Academy of PHYSICAL MEDICINE

Transcript

Protecting your Data With Andrew Eardley

Cast List

Steven Bruce	S
Andrew Eardley	A

S: Well good afternoon. Welcome again to the Academy of Physical Medicine. Great to have you with us for a lunchtime broadcast. Only 45 minutes this lunchtime, but a vitally important subject, as I'm sure you're all aware. It's not just about GDPR. It's just not just about patient data. It's about also protecting yourselves. We're going to be talking about what's available on the internet possibly regarding your own clinic, your own website, but also we're going to be talking about what you should do to protect yourself against potential invasion by hackers or others who want to steal your data. I know bugger all about this sort of thing so I've got Andrew Eardley from Prompt PC to come in and talk to me about it.

Andrew, welcome.

A: Pleased to meet you.

S: Great to have you on the set here. What's your expertise in the dark web?

A: Well, we've been in business 22 years now. We've seen such a dramatic increase in cyber crime with our clients. We look after about 300, 400 client companies, somewhere in the region of about four and a half thousand

people we're looking after. We've seen a tremendous spike. It's exponential growth in terms of attacks now coming into our client base.

S: So basically you're a nerd.

A: Yep.

S: And you've had 23 years experience of protecting people from hacks on their sites and other stuff to do with PCs, so you kinda know what you're talking about.

A: Absolutely.

S: Well, most of us don't and I dug this picture off the internet earlier on, which explains what the dark web is. Could you explain to people what the dark web is?

A: Yeah, absolutely. Public web, everybody's got access, all the normal stuff you find in the search engines.

S: Right. So if someone puts a term into a search engine, that public web is what it's gonna be looking for.

A: Correct.

S: It's indexed or-

A: It's indexed. The next step beneath that is the deep web. This is where there's data there which is not indexed. If you go hunting and you know where to go looking, you can get into it. Then the dark web. Now the dark web-

S: This is the bottom of the iceberg.

A: This is the bottom. This is the dregs. But this is where all the dirty stuff is kept, all the secrets, but it's done anonymously. No one else knows what's going on. If you're in the dark web, very secure. It's done so it can't be found out. This is where they sell secrets. If you want to know where to make bombs, that's where you go hunting. If you wanna go and buy drugs, that's where you go. It's also where they keep the dark secrets about the passwords that they've taken. And this is where they sell them between each other.

S: Okay. Now before we started this only a few days ago, I sent you a list of all those people who had asked me if we could check their domains to see whether their information was available on the dark web. And you've given me a list of all those that were-

A: I did.

S: I think you said 60% had information available on the dark web?

A: Yes.

S: And that's all been ... Those are breaches within the last two years, aren't they, you said?

A: Of the breaches that have happened, 60% have happened in the last two years. We typically find that 70 to 80% of people, of businesses, have data that's been breached. That's typical. If the people that you've sent in from, it's a little bit lower than that overall-

S: That's good.

A: But that might be because of the size of the business. Normally one-man bands, two-man bands have less impact. The larger the organization, the higher the possibility and probability that passwords are gonna get breached.

S: Now, we've talked about this at some length. I felt a bit awkward about putting this file up publicly for everyone to download on our broadcast, on our stream so I'm actually gonna read through the websites that have suffered breaches. These are not everybody that asked. If I don't read your name out and you provided us with your website, then I'm pretty sure that we're not aware of any breaches.

But I'll read through these, and you'll be pleased to know that my own website, my own clinic website, was very close to the top of the list. But a new website is about to go live, and hopefully we'll protect that one a bit better. These are all .co.uk sites unless I say otherwise. So we've got Physic.co.uk. Top of the list, 16 breaches. Addington Palace, North Beds Osteos, then my own clinic, Ashgrove Health, Good Health Centre, Harrison Clinic, Camden Practice, Hunts Osteopaths, Caithness.org, carolynnorgate.com, pegasusclinics.com, Health Focus ... where are we? Irwin Osteopathy, mercyroadclinic.co.uk, Osteopaths Online, The Forge Clinic, The Osteopaths, dembones.biz, Fishponds Practice, getwelluk.com, Glasgow Osteopaths, jadepathway.com, jerseyosteopath.com, Kim Burnett, Penn Clinic, Retford Osteopaths. Sorry, this is gonna sound a bit tedious, but actually it's worth me running through these.

Solace Healthcare, StoneHouse Clinic, Walnut Grove Clinic, Working Bodies, Acupuncture South Devon, Alternative Therapy Northwest, Amber Osteopathy, Anipulation, Backworking, Barry Lonegan, Bodywise Osteopathy, Broadstairs Osteopath, buckinghamclinic.com, churchstreetpractice.com, Glos Clinic. That's the first page done. So if you're on there then you've got at least two breaches, all within the last year.

So the last page. Hale Health Clinic, Hands On Health Marlow, James Booth Osteopath. James, old friend of mine, you're way down the list from me, but

still two breaches. Lake View Osteopathy, Tilley, two breaches. Movement is Life, Osteopathy Derby, Osteopathy For All, Oxted Osteopathy, The Wellpark Clinic, Wakefield Osteopaths, York Clinic, Aching Back. We're down into the single figures now. So these are the ones who've only had one breach in the last two years. So that was Aching Back. Amber Care, BackACTIVE Chiropractic, Back Mechanic, Belmore Center, bodyflowosteo.com, Carlton Road Clinic, Cheyham Lodge, C-H-E-Y ham Lodge, Clapham Osteopath, Krista Galley, Dynamic Osteopathy, Gingerbread Clinic, Hamworthy Osteo, Jeremy James Osteopath, J Howton Osteopath, jointsolutionsuk.com, Kendal House Clinic, L-O-S-I-C, Losic.co.uk, My-Bones, NHC Newbury, Osteopathy In Action, Oxalis Osteopathy, Palmer's Clinic, Parkview Clinic, Pennington Osteopathy, QM Osteopathy, Rob Altrum, St. Andrews Osteopaths, The Luxton Clinic, The Old Bakery Dental, The Wellhead Practice, Wadsworth Osteopaths and wobernsandsclinic.co.uk. A long list. If you want to check with me afterwards to find out whether you were on that list or not, then by all means send us an email, and we'll confirm or deny it.

I haven't given away any secure information in that. Your websites are freely available to anybody who wants them. And anybody who wants to hack into your website will know where to look for that. And if they don't know where to look, they can't do it.

Turning to the significance of all that, Andrew, what does it mean? The fact that I have had, in my clinic, I've had seven breaches and Wobern Sands Clinic has had one breach. And theirs was on the 10th of March this year.

A: Basically, a password is out there associated with your email address. It could be, and quite a number of them may have been several years ago, when Dropbox got breached. If you were storing files in Dropbox, there was a breach that was made public, and those user names and passwords were sold. And those passwords were sold in the dark web.

S: Now that would have been presumably the password to get into Dropbox.

A: Correct. When you're breached, it's not necessarily your website that's being breached. It's your user name and your password has been. And that could be for any site. There was an example a short time ago with British Airways, where you were flying off and British Airways got breached. Now if you've been listening to the news about that, they're potentially gonna get a 500 million pound fine for it. In terms of that, they also had their user names and their passwords, so you would have signed in with Steven S, and put your password in. One of the conversations we were having before we started was how many passwords have you got Steven? And how many variants do you have on it?

S: When you gave the briefing that I listened to a couple of weeks ago, and I'm ashamed to admit this, all of our passwords were virtually the same format.

They were always the name of the company, one of the special characters, and then a word with the letters changed to numbers. The same word with letters changed to numbers. I'm guessing if someone's hacked one ... found that password, they probably scratched their head once and think, "Well, that's obviously the format for all his passwords."

A: Correct.

S: And they'd have been on to a winner. I've changed it since then.

A: And that's what they do. They take one password, and then they look at the variants of it. It's not someone sitting there thinking about it, actually they put a password into a spreadsheet and it automatically produces another thousand, 2,000 password variants. And then they go in there, and they brute force attack the accounts that they're after. It might be that you lost your password for Dropbox. It got breached and they got the password for that. But it's a variant. So they'll go to your Amazon account. They'll go to your Office 365 account. They'll go to your Google account. They'll try anywhere where there's a potential to either gain money directly or to gain data. In the industries that you're in, it's confidential client information they're after. The data's valuable.

S: It is sensitive personal data according to the GDPR, and therefore, we're required to treat it with greater, what's the word, greater care than normal data. What's a hacker gonna do with this 'cause it isn't always that they're just gonna use that information immediately, are they?

A: No.

S: There's a good story that came out of the briefing that I listened to about a three-month hack or something.

A: Yeah. It's a three-month hack, and this is quite common. This is very typical. They get access with a user name and password to the email account. So they sit ... They get your email account, they've sent a spurious email, it's not necessarily off the dark web, they've socially engineered you to give you the password. They then sit and watch your emails. They'll either sit in the account just watching or they forward every email on. The example that I've got, I've renamed this for good reason. Let's just call the setup as Dave and Sue. Dave and Sue run a 1.5 million turnover business. They employ 15 people. They are bright, switched on people.

S: We're not talking about your Nigerian uncle scams, are we? We're talking about people being much more sophisticated-

A: It's a very, very sophisticated business. I'll come back to you on the figures in a minute what it's costing the UK economy. These are very bright, switched on people that are doing it. So they socially engineered David to give them

the password to his Office account, his Office 365 account. And what they did, they sat there for about seven weeks watching and waiting.

And they were waiting for the time when they were due to pay a supplier. The supplier, let's call them Smith and Smith. Sara from Smith and Smith, someone they knew really, really well, sent an email saying partway through the chain I should say as the supplier was chasing the money, "We've had our bank account compromised. Would you mind paying the money that you owe us, reference invoice #X, which was about just over 20,000 pounds, into this bank account please." This bank account number at the same branch, but to a different bank account number. Sue, who runs accounts, had a conversation with David, and Sara had asked we get paid on the Monday morning. A little white lie.

Sue said we would pay it on the Monday, but Sue and David agreed that actually we'll pay it on Tuesday because of cash flow reasons, which we all suffer with. As Tuesday morning came, Sue went to pay the account. Couldn't pay it. Tried three times. She picks the phone up to Sara, that's Smith and Smith and says, "I'm really sorry Sara, it won't go through. The bank won't let me pay it to you." Sara then promptly says, "I know nothing about this. I've not asked for anything to be changed." What had actually happened was the hackers had been in it, they'd gained access, they'd learnt the language. They knew the relationship between Sue and Sara. Sara had been talking about Holidays, and Sue had been talking about hers and they'd interjected and played along. They'd signed off with Best Regards, as Sue always does. They learnt the language.

S: Was there anything that they could have spotted about this? If they'd looked at the actual email address behind Sara's name, would they have seen that it wasn't quite-

A: Not at all.

S: It was all identical.

A: It was all identical because they were in the system. They got in.

S: And it's not difficult to-

A: It's not difficult.

S: Steal someone's email address, is it?

A: It's not easy to spoof an email account either. And because they got into the email systems, they got in. This is very, very common. We've seen this. We've had one client lose 40,000 pounds for virtually the same thing.

S: And on this particular occasion, if I remember rightly, you said that when it was investigated by the police or whoever, they found that the account that they should have paid the money in had, had 85,000-

A: 85,000-

S: Paid into it, and had been closed that day, which is why they couldn't then pay money into the next day. So they were saved their 25 grand or whatever it was, but the hackers still got away with a lot of money.

A: They got away with 85,000 from seven other businesses.

S: And is not the scary thing about this if you have willingly paid money into an account, then you're not insured by anybody?

A: Correct.

S: 'Cause you did it deliberately.

A: Well, the banks, in terms of the figures, and this came from Staffordshire Police who we were with a couple of weeks ago, the UK police retrieve four percent of any money that's paid out on average. The banks return 20% if you're lucky. 80% of people lose everything. The only way around that is to make sure you protect with cyber insurance, which is part of one of the steps in my 16 step plan that every business should be dealing with to combat this issue.

S: Although I suspect that a lot of people might be watching this because they're worried about GDPR and protecting patients' confidential data, actually it's probably a bigger threat that someone is just trying to get money out of them, isn't it?

A: Yeah. To begin with, it's money. Lots of businesses think, "It's not gonna happen to me. We're too small. Who's gonna be bothered to target a business in Stoke-On-Trent, Northampton, Norton Canes. We're too small. No one's bothered with us." It's not true. Your money's as good as anybody else's. Your business, you're listed on company's house, you pay your tax, and you can be easily found.

S: Right. So there is a real risk there. And actually any of our businesses, if we were spoofed out of 10,000 quid, actually that could endanger our businesses completely because we're not dealing with high cash flow in our businesses generally. It's worth knowing. A question I had for you. If you aren't on the list that you produced of people that have been hacked, does that mean you're perfectly safe?

A: You're safe today.

S: Right. So there's nothing out on the dark web about any of these businesses?

A: Not today. But that's only what's on the dark web. Again, government statistics from the National Crime Services, N-C-S-C, which is government funded. It's the National Cyber Security Center, 43% of all businesses in the UK were breached in 2018.

S: 43?

A: 43%. The police officer-

S: Does that mean something nasty happened or just that a password was available?

A: No. It's something nasty. Passwords have been hacked. Information's been lost. There's some serious amount of information gone or money, and the police are telling us that 43% has happened in the last year. They're saying that one out of every two businesses virtually has been compromised in some form or fashion. They're extremely concerned about it. The police nationwide are trying to communicate with the businesses in the United Kingdom to make them aware.

S: Now, with all these people on here who do have breaches against their names over the last two years, I guess they need to do something today, don't they? Because there is a password out there, which may or may not be current, but there is a password out there which someone on the dark web could buy if they wanted to get into these businesses. We'll talk about what they should do in a minute. How do the hackers actually work? Why can't I just go into the dark web and see this stuff?

A: It's very difficult. From a technical perspective, you have to have certain browsers installed. You have to have BitCoins. You don't buy things with cash. You have BitCoins. It's a very dark and complex place that you lift the cover up and you wanna put it straight back down. Let me just say this. If you're determined, anybody can do anything. If you want to go into the dark web, then you can. It just takes time and effort.

S: Well, I must admit I Googled how to do it the other day. I didn't get very far.

A: It's not fun.

S: I don't pretend to be a ... I'm computer literate, but I'm not a computer expert by any means.

A: This is a business. At the end of the day, it's another marketing tool. But this is a marketing tool for big crimes. In the UK, it's estimated ... again, these are government statistics ... It's anywhere between 11.9 billion pounds and 195 billion pounds to cost the UK. People are earning big money out of it.

People sit in a big boardroom, they come in and all sit around in a room and say, "Fine. Who we gonna target this week? Let's pick on Stoke-On-Trent, that's where we come from and now pick a business park and now look at the hundred businesses on that business park," and within 15 minutes, they've got the name of every company, they've got the domain, they know the managing director, they know his date of birth or her date of birth and now go and do some searches on social media. I'll get to know them. And then from that, they'll then start an attack very much like we'll do a marketing campaign.

S: So this isn't just spotty teenagers in their bedroom-

A: No. It's definitely not.

This is not that anymore. That used to be the case. Go back five, 10 years, that was the case. But now it's big crime.

In terms of crime statistics, 50% of all crime in the UK is now cyber crime. In terms of threats to the nation, and this is threat levels, at the very top is terrorism, number two, cyber crime. Because cyber crime can take businesses down. We've seen examples of this. Only recently, there was the one in Croatia with the NHS. We had people that were at a seminar, and they said that on the day that the WannaCry kicked in, there were people in there that had accidents that were in the ambulances and normally the ambulances can check to see what medication is required. None of that was available. They were given medicines to patients not knowing what they were allergic to. Cyber crime is a significant threat, and it can't be ignored any more.

S: Just in terms of the scale of the threat to businesses like the ones on my list here, they won't all be one-man bands. But some of them are. They're likely to be, four or five-person clinics, so their turnover is going to be well short of the million pounds a year that you spoke about earlier on. Do you think that makes them less of a target?

A: No. Makes them more of a target.

S: Simply because they're likely to be less savvy?

A: They're less savvy, less protected, less secure. If they attack ... If you've got 100 people to attack, if you only got 2,000 pounds out of two or three people, how long's it take you to earn 2,000 pounds? A typical ... For a small business it's not unusual to pay a bill for 2,000, 3,000, 4,000 pounds, is it? But it's also the data's that for sale. How much is that data worth? Because they can not only just con, take the money out of the business. If you've got access to 200 or 300 clients that work for XYZ Osteopath, then we've all had those calls from Microsoft. "Sorry to tell you sir, you've got a problem on your computer. Can we get on? Can we fix it?" And then charge you for it. Well,

they can do the same again. There's always something they can sell. There's always some way to extract money.

S: I suppose in theory also there's the opportunity for a ransomware thing, isn't there?

A: Absolutely.

S: I've got access to all your database. If you don't wanna have a security breach, then how much are you gonna cough up? Your presentation's very timely because a company called Rushcliff.com had a problem with the whole of their patient database recently. They provide online clinic diaries and clinic notes for a huge number of osteopaths, chiropractors and others. For a period of about two weeks, my business and a lot of others lost access to their whole diaries. So we couldn't tell who was coming in. We had no access to the notes of people who had been in. We couldn't put new patients in because we didn't what was in the diary because we couldn't access it. Rushcliff are claiming that they were hacked. I suspect that's so they can get out of having to pay any compensation for something which might well have been a software update problem. We'll be looking into that once the whole problem's resolved.

A: It's a very poor excuse. You have to prepare. We talk a lot about preparation. You plan, you prepare, you predict that it's going to happen, and you have plans in place for if it does. Looking at that-

S: There are some computer experts who have, also practitioners, who have been using them and saying, "Well, actually they should have had these procedures in place and they didn't-

A: Yes.

S: And those procedures should have been sufficiently protected from the main site that they could have been backed up straight away.

A: Correct.

S: Enough on that. Did you have stuff that you wanted to tell us specifically? There was a video you wanted to show-

A: Yeah. There's a video ... There's a couple of videos. There's a good video that just identifies why they want to attack. So I'm just gonna skim through it.

S: Yeah, please do.

A: To just get to the point where it shows, but this is a very good British one that was made by the police. I've got a few in so it's not that one?

S: That one we might make available to people-

A: Yeah, that one. The email that ruined Christmas.

Video: Hello. I'm sending you an email impersonating your boss. I want you to make a payment. Quite a significant one. I'm not really your boss, but I do know a lot about him and you. Thanks to his out of office and his social media, I know he's on Holiday. Thanks for the info Martin.

You, you're in Finance. Busy. You're inbox is probably full of unopened messages. That's why you'll only scan the email from Martin. You won't notice that the email address isn't quite right. Oh, and don't try to phone him for confirmation. Martin is about to spend the morning in the spa. Do not disturb.

That's what I rely on, see? Busy people. People under too much pressure to notice such an odd request. I'll even send you another email in about 30 minutes just to check it's been done. More pressure. You could check with someone, but I bet you won't because your boss wants it done now. Chop, chop. Twenty-five grand though. Seems a lot to ask for. But I know your company's big enough to make payments this size, but also small enough not to have safety procedures getting in the way. You hate red tape.

It stops me getting what I want. And what I want is your money. You have the power to stop me, but will you?

S: Okay, we're back in the room.

A: Absolutely.

S: It's a fairly powerful video, isn't it?

A: Very powerful. And we see this happen. They do sit. They do wait. They do know when the boss goes away on Holiday. We had a good example only a couple of weeks ago. 13,000 pounds got directed out to a business' account using exactly that scam. The money's come back by the way, but-

S: How does that work then? How do they know the boss is away on Holiday?

A: Again, they're sitting there watching the emails. The out of office message. They're concerned about what you're doing there, looking at your social media. If you're into your social media, I'm going to Holiday next week.

S: But also people are quite keen on many occasions to have an auto respond which says, I'm out of the office until blah, blah, blah 'cause I'm on Holiday or whatever. If you've got any questions, talk to so-and-so. That's a nice indicator to somebody that maybe they can use your email address freely 'cause you're not gonna see the results.

A: Absolutely. And as we said in the video, the smaller the business, the less chance there is a procedure in place. These are the things that you have to build into the business. There are some rather gruff managing directors that don't want to be disturbed, but actually they will want to be disturbed if they think 40,000 pounds going out of their bank account. But they've gotta have a procedure in place, and a policy, and these are the things that you have to think about. It has to start at the top. It's all very well and good with someone lower down the chain putting this in.

S: All that being said, what do we do to make this easy enough for people to do something which is going to protect their businesses without it becoming such a nightmare that you need a dedicated cyber security officer?

A: You don't need to have someone that dedicated, but you do have to put time into it. You have to think about it. You've gotta put time aside and there are certain things that I am recommending that you do. There is a 16 point step that I'm talking about. I'm just gonna get to it.

Predict and plan. Have a security policy. Actually, there are plenty of security policies out there. You can download them off the web. I'm sure I can make one available for you to peruse. But this is where you actually go through and think about the business, and you spend the time at it. Probably gonna take you a couple of hours. Ideally, you do it with an IT specialist. Don't have to, but if you're unsure what the terminology means, it's well worth the time and effort of getting an IT specialist in to talk it through. It discusses what you're doing and how to react. What happens when? It's not what happens if ... what happens when. And these things you gotta plan for. So you gotta plan for it.

You know which member of the team is gonna do what. What happens if you have got a data breach? Who do you notify? Those type of things.

S: How would you know you have a data breach then?

A: Some you do, some you don't. The classical one is you start getting lots of emails from your clients saying, "I don't know where this email's from. We've not gotten any invoices out with you." Typically, that's a data breach. Someone has gained access to your email system, taken all your contacts, and now they're emailing all your contacts, or potentially your clients. And again, those are the type of things that you have to be aware of. You do need a plan in place if requests are made to change bank payments or to create new accounts. It shouldn't just be accepted via email or from a telephone call even from somebody you've not met before or discussed. So you gotta have a plan.

Education, education, education. You need to educate your staff. You need to educate yourself. You don't know what you don't know. You need to again,

either talk to somebody who understands it and understands the implications, but keep the training constant. It's gotta be at the top of your brain. We've all learned to drive at some point. It's not until you actually do it do you start to learn and you have to ... It's only if you do more and more do you actually learn and become more and more aware. Do you remember when you first started to drive? And you had that driving instructor next to you that was guiding you and making sure you didn't make any mistakes. That's where it starts. You really start to learn when you're on your own. But you have to keep on going. There's plenty of things. Again, talk to your cyber specialists or your IT companies. You can be offered constant training at normally a very sensible price.

S: But is it enough to have antivirus software and malware, anti malware stuff-

A: They're pretty essential. They're part way. Then a little bit further on, you've got to have those-

S: Even on a Mac, 'cause Macs are always said to be-

A: Even on Mac. It's a complete fallacy that Macs are safe. They're as prone as anything else. Apple iPhones can be hacked as much as Android phone. Macs are just as liable for attack. It's just about numbers. 98% of businesses use PCs. Two percent use Macs. But, you have a highly target marketplace, normally you've got a high net worth so normally you're quite nice people to breach. You do need antivirus, you do need anti malware. You need to look after your data on bring-your-own devices, so if in a practice of four or five people and you've given your staff access to emails and data on their mobile devices, you've gotta have a policy in place to protect that device. What about protecting the data on that device? You need to think about these things. Again, it becomes part of your security review, but you definitely need a bring-your-own device policy, BYOD device policy so you need to be aware of that.

Sorry, I keep looking down. Change your passwords. Please. Change them regularly. Under GDPR, you have a requirement to change your passwords every 90 days. But keep them changed and make them complex. Again, if you follow the National Cyber Security strategy, pick three random words. Doesn't matter. Pink. Brick. Wall. Whatever, as long as they're long words. You wanna be over 12 characters and ideally if you can put some special characters in, great. But please don't just substitute an O for a zero. They're clever than that. You can do some substitutions. You might use a dollar sign, but don't use it for an S, use it for an N or a P or T. You can keep that in your head, but it's the length that's critical.

S: I can't remember if it was you that was telling me that with complicated passwords, and these were passwords which didn't have any special

characters in them, I think if you had 15 letters or something, it's gonna take 150 years for an automatic process to hack through that. Is that-

A: Yeah, I think it's actually a bit longer than that.

S: So that's at a rate of something like God knows how many per minute as well. 'Cause there are so many permutations and assuming it's not one of the middle permutations that it comes across.

A: I think if by the time you get up to 17 or 18, you're talking trillions of years to break them because there's that many permutations. So the longer your password, the better. But don't go for obvious stuff but use just random words.

S: But isn't it the case that most sites, if you've had three attempts, then they stop you having any more or impose a delay because that way your automatic system is trying do 200 hacks a minute.

A: Some sites do. Some sites don't. Quite a lot don't. You can change that on your systems. If you use Google or Office 365, you can actually set it to reject after a set period of time. If you've had five attempts in the last two hours and failed, then lock the site for two or three hours. Especially on websites that hold critical data. If you're using WordPress or anything like that, talk to the website designers about how to lock passwords. If you've got websites where your patients or your staff can access data, get that locked down. Seriously, change your passwords on a regular basis and do your damnedest to not remember them, but we'll come up to that a little bit later on.

S: I suspect also that one of the problems is for example, in my own practice we've got four or five receptionists who only access to the main computer, so therefore, they all know what the password is. Bless their little cotton socks, I suspect they're not terribly keen on trying to remember passwords, so I'll bet it's written down somewhere.

A: Absolutely. You're saying if you've got four or five different people accessing data, ideally you want to each user to have their own unique user name or password. So change the systems to make it. What you want is security by design. Don't share passwords ever. There's no reason in a business structure that you need to share the password with anybody. As a managing director of the business, you can have access to all the data, but normally through some other format. But on a regular basis, you don't want to have that.

S: So what's this gobbledygook here?

A: Gobbledygook.

S: Coming up here.

A: Encrypt your data. So make sure your hard drive's encrypted. For example, if I walk into most of your osteopaths and chiropractors, their data's stored on a hard drive in their computer. Now we just got a user name and a password to get into the computer. I don't care about that 'cause what I can, as an IT expert, and I can literally take the hard drive out, put it into the computer, extract all the data.

S: Really?

A: Yes, absolutely.

S: So it's not the hard drive that's protected by the password then?

A: No. It's just a simple entry. You get into the computer and then you get in. But most businesses, the data's there for the taking. If I can get access to the hard drive, I've got the data unless it's encrypted. Encrypt the hard drive. In Windows 10 Professional, you turn on BitLocker. It's free. Doesn't cost you anything. And that encrypts the hard drive. If I extract that hard drive, put it into my computer, all I see is rubbish. It's pure gobbledygook.

S: So Windows 10 BitLocker and for Macs?

A: There is a product. I'm not an expert on Macs, but it's in the new version. It's there.

S: Okay. I'll find out. We'll make sure that's-

A: That's fine. The next one's emails. When you send an email, it's unencrypted basically if you sat in a public area, you don't have to be in a public area, you can do it from anywhere in the world, the emails you transmit and all the attachments are unencrypted. If you've got an Excel spreadsheet with all your clients in them, and you email that to somebody else, a hacker can intercept that email, extract all the data.

S: Surely, encryption can only work if the person at the other end's got the key.

A: Depends how it works. If you're in Office 365 for example, I can send you an encrypted email, so I have to pay for that function, turn on encryption, but you at the other end don't need to pay anything. The issue is that when I send an encrypted email to somebody that's not in the Office platform, it will tell you that you've got a link to an encrypted email. What do I always tell people about opening emails with links? Don't do it.

S: Don't do it.

A: You have to notify people that you're sending an encrypted email. But it's a way of sending secure data. Even if that email gets intercepted, no one's got access to it.

S: Good advice for transmitting patient data given that we have to protect that sensitive data.

A: Talk to your IT companies.

S: It's not essential under GDPR to encrypt emails?

A: No, it's not. Only for sensitive data. Sensitive data, remember-

S: It's patient data.

A: Yep. Includes anything to do with children. If it's got anything to do with children, it should be encrypted. Also, sexuality and stuff like that from a health perspective.

S: We've only got a few minutes left. We better crack on these.

A: That's fine. We'll crack on. We'll be very quick. Patch and update. Make sure machines are updated. Security issues, people getting through unencrypted data. Have antivirus. Get an antivirus and pay for it. What you get for free in this life, nothing. Have a hardware firewall. Basically it's a device that sits in front of your router and stops the data from being breached, and it can look for data going out as well as coming in.

Do your damnedest to forget your passwords. Ideally you should only have two passwords. One password that you remember. The password to get into your password manager. Something like Dashlane or LastPass, 30, 40 pounds a year, and literally every single password that you've got, you can keep.

S: Now, we're pushing up against the clocks here. We've only got five minutes left. But this is what we did after I saw Andrew's briefing a week or so ago. We stripped all our passwords out. We put them into LastPass, L-A-S-T-P-A-S-S.com I think it is.

A: Yes, I think it is.

S: And so I have to remember the one password to get into LastPass. Once that's active on the computer, it will auto fill my passwords for me. I have one password to get into my computer. Those are the two different passwords that I have to remember, but I also have to remember to tell my computer to stop remembering passwords.

A: Correct.

S: Otherwise anyone who gets into it goes into Safarians or whatever the browser is and says, "Show us the history of all these passwords," and you've got them all.

A: I've got a quick video that shows you how quick I can get a password off your system. If you look at this, this is for Ebuyer. It's got my email address, and it's got a password there that's all starred out. If I click that, it should then play hopefully. Oh, no, I've gone too far. But basically your right mouse button of where the password is, and we'll share this a bit later on. Click inspect. You then go to the right-hand side and you change the word 'passwords' to the word, 'word' and instantaneously the password appears where the stars are.

S: My God.

A: It's very quick. It's a two-second job for me to reveal that password that's behind there. When you've saved your passwords in Chrome or Firefox or whatever you're using, I can get at it really quickly. And this is what cyber criminals are doing.

The next thing is no phone or key, you can't access the internet. You can't access your information. What I would strongly recommend on your LastPass is that you use two factual authentications-

S: I am.

A: Perfect. So every time you need to access that site, it asks you to look at your mobile phone for a security code.

S: We just had a question about authenticators. The app that I use is called Authenticator I think, and I use it for our accounting package and for LastPass, and I'll use it for anything else that it will. It's a slight embuggerance 'cause I will look at my phone, but I suddenly realized I've got to be embuggered occasionally because otherwise-

A: You have. It's a slight encumbrance. There's Google. There's Microsoft and there's some others out there. Trust either Google or Microsoft unless you're dictated to otherwise.

S: This question says what about authenticators? Are they any use? And password apps that store all your passwords with one password lock, which I think we just covered with LastPass.

A: Exactly.

S: I think they're good. I'm getting it from you, I'm getting the sense that they're good provided they don't open automatically when you go into the computer-

A: Correct.

S: Because as soon as you go into the computer obviously-

A: You don't want them to open automatically 'cause if someone has compromised your machine, they've got access to all your passwords.

S: Everything, yeah.

A: So you must have it so it comes on, and every day you have to sign in with your two factual authentication.

Next thing, we were talking about the websites earlier on. Make sure you have a backup. Just because it's in the Cloud doesn't mean it's backed up. Office 365 is not backed up. Dropbox isn't backed up. Google isn't backed up. They hold data for a certain period of time. It's not backed up. You have to pay for a backup solution. It's low cost. Typically, a couple of pounds a month will back up each user account. But make sure your data's backed up. Again, you're not experts. Talk to an expert. Pay the money. It's well worth it.

Don't forget your desktops. Don't forget your My Documents. It's really important and crucially, you've gotta work on the basis that they have got through. They have breached your system because the probabilities are quite high that they're going to.

You do now need to have and pay for cyber insurance. This gives you many, many things. It covers the money that you've lost, which does help. But it's not just the money. If you've been extorted, instant responses, legal costs because you may have to pay someone to fix this, to get it fixed, but you may also be sued by ... What happens if your clients sue you for loss of data? It protects you against that. Currently, cyber insurance will pay any legal fees that you may be charged by fines from the ICO, et cetera. Really critical you talk to your insurance agents and talk about cyber insurance. It's a necessity nowadays. You wouldn't dream of not having insurance on your house. You've got public liability insurance. When was the last time you claimed on it? There's a much higher probability you're gonna claim on your cyber insurance than you're ever gonna claim on your public liability insurance.

S: That's not to say you should change from one to the other-

A: No.

S: Because obviously you're required by law to have the public liability insurance.

A: You are. What I foresee is that cyber insurance will become the same. And I do foresee that your general insurance will force you to have cyber insurance.

S: We've got a minute before we're gonna lose a lot of our audience 'cause they've got patients at 2:00.

A: Who has your passwords? We're talking about the dark web. We talked about that earlier on. So I'm gonna skip that.

Who's looking over your shoulder? Who is in your email systems? Again, there are functions, there are features that we can do and other people can do to look at that.

If you're using desk-based solutions, desk-based servers to store your data, I strongly advise you move to the Cloud. Get your data into the Cloud. Way more secure than you can ever spend. Microsoft will spend 20 billion dollars a year on their systems. How does that compare to what you're spending on yours?

S: It's a bit more than we do in my clinic.

A: Yeah, just a little. And then finally, get Cyber Essentials certified. We work with dental practices, and all the dental practices have a requirement in the next two years to become Cyber Essentials certified.

S: Cyber Essentials.

A: Cyber Essentials. It's a government standard that makes sure your business has got the right security levels. It's gonna cost you a little bit of money, but it will help reduce your cyber issuance costs as well. But it's a good policy, it's a good mechanism to make sure your business is secure.

S: When I booted this presentation to Andrew, Nancy said, "Ooh 45 minutes, isn't that a bit long?" And here we are. We've had to rush to get it in, in the 45 minutes. We are not selling Prompt PC as the solution to all your problems or your cybersecurity issues. But I listened to Andrew's presentation a few weeks ago and was very impressed with that. If you want to get in touch with him, then his details have been on the presentation that we've shown you. You can Google Prompt PC, and we'll put his contact details on the website.

If you were one of the websites that's got a breach, that's had a breach and you have a question about it, what was breached, when was it breached, how many times were you breached, then Andrew will answer that question for you. But it costs him money to do the research so yeah, you'll have to pay to get that information. I'm sorry to say that, but it’s only fair. If you need any advice about PCs, then find someone like Andrew, if not Andrew, to do that for you because I thought I was pretty savvy on all this stuff until I listened to your presentation. And even today, having done all the things I have, I still realize there's a whole lot of stuff that I've got to do to protect me, my bank account, my business bank account and that sensitive personal data that we've got on our systems. And I'm sorry if this is a scary broadcast, and it just puts another worry in your mind while you're still trying to make a living out of your business, but it's something that we just can't afford to ignore.

Andrew, it's been great having you here. Thank you for coming in.

A: It's a pleasure.

S: And I apologize that we've run over for a couple of minutes. I hope it's been useful to you. Send me any questions you've got. I'll put them to Andrew, and I'm sure he'd be delighted to answer them.