Daniël Verlaan – *I Know Your Password*

347 pages, 70.000 words. Published in October 2020 by Das Mag Publishers. 30.000 copies sold.
Translation subsidy provided by the Dutch Foundation for Literature.
English sample translation available.

You buy something online and all of a sudden your bank account is being emptied out; your smart thermostat has been hacked and set to 37 degrees, unless you pay up; your brand new security camera suddenly shouts "suck my dick" at you.

The internet is a world full of possibilities – also for criminals.

These are scary yet mesmerising stories, full of dangers against which you can protect yourself. How? Tech journalist Daniël Verlaan will tell you how.

He went undercover in shady networks, spoke to the teenagers who hacked the Dutch banks and found out how a small arthouse cinema took our computers hostage in a large-scale operation.

I Know Your Password is not trying to make you paranoid, just less naive. Read Daniël Verlaan's stories and be prepared.

Daniël Verlaan (1989) is one of today's leading Dutch tech journalists. He works for RTL, a Dutch news broadcasting channel. Last year he received the Loep, the prize for leading research journalism, as well as the Tegel, the most prestigious journalistic prize in the Netherlands.

For more information, please contact Stella Rieck: rieck@cossee.com or visit www.cossee.com/foreignrights. |
translation grants can be obtained through The Dutch Foundation For Literature: www.letterenfonds.nl/en/grants

Press – *I Know Your Password*

"*I Know Your Password* reads like a journalistic thriller. Verlaan initially wanted to put that in the subtitle, if it weren't for the fact that the word 'thriller' insinuates fiction, and the stories he tells are by no means fictitious. In a compelling manner, Verlaan takes the reader on his descent into the dark web, looking over the shoulders of hackers, cyber criminals and victims. The casually accompanies his stories with tips on how to defend oneself against digital vulnerability, useful for everyone who uses the internet." – *de Volkskrant*

"The best thing about *I Know Your Password* is that it makes these stories serious enough without overdramatising them. It plays poker with your trust, but always returns a few of the chips at the end of each chapter, and in doing so teaches you how to call the bluff of the elusive world of cybercrime." – *Demo Magazine*

"*I Know Your Password* by technology journalist Daniël Verlaan provides a practical and convincing handbook in a time of information deprivation … Verlaan deserves compliments for the way in which he illustrates a theme that is complicated to a lot of people. As Verlaan himself says: "Step one is knowing what to defend yourself against." After reading *I Know Your Password*, you will have taken that first step." – *Athenaeum Booksellers*

Endorsement by the Dutch minister of Justice and Security

The Dutch Minister of Justice and Security, Ferdinand Grapperhaus, recently recommended *I Know Your Password* and gifted it to the entire Committee of Justice and Security:

"Chairman, I've brought something along for you and I'd like to suggest – it's less than fifty euro's, I've left the price tag on – that you might possibly share it with the committee members, because this book really got to me on a number of fronts, also because of the personal aspects in Daniël Verlaan's story. It's the book *I Know Your Password*, chairman, and this is such an important subject, which on a micro level symbolises cyber security. I think cyber security starts with all of us, at our kitchen tables, and I'll admit, I'm just going to say it, during the first years of the internet, my favourite passwords were ferd1959 or 1959ferd. Yes, my year of birth and first name, which is not very smart, and one realises this soon enough. But there is much more to this, and that is why I wanted to offer this to you just before the holidays. This book, I'll do it this way from now on, that's how to do it these days."

Click *here* for the full video in Dutch.

Sample – *I Know Your Password*

Translation by Isadora Goudsblom.

So now I am older
Than my mother and father
When they had their daughter
Now what does that say about me?

These are the first lines Fleet Foxes-singer Robin Pecknold wrote for 'Montezuma'. Not only was it one of my favourite songs of 2011, it was also my most important password. What I didn't know then was that this password could be cracked within seconds.

It isn't the only weak password I've had. As a teenager I used the password 'google' and in 2006 I changed it to 'thefeeling', after the British pop group that was behind the infectious song 'Sewn'. Those passwords can also easily be cracked within seconds.

Pleased to meet you. I'm Daniël Verlaan and for years I used lousy passwords. For a book carrying a title like this, I thought it'd be more than fair to share some of my passwords with you.

For my job, I craft stories about the dark side of the internet, ranging from hackers and ransomware to phishing and the dark web. Every year more and more Dutch people fall victim to cyber criminality, and that amount – in the order of millions of people – won't be going down in the coming years.

On the one hand this is due to the fact that traditional crimes, such as burglaries and theft, are increasingly making way for internet criminality. It is now more lucrative for criminals to hack people than to steal a phone or watch. On the other hand we've become more vulnerable as a society because our lives are digitalising at a high pace; and this whilst most people have only little knowledge of technology, online safety and privacy.

When we leave our homes we lock the door and close the windows, but we often leave our digital doors wide open. We use bad passwords, click on weird links and download and open all sorts of files blindly. To put it simply: most people – and you might just be one of them – are pretty easy to hack.

This may sound slightly frightening. My aim is not to scare you, but rather to ensure you become a little less scared of everything that's happening on the internet. That fear often stems from ignorance.

If you know little about technology, the first reaction is often: I've been hacked. Even if there's nothing going on. At the same time people are often hacked because they have limited knowledge of technology. The one reinforces the other.

On the other side, I actually *want* some people to become slightly more scared of the internet. For them to stop thinking: well, that won't happen to me anyway.

Ten years ago I also knew very little about hackers and that criminal online world. I'd just started the School of Journalism, where I quickly turned into the school's enfant terrible. I cut classes, got into fights with teachers and was expelled. Both the school and my parents were worried about my future. My dream was to become a music journalist, but despite a minor programme in Musicology, in which I learned everything about Schönberg's pantonality, it turned out I wasn't all too good at that. Then I decided to change my course and write about my other passion: technology.

The first few years my stories mostly revolved around gadgets, apps and games. I was always interested in those: as a nerd I used to put computers together from scratch, build websites and spend quite some hours behind the Playstation. But I knew nothing about cyber criminality and online safety. It wasn't until I started to work for *RTL Nieuws* in 2015, and dove into a very delicate and dangerous data leak during my first workweek, that I found out that this is what interests me. I started to understand what journalism was all about: following your intuition, diving into the things that are fishy, biting your teeth in and not letting go.

9

Internet of Things

What to do when your security camera suddenly says 'Suck my dick'

Internet of Things

- The *internet of things* is the collective name for smart devices connected to the internet – ranging from security cameras and robot vacuum cleaners to fridges that send you a notification as soon as your beer is cold.

- Because more and more machines are becoming 'smart', there's more to hack – including places that were once impossible to get into for hackers, like cars, smoke alarms and pacemakers.
- Due to the explosive rise in smart devices, it's become a sort of Wild West where everyone can get their piece, whether they're a seasoned criminal or a bored teenager.

It's just another typical day for Rilana, a blonde woman from Brummen, Gelderland. October 1st 2017, the sun is shining and she's doing her daily shopping at the local supermarket. At home, she's busy taking the items out of her shopping bags when she hears something in the living room. It's a sort of crackling sound, as though someone is panting into a very big megaphone. She walks into the living room and sees her camera turning in all sorts of directions. How is this possible? Her phone is on the bed, so she's not controlling the camera. Might it be updating? She turns around and continues unpacking the groceries.

Rilana bought that camera a month or two ago at the Action for 35 euros – a good Dutch price. She bought it to keep her eyes on her dog. The white little pup makes a mess in the house, and she wants to keep an eye out during the moments she's gone, to prevent her beloved pet from ruining her house. The camera hooks up to the Wi-Fi network and with an app on her phone she can see what's going on in the living room at any time or place. There's even a microphone in it so she can speak to her pup strictly if necessary. And a password. That makes her feel at ease.

Suddenly Rilana hears rummaging about coming from the living room again. She puts the groceries down and walks back into the room. The camera towards her and says to her: 'Bonjour, madame!'. It scares the hell out of her. What's this? 'Hello, is anybody there?' she responds. The sound stops. Rilana walks to the other side of the living room, and the camera turns with her. She walks to the other side, and the device follows her almost directly. Is this really happening? In a panic she calls a friend and starts a video call, so her friend can see what's going on. With her phone in hand she walks back into the living room. 'Bonjour, madame, vous allez bien?' the camera says again. See! The thing is actually speaking to me. Someone is peering into my house goddammit! She runs towards the camera, pulls the plug and throws it back into the box.

In the evening she dares to turn on the camera one more time. She turns the lens to the wall and puts the plug into the socket. She presses the record button on her phone to make a video. This time she'll have the evidence. Within a minute the camera is at it again, the lens turns towards her and the camera starts talking. 'Hello, do you speak French?' the device says.

'Sorry?' Rilana says.

Again it sounds: 'Do you speak French?'

She answers: 'No, English!'

It's quiet for a bit. 'What did you do?' Rilana asks.

'Is it good?' the camera asks.

'No, get the fuck out of my house, now! Shut the fuck up, go away!' she yells.

Suddenly the camera switches language. 'Hola, senorita,' suddenly comes out. 'Oh, suck my dick!'

Rilana pulls the plug from the socket and bursts into tears. She's terrified and doesn't feel safe in her own home anymore. How long has that creep been watching? What has he seen? And who *is* he? She changes all her passwords and returns the camera to the Action.

Lights, camera, Action

Rilana's story reaches me through regional media. She posted the video on Facebook in which you can see how the camera started talking to her, in order to warn as many people as possible for this camera that Action sells. It's a clear example of the danger of the so-called 'internet of things': smart devices that are connected to the internet. Whether it's a robot vacuum cleaner, coffee maker with Wi-Fi or a smart doorbell.

My interest has been piqued: how was Rilana's camera hacked? And does this pose a threat to other Dutch people who bought the same camera at Action? On Action's website I find the camera type: the HD Rotating Wi-Fi Safety Camera from the Maxxter brand. This brand imports cheap gadgets from China, sticks their own brand on them and sells these gadgets in the Netherlands.

I call a few Actions in the neighbourhood to find out if the device is still for sale somewhere, as I'd like to try it out myself. I get the same answer everywhere: the camera is sold out. Action's spokesperson confirms the popularity of this specific camera. Rilana's situation is being looked into, but they cannot say anything else about it. They're working together on it with Maxxter, I am told.

I'm not going to sit around waiting for that. I find the type number of the camera: ACT-IPC-01, with which you can often find the user manual. It exists, on Maxxter's website. The Dutch user manual gives a step-by-step description of how to use the camera. This happens with an app:

iView Pro, it's called. I've never heard of it, but it's available for both Android and iOS. Once installed, I get to a screen where I need to fill in two things: a device ID and a password.

Then my eye catches a piece of text in the user manual:

> 'The ID number is on a sticker on the camera. The standard password is 123, but if you've ever changed the password of the camera (recommended), then you'll need the current self-made password of the camera to be able to add it to the app on another tablet/phone.'

So Maxxter 'secures' its smart cameras with the standard password 123? Not even a unique password for each device? That ought to be normal: routers – also important devices in your home – are protected by such a unique password. I put it to the test and enter a few random numbers in the device ID and 123 as the password. After pressing the large blue connect button, nothing happens. The device ID can't be found. Yes, this is what I had expected. I can't find such a device ID anywhere, not in the user manual either. How do I get the number if I don't have a camera and they're sold out everywhere?

In my free time I like to watch so-called unboxing videos. These are videos in which someone unpacks something. It sounds really lame, and maybe it is, but it always makes me feel extremely zen. My favourite YouTuber is Marques Brownlee, known as MKBHD, who makes wonderful videos about the latest gadgets. He brings out the box of a new smartphone, turns it around and then opens it. Step by step he shows us what's in it: the charger, earphones and of course, the phone itself. The way he takes off a piece of protective foil from a brand new screen is nearly pornographic.

So I suddenly get the idea: would someone have made an unboxing video of Maxxters HD Rotating WiFi Safety Camera? I enter the name into YouTube and what do you know: I find a video of a Dutch man discussing the camera. He turns the device around and shows the bottom as well: exactly where the ID number should be visible. I hit the pause button, zoom in and after a little bit of tinkering figure out what his camera's ID number is. Bingo.

I enter the ID-number in the app along with the password 123 and press the connect button. To be clear: this is a punishable offence, for journalists too, because it's computer intrusion. But sometimes you have to break the law to reveal an injustice. The chief editors and our lawyers know about it and as most often their advice is: only do what is strictly necessary. But my attempt has failed again; the man from the YouTube video has changed his password. I change the last

digit of the device ID to a random different digit and press the button again. The app suddenly takes longer to process the change and the screen of my phone turns black. There's some interference on the black screen until I am suddenly in the living room of an older woman. I see her sitting there at the table with a cup of coffee. Max broadcasting is on in the background.

What the fuck.

I pull this trick a couple more times. Within a few minutes I'm inside various peoples' homes. One of them has the camera hanging in the shed and I can only see a workbench, another shows a girl in her twenties coming out of the shower. Other than watching you can also manage the camera and turn it in any direction, talk through the speakerphone and change the password in the settings, so the owner will no longer have access to the camera. I delete the cameras from the app and run, still knee-deep in my adrenaline rush, to my editor: 'I have a story! Those popular cameras from the Action are as leaky as a sieve.'

These are all people who didn't change the standard password. You can't blame them really: nowhere does Maxxter require them to change the password, and nowhere does the company clarify that other people can get in with just a device ID and '123'. But if you are able to watch the images of your smart camera at all time and in all places, so can others. Rilana had no idea this was possible, nor did the showering girl, the owner of the workbench or the Max broadcasting viewer, and I suspect many, many others.

This hack just goes to show how easy it can sometimes be. You don't even have to have technical knowledge to do it, you only need to enter a number into an app.

Be smart

The internet of things is one of the greatest dangers coming at us. We live in a time in which for many people a normal kettle isn't even enough anymore. No, a kettle with WiFi, now that is useful! Then you can just press a button and stay in bed while the water boils. Once you've had a shower the water will be just the right temperature to make a nice cup of tea. Saves you an entire walk to the kettle!

This may be a slightly overdramatic example, but this is the kind of sales trick you see everywhere. Devices that needn't be smart at all are suddenly made smart to boost sales. What about a smart fridge that has an app in which you can see whether you still have enough milk, eggs or beer? Or a smart barbeque that also has an app in which you can see and control the temperature? Such a barbeque has, by the way, been hacked before, during which the hackers let

the meat burn. Not the worst that could happen to you, but still, what a waste of your delicious steak.

Seemingly useful smart devices can also pose a threat. Take the robot vacuum cleaner, a machine that vacuums your home while you're at work. The thing recognises walls and objects and makes his way using sensors through all the rooms. The popular robot vacuum cleaner Hom-Bot by the South-Korean LG was hacked and attackers were able to take over the machine. Now that doesn't sound all that bad: what's a hacker to do with such a machine? Ensure your home isn't vacuumed properly? No, the Hom-Bot has a camera on board so you can keep your eyes on, say, your pet. Besides a vacuum cleaner, the thing serves as a driving security camera, a lot of people seem to think that's useful. This way, a hacker can spy on you in your own home, make compromising videos of you and blackmail you with them. Equally popular in the Netherlands: the smart thermostat. That too is not safe against hackers. Two American researchers showed how they took over a smart thermostat, uploaded ransomware and made the temperature rise to 37 degrees Celsius. If you didn't pay the ransom, your thermostat would stay on that temperature forever. It would literally and figuratively become too hot under your feet, so you'd gladly pay the 500 euro ransom: you'd lose much more to your energy suppliers the coming years.

Or what about the smart Hello Barbie doll, that's connected to WiFi and responds to the vocal sound of a child? There's a microphone in it that analyses the words of children and on that basis provides answers. A hacker showed how he hacked into the Barbie and could then always listen in through the microphone. This means not only the conversations of children could be recorded, but also the conversations of parents standing near the Barbie.

Some hacks can be really dangerous. Hackers have shown how they can hack smart cars from a distance and take over the steering, with all its consequences. Various hoverboards have also been taken over, whereby the ill-intentioned can make the thing go really fast or rather step on the brakes. I've stood on one of those hoverboards once and it takes very little to fall off it – especially if a hacker suddenly hits the brakes. It takes little imagination to think what kind of things might happen.

There are plenty of these kinds of examples out there. Smart devices run on software connected to the internet. That combination makes these types of devices vulnerable. Anything running on software that is also connected to the internet, is vulnerable. The problem with the internet of things is that it's in the early stages and that the focus is mainly: does it actually work? Safety doesn't seem to really be an issue yet for many devices. Unlike computers and smartphones, where safety now is one of the most important issues.

What's more is that many of these sorts of smart devices are made by companies that haven't understood all too much about online safety. Take a company like Mattel, the maker of the Barbie. That club knows how to make a doll, but not how to prevent hackers from taking over a microphone. This is a big problem in the world of the internet of things: companies who must suddenly specialise in cyber security. They often don't: their purpose is to sell as many products as possible, not to make products as safe as possible.

AliExpress, the Chinese web shop filled with cheap gadgets, also contributes to the distribution of these sorts of unsafe devices. A lot of good quality stuff is made in China, like your expensive smartphone or laptop, but a lot of crap too. This often concerns factories that produce lots of knickknacks as cheaply as possible, ranging from things like smart watches for children to security cameras. Those kinds of products are all over AliExpress.

What is often forgotten is that smart devices can also provide access to your better protected devices. Imagine you have a smart kettle at home. If that device is hacked, the attacker can turn it on or off from a distance. Well, there are worse things of course, but that same attacker is also able to see whether there are any other devices within the same WiFi network. Think of your smartphone, computer, tablet, laptop, router or game console. Those devices are much better equipped to handle attacks from the outside, but become much more vulnerable if the hacker is already on the WiFi network. In theory it could be possible for a hacker to take over your properly secured computer to then go on to empty your bank accounts. And all this because of a smart kettle you'd bought to have your cup of tea ready at exactly the right time.

Sauna & Beauty Oase

'I have 24/7 access to three dressing rooms where a camera is recording,' a certain *awaterbottle* writes on a forum for peeping toms. 'We have to look at the footage and select the best. I can watch live too.' He posts some images of naked women. 'What do you think of these? Do you prefer white girls, or black girls? Fat? Thin? Young or old? I've mostly shared images of girls I like, but I'd like to share a few of girls you find attractive as well.'

'Holy shit! Post those images and you'll be a hero,' one responds.

Security cameras are a beloved target for hackers. They offer a peek into a surrounding they usually can't just access. We use them to keep an eye on our most cherished places: our back garden, driveway or even our living room or nursery. One thing they have in common: they are

connected to the internet, which makes it possible for hackers to access to them. In a sauna in Nederasselt in Gelderland they know all about that.

It's just another typical day for me, in March 2018, when I get a tip from a colleague through WhatsApp. Supposedly, there was a video on a porn site with our national handball players in it, not in their orange uniform this time, but naked. Of course, a video of naked people on a porn site isn't uncommon, but it is when it concerns the Dutch handball team. The video is indeed online and seems to have been made in a dressing room by a camera on the ceiling. You see how seven women are taking off their training gear and, while talking sociably – at least, that's what it looks like, the video doesn't have any audio — put on white bathrobes. I've never been to a sauna, but those white robes and slippers strongly suggests that the footage was recorded in a sauna.

I know little about handball or the Dutch handball team. I know two players: Estavana Polman, soccer player Rafael van der Vaart's girlfriend, and the ever cheerful handball goalie Tess Wester. The former I know because I *am* a big soccer enthusiast, and Tess I've seen on television a couple of times. Ever since they became world champion in 2019, the sport has become much more popular – but all this takes place a year prior to the event.

I recognise Estavana nor Tess in the footage. I ask a sports colleague to help me out: are these really players of the Dutch handball team? She recognises three straight away. Yes, they are. It seems to be older footage because some of the players no longer play on the current national team. With this limited information I call the team's spokesperson. 'Good afternoon, this is Daniël Verlaan with *RTL News*. Can I ask you something: are you familiar with the fact that there's a porn website with on it a video of players on your team, naked?

It's quiet for a few seconds. Then she says: 'In the interest of the investigation we cannot make any statements regarding this.' This confirms that the handball union is aware of it. I continue to ask various questions: where was the footage taken? Do you know who's behind it? Have charges been pressed? I get a lot of no answers. I'll have to make do with it. While I'm on the phone, I refresh the video on the porn site, but it's suddenly disappeared. The video clip had only been online for a couple of hours but had already been watched over 10.000 times. Because the video is offline, I decide to publish right after the telephone conversation, to minimise the damage for the players as much as possible.

Then the search to find the place where the footage was taken starts. The clip seems to have been made with a security camera, but those things aren't supposed to be allowed in dressing rooms.

And how do those sorts of images turn up online? Are those cameras connected to the internet? Has the computer to which they are linked been hacked? Is the camera footage saved onto an unsafe server? Many questions, but so far, no answers.

And there are countless saunas in the Netherlands, so where does one begin to search?

One things strikes me about the clip: in the top right corner there's the text 'dressing space 2'. I find this odd: I always say dressing room and never dressing space. Maybe it's a sauna that specifically uses the term 'dressing space'. I decide to do a bit of Googling with a specific search term: *'dressing space 2' sauna filetype:pdf*. Using that search term you'll find all pdf files with the term 'dressing space 2' that are linked to a sauna. The first search result is a certain Sauna & Beauty Oase in Nederasselt.

I look at the map and the shape of dressing space 2 matches that of the clip precisely. That must be it. I call the sauna and am put through to the owner in a friendly manner, his name is Erik van Ingen Schenau. I ask him the same question: has footage been taken of the Dutch handball players in your sauna, that were later published on a porn site? He responds immediately: 'Yes, this happened here, we were hacked two years ago.' During that hack, that footage was stolen, he says on the phone.

The company has cameras in the dressing rooms to prevent theft, Erik says. All sorts of things – from jewellery and phones to wallets and even shoes – are stolen, and the footage shows who stole it. I find this all very hard to believe and remind him it is illegal to hang cameras in dressing rooms. He has a different view, he says: he doesn't want to take the chance, and this way he can prevent theft.

Two years ago, in 2016, Erik received a message on Facebook from an unknown person, so he tells me. He was warned that it was possible to tune into the cameras. Erik then turned all the cameras off, he says, and had a specialist look at them. Three months later they went back online. Only he and his wife, with whom he runs the sauna, have access to the camera footage. The cameras are connected to the internet so that Erik can watch the footage at home too, which he thinks is handy if the burglar alarm goes off.

After the publication of the story about the Dutch handball players, everything went into a fast track. More videos are found in which naked visitors of Sauna & Beauty Oase can be seen. They can be found on porn sites and forums for peeping toms, where videos are shared that have been made secretly: from someone getting changed in a changing room to a couple having sex in an Airbnb apartment. And the footage of the Dutch handball players too, that appeared there first.

On that same forum there's frequent footage of a showering room in Gent, showing all sorts of naked women. A 41-year-old gym teacher turned out to be filming them secretly through the keyhole. The Belgian police had already picked up a suspect, but the gym teacher made a stupid mistake: he deleted al his videos right when the other suspect was being detained. Of course the police then knew: we have the wrong guy. They quickly found the real perpetrator. Moreover, he wasn't as anonymous as he thought. On the forum, he used the username *DgreedB,* aka: greed, between D and B, his initials.

Meanwhile, the Dutch police hasn't been sitting still either, and within a few days after my publication bursts into Sauna & Beauty Oase. They find a hidden camera that at the time of the raid is still online, the rest has been turned off. The hidden camera is buried in the smoke alarm and is directed closely at the massage tables in the sauna. And yes, that footage too – how naked female bodies are being massaged – can be found online.

According to Erik the camera is up there to register harassment. A lot of young girls there work late, massaging men. Some feel unsafe from time to time, Erik says, and the camera gives them a peace of mind: there's someone keeping tabs. The guests however, don't know they're being filmed, as the camera has been hidden in the smoke alarm.

Because of the hidden camera, Erik and his wife have become suspects in the investigation into the sauna footage that has appeared online. They're suspected of surreptitiously filming visitors, but not of posting the footage online. For that, another suspect has been arrested: a 40-year-old man from Drachten. The man found the videos on the forum, downloaded them and uploaded them onto the porn site. He has been sentenced to eighty hours of community service.

It all begins with that peeping tom platform. That is where the sauna footage first appeared, in late 2016. It's the same forum *awaterbottle* is a part of. Together with other users, he picks the most attractive women to cut out of the footage and spread on the forum (he even delivers upon request: if someone has a thing for red heads, he'll specifically look for women with red hair). This is how the handball players turned up online: the footage was made in 2016 and spread on the private peeping tom platform, but didn't appear on a porn site until 2018.

The big question remains: who is *awaterbottle*?

We don't know. Despite a large investigation led by the police and the Public Prosecution Service, it is still unclear who *awaterbottle* is. Is it Erik? The police doesn't seem to think so: the case against him and his wife has been dropped due to lack of evidence. Despite the dubious choice to install a hidden camera, his statement can be somewhat understood: he wants to

protect his staff. It might well be possible that his cameras have been hacked: by his own admission, the user *awaterbottle* only had a few months worth of access to the footage – right up until the moment Erik took on the help of a specialist. After this, no more images turned up online.

'Why would I ruin my lovely company?' Erik tells the newspaper the *Algemeen Dagblad* when he is asked if he wasn't the one who'd put the footage online.
'The company we work so very hard for and which we're extremely proud of? I've worked here for 22 years now. We deal with naked people every day. You wouldn't take advantage of that would you?'

A couple of years later Erik files for bankruptcy: visitors steered clear of his sauna, for fear of turning up online too. The case was never really clarified.

Babies

No matter how effectively you secure a smart camera, they can always be hacked. People often wrongly think a password makes for adequate security. It happened to owners of the 'Ring security cameras', that are especially popular in the States. These Ring cameras are seen as safe devices. They're on the expensive side and are made by one of the most famous companies: Amazon. It costs a few bucks, but it's worth it, so people thought.

Until a Ring camera started talking to a young girl. 'Who are you?' the 8-year-old girl asked anxiously. 'I'm Santa Clause, your great friend,' the camera answered.

Through cameras like these, hackers sometimes make racist statements, wake up people in the middle of the night by yelling really loudly or demanding ransom money in Bitcoins. There's even a group of several hundreds of hackers who hack Ring cameras together and make live reports of it. The goal: trolling random people, which is internet speak for messing around or harassing people. Trolling is often seen as a type of mischief. Maybe the hackers actually think they're just having a bit of fun, but hacking into a camera in someone's home and scaring the hell out of him or her is, to put it simply, criminal.

The hackers were given access to the cameras through a specially developed programme to introduce automated usernames and passwords for Ring. That data came from data leaks and if someone used the same leaked password for Ring, a hacker was able to get access to the camera – the same method as in chapter 3 about data leaks. All successful login attempts were

saved and shared among hackers. One used it to troll, the other tried to record nude images and blackmail the person concerned. Others simply thought it was exciting to lurk around with.

You might think: it's not very smart to use the same old passwords for your smart camera. But even if you're using a unique and difficult password, you're not always safe.

Late 2019 I received an anonymous tip about a leak in smart cameras. The cameras were supposedly being used in the Netherlands as well, especially in baby rooms. The tipster fears peadosexuals are lurking and feasting on young children who are dressed. He asks whether I'm interested in diving into the leak. It involves cameras from the Chinese Apexis and their subsidiary Summple. The devices are for sale at Amazon and the cheaper web shops AliExpress and Wish. Bol.com also had Apexis products in their assortment.

This email comes from the Arcanum Group, an anonymous hackers collective which parents are a part of. They've reported the leak at the manufacturer, but without result. 'Because there are children involved due to the baby monitors, we feel obliged to inform people through the media about this leak,' one of the members writes.

These cameras are also secured with a username and a password. Apexis saves all that data in a database. That makes sense: without a database the company won't know whether you're entering the right login details. But the password for this database is so poor that it appears in the list of worst passwords ever. The password can actually be found in the rule code of the camera software.

But that's not the worst of it. Apexis accidentally saves those passwords unencrypted, so hackers needn't even crack the passwords in order to hack cameras. It makes no difference then how strong or unique your password is, it's just out there in plain sight in that barely secured database! There's no point in changing your password at that stage: the new password will just go into that same database.

To confirm the leak, the hackers of The Arcanum Group send me a couple of usernames and passwords. They all work. Because it concerns incredibly sensitive data, I suggest to the hackers collective to meet somewhere and investigate the leak.

I meet a Dutch hacker somewhere in a remote industrial area. He's friendly, well-spoken and well-dressed. And he's worried: this data can be abused by a lot of ill-intentioned people. If you have access to the camera, not only can you watch live, but you can also turn the camera from a distance and speak through the microphone.

During my testing, I visit Dutch living rooms where a family discuss their day during dinner. I see a couple watching TV on the sofa. Through another camera I suddenly get to see a

garden in which someone is enjoying the sun. And sure enough, a lot of nurseries, where the camera is mainly directly facing the commode and cot.

As soon as I have the leak in sight and have verified the leaked data myself, I contact Apexis. Phone calls to China aren't answered and I don't receive any response to my emails either. After a week I decide to publish in order to warn the thousands of Dutch people with cameras of that sort: pull the plug as soon as you can, the device is unsafe.

A few days after publication, I suddenly get an email sent by a Chinese address. It's Apexis. They've solved the problems, thank me for drawing attention to the problem *and* offer their apologies. After a check it seems the leak has indeed been closed – but in a shoestring manner that doesn't take away my worries.

Have there been men recording footage of naked babies so they can share it on a forum for child molesters? I'm afraid I can't rule out this possibility. And that uncertainty still hurts for some owners who used this smart camera as a baby monitor. The idea alone that ill-intentioned people have been lurking at your naked baby: it gives you the creeps. One of the victims threw the camera straight into the rubbish bin. No more smart camera for her. She now uses a baby monitor you don't need to connect to the WiFi.

The huge increase in the amount of smart devices in our lives is something experts have been worrying a lot about for years. Our lives, the cities we live in, the whole society is being digitised further and further. If you can already hack smart cars, what is the future going to bring? Hacking into traffic systems and causing accidents? There are even researchers who've hacked a smart pacemaker; this way heart failure can be induced, with death as a possible result.

That is precisely why I barely have smart devices in my home: not only are they smart, they are terrifying too. And it's not particularly easy to get rid of all smartphones: try and find a television that isn't smart. Those are practically not for sale anymore, while a lot of smart TV's run on the most unsafe software there is. My fear is that we're on our way to a society in which you, as a consumer, no longer have the choice between a stupid or smart device. That companies and our government keep making everything *smart* for the purpose of 'progress', but don't contemplate the dangers that might be a part of it.

For now I've chosen to just not connect my smart TV to the WiFi.

Tips

You could – like me – decide to have as little smart devices in your house as possible, but I know: that can be quite a challenge. So if you ever decide to buy a smart device, always check whether you actually want to use the smart functions. In the case of a smart TV I chose another solution: I don't hook the television up to the internet, but have bought a separate media player, an Apple TV, that I *do* connect to the WiFi. An Apple TV is much better secured than the average television. This could be a way to solve the problem.

If you do decide to bring a smart device into your home, like a thermostat, smoke alarm or lamps you can control from a distance, pay close attention to the brand. Companies such as Google, Apple and Amazon have more experience with securing a device than an unknown Chinese brand you can only order on AliExpress. In that case it's preferable to chose a well-know brand with a good reputation regarding online safety. That doesn't mean however that those devices can't be hacked: Amazon's Ring camera shows us that things made by large names in the field of tech are vulnerable.

Another tip is to create a guest network in your router. This is a technical job, but by doing this you'll be creating a second WiFi network that is completely closed off and doesn't have access to your most important devices that you've connected to your *real* WiFi network. If a smart device is hacked and it's connected to the guest network, the hacker won't be able to get to the other devices in your home, such as your computer or phone.

With smart cameras it's useful to give the device a physical slider so you can cover the lens when you're at home. When installing the camera keep in mind hackers can take over the device, and adapt the image to that. Finally, it's important to always have the latest updates installed and to use a good and unique password. Those tips are always useful by the way, not only for your smart camera.