistance sites. Compared to the real thing, they offer everything from live chat to pages of unrelated but helpful advice on travel customs, sights to see, and more. If you were in a position where you needed assistance with an ESTA or a lottery application, which one would you choose?

FAKE WHATSAPP VISA OFFERS

WhatsApp is a fantastically convenient method of communication, but its ease of use is being ruthlessly exploited by visa fraudsters. Likely inspired by the use of IM comms during the pandemic, they're cynically targeting some of the most desperately needed areas of the UK workforce and exploiting visa applicants along with it.

The UK is currently in dire straits where hospital and care worker staff are concerned, with major recruitment drives taking place overseas in recent years [11]. Some health professionals are so thin on the ground that those roles fall under the 'shortage occupation list'. These positions can potentially be paid a lower wage than other jobs, but the requirements for gaining these roles may be less harsh than other positions as a result. This makes them attractive to applicants, and scammers know that there are lots of medical applicants out there.

One of the first prototype versions of this scam targeted visa applicants generally in the middle of 2022 [12], with websites claiming the below:

> '*UK GOVERNMENT JOB RECRUITMENT 2022: This is open to all Individuals who want to work in the UK, Here is a great chance for you all to work conveniently in the UK. The UK needs over 132,000 workers in 2022. Over 186,000 Jobs are Open for applying. THE PROGRAM COVERS: Travel expense. Housing. Accommodation. Medical facilities. Applicants must be 16 years or above. Can speak basic English. BENEFIT OF THE PROGRAM: Instant work permit. Visa application assistance. All nationalities can apply. Open to all individuals and students who want to work and study. Apply here [URL removed].*'

Anyone familiar with the UKVI system would spot multiple warning signs in the above message. The Home Office does not cover the cost of accommodation or flights. 'Free access' for visa holders does not exist. All applicants pay an annual immigration health surcharge to grant access to NHS services, and this fee is paid upfront before a single line of the visa application is entered. The minimum age for a work visa is 18, not 16, and in most cases you need to be able to display knowledge of the English language through one of several qualifications.

'Can speak basic English' likely won't satisfy entry requirements. The scammers even claim an 'instant work permit' is possible, without mentioning that additional fees are required for same day/next day processing. Even then, many fast-track processing services were still offline when these messages were being sent out, either because of the pandemic [13] or because of the invasion of Ukraine [14].

Sadly for applicants, there's a good chance they won't know all of the fine details of this complicated system. The site asked for some basic personal information, and then directed applicants to a series of survey scams and other sign-up forms.

Wind forward to March 2023 and the stakes have risen even higher. The Law Society of Scotland is now warning of a rise in fraudsters impersonating solicitors, with these scams becoming visible from around February 2023 [15].

These scams take the *WhatsApp* tactics a step further, claiming to offer assistance with crucial health and social care visas in return for fees totalling 'hundreds of pounds'. What this means in practice is people potentially losing all of their application money, their chance to obtain a visa, and the UK missing out on someone who otherwise would have moved to the UK and started working as a healthcare professional. The scammers are also mentioned as having asked for additional documentation such as passport scans.

Additionally, they're reported to use the logos and addresses of genuine law firms [16, 17]. This information is fairly easy to obtain online, either from the British Office of the Immigration Service Commissioner list for OISC approved immigration advisers, or by searching for law firms generally.

TARGETING INTERNATIONAL STUDENTS

Students make up the biggest annual number of long-term residents in the UK, with yearly cohorts numbering in the hundreds of thousands. In the year ending March 2023, there were roughly 480,000 student visa grants, which is a 22% increase on the previous year [18]. Until recently China generated the biggest student numbers, with India now taking the top spot. Despite this, the most recent Chinese cohort is around 100,000 visas. This is fertile ground for scams and targeted attacks, some of which descend into blackmail.

One reason why fraudsters target students generally is because international student visas are a potentially expensive proposition for someone intending to study in the UK. The cost of courses can range between £11,400 to as much as £32,081 [19]. There are also visa fees to consider, including the immigration health surcharge and additional costs if the student is allowed to bring dependents.

This means there is a natural assumption that students are incredibly wealthy and so worthy of being targeted. As the UK receives so many students from China, scammers likely assume students from China have a lot of money – something that students themselves have noted [20].

2018 and 2019 were interesting years for attacks on students, with many cases of them being turned into money mules and dragged into money laundering cases. One such example involved the British National Crime Agency freezing close to 100 bank accounts, with the students affected 'mostly from China' [21]. With the students likely unaware that using their bank accounts in this way could get them into trouble, many will already have returned to China by the time the fraud has been discovered.

Elsewhere, Belfast saw at least 12 students accused of connections to an alleged £16 million money laundering scam run by a 'Chinese crime gang' [22]. In that particular case, students claimed they were offered £300 to open a bank account on behalf of the fraudsters. When you're an international student, every penny counts and there's no doubt a lot of individuals would have no idea quite what they were getting into.

While these are more general attacks exploiting students as money mule prospects, warnings from education institutions first become noticeable somewhere around 2016 onward, with the UK Council for International Student Affairs warning of the following potential threats to international students' wellbeing [23]:

- Criminals pretending to be in education, UKCISA itself, or the Home Office.
- Payment demanded via *Western Union* to avoid problems or deportation.
- Potential mention of some personal information to make the scam seem more genuine.
- Fictitious claims of immigration problems related to their visa, resulting in a fine.

The tactics used vary, but these are the main concerns as far as educational institutions go. Likely recognizing the large number of Indian students attending UK universities, some of these attacks quickly broadened out to include said cohort as a target alongside students from China. In 2018, Manchester University's Student Union warned of a phone scam leading to thousands of pounds in losses [24].

Both Chinese and Indian students reported phone calls from individuals claiming to be law enforcement and/or the Home Office asking for money to avoid potential visa disputes. Threatened with claims of involvement with criminal activity should the student hang up the call, they would cite deportation notices and a 10-year entry ban should the 'fee' not be paid immediately.

Another more complicated scam targeting Chinese students involved receiving a call from someone pretending to work for a package delivery firm [25]. In this example, the fraudster informs the student that the package contains something 'incriminating' and has the student's name on it.

They then call the student while claiming to be law enforcement from Shanghai, and make reference to the supposedly incriminating parcel. At this point, the student is told to make a financial transaction so the police can check that the student is innocent. The number the scammers use is a clone of the genuine Shanghai police force, so a quick *Google* search would make it all look very realistic despite the absurdity of the premise.

Paying money isn't the end of the ordeal, and the student is asked for more money along with copies of bank details, passport, and ID card. This attack has netted considerably larger profits elsewhere, with one student in Hong Kong losing roughly £306,000 via the 'suspicious parcel/police have been alerted' routine [26].

A few unfortunate individuals appear to have fallen victim to attacks almost as soon as they landed in the UK. In 2019, a first year student had their laptop taken at Heathrow Airport. Phone calls to the student began shortly after, with criminals using the fake law enforcement tactics mentioned above [27]. They claimed to be from the Chinese embassy, having been referred by police officials insisting the student was involved in money laundering. This is how many of these attacks play out, but this one was to have a surprising twist.

The student was directed to a website claiming to belong to the prosecutor general's office. Said website contained uploads of the student's personal details, including her national ID card and photograph. All this information plus banking details had been left unsecured on the stolen device, and now the criminals were happy to make use of it.

She was threatened with deportation and imprisonment via web streams of men wearing police costumes, and forced to upload a recorded statement to social/IM service *QQ*. £30,000 was gone forever after being sent to the fake embassy workers.

This is a very alarming occurrence. Are there gangs specifically stealing laptops from students to grab exposed personal information, then sending it to mainland China for the second stage of a very costly ruse? Or did someone randomly steal a laptop and somehow get in touch with a criminal gang who likes to play dress-up and spend their time extorting students? The latter seems unlikely, while the former raises many more questions.

Is this a common occurrence? Is this a one-time-only group who came up with a very niche fraud angle? Either way, a new arrival to the UK would almost certainly have no idea that such an elaborate scam exists. If someone has a laptop on display, there's every chance some juicy data is on board and could be used against them further down the line.

ATTACKS ON REFUGEE SUPPORT ORGANIZATIONS

The invasion of Ukraine led to multiple evacuation and visa schemes around the world, and with it came opportunity for fraudsters. Whenever a major international incident or natural disaster occurs, they're quickly on the scene trying to generate profit. In many cases, this could be potentially harmful or even fatal to those affected. When fake charity schemes and bogus help efforts make their way online, life-saving funds are diverted to people who have no business receiving it.

These tactics were prominent during, for example, the Japanese earthquake and tsunami of 2011. Sadly, things are no different more than a decade later, with the targets often being refugees and organizations designed to give assistance.

One of the most prominent Ukraine assistance schemes is the 'Ukraine Sponsorship Scheme (Homes for Ukraine)', a visa path created by UKGOV in March 2022 [28]. Roughly a year later, some 150,000 visas have been issued to people fleeing the invasion. It caused significant strain on the UK visa system generally, creating delays and backlogs on unrelated visa paths of up to 6 months and beyond.

As a result, any attack on the Homes for Ukraine scheme could potentially delay those visa paths further. This would have severe ramifications for those waiting to start a university course, work, or join a British spouse. There would also be potentially major ramifications for those both inside and out of Ukraine should any sensitive data be exfiltrated. A large number of volunteer organizations with potentially little to no experience of online security, or basic cybersecurity funding, would be prime targets for attackers.

The Advanced Persistent Threat (APT) group Evilnum was found to be targeting European migration organizations shortly after the invasion began [29]. Booby-trapped ‘compliance’ documents sent by email led to backdoors and data exfiltration from the targeted organizations.

I spoke to immigration workers for several Ukraine assistance efforts, and the general feeling was concern over potential cybersecurity issues. Setting up a domain correctly and secure comms were of primary concern, along with the potential for social engineering/data harvesting.

In February 2023, concerns about social engineering came to the fore. Several similarly worded letters were in circulation across multiple countries, asking for information on male Ukrainian refugees living with sponsor families [30]. This information was to be sent via email. The letters were seen in the UK, Latvia and Lithuania. In some cases, the letters insisted the men needed to return to Ukraine for conscription. All of these letters were found to be false, with the intention of data harvesting and spreading misinformation into the bargain.

HMRC/TAX-THEMED VISA SCAMS

Tax threats frequently go hand-in-hand with visa scams, as it’s a great way for fraudsters to keep piling on the pressure. This is particularly effective in immigration circles, where new arrivals may not be familiar with how the system is supposed to work. Back in March 2023, Warwick University’s Student Union was warning of their students being targeted in such a fashion [31].

The Tweet says:

> ‘*Warwick students have recently been conned into making payments over the phone to people pretending to be from HMRC or Immigration/Visa Control.*’

Occasionally, fraudsters will combine a tax and visa scam as per following (now deleted) Tweet:

> ‘*I just received a call from the usual UK number, the man told me that I have some legal notice from HMRC and I need to pay the immigration fee around £500, and since it is the first notice this money will be refunded to me in 24 hours.*’

The above Tweet was sent on 2 June 2023.

DATA DISCLOSURE CONCERNS

I have extensive experience of the British immigration system. My wife was present in the UK on a spouse visa from 2016 until 2021, when she applied for, and was granted, Indefinite Leave to Remain (permanent residency). Migrants who reside in the UK for more than six months are issued an identification card called a Biometric Residence Permit [32].

The permit contains the holder’s digital image, name, valid until date, place and date of issue, permit type (student, spouse, skilled worker), general remarks, and unique permit number, among other things. Some cards also include the holder’s National Insurance number.

The card also contains other biometric data, such as fingerprints. Additionally, the Home Office requested duplicate copies of my wife’s biometrics at various points throughout the five-year period.

These tasks are generally handled by third-party contractors/subcontractors working on behalf of the Home Office, such as *VFS Global* [33].

When my wife had to update her address with UKVI, this was processed via a secure online form. A few days later, confirmation came via email that the change had been processed. However, the email needlessly included visible copies of both her passport identity page and biometric identity card scans. There are several reasons this isn’t an ideal practice, not least because if the mailbox were to be compromised then the documents would potentially be at risk if left in the mailbox.

Many immigration lawyers make use of secure, in-house upload facilities to avoid exposing data via postal services or just sending data openly via email and attachments. Lawyers are expected to comply with GDPR and the Data Protection Act, with specific requirements for accidental data disclosure [34, 35]. The fact that data belonging to people in the British immigration system is being sent out in this way by UKVI seems at odds with how things are supposed to be done.

Speaking of how things are supposed to be done, social media continues to play a problematic role where making it easier for scammers is concerned. One of the fastest ways to promote an immigration firm’s talents and successes is to post to *Twitter*. Unfortunately, many firms based outside of the UK post ‘Congratulations’ images of successful applicants holding up their visa/passport pages.

While some firms redact certain pieces of information, many others will post unedited shots which reveal everything from date/place of birth and type of permit to signature and unique permit number. Any of this information could be used in some of the blackmail/phishing tactics discussed above.

CONCLUSION

Visa holders in all regions remain a uniquely vulnerable group, with a successful scam potentially resulting in criminal charges or even removal (by choice or otherwise) due to funds being lost. In situations where the migrant is struck by any form of criminal charges, the implications can be severe, with lengthy bans potentially separating spouses from family members for up to a decade or ruining a promising career [36].

It's very unlikely that a government's immigration agency requiring an expensive renewal would waive fees in such a scenario, and as far as scams go, the visa holder and family really are on their own.

Legal assistance is expensive, there is little room for leniency in immigration departments, and when most aspects of the visa process are so costly there's significant opportunity for fraudsters. Either they swoop in and steal savings intended for the next application, or they prey on applicants desperately in need of money. That 'good deal' may sound like a simple bank transfer, but is just one step away from having to talk to the authorities at a later date.

There are a couple of solutions to a few of these problems. Some institutions which interact with visa holders, such as universities and community assistance groups, have help pages and scam warnings. Even so, we need much more work to be done in this area. Some employers have internal help/warning pages for new immigrant hires, and many qualified immigration experts offer casual help on social media where possible.

The government departments handling visa applications do occasionally provide information on certain scams. For example, the US Diversity Lottery page does clearly link to known scams targeting applicants alongside details of how to report fraud [37].

Even here though, there are no apparent exemptions for fraud victims and this is more than many governments do in relation to scams targeting applicants. With fees increasing, rules becoming tougher, and increasing numbers of refugees displaced due to war and climate change/natural disaster, this is an area of research that desperately needs more exploration and support for those who may be affected.

REFERENCES

[1] Yeo, C. Immigration and nationality fees for 2022/23. Free Movement. 7 April 2022. https://freemovement.org.uk/immigration-nationality-application-fees-2022-23/.

[2] GOV.UK. Home Office immigration and nationality fees: 6 April 2022. https://www.gov.uk/government/publications/visa-regulations-revised-table/home-office-immigration-and-nationality-fees-6-april-2022.

[3] Fox, C. Google promises to clean up Esta ads after eight years. BBC News. 23 November 2018. https://www.bbc.co.uk/news/technology-46316655.

[4] Google. Advertising policies. https://web.archive.org/web/20190705000700/https://support.google.com/adspolicy/answer/6368711?hl=en.

[5] Chadwick, J. Google is hosting ads that charge more than FIVEFOLD the original price for government services like applying for a driver's licence or getting a travel permit, investigation finds. Mail Online. May 2021. https://www.dailymail.co.uk/sciencetech/article-9537043/Google-hosting-ads-charge-free-services.html.

[6] Google. New Government Services Policy (May 2020). https://support.google.com/adspolicy/answer/9736337?hl=en-GB.

[7] Wikipedia. Diversity Immigrant Visa. https://en.wikipedia.org/wiki/Diversity_Immigrant_Visa.

[8] Travel.State.Gov. Diversity Visa Program. https://travel.state.gov/content/travel/en/us-visas/immigrate/diversity-visa-program-entry/diversity-visa-submit-entry1.html.

[9] Federal Trade Commision Consumer Advice. Avoid Immigration Scams and Get Real Help: Diversity Lottery Scams. https://consumer.ftc.gov/articles/avoid-immigration-scams-get-real-help#diversity%20lottery.

[10] Tsing, W. Green card scams: preying on the desperate. Malwarebytes. 24 August 2018. https://www.malwarebytes.com/blog/news/2018/08/green-card-scams-preying-desperate.

[11] Waitzman, E. Staff shortages in the NHS and social care sectors. UK Parliament House of Lords Library. 9 December 2022. https://lordslibrary.parliament.uk/staff-shortages-in-the-nhs-and-social-care-sectors/.

[12] Boyd, C. "Free UK visa" offers on WhatsApp are fakes. Malwarebytes. 4 July 2022. https://www.malwarebytes.com/blog/news/2022/07/free-uk-visa-offers-on-whatsapp-are-fakes.

[13] Wiberg, V. The impact of coronavirus on UK visa holders and sponsors. TaylorWessing. 28 April 2020. https://www.taylorwessing.com/en/insights-and-events/insights/2020/04/the-impact-of-coronavirus-on-uk-visa-holders-and-sponsors.

[14] ICEF Monitor. UK resumes priority visa processing. 17 August 2022. https://monitor.icef.com/2022/08/uk-resumes-priority-visa-processing/.

[15] Law Society of Scotland. Fraud alert – scam WhatsApp messages. 1 February 2023. https://www.lawscot.org.uk/news-and-events/law-society-news/fraud-alert-scam-whatsapp-messages/.

[16] Law Society of Scotland. Fraud alert – scam WhatsApp messages 'from Thorntons'. 9 March 2023. https://www.lawscot.org.uk/news-and-events/law-society-news/fraud-alert-scam-whatsapp-messages-from-thorntons/.

[17] Law Society of Scotland. Fraud alert – scam messages claiming to be Teneu Legal. 9 March 2023. https://www.lawscot.org.uk/news-and-events/law-society-news/fraud-alert-scam-messages-claiming-to-be-teneu-legal/.

[18] GOV.UK. National statistics. Why do people come to the UK? To study. 25 May 2023. https://www.gov.uk/government/statistics/immigration-system-statistics-year-ending-march-2023/why-do-people-come-to-the-uk-to-study.

[19] Murray, J. UK tuition fees for international students. Save the Student! https://www.savethestudent.org/international-students/international-student-fees.html.

[20] Weale, S. Chinese students' applications to UK universities up by 30%. The Guardian. 11 July 2019. https://www.theguardian.com/education/2019/jul/11/chinese-students-applications-to-uk-universities-up-by-30.

[21] Sharma, Y. Crime agency freezes foreign students' bank accounts. University World News. 7 March 2019. https://www.universityworldnews.com/post.php?story=20190307200521986.

[22] Erwin, A. Queen's student 'paid £300' in £16m Belfast money laundering operation, court told. Belfast Telegraph. 6 August 2019. https://www.belfasttelegraph.co.uk/news/courts/queens-student-paid-300-in-16m-belfast-money-laundering-operation-court-told/38379560.html.

[23] UK Council for International Student Affairs. Frauds and scams. https://www.ukcisa.org.uk/Information--Advice/Studying--living-in-the-UK/Frauds-and-scams.

[24] Students' Union University of Manchester. Statement on Recent Phone Scam Targeting Non-EU International Students. 7 August 2018. https://web.archive.org/web/20200613184730/https://manchesterstudentsunion.com/articles/statement-on-recent-phone-scam-targeting-non-eu-international-students.

[25] The University of Sheffield. New scam targets Chinese students in the UK. 22 August 2018. https://web.archive.org/web/20200811194231/https://www.sheffield.ac.uk/students/news/phone-scam-2018-1.799166.

[26] Mok, D. Phone scammers cheat mainland Chinese student in Hong Kong of more than HK$3 million. South China Morning Post. 2 April 2019. https://www.scmp.com/news/hong-kong/law-and-crime/article/3004234/phone-scammers-cheat-mainland-student-hong-kong-more.

[27] Boyd, C. International students in UK targeted by visa scammers. Malwarebytes. 18 September 2019. https://www.malwarebytes.com/blog/news/2019/09/international-students-in-uk-targeted-by-visa-scammers.

[28] GOV.UK. Apply for a visa under the Ukraine Sponsorship Scheme (Homes for Ukraine). 18 March 2022. https://www.gov.uk/guidance/apply-for-a-visa-under-the-ukraine-sponsorship-scheme.

[29] Boyd, C. Immigration organisations targeted by APT group Evilnum. Malwarebytes. 30 June 2022. https://www.malwarebytes.com/blog/news/2022/06/immigration-organisations-targeted-by-apt-group-evilnum.

[30] Antoniuk, D. Poland, Lithuania and UK warn of data-collection scam against Ukrainian refugees. The Record. 9 February 2023. https://therecord.media/ukrainian-refugees-poland-lithuania-uk-warning-data-collection-scam.

[31] https://twitter.com/WarwickSU/status/1630880581641728001.

[32] Home Office. Guidance notes Biometric residence permits (BRPs): General information for overseas applicants, their employers and sponsors. July 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/533854/BRP_OA_information_leaflet_-_July_2016.pdf.

[33] Gibbs, M. VFS: Who is the company subcontracted by the Home Office to process visa applications? The Independent. 18 August 2019. https://www.independent.co.uk/news/uk/home-news/vfs-global-home-office-outsourcing-visa-applications-a9061476.html.

[34] The Law Society. LPP and client confidentiality. 12 March 2020. https://www.lawsociety.org.uk/topics/gdpr/lpp-and-client-confidentiality.

[35] The Law Society. A client's personal data has been accidentally disclosed. Can I delay reporting until I have the full facts? https://www.lawsociety.org.uk/Contact-or-visit-us/Helplines/Practice-advice-service/Q-and-As/A-clients-personal-data-breach-reporting.

[36] Gbikpi, N. General grounds for refusal: understanding re-entry bans. Free Movement. 26 May 2020. https://freemovement.org.uk/general-grounds-refusal-understanding-re-entry-bans/.

[37] Travel.State.Gov. Fraud Warning: Diversity Visa: Program Scammers Sending Fraudulent Emails and Letters. https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/fraud.html.