Hackspace

Les Pounder talks to enigmatic hacker Freakyclown about the future of online security in a world where every click is under surveillance.

The world of hacking is a shady place full of secrets and lies, but in recent years this world has been dragged by the scruff of the neck into the media spotlight through the likes of WikiLeaks, the Snowden files and high-profile hacks on major corporations by clandestine groups. But hacking is as old as technology itself and not all hackers are malicious. Recently we met Freakyclown, a hacker and penetration tester who works to make the world a safer place, one client at a time.

Freakyclown is a rare type of person; while he protects his real identity, he's content to speak in public about his profession, and he's become a popular speaker at UK events. He's also a keen supporter of the Raspberry Pi Foundation and its mission.

LXF: You're quite an enigmatic celebrity in the unconference and events world. Can you tell us a little about your history?

Freakyclown: Well, I'm originally from Essex and I grew up pretty poor, but thanks to my mates, who are more like brothers to me, we kept a tight-knit group that got us all through the hard times.

I got into computing pretty young. My first computer was a Binatone dual paddle game system with analogue controllers and metal toggle switches to select *Tennis* or *Pong* and so on. I went through a couple of machines including an Atari 2600, my best mate Lee still has his wood-faced one! Then I got an Amstrad CPC464, which was my first real computer with a keyboard, and that got me into a little programming. Eventually I traded in my Amstrad for a Commodore 64 and then finally upgraded to the Amiga 500 and 1200, which is when computing really took off for me. I started hitting bulletin boards and other dial-up places.

It was around this time I started hanging out with 2600 hacking groups. Before long I started going along to their London meetings and making friends, but most importantly the group gave me a huge help in learning things. Skip forward a fair few years later and I'm now working as a professional hacker or penetration tester (pentester).

LXF: Was there an event in your life that triggered your interest in hacking?

FC: I don't think becoming a hacker is something that is triggered by an event. It's a mindset and a way of life you are born with – a thirst to want to understand and change things. I don't think there was a key moment where I suddenly exclaimed "Eureka!" and went off to learn hacking. I believe it grew out of an innate need to learn not only how stuff worked, but how to make it do what I wanted it to do. Sure, it's fun to sit and play videogames but there is nothing like the feeling of making one yourself no matter how crude and simple it may be. This mindset helps when testing networks, web applications, binary applications and building security. We come at them from a completely different angle to the end user and the developer. When pointing out security flaws I often get told "I would never have noticed that," or "I wouldn't have imagined doing that." This comes from a lifetime of looking at things in a completely different way. A lot of people think that you need to be part-criminal or an ex-criminal to do the job we do, but that isn't true at all. In fact, it would mean you would almost never get a job like this – it's like saying that a policeman would need to be a criminal to catch them. It's all about the mindset.

ON THE PERCEPTION OF HACKERS

"People think you need to be an ex-criminal to do the job we do, but that isn't true."

LXF: You work for a company called Portcullis Security – can you tell us a little about the work that you do for it?

FC: Portcullis is one of the largest computer security firms in the UK. It has been going since 1986 and has about 40 pentesters. Most of the work that I do is web application testing and network testing. We have specialists in almost every field from iOS phone testers through to criminal forensics. We are very active at releasing new tools and blog posts to the world via our own dedicated labs site (**http://labs.portcullis.co.uk**). When I'm not doing 'normal' pentest, work I get to indulge in my speciality – social engineering!

LXF: So what is social engineering?

FC: Social engineering is basically convincing people to provide you with information or access to places they shouldn't. Although this does include things people may have heard of, such as email phishing attacks, we use social engineering to test the physical security of buildings ranging from small offices through to banks and more secure places that I can't mention. I've been doing this type of testing for many years and have a 100% success rate getting into every target I've been given. I'm not sure whether this means I'm great at my job, or that across the board people do physical security really badly. I spend a lot of time trying to convince people that it's a very important aspect of IT security. Many times I have gone against a firm that have spent millions of pounds on their network security only to rock up and walk into their building and remove the computers that they have worked so hard to protect. I have literally thousands of stories of interesting events and situations that I have gotten into doing social engineering testings and I am slowly writing a small book of them, readers that are interested in that should hit me up on Twitter or IRC to encourage me along with that, cause I need the motivation to finish it up.

LXF: Have you ever come across security issues in a service or product that have forced you to reconsider using it yourself?

FC: Oh yeah, I hear of loads of things that concern me and make me want to stop using some products or services. I've heard of everything from those NFC-enabled bank cards (which I love to do a live demonstration with during my talks, illustrating how easy they are to steal data from), through to whole companies whose networks I know are insecure, and I fear for my own personal data! I'm sure someone with a normal mental

› *Linux Format* would like to thank the Museum of Computing in Swindon for its kind help with the production of this interview. Go give it a visit: www.museum-of-computing.org.uk

attitude wouldn't sleep well at night. One sneaky trick to help people track who's selling their information is to sign up to Google and then give + emails to companies. For example, MrFoo@gmail.com can use MrFoo+ElectricCo@gmail.com for the electric company and it will come through to MrFoo@gmail.com and you can separate out emails easier, but if a gas company starts emailing you on MrFoo+ElectricCo@gmail.com then you know who passed it on, which makes it easier to block and report spam.

LXF: As part of your presentation for various events, you introduce yourself via a series of quick slides. Have you had any brushes with the law, and if so, how do they perceive a 'hacker'?

FC: Well, there was this one time when I got arrested for the CMA (Computer Misuse Act) Section 3, which got a little out of hand to be honest, but the law saw sense after many, many months of me agonising and waiting until the bail case was finally dropped! Another funny moment was in London, when I was undertaking a social engineering job. It was about 2am or 3am and I was scoping out this building for weaknesses ready for the next morning. I wanted to see what ways I could infiltrate this massively secure building. Suddenly I heard a cough from behind me and someone asked me what I was doing. Obviously being sleep deprived and focused on the task at hand, I casually said "Trying to work out how to break into this bank tomorrow". It was then that I realised that two coppers were standing there staring at me in disbelief. That took some explaining! A third time involved a social engineering test against a high street bank that suddenly took a turn for the worse when the bank was surrounded by police and I had to spend a fair amount of time explaining and proving that I was a good guy!

ON BRUSHES WITH THE LAW

"The bank was surrounded by police, and I had to explain and prove I was a good guy."

But to answer the question, the average policeman doesn't seem to understand hacking, in much the same way that the general public don't (they are normal human »

» beings remember!) and frankly it is not their job to. It's the job of the courts and judges to understand and interpret the very grey guides given in laws and hopefully see sense in it all.

LXF: Your talks are always very popular and you draw quite a crowd – what do you think attracts people to them?
FC: I genuinely have no idea why people even come along, let alone why I get invited to headline at events, but I've been told its a combination of scaring the audience as well as making them laugh. I get the biggest range of reactions to my talks, from people asking for signed stuff through to people crying at the subject matter that has upset them. I like to make my talks a mix of simple explanations of complex subjects and super technical explanations to make sure that everyone who comes along can take something away from them. If I can get across the actual reason why people should use secure passwords or not post their photos on Facebook, and they can explain that to their friends in a way that isn't technical, but they can give the real world reasons, then I think a talk has been successful.

LXF: The actions of Edward Snowden, and his release of top secret documents to media and other websites have given him a pseudo-celebrity status. Should an action such as this be celebrated?
FC: I know I am going to get some flack for this, but I think Snowden should be tried as a traitor. He took a job for the NSA and then years later grew a conscience? Oh please, you don't become a vet and not expect to be putting fluffy kittens down, and then cry about it to the papers that other vets are doing the same. The agency he worked for has a job to do and should be allowed to do it! Honestly, nothing he has released has been mind-blowing or at least not suspected. The only fact that we've learned is that the NSA is terrible at presentations!

The mass media like to make things appear a thousand times worse than they actually are, and yes, they will moan about the way that certain secret agencies act, but they only see one side of things. There are many decisions and actions to be done in order to protect the way of life that we have, and they aren't always pleasant. As Spock once said, "The needs of the many outweigh the needs of the few."

LXF: We've heard many stories about the NSA spying on and monitoring civilians' communications. What is your take on this?
FC: The clue is in the name. Throughout history, mankind have spied on each other – it is the way of the world and will not change! As I already said, we need these agencies in order to enjoy the freedom and liberties that we have. I have no issue with the way they do things – in fact I salivate about the awesome technologies they are involved with, and the projects that the general public have no idea about. Just read the history of Menwith Hill!

LXF: How is Menwith Hill related to hacking, and what technologies have been used or created there that are now commonplace?
FC: Well, Menwith Hill is a small hub in the worldwide Echelon system run jointly by the UK, USA, New Zealand, Australia and Canada. It's been around since the 1960s and is used to sniff traffic, then the data is given to other agencies. That's because it's illegal to snoop on your own country, but not on each other's. Menwith came onto people's radar (no pun intended), when documents brought out in a trial in the 1990s showed that it had fibre lines from the UK phone trunks capable of handling 100,000 concurrent phone lines. People used to think it was all conspiracy theory stuff until Snowden started releasing documents and now it's coming back into the public's mind.

LXF: What's your definition of the term 'hacker'?
FC: I grew up when hacking was the old school term, meaning if you use something in a way it's not designed for, it's technically hacking, or if you cobble something together to enable you to use something in a way it wasn't designed to be used, then that's hacking. However, nowadays it is more generally meant for computer-based stuff. The mass media have totally ruined the word, and I urge the geek community to try and steal it back and reclaim it for its original intention.

I helped start the Surrey and Hampshire Hackspace (**http://sh-hackspace.org.uk**), and it's not about hacking computers in the sense of breaking into computer systems. We do everything from wool-spinning through to robots. Some people think we should be called a makerspace, but I love that we have stuck to the old ways and are known as a hackspace.

LXF: Tor has been seen as the best way to stay anonymous online, but there are reports that it's been compromised by government agencies. Are we seeing an increase in surveillance at the expense of liberty?
FC: Never ever rely on a single point to remain anonymous. Tor's logo is an onion for a reason. Use Tor, for sure, but use it like a skin of an onion – layers upon layers upon layers. Encryption is another thing people do badly but depending what you want to do take the appropriate measurements. You don't need to fly to Thailand and use a stolen laptop with stolen Wi-Fi from a nearby cafe to browse the secret wiki on the undernet, but if you are probing NASA servers for proof of aliens, don't do that from your parents' house!

LXF: Are we moving blindly towards a controlled internet, where organisations can lock content? For example, ISPs blocking torrent sites due to illegal file sharing?
FC: No not blindly. We have always had this, and people thinking otherwise are just not informed enough. Deep packet inspection and QoS have always been available to even the most basic networks. If you don't like what's being blocked, there is always a way around it. Again, we need to protect the innocent, like kids with bad parents, from seeing stuff that's not appropriate. The people that moan about things being blocked by default generally have the technical knowhow to bypass them and assume that the general public want the access they need, in much the same way that people assume the speed limit should be raised, when most people cant drive safely at 15mph in a car park. We have to protect the masses from themselves not for the few Michael Schumachers and geek wizards.

[LXF: The Internet of Things is slowly becoming a reality. Recently fridges were found to be part of a botnet sending 750,000 spam emails. Do we really need to have every device on the internet? And if so, how can we reduce the chance that our fridges become part of Skynet?

FC: Until IPv6 finally takes off, I can't ever imagine that everything will be connected. Nor do I worry that Skynet will be made from fridges! There's a fantastic film called *Maximum Overdrive* (1986) where all the computer-controlled devices on Earth start to turn on people and kill them, maybe this is more of the future than *Terminator* style wars. Computers are extremely fickle. I can't imagine Skynet running for more than two weeks without needing a reboot due to an update being required.

LXF: Google has bought quite a lot of interesting companies lately, including the robotics company Boston Dynamics and, more recently, Nest, the remote-controlled central heating project. With its purchase of Nest, are we looking at a potential security risk to life and liberty?
FC: I think Google gets a lot more flack than it deserves. Google is not military funded, and nor is it doing R&D on behalf of the military. Google just has too much money and is trying to find the next big thing. People love to hate on success. In the 1980s and 1990s everyone hated Microsoft; now everyone hates Google, Facebook and *Flappy Bird*.

LXF: How can users stay safe online?
FC: Trust no one. Make sure you've installed every update you're asked to install (after checking its authentic). Run a decent free antivirus solution. Make sure that you actually understand the risks. I suspect the average reader of this magazine is more savvy than most, so I ask the dear readers to teach others some basics that they already know.

LXF: Devices such as the Raspberry Pi and Arduino have made tinkering and hacking more accessible for learners. Have you come across any nefarious uses for these devices?
FC: Yeah, in fact I've created a few myself. One is a VoIP phone that has a Raspberry Pi embedded into it. The host phone provides the hidden Pi with an Ethernet network connection to the target's network. The Pi also creates a wireless access point, so it can be left plugged into a target's network and work as a VoIP phone, but allow attackers to wirelessly attack their network.

LXF: On the subject of nefarious devices, what's your take on the use of drones? With kit being easily available online, are we risking our privacy?
FC: Like all new technology there's always going to be a risk that it could be used for harm as well as good. I mean, how long until we see someone attach a grenade to a drone and swoop in on Justin Bieber concert, or fly over military bases to snoop for secrets?

LXF: There are many user groups and hackspaces starting up around the world. What would be your advice to a group, and what lessons did you learn along the way?
FC: Let's first clear up for the readers that we are talking about spaces where people can learn things such as electronics, weaving, woodwork, and any other skills the members may have. They get to build 3D printers, use lathes, drills and sometimes some computer stuff happens. A hackspace is not a place you would go to learn illegal 'hacking' skills.

As I mentioned, I helped start the Surrey and Hampshire Hackspace in Farnborough, so I have some experience of what it's like to need and then start a hackspace. I would suggest you have a really good look around first. There might already be a hackspace in your area. If like me, you find there isn't one, then it's best to start off small. Start with simple meetings in a local pub or coffee shop to make sure you get the core people in place. It's this core that will see you through the next few years until you get your first space. Take baby steps. We did pub meetings, then found pubs that let us use the back room for free, and then moved on from there. We're always available on IRC on **freenode #sh-hackspace** if anyone wants to come and ask for more advice.

LXF: If anyone is interested in a future security or hacking career, what advice would you give them?
FC: Learn the basics. Make sure you know the fundamental ways things work – networking, code, packets and wires and so on – because only when you understand the fundamentals can you start to work out how to build on these things and then start to make them behave in ways to your advantage. If you are young and looking at college or university, then try to get onto a course that covers as much stuff as possible rather than focused on one area. Pentesting requires not only the correct mindset but also having a broad knowledge. If you are older or already have a job so can't get on a full-time course, your best bet is to look at getting a certification. In the UK you should check out Crest or Tiger Scheme as these are well known and the industry will look favourably on people that have gotten those certificates above, say, a CCNA or MS cert. There are also many free tutorials out there, and there are loads of downloadable live CDs that have tools and applications to help you learn, such as Kali Linux, Black Arch and then you have live CDs for setting up testing labs, such as WebGoat and DamnVulnerable Web App. Remember: if you don't have permission, you shouldn't be touching it or you will end up in trouble and that will ruin any chance of getting a job.

LXF: Are there any hacks committed by other hackers that you wish you had done? If so, which and why?
FC: [laughs] I'm not sure I would want to have done any because they generally got caught, but I think Gary McKinnon's was the most interesting one to me due to my interest in UFOs. The trouble is, having briefly met him at a conference, I don't believe a word of what he says he saw. LXF

ON THE INTERNET OF THINGS
"I can't imagine Skynet running for more than two weeks without a reboot."