Crime Interrupted
An AFP and Casefile Presents podcast.
Episode 2, Operation Balah

Host – introduction
The Australian Federal Police is Australia's national policing agency. It's aim? To protect Australians and Australia's way of life. The AFP works with Australian and international partners to combat cybercrime, online child sexual exploitation, transnational serious organised crime, fraud and corruption, and terrorism, espionage and foreign interference.

The AFP leads the Joint Policing Cybercrime Coordination Centre (JPC3) which includes all Australian policing jurisdictions and several key private sector partners. The JPC3 delivers maximum impact on high-harm, high-volume cybercrime affecting the community.

The AFP also protects the safety, security and dignity of Australian high office holders, federal parliamentarians, prescribed representatives and officials.

These are the real stories of the AFP. Everyday people doing legendary work.

Before we start, a word of warning that this podcast contains content that may be distressing for some listeners. Listener discretion is advised.

Host
Operation Balah was an AFP investigation that began in 2019 when millions of derogatory emails were sent out about Wentworth candidates, an electorate in the Eastern suburbs of Sydney, during the 2019 Australian federal election. Cybercrime investigators had never seen anything like it. The written attacks on the politicians were vicious and potentially harmful to their political careers, not to mention their families and friends. In 2019, the offender was unable to be identified and the trail went cold. In the lead-up to the 2020 Eden Monaro by-election, the nasty email campaign started up again targeting a new set of politicians based in this regional NSW electorate. In this latest spate of emails, Labor's Eden-Monaro candidate Kristy McBain, seemed to be the main target.

Kristy McBain
This person had hacked multiple legitimate business emails and sent out emails from legitimate organisations and a lot of those organisations then also had people ringing them saying, *What is this? Who said this? This is cruel and unfair*. So there were, I guess, multiple victims in the stream from those reputable organisations that had their emails hacked, to the thousands of thousands of people that receive these emails unsolicited.

Host
When she first heard about the emails, Kristy put it down to being a natural consequence of putting herself into the public eye.

Kristy McBain

The first I became aware of it was when one of the people working on my campaign had received one and said, have you seen this and showed me, which was a bit of a shock, but I put it down to someone wanting to influence the outcome of the election didn't really think too much about it. And then my sister received one. She lives in Victoria and received it through to her work email and the content was a little bit different again, but I kind of thought, *oh, well, it is what it is* type thing. But then my aunty received one, and the content was just slowly becoming weirder and more intrusive; asking for my husband's phone number. And then I started to really worry about the potential impacts on my family. Like, I'd put myself up for election and you kind of expect a certain amount of blow back and people with different opinions. But then I started to worry about the safety of my own three kids.

Host
Complaints about the emails flooded into the Australian Electoral Commission. Jeff Pope was the Deputy Electoral Commissioner at the time of both the spate of emails in 2019 and in the 2020 by-election.

Jeff Pope
I do recall offensive emails being distributed in the context of the 2019 election. But whilst we received a lot of complaints with respect to those, they didn't actually raise matters that the Australian Electoral Commission would actually have the legislative authority to get involved in. They were highly offensive at the candidates that they were targeted at, but they didn't actually relate to the electoral process and the Electoral Commission is to administer the electoral process and deliver the election with respect to the legislation as it's set out in the Commonwealth Electoral Act. So, with respect to those particular emails in 2019, we didn't actually have any legislative authority to be addressing those.

Host
So while the malicious emails didn't actually interfere in the integrity of the election process, there was another avenue the Australian Electoral Commission could utilise.

Jeff Pope
Even though we may not have the legislative authority to do anything with it, we would certainly be advising other agencies in this context, particularly the Australian Federal Police who obviously have a law enforcement function, but they also have a function to protect some members of parliament as well. So those sorts of emails that could be relevant to law enforcement agencies we will absolutely pass that information on, which we did in the context of the 2019 election.

Host
As soon as the 2019 election happened, the emails stopped leaving the trail cold for investigators for a time... but the AFP hadn't given up.

Jeff Pope
They weren't able to easily identify where those emails were coming from. I think the AFP had a good crack at it when they possibly could, but then the emails actually just go dead quiet, nothing, until the Eden-Monaro by-election comes around in 2020, which of course was on the

cusp of COVID. And they reared their ugly head again. And when I say ugly, they were absolutely ugly both in terms of the content and how they were targeting the couple of particular candidates in that by-election.

Host
What made the emails different in the Eden-Monaro by-election was that this time, they did have the potential to interfere with the integrity of the election process.

Jeff Pope
Whilst the emails were disgusting and vile and offensive, they started to drift away from targeting just the two main candidates into actually then impacting on the electoral process. And for us, that is where our jurisdiction then starts to really kick in. So, it started on the 21st of June 2020, which was the Sunday just before early polling started. And emails then start to talk about the fact that Kristy McBain is actually withdrawing from the electoral process: the actual words were: *Hi, Kristy McBain has withdrawn from the Eden-Monaro race this morning. She is no longer contesting the seat. Please divert your support*. S*ince the voting card has been printed and early polling is underway. You will start to see her name, McBain, on the card, but she's already quit*. *Please put Dr Kotvojs in front of McBain or your card will be invalid.* And when they're referring to card, they're talking about their ballot paper. So when you start to talk about the fact that a candidate has withdrawn from the election, and that is completely wrong and false, then you're affecting the electoral process. And what you're also then starting to do is potentially affect how people may actually cast their ballot. And there's a little-known section in the Commonwealth Electoral Act, Section 329, which is called Misleading or Deceptive Publications. And that is actually a criminal offence where it effectively says that a person shall not, during the voting period, print, publish, distribute or cause or permit any material or any matter or thing, that is likely to mislead or deceive an elector in relation to the casting of a vote. And it's those final words, 'mislead or deceive an elector in relation to the casting of a vote' that creates that offence.

Host
And this was where the AFP came into it again.

Jeff Pope
We have this body, which is called the Electoral Integrity Assurance Task Force, which started up in 2018, and the task force is a collaboration of agencies, AEC, National intelligence agencies, the Australian Federal Police, Attorney General's department, and a bunch of other organisations who all contribute resources and information and intelligence and capabilities to support the AEC, and this body is like our right hand. It's something we now can no longer live without. So we refer to the Electoral Integrity Assurance Taskforce and the agencies in that task force then started to investigate this email trial.

Host
Detective Inspector Aidan Milner worked at the Australian Federal Police Cybercrime Unit when Operation Balah came onto his radar through a work colleague. Typical jobs in Cybercrime were large-scale organised crime activities and hacking against banks or the Australian Government. But this one was different.

Aidan Milner
I got a call from a member that I used to work with in ACT policing. And so he was actually a member of the Electoral Integrity Network. And they'd received a referral from the Australian Electoral Commission in relation to some spam and offensive emails that had been sent out regarding the upcoming Eden-Monaro election. And they'd noticed some similarities in those emails in terms of the content and the targeting of those emails to some emails that we'd seen about a year earlier in relation to the Wentworth election. So, our team in Cybercrime was a very technically proficient team, and it was a bit of a go to area where other investigation areas needed a bit of advice, when you're dealing with some pretty complex technical issues. So I was invited to that sort of initial scoping meeting just to discuss the referral that had been made into the AFP from the Electoral Integrity Network. And that's where I allocated one of my members, Glen, to be the point of contact and start providing some technical assistance to the other teams as they were running the investigation. So it was still their investigation and we were just providing some assistance at that stage.

Host
Leading Senior Constable Glen Brazendale investigates cybercrime for the AFP, and while he wasn't directly involved in the 2019 investigation, it had come onto his radar.

Glen Brazendale
In the 2019 election, we saw a number of emails come across to the AFP. I wasn't involved in this investigation, but what we saw was that these emails were referred in to us. The emails were offensive in nature even from an experienced kind of perspective. We conducted an investigation around those emails and what we saw was that the offenders were hiding where they were originating their telecommunications from, and as a consequence of that, we were delayed in being able to determine their locations. So at the conclusion of the election period, we hadn't managed to determine who the offender or offenders were. So when we saw this same offending start to occur during the 2020 election, Commander Chris Goldsmith came to me and he asked for me to do a comparison between what we were currently seeing and what we'd seen during the 2019 election.

Host
There were enough similarities to suggest it could be the same offender, and with the election just weeks away on Saturday the 4th of July, the cybercrime team entered a race against time. If it was the same offender as in the 2019 elections, on voting day, the transmissions ceased and so did any chance of tracking the perpetrator.

Aidan Milner
It was made quite clear to us that with the previous investigation, the emails and the offending came to a very abrupt stop once that election had been held. And so, thinking there were similarities between the two, and certainly we were very mindful that it was the same offender, we were quite certain that if we couldn't locate this person before the election had run its course, we were thinking that the, that offending activity was just going to stop. We had the election coming up within about, I think it was 10 days or so, and we had the benefits of some previous investigations. We'd gathered some evidence previously, including a lot of telecommunications data. And we sort of had the right idea of where to start looking and what to look out for and to try and find some similarities and some convergences between the

previous investigation and the matters that we were currently looking at. And that's where Glen with his skills managed to find a few little indicators that were consistent and common between both matters.

Host
Due to the nature of the emails, we are not going to share the contents, but rather, do our best to describe the effect they had.

Glen Brazendale
We're not talking emails that are impolite. We're talking outright rude and offensive. If you'd received some of these emails, you'd be pretty angry and pretty upset. And I think by all standards, they were offensive. And when we're talking some emails, we're not just talking one or two emails. In total, we were able to determine that the offender had sent over 23 million emails to members of the Australian public all over Australia.

Host
Whoever was sending out the emails would continuously tweak the content to cause mass offence. As one of the main targets, Kristy McBain grew more worried with each one.

Kristy McBain
I think there were 11 or 13 emails all up in the end and the content just became more and more unhinged. And that was when I really started to worry about the safety of my family because I was away for long stretches of time. As a mum, you want to be there with your kids if they're ever feeling uneasy or unsettled. And I was away a lot of that time, because Eden-Monaro is a big electorate, obviously. And I hadn't told my parents about the emails because I didn't want them to worry either but when my aunty received an email, she forwarded it to my mum. And that was difficult to try to explain to mum that there's nothing to worry about. It was all going to be okay. And they weren't used to that type of content or harassment, I guess, either. So that was tough. The emails started with calling me names and saying I'd pulled out of an election to some very unhinged, comments about paedophilia and children in basements.

Host
Liberal candidate Dr Fiona Kotvojs found herself caught up in the horror. With the targeted campaign against Kristy, many assumed Fiona must have been behind it.

Fiona Kotvojs
The way they were written, it sounded as though in some way, I was behind the letters. And I knew absolutely nothing about the letters until I had some phone calls from people. People pretty much verbally abused me in the street. And then the Liberal Party also found out about them and contacted me I guess a lot of people didn't really understand that somebody could write a letter and just because they'd written it and made it sound as though it was from you or you supported it, you had nothing to do with it. And for me, everything about those letters was absolutely abhorrent. I used to be a Lifeline counsellor and a Youthline counsellor. And so, anything about paedophilia, I just found that incredibly distressing and, to be honest, really emotionally draining. It was one of the most emotionally draining things, I think, through the campaign. Because, I knew that if somebody received that, who had been a victim of a paedophile, the impact on them was likely to be horrendous. And there was absolutely nothing I could do to stop it, to make it go away, to reduce who got these letters and where they went.

So that was probably the hardest and that knowing the effects on people who received it, who had been victims in the past, for me personally, that was the worst part.

Host
Normally the source of an email is easy to determine, but the offender had gone to great lengths to hide this. It was clear the email culprit was a person of some technical skill.

Glen Brazendale
It required a bit of work on our behalf to be able to work our way through how he managed to hide the origin of the emails. So we started reaching out to various companies online and bearing in mind we're looking at this probably getting towards about the 20th of June and we know that the election's on the 4th of July and that the offending is going to cease on or about that date. So we really had a time crunch to work our way through. So what we started to do was make subscriber checks through on the emails to determine IP addresses. We started to look at the phone numbers that we were able to see. And what we saw was that they were all coming back to different people. And this was quite unusual. When you see subscriber checks coming back from the same email address, but for different names, it starts to make you think, well, is the name behind the email address really the name of the offender and is that their email address? And I think the answer that we came to relatively quickly was that the names and email addresses were created specifically for this offending, and they were only used for the offending. The offender like it wasn't their personal home email address or anything like that. It was just purely manufactured emails for the purposes of, this offending.

Host
One of the first things Glen did when he began working on Operation Balah was to brief Cybercrime Operation's Technical Analysist Scott Bailey.

Scott Bailey
I was working as an embedded specialist within the Cybercrime team and shortly after it was allocated to Glen, who wrote me in to give me a briefing on the case, and the first thing that came to mind that was that it was very similar to offending we'd seen in the past. After that briefing, we kind of understood that there was a wide range of spam messages that were being delivered out, some of them targeting members of the Eden-Monaro by-election amongst a whole swathe of other sorts of offending at the same time related to derogatory and offensive emails being sent out to the community.

Host
While fixation-type offending wasn't unheard of in cybercrime, it was less common than other types of offending.

Scott Bailey
The level of fixation was quite unique. One of the things that stands out with that fixation element, there's a real consistent amount of offending of the same type. And that fixation led us to being able to collect a wide range of emails as a result of the continued offending of the same type.

Host
What the Cybercrime team noticed was a refinement in the content of the emails.

Scott Bailey
What we found with each campaign was there was a particular message body that was crafted by the offender. And through the use of some software and tools, he was able to automate the process of delivering those messages on bulk to a large set of victims. And so, you would see that there would be some changes to the way the script operates. There'd be changes to the content, then those messages would be re-delivered to what was a quite a large list of email addresses for Australian citizens.

Host
As the experts combed through the emails looking for clues, they knew the offender was not using the internet in the usual way. They were using a special device both to connect to the internet and mask their location.

Glen Brazendale
During the 2019 offending, we were able to determine that the offender was using a dongle to send emails or communicate with the telecommunications network. Essentially, it's a USB device, plug into your computer and it provides communications between your computer and a cell tower. So we knew that if we came to the election day in 2020 and we didn't have that dongle in our possession, it was likely to be destroyed, because we'd seen the dongle disappear off the telecommunications network in 2019 after election day. So we knew we had to find it. Obviously, we also wanted to prevent the continuation of the offending during the election period. I mean, these are pretty horrendous emails, but we also knew that if we didn't, then we were also unlikely to.

Host
Other clues that could lead to the offender lay in the coding used to send out the emails.

Glen Brazendale
The ability to write codes that sends out email, some of the stuff that he was doing though was pulling names from lists and pulling emails from lists. Again, it's not hard. It's something that's normally done though, more for a corporate kind of sending of emails. So let's say as an advertiser, you might want to send a whole bunch of emails to email addresses. So what you'd do is you'd tell the client, select from this list of email addresses and send them this email. He did some stuff that was slightly more complex in that he told the program that he'd written to select out from that list, a first name and a last name, if it could determine it, but from a perspective of what we were seeing and why we knew it was being done programmatically, was that you'd quite often see abnormalities in naming conventions. So things like 'Dear admin' is normally a pretty good indication that the email address is admin at something and it's just pulled the prefix of admin and said that that's the first name. So we kind of knew that it was being done programmatically before we even went through the door but again, it's not super complex in how it's done.

Host
While the team was trying to trace the emails to their source, Aidan explains that it was hard to figure out what the sender's aim actually was.

Aidan Milner

There was so much content in some of these emails and it was so varied, it was quite challenging to work out what this person was trying to achieve. It was just a bit of an anarchist approach. There was a lot of disinformation and rumour mongering and hateful speech around a couple of politicians in particular. But, the bottom line is a lot of the emails were just plainly offensive. So you often wonder how you'd be trying to influence someone at the same time you're making such disparaging and awful offensive remarks. The content was just quite bizarre and it just seemed to be generated to really try and antagonise and rile up people and get them infuriated about who was running in the voting process. So even where some of the emails might've been appearing to try and favour one person over the other, there'd then still be some of this offensive and derogatory rhetoric the other person in other emails. So that's why we were quite confused initially, because bottom line, it just seemed like it was someone out to really try and promote hateful ideologies and generate emotion amongst the voting public. And I suppose it was trying to promote people to land on one side or another with such extreme views.

Host
While the cybercrime team raced against time to find out who was behind the emails, election candidates Kristy McBain and Fiona Kotvojs were feeling the effects of them.

Kristy McBain
By the time the campaign was in full swing, these emails were going to most of the east coast of Australia. So, there wasn't a day that went by where someone didn't contact our campaign office to tell us that they'd received an email or that media weren't asking about it. It becomes that self-perpetuating story because the emails keep coming, the questions keep getting asked. So we weren't for a period of time able to focus on some of the things that we wanted to say because we were responding to what was happening. And I know Fiona and myself were both doing that and whilst both also trying to divert attention back to the issues that we did want to talk about as well. So it kind of did take over for a little while.

Host
Fiona felt it too. The focus of the Eden Monaro by-election became the emails.

Fiona Kotvojs
During that period, I think almost every interview I did with media, they weren't interested about the issues of the political campaign, our policies, or what we were trying to put forward. The questions always came back to those letters. And so that means that you can't communicate the message that you want to get out to people from a political perspective.

Host
The Cybercrime team looked at the case from every possible angle. Aidan still remembers the moment Glen came to him with a breakthrough.

Aidan Milner
This is where I was quietly confident in Glen. From the start where he'd identified a couple of little things that stood out. And I said to Glen, 'Let's go for it.' And I still remember Glen coming to me with a whole bunch of telephone checks and other checks. And he said, 'Here, have a look at this. Does anything stand out?' And I saw something and pointed at it. 'Is that it?' And he went, 'Yeah, that's it. That's it!' And he was so excited. And I knew, look, this is

great. We've got it. We're on the front foot. We've just got to keep pushing ahead. As clever as this person might be, we've got the upper hand now.

Host
While we can't tell you exactly how they did it because there are some technologies the AFP Cybercrime team want to keep classified, we can say this: as the election day grew closer, they got an address.

Glen Brazendale
During the process, we managed to determine a location. So this was now, I think the second day of July 2020. As a consequence of the inquiries, we drew up a search warrant, drove from Canberra to Sydney, had the search warrant signed by a judge, and then we executed the search warrant.

Host
As a technical analyst, Scott played an important role in the resolution phase.

Scott
I joined Glen and Aidan in the search warrant, and my role in that search warrant is to assist in the triaging of devices on site to validate evidence that we find and make sure it's relevant to the offending. And basically, give an indication to the investigative team that A) we're in the right place, and B) that there's evidence here that we should be collecting to put forward in a brief. So my role was to support the technical review of devices on site.

Host
Whoever was on the other side of the door, the team needed to contain him quickly. There was every chance the person they were after would have some sort of kill-switch on his program that could interfere with the team's efforts to find the evidence on his devices.

Aidan Milner
That was one of our primary considerations going in. And certainly it was one of the reasons we were pretty quick to get inside and pretty quick to grab him because we didn't want any of that equipment that we believed was in the house being interfered with. And from a forensic perspective, when we do these search warrants, we have our digital forensics and our technical analysts with us. And we really wanted any technology, any computers, any infrastructure, any communications devices that we were anticipating at that residence, we didn't want them interfered with. We wanted to be able to have a look at them and make our own assessments about what was going on, how they'd been set up.

Host
Standing at the front door of a house in Sydney, it was hard to imagine what the offender would be like, given that the cybercrime team had only been exposed to his incredibly offensive emails. When they arrived, the suspect tried to flee upstairs.

Glen Brazendale
We had to give quite firm commands for him not to do that, and to come to us at the front door. We detained this male person and we took a phone from him and we then started to talk to him. Initial conversations were in English, however, very quickly, the offender claimed not to speak

sufficient English and, we had already organised, because we were quite prepared, a translator for the language that he spoke. Now, that translator started translating all the things that we were saying, and the offender started to correct him on what he was saying, indicating to us that he actually understood what we were saying, he just chose not to speak to us. Eventually, after quite some time, after explaining his rights, and explaining the warrant and the process, and him claiming not to understand, and then correcting the translator, we determined that he wasn't being helpful and not only was he not helpful, he was obstructing us in our search warrant.

Host
Aidan had a similar impression of the offender. It was perhaps not surprising considering this man had set out to be as offensive as he could to as many people as he could in the content of his emails.

Aidan Milner
He was really antagonistic and uncooperative. And I'll be really clear, he's under no obligation to cooperate or engage with us or say anything. So we've got to go through a lot of legal processes. We've got to inform him of his rights. There's quite a few things we need to discuss with him because of the invasive nature of a search warrant. So we were explaining a lot of these things to him. And what we found was that very early on, when we were engaging with him and speaking to him, particularly when we first came in through that door and we were talking to him, okay, in English. And as pretty much after we'd started engaging with him, all of a sudden, he couldn't speak English. And we had to go through interpreters and translators, and even that became challenging. So he didn't like the people that he was speaking to or they were having issues or he was objecting to some of the processes that we were trying to follow when we were running the search warrant. So he was really antagonistic and it just made the whole process lengthy, tiresome, really drawn out. And again, I'll make the point, he had no obligation to cooperate. But the impression that Glen and I distinctly had was, this is a step beyond. This is not just not cooperating, this is actively trying to make things hard for us. He just didn't want a bar of it. He just didn't want to listen. He wouldn't engage with us. He wouldn't engage with interpreters. And so we had to effectively read that search warrant out to him. And even then, he didn't want to pay attention. He argued, he objected, and it just made for a really challenging search warrant. But that was all right because whilst we were having a chat with him and it was a bit of an initial delay because of some of the discussions with him, but we got to the stage where we were quite comfortable that we'd done what we needed to do and we'd gone through some of those legal obligations and his legal rights with him. And then we could get our technical staff and our digital forensic staff started. And that was fine because I was happy with Glen to lead the engagement with this individual, have a chat with him and we could just let our techs and our digital forensics go off and do what they needed to do.

Host
When the Cybercrime tech team finally got upstairs to the offender's study, they found exactly what they thought they would.

Scott Bailey
We walked into a room where the screen was off. So, it didn't actually appear like the computer was on initially but surrounding the computer was SIM cards, wireless dongles, there was a GPS jammer in the corner. There was antennas on modems and different things going on. So

it was a real clichéd image of what you might expect when you walk into the room of a cybercrime offender. And then obviously once we have a look at the device and determine that it was running and actually running the software that was sending messages as we were there, it was a real validation of the work that we'd put in. And then quickly we turned our mind to assessing what exactly was going on here in its entirety. Having put together a picture in our minds based on the evidence we saw, we now had the opportunity to look at firsthand what was being used to send the messages and the different artifacts that had led to where we were.

Host
It would be a long night ahead for the AFP Cybercrime team. The offender's behaviour cost them hours, but they needed to know he understood the warrant before they began collecting evidence. Seeing his computer sending emails, they couldn't help but wonder if his delaying tactics were to ensure thousands of emails went out during those hours of delay.
Host
Scott's job was to find immediate evidence of the emails that had been sent out to disrupt the Eden-Monaro by-election. When he finally got to inspect the equipment, he found exactly what he was looking for.

Scott Bailey
It was a relief to finally get started, which was late into the evening, and start the process of triaging and, and seeing what we have. Glen and Aidan, their real focus was on talking to the offender. And while that was occurring, I was working on triaging devices, validating whether there was evidence of the messages that we knew about within the system itself, which I was able to do. I was able to show Glen that the messages that we had identified as part of the campaigns against the Eden Monaro by-election were present in the logs, so they had been sent by that computer. So there was a real linkage of the device being used, the services in which they were subscribed with the fraudulent documents, and then evidence of the messages being sent from the computer.

Host
As well as 'catching him in the act' seeing the computer sending out emails right before their eyes, there was something else Scott found interesting that would ultimately lead to further charges.

Scott Bailey
The other aspect that I found was quite interesting was the use of mobile services in order to deliver the messages. So a lot of the operation was conducted on the computer that we ultimately found at his premises And that was enabled by wireless dongles. And the uniqueness to that was the subscribers for each of the mobile services that were used in the campaigns was a fraudulently obtained subscriber information. And further investigation of the computer also revealed a collection of identity documents on the computer that related to subscribers that we had attributed to the sending of some of the messages in some of the campaigns. So we're talking about identity documents that were obtained through identity fraud. So often identity documents, can be purchased on the dark web or obtained in bulk. So one of the real risks of a data breach, particularly of ID information, is that it can become into the hands of the wrong people and then used for these sorts of purposes. You know, setting up accounts in the names of other people, for instance. What we found with this one was that the, the way that the offender had obtained those identity documents was actually through a more specific targeting

himself. So setting up a campaign to, to obtain those IDs himself rather than purchasing online or obtaining through another data set. So there was a level of personal commitment to obtaining those documents and then using them for the purposes of the offending, which was, I would say is quite unique.

Host
The reason the equipment was at first examined at the home of the offender was the Cybercrime team had to collate the evidence to lay charges. Aidan remembers a long night for the entire crew.

Aidan Milner
I remember Glen sitting outside on the little patio with a laptop on his legs, I think at like 2am. It was quite cold and he's there madly trying to type up a Statement of Facts around the arrest process to justify the charging and give further consideration to things like bail and so forth. So, Glen was out the back doing that. He was getting input from Scott, our tech, and from other staff there about what we'd seen, what was going on. Described some of the emails that were going out and the processes. And we were populating that in a Statement of Facts so that then, uh, earlier that morning, or later that morning I should say, Glen was in a position to convey him to a local New South Wales police station for an arrest and charge and bail process.

Host
In TV shows, the arrest is usually the end of the story, but in reality, it marks the beginning of a long process of preparing a case to go to court. Taya Simmonds is a Senior Constable with the Australian Federal Police. She joined the AFP after getting a law degree.

Taya Simmonds
I was on leave when Glen and the team actually went and executed the search warrant. So I found out when I came back from leave, I think it was the weekend, the week after they did the search warrant. And I remember getting an email from Glen asking me to look into the victims of the ID theft.

Host
The AFP tracked down the unsuspecting people who'd had their identity documents stolen and used in the offending when ID was necessary to purchase dongles or register email addresses. The offender had used a simple ruse to steal the documents.

Taya Simmonds
They did an analysis on his laptop and they found a whole bunch of identity documents. When they were conducting checks prior to executing the search warrants the phone numbers and the SIM cards weren't necessarily registered in the offender's name. They were registered in names that they couldn't tie back to the offender. So there was a big question about I guess who the offender was, where he got these names from, and through technical analysis of the offender's laptop, we came to the conclusion that he created a fake company, advertised jobs through the company on Indeed.com, and people were applying for jobs through this company. And then when the offender would receive their job application, he would go back to them and ask for their identity documents to prove who they were for a prospective job. And when they sent through either their driver's licence or their passport, the offender obviously had all the

information that he needed, and they never heard from him again. And obviously there was no job, so they didn't get employed.

Host
When they didn't hear back from their job application, the applicants had no idea their identities had been compromised.

Taya Simmonds
When Glenn and I spoke to the victims of the identity theft, they were unaware that their documents and that their names were had been used in this offending, and they were quite shocked and appalled that they had kind of been brought into this, obviously without their permission, without their knowledge, and I guess they were just lucky that nothing ever seriously happened; it was just isolated to that particular offending. But our advice to the victims after they found out that their identity documents were stolen was to apply for new ones. And that's an administrative nightmare as well. And something that I'm sure that they wish that they didn't have to do considering all they were doing was applying for an appointment.

Host
The case was complex. There was the identity theft, and then proving the charge involving Section 329 of the Commonwealth Electoral Act – that the offender had interfered with the election process. There were also the politicians to speak to; Kristy and Fiona from the recent by-election and two others targeted in the 2019 election.

Aidan Milner
So early on, it was a case of, I want Glen and Taya dealing with these politicians. Can we deal with them directly? And the four politicians that we dealt with were fantastic. They were really engaging. They were really sympathetic. They were really supportive and understanding of not just their own lives being impacted, but that millions of Australians had seen these emails and been aggrieved and offended and were complaining and obviously affected through this process. So they were really sympathetic and very supportive of our investigation and putting this matter before the court.

Host
Glen and Taya spoke to Dr Fiona Kotvojs and both immediately noticed the effect the emails had on her.

Taya Simmonds
I have a particular memory when Glen and I went to visit Fiona and the level of concern and stress that these events has caused her. It's kind of stuck with me and it seemed to me that she took on a lot of, a lot of it personally and like held a lot of personal responsibility for the information that was out there and how she was perceived by the community afterwards, and you could tell that it affected them personally but also like their family members, the community in the electorate that they want to represent, and those people don't get a say. Politicians, to a certain extent, putting themselves out in the public domain, I think would expect some comment on their persons, but their family and their friends, their work colleagues, and the community that they exist in, don't sign up for that, and it seemed to me that they took

a lot of personal responsibility for how it impacted their like close friends and family and community.

Host
Taya could see how hard it was for Fiona whose life was devoted to serving her community only to be accused of spreading such incredible malice about her political opponent.

Taya Simmonds
She was a Lifeline counsellor. She is involved in the Army Reserves. She does a lot to give back to the community, for then to have information or disinformation out there about, about her and quite damaging and harming to her reputation can be quite demoralising. And the nature of everything being on the internet now, a lot of people can recognise, *I know Fiona, that's not true*. But it's very hard to make people forget that those things were ever said about you. So I think like they've had to do a lot of work to kind of get back to where they were prior to all the misinformation getting out in the public.

Glen Brazendale
In speaking to the politicians, I think probably one of the things that was the most important is that they were affected. Politicians put on a face, but they're real people and I think when I saw the responses that were coming out publicly from the politicians, I was really proud to be Australian, because the politicians were not blaming a political party on the other side. They weren't blaming a politician on the other side. They knew that it was an offender. It wasn't something that was being done by a political opposition and watching the politicians not try and make political mileage of it and to try and take advantage of it. What they were really trying to do was I guess not be divisive on the basis of these emails. And they were not trying to place blame anywhere other than where it belonged on the shoulders of a particular individual.

Host
When it came time to prepare for court, the cybercrime team knew they had to simplify the complex web of offending so that a potential jury would understand it.

Glen Brazendale
In the preparation for the brief of evidence, we recognised that there was an overwhelming amount of evidence. The Statement of Facts ended up being 139 pages long by the time I'd finished And in presenting, uh, the evidence, I thought it went quite well. We had two kind of defining moments. The barrister indicated to us that he thought we had a strong case, which is always good, but when the lawyer indicated to us that the evidence looked really good and he challenging the evidence was going to be difficult, so rather than challenge the evidence, he was going to challenge the law, and that, to me, always says that, *hey, we're in a really good place in terms of our evidence.* And being able to present it such that a jury could understand it, because it's terribly complex. But being in that position gave us a very positive vibe.

Host
The offender was eventually convicted of several offences relating to the offensive emails sent during the by-election campaign and sentenced to 20 months' imprisonment, wholly suspended. the cybercrime team could see the level of distress and disruption that the millions

of emails caused to the targets and the members of the public who received them. Taya explains one positive outcome.

Taya Simmonds
When we first started investigating this particular offence, the penalty was quite low. And from, I guess, the awareness of the impact that interfering with an election can have, the penalty was increased in 2022 to three years imprisonment. So just, being able to identify that people are actually committing these offences and highlighting it to the community and to the politicians and the government can actually have an impact on legislation and the penalties.

Host
The AFP Cybercrime team found it interesting reading the emails sent back to the offender because not one person supported him. Quite the opposite, in fact.

Glen Brazendale
One of the things that we got to examine were emails that were sent back. Now, he had used fake email addresses that didn't actually exist to send out these emails. And in doing so, he'd also put a reply email address that was real. So if someone tried to reply to him, that would come up as a real email address, and we were able, on a number of occasions, to access those email accounts. In accessing those email accounts, and in reading a lot of those emails, I was pretty I'm pretty proud to be an Australian, looking at some of those responses, calling him out for what he was doing, and stating outright what they thought of him, and whilst in a podcast I probably can't use many of the words that were used by members of the Australian public, it was really nice to see people pushing back against division, people pushing back against things that they know were not true, and calling it out, saying what they thought.

Host
They were calling out the unethical nature and the impact of his actions.

Glen Brazendale
I also, on a number of occasions, saw some quite personal responses from people. And this is one of the things that really comes down to it. When you've been a victim of a crime, you tend to flavour many of the things that you see and do with being a victim of that crime. When something affects your life in such a major and traumatic way. What I saw in some of those emails was some of the tragedy for these poor people who are now being victimised again on the basis of these accusations, and it made me even prouder to read some of the other emails where people were pushing back against it and calling him out for what it was.

Taya Simmonds
I was reading some of those as well, and also, super proud of people actually replying because myself, I would have probably would have read something like that and probably just deleted it. But for people to actually take the time to respond, and these weren't just one-line emails, they were paragraphs long, explaining, or basically telling off the offender, saying, *how dare you say these things*. And they've had personal experiences or they know someone who have

had experiences, and they just basically saying it's inappropriate, stop doing this, like you're a menace to society type of thing.

Host
Kristy McBain also saw how discerning members of the Australian public were in the wake of the emails.

Kristy McBain
I think that was the most amazing part of this journey was the support that I received from people from all over the country saying, 'I've received this email. I've reported it. I think it's terrible. Good luck in the campaign.' At the end of the day, the aim of trying to disrupt the election didn't work and Australians saw through that pitiful attempt to influence their views and went out and voted accordingly, which it's fantastic. It's nice to see that so many people who contacted me, contacted Fiona, contacted the AFP said that this was not right and something had to be done about it.

Host
Dr Fiona Kotvojs was thankful to the AFP and their Cyber team, not just for catching the offender, but for keeping her in the loop afterwards.

Fiona Kotvojs
I think the AFP, from my perspective, did an amazing job in being able to locate him. I don't really understand how they did all of that, but I think they did an amazing job. They also did a really good job in keeping me informed. Because it was a really long process after when they charged him to when it all went through court and then continued. It was years.

Host
Taya was proud of the Cybercrime team and the work they did on Operation Balah. For all of them, it was not just about stopping the offender, but it was about the wider reaching impact.

Taya Simmonds
But when it's a smear campaign not based on facts, just misinformation and lies, in my opinion, definitely crosses the line. And they can have wide ranging impacts that, like, for years to come. And this is people's jobs, it's their lifeline, it's their career, and you just don't know the flow on effect that something like this can have on somebody.

Host
Deputy Electoral Commissioner Jeff Pope was pleased but not surprised by the response of the public to the email campaign.

Jeff Pope
That's one of the great things about Australians and Australian society and Australian elections. We've got nearly 18 million friends out there being 18 million electors who all treasure the electoral process and electoral environment in Australia and they're in their own way, they are defending what they love.

Outro
Host
The AFP offers a lifetime of opportunities with over 200 diverse roles across Australia and the world.

Interested in learning more about how the AFP works to protect Australians against people who break the law online? Visit a-f-p-dot-gov-dot-a-u to discover more.

The AFP. Everyday people, doing legendary work.