A new generation of security specialists guards the elite against blackmail, ransom and theft – by hackers. Simon Usborne meets the cyber detectives

Photographs by Jason Bell

Gone PHISHING

In the corner of a pub on a quiet side street in Bloomsbury, a young woman sits at her Macbook. Stickers cover its lid: "Hack the Planet"; "Encryption is not a crime"; "One nation under surveillance". A lunchtime crowd of office workers and tourists is beginning to drown out the football highlights streaming from three televisions. Zoë Rose, who wears a houndstooth blazer, her dark red hair swept back into a ponytail, likes it busy – and anonymous. "People usually watch the games and little else," she says, clutching a mug of tea.

Rose, a former botanist from the Canadian Prairies, opens her laptop and plugs in a device with two stubby antennae called a Pineapple. She uses it to generate a wireless internet connection, which she names loosely after the pub. (I won't name the pub, but think "dogandduckFreewifi".) "To my target it looks like legitimate Wi-Fi," she explains. "He's working on his laptop, he wants internet, so he connects. Now he's on my network." It takes several rapidly typed lines of commands for >

"Above all, these criminals are confident in their ability to be anonymous…" Cyber security specialists, *from left*, Jenny Afia, Laura Hawkes and Zoë Rose, photographed at the ME Hotel, WC2. Hair: Selena Middleton. Make-up: Rebekah Lidstone. Sittings editor: Julia Brenard

JENNY WEARS DRESS, OSMAN. SANDALS, JIMMY CHOO. EARRINGS, SARAH & SEBASTIAN. LAURA WEARS SHIRT, CHLOÉ. TROUSERS, VILSHENKO. BOOTS, FENDI. ZOE WEARS DRESS, ISABEL MARANT. SHOES, TABITHA SIMMONS

Rose, 27, to break into her target's computer. A list of its files and folders is now visible on her screen. She could copy them, or add new ones, and her victim would never know. She types a screenshot command. A new picture file lands on her desktop. She opens it to reveal a grab of her target's screen. He was in the process of logging into his bank account. An Excel spreadsheet called Passwords.xls is open next to the web browser. The password column for Facebook and "bank" is the same: "Snugglebuns1966!"

Rose prepares her *coup de grâce*, typing a line that includes the command "webcam_stream". A new window pops up. Suddenly, a bearded man wearing a shirt and tie looks back at us, not noticing the tiny light that has come on next to his laptop webcam. "There are ways to do this so the light doesn't even come on," Rose says. The view behind the man looks familiar. Rose looks across the pub, past a waitress bringing steaks to a neighbouring table, at a bearded man wearing a shirt and tie. "Smile!" she says, waving at him.

Rose is a cyber security analyst and she has just broken several laws. Or at least she would have done. Her victim today is not the unsuspecting owner of a now-emptying bank account, but her colleague, Matt, whom she has planted in the pub to demonstrate her work as a "white hat" or ethical hacker. Rose's job is to prevent and respond to the dizzying array of virtual weapons now firing across cyberspace. It places her in growing demand. When a plant allergy forced her to quit botany, Rose stayed in Manitoba, where she comes from a family of farmers, and retrained as a network security specialist. An encounter at a conference in Cambridge last year led her to a job with Schillings, the London law firm specialising in reputation and privacy, whose clients have included JK Rowling and Brad Pitt.

In the analogue age, when threats for the very wealthy or famous ranged from tabloid stings to robbery and kidnapping, muscle-bound bodyguards and decent lawyers were protection enough. In the digital era, dangers lurk in virtual corners. Ransom demands spring up on computer screens, to be paid in virtual currencies to anonymous accounts, as the NHS and other victims of last May's global ransomware attack found to their cost. But for every major hack on a corporation, government – or presidential campaign, countless more occur every day, targeting the emails, photos and whereabouts of wealthy individuals.

Ask David Beckham, whose hacked emails were leaked in February, revealing his frustrated longing for a knighthood, among other embarrassing titbits. Or Kim Kardashian, whose Instagram posts flagged her whereabouts before she fell victim to an £8 million diamond heist in Paris in 2016. Or the dozens of celebrities, including Pippa Middleton and Jennifer Lawrence, whose private iPhone photos have been stolen from the cloud and circulated online.

As fear and paranoia stalk the domains of the one per cent, their entourages are growing to include a new generation of security consultants and tech-savvy lawyers working alongside the ex-army and police who typically make up the industry. And in a chronically male-dominated field, that can only mean more women as clients look beyond muscle. "Even just five years ago, we'd still be looking at terrorism, ransom – physical threats," says Laura Hawkes, a former terrorism and security academic who specialised in the online radicalisation

> In the increasingly connected home and workplace is an emerging cyber threat. For "smart", read "hackable"

of Islamic extremists. She now works with high-net-worth clients at Another Day, a London security consultancy founded by former marines. "Now a client might say, 'Thanks for all the cameras and bollards, but I've just been hacked.'"

Hawkes went to school in Kuwait, where her British father worked in finance and where she developed a fascination with the Middle East. She wears a silk blouse and carries a black leather Céline handbag. The attractive 24-year-old sometimes has to convince new clients that she works in security. "It's seen as a big, burly man thing and there's a little blonde girl talking to them and they're like, what?" she says, her international-school voice betraying hints of her earlier childhood in Essex. Yet dealing with clients can be easier when she defies expectations, particularly if they are fearful members of wealthy households sharing personal information. "They feel I can relate to them more," she adds.

Across the world's wealth capitals, security and intelligence firms are adapting. In New York, Abigail Stanglin is an investigator specialising in art fraud at K2 Intelligence. The firm, founded in 2009 by Jeremy Kroll and his father, Jules, himself the founder of pioneering corporate intelligence firm Kroll Inc, is expanding its private client group and cyber defence practice. Stanglin, who is 34, has adapted quickly. She, too, says being a young woman can be an advantage when, for example, investigations lead to the door of a 17-year-old hacker. "If we end up going with someone who might be ex-NYPD, it's not exactly good cop/bad cop, but I'm going to immediately put them at ease."

A few weeks before I watch Rose in action, I meet her boss at her club across town in Mayfair. Jenny Afia is a former corporate solicitor who joined Schillings in 2006. She is now a partner at the firm and has rapidly developed an understanding of the new cyber threat. Though she is too discreet to name them, she is the go-to woman for about a dozen high-profile clients, and works with many more. They include actors, models and hedge-fund managers. "Super-wealthy and superstars, those are my people," she says over coffee at the Arts Club.

"People are thinking not 'what if', but 'when' now," Afia, who is 38, says. Whip-smart and straight-talking, she wears Dior boots, black jeans and a white polka-dot tank top. Email hacking is the biggest concern. Beckham was not even hacked directly; servers were compromised at Doyen Sports, a Lisbon-based agency founded by the footballer's PR man, Simon Oliveira. The company refused to pay a reported ransom demand of £1 million for the return of the files. The hacker could not be traced, and Beckham's lawyers could not prevent the email from being spread on the Wild West of the web.

"You know that feeling when you send an email and you think you've sent it to the wrong person?" Afia asks. "Your stomach drops. That's what it's like for a celebrity who's about to have their emails revealed to the world, but on a much, much bigger scale." Afia says that, while clients traditionally were advised never to pay blackmailers, fear of leaks and the anonymity of online ransom attacks means that increasingly they now do, often in bitcoins, the virtual currency.

Afia remembers a case in 2008 as a turning point. A client was fighting to stop the spread of some leaked confidential banking documents, which had been posted on an obscure website. The firm won an injunction to get the files taken down. "But the next day 50 versions of that site sprang up across the internet," Afia recalls. The site was called Wikileaks. "No one had heard of it then. There was this gentleman called Julian Assange who we thought was a bit odd… but he completely outfoxed us. It was an early lesson in how the internet was going to change everything."

As it responds to multiplying online threats – from organised crime, bedroom activists, recreational hackers, hostile governments and grudge-bearers – Schillings has doubled its workforce to almost 100 in the past few years, creating a cyber division and hiring almost a dozen experts and hackers, including Zoë Rose. "They're not like us – they think differently, and sit in our situation room on their Macs with their headphones on – but that's what we need," Afia says. "I never do a case just with lawyers any more."

Security at this end of the market is lucrative, as well as demanding (Afia can never turn off her phone) and – occasionally – exciting. Hawkes says she declined a job offer from the Home Office to work on counter-radicalisation, and has not regretted it. She is "permanently single", she says with a sigh, but has a rich social life. "My friends think it's kind of strange what I do," she adds. "They work in the arts or journalism and think it's really interesting but at dinner parties they'll talk about someone's new album and I'll start talking about Isis beheadings and they say, 'OK, maybe don't talk about that.'"

In the male-dominated field of security, wealthy clients are now looking beyond muscle. "They feel I can relate to them more," says Laura Hawkes, *above right*

JASON BELL. ZOE WEARS TOP AND SKIRT, NEHERA JENNY WEARS SHIRT, MARGARET HOWELL TROUSERS, RACIL LAURA WEARS DRESS, ALTUZARRA

New clients undergo a security review, often including a penetration or "pen" test, an attempt to expose vulnerabilities. At 12 Hay Hill, another Mayfair club, Hawkes shows me an Another Day Safe Life report recently prepared for a client with homes in Holland Park and Oxfordshire. For my benefit it has been stripped of any identifying information, but it covers the family's houses, cars, schools and haunts, from a local prep school to Hakkasan, as well as the driver, nanny and housekeeper, who are given risk ratings based on their online footprints. It recommends new CCTV cameras and motion sensors, but also the upgrade of all Apple devices with improved encryption settings.

In the increasingly connected home and workplace, Hawkes identifies the rise of the "internet of things" as an emerging cyber threat. For "smart", read also "hackable". Thermostats, fridges, cars and CCTV cameras are all now online, often shipping with default passwords that are easily guessed or found elsewhere. Shodan, a site commonly used by ethical hackers to locate vulnerabilities, can also be used to find unprotected devices. In 2013, Marc Gilbert, a father in Houston, Texas, heard noises coming from his two-year-old daughter's bedroom. When he went to investigate, he found a strange British man's voice was coming out of the girl's Wi-Fi-connected baby monitor, insulting her by name. As Gilbert walked in, the man began insulting him, too. It was impossible to say who the man was, or how long he had been watching the baby.

The penetration test at Schillings, part of a package that Afia says costs roughly "the price of a return first-class flight" (the best part of £10,000, let's say – she prefers not to be more precise), goes much further. Hackers may use special memory sticks, or USB thumb drives, preloaded with hidden files designed to, for example, transmit every keystroke on the target's keyboard, including any email or password. "So we might drop one on the floor outside a client's household office with the words 'salaries: confidential' on it to see who plugs it in," Afia says. Somebody always does.

Hackers may be more sophisticated, applying "social engineering" techniques to build a picture of a victim's life, perhaps posting a memory stick using the forged letterhead of an agent or PA. Personalised attacks are more common the wealthier the target gets, and can be easy to research in the age of social media. Emily Orton, an executive at Darktrace, a London cyber security firm, tells me about a case in which a CEO received an email from his son's football coach containing a link to the fixture list. The link was in fact part of an elaborate phishing expedition to compromise the CEO's security, using intelligence gathered from his son's Facebook account.

Children can be a weak spot, and Schillings investigates them thoroughly, often dispensing tough love. "Sometimes we'll mock up a newspaper front page full of stories and say, 'This is everything we found out about you and your family,'" Afia says. "Stuff about them drinking or taking drugs, stuff with financial ramifications – pictures of their parents' cars and yachts. We don't do it with the parents in the room, and the children tend to be horrified." Afia says her cyber team also investigate online friendship groups. "Sometimes they have no idea that one of their 1,000-plus followers is actually a tabloid journalist," she says.

Perpetrators are often known to victims, or not far removed. There was a time when anyone seeking to photograph a private occasion had to hide in the church (a man was caught at Dornoch Cathedral in Scotland after the christening of Madonna's baby son Rocco in 2001 – he had hidden inside the organ). Today your guests are the more likely culprits. Schillings also now sends "digital bouncers" to events. A member of the cyber team working in the situation room alerts them to potential breaches. A polite tap on the shoulder follows. "If we can turn off the Wi-Fi at the property, we'll often do that as well," Afia says.

Schillings was recently called to a large London house where the client was concerned that her husband, whom she was divorcing, appeared to know more than he should about her movements. Her emails and devices were secure, but a search revealed a small white camera hidden on a white bookshelf, and another in the bedroom. "When I did a forensic audit of the devices they were linked to a Dropbox account, and that account was > 166

linked to the ex," Rose says. The devices were programmed to automatically transmit video footage to a cloud storage service. "Who also had access to that account? It was terrifying but shockingly not uncommon."

Hawkes says that fear among clients peaks after big attacks, either physical or cyber. Phones at Another Day rang hard after this year's terror attacks, just as they did after the Kardashian heist. Reassuring clients increasingly requires difficult conversations about how much to share. After our meeting, Hawkes shows me the latest edition of an English-language propaganda magazine published by Isis. An earlier edition included an article calling for an increase in random knife attacks. "And we have seen an uptick in knife attacks," says Hawkes, who believes the magazine may have contributed to this. "In the new edition they say, go and target high-net-worth individuals and rich businesses." The article, headlined "The kafir's wealth is halal for you, so take it", includes lifestyle shots of jewellery and a London luxury car showroom.

A siege mentality is understandable, and security firms are warning that there is only so much even they can do in the digital age. "Imagine the old model of a medieval town with big walls and a moat – you were in or out," Emily Orton at Darktrace says. "The idea of cyber security used to be the same, but modern cities don't have walls, and now we're accepting the idea that people will come into your network, just like anyone can visit your city. You have to rely on good internal security."

The default position is defensive, but back in the Bloomsbury pub, Rose is bursting to tell me about the time she fought back. For two years a client had been targeted by phishing emails at her work address, in an attempt to access her private email account and harvest sensitive financial information. A link in the emails would prompt the client to enter private details including email passwords. She was wise to the attempts, so did not click, but the identity of the hacker remained a mystery.

Rose created a new Gmail account in her client's name and generated three months' worth of fake emails made to look as if they belonged in her inbox – receipts for big purchases, conversations with her PA. One email from her PA was marked "urgent" and contained a link to access a confidential financial document. The digital honeypot filled, Rose logged out and waited for the next phishing attack on the client's work email. This time, the client did click the link, but entered the sham Gmail address and password, knowing that the hacker would receive them. More waiting, although not for long.

"It was an obnoxious time in the morning when the criminal logged in," Rose recalls. Moments later, the hacker clicked on the "urgent" link. It looked to him like a Google document address, but in fact diverted to a website Rose had also built as part of the sting – a fake virus scan page that would run for a few seconds before getting stuck. Rose had programmed the "scan" to harvest the attacker's IP address, the numeric identifier assigned to every connected device. Rose used that information to identify the man, who, it turned out, was known by the victim. When he realised the game was up he never contacted the client, who chose not pursue criminal charges under fraud laws.

Rose, who watched the email sting unfold at home in the early hours, is packing her bag as she sets off for the office to start work on her next case. She does not have the demeanour of a soldier fighting a losing battle. Victories, when they come, are all the sweeter given the scale of the challenge. "Above all, these criminals are confident in their ability to be anonymous," she says. "Their intentions are selfish, they sit there not thinking about the consequences of their actions, or ever expecting to be caught. And what they really don't expect is that anyone will hack them back." ■

side projects and shoots for non-surf companies. It's enabled me to find my own image and wear clothes that I personally like." That's labels such as Isabel Marant and Valentino, says Frankie, who last year bought a pair of Valentino Astro Couture ankle boots which she "won't take off". Mother and daughter have been hitting the shops in London in search of Le Labo's Santal 33 fragrance, and Frankie confesses to having a weakness for vintage, as well as a tendency to raid her impossibly chic mother's wardrobe. "Growing up, my mom wore a lot of cool, different clothes," she says, "so I snoop in her closet and steal her things. She has a lot by The Row and a vast cashmere collection – primarily grey, navy, black… But if she finds a jumper she likes, she will buy it in every colour."

In the four months of the year she's not travelling the world surfing, Frankie hangs out with her family (she has three siblings), who are an established part of the Malibu socialocracy. She is frequently found on horseback on the trails at nearby One Gun Ranch, Alice Bamford's property (Alice is Simone's best friend). Cindy Crawford and Rande Gerber are not only neighbours but close personal friends of the family. "My little sister Allegra is best friends with Kaia – they're both home-schooled," Frankie explains, cradling a cup of black coffee to combat her jet-lag. "We always used to go on family vacations with the Gerbers. I surfed a lot with Kaia's brother, Presley." A recent "little fundraiser" in the family's backyard saw Gwyneth Paltrow in the audience when Chris Martin performed for the Boys & Girls Fund – a local after-school youth club. "Chris and a bunch of people – Beck, Jakob Dylan – came and played in our backyard," says Frankie. "Chris's kids, Moses and Apple, also sang a couple of songs and they were really good… I thought they were more amazing than him!" she laughs. "They were crazy. Chris surfs a lot, too; he's obsessed with surfing."

So how does it feel to be a woman in the surfing world? Would she date a male surfer? "I'm single at the moment…" She pauses. "There are a lot more prima donnas in male surfing. They know girls love a pro surfer and they definitely play up to that – seeing it up close is not the most attractive thing. But I'm good friends with the boys and we make fun of them. So while in theory I would date a surfer, as I know a lot of them on the circuit, I'd have to say probably not! The surfing world is very wholesome and very small. We're from all over the world and we go everywhere together; we're all good friends and very close. A lot of the contests are held in secluded, remote places, but often there's not much going on. In Hawaii, for example, everything is closed from 9pm." Frankie says that while men and women make the same money from contests, boys earn a lot more from sponsorship. "But that is starting to change," she says. "Female surfers have a lot more adaptability. I'm really happy it's now seen as cool to be a female athlete and a role model for younger girls."

"What about sharks?" I ask. As an archetypal city-dweller it's one of the first perils that crosses my mind when I think of surfing. "Yeah, it's not something I've really worried about too much in southern California," she muses. "But in the past two weeks, two women have been attacked by sharks. One was like 20 minutes from where I live, and another woman in Orange County got her thigh bitten off." It's just as well Frankie isn't overly concerned about the threat: her mum shows me a picture of a huge and beautiful painting of a Great White she recently bought for the family dining room.

So what does the future hold for Frankie Harrer? She's bidding for a place in the world's top 22 surfers, and the Olympics also beckons. (Frankie's family is German, and she hopes to compete for that national team when surfing becomes an Olympic sport in 2020.) "When I was younger, I struggled accepting losses," she admits. "But in any competitive sport, you lose a lot more than you win. Competitive surfing is something women can do until they're about 30. That's 11 more years of travelling a lot and, while I love it, I think by that time I'll be ready to do something else," she grins. "Probably…" ■