Spoke media.

KELLY: Hey Bob.

BOB: Hey Kelly.

KELLY: So it's just you and me today because when Alia is not here, we do a minisode. Bob, can you tell us what a minisode is?

BOB: Sure. Listeners send us questions all the time through our email, SoBob@spokemedia.io or over Twitter @SoBobPod, and in the minisode we're going to take one question and do a deep dive and try to explain it in a way that gives you really practical advice so you can be a little safer, uh feel a little less anxious or just not as annoyed by technology.

KELLY: Okay. So here's our question, and it's actually from a listener of Bob and Alia's other podcast, Breach, which you should go check out if you haven't.

LISTENER: Hi folks. Loving the podcast. Wondering if you'd look at the security that password protection service companies like LastPass and Dashlane, etc., use, why are they safe or not?

KELLY: So Bob, do you think you can help us figure out this whole password situation?

BOB: I can definitely help with the password situation.

KELLY: Awesome. Well, we'll figure it out after the break.

[BREAK.]

BOB: Nothing is completely safe. The security at these password management companies isn't bulletproof. No, nothing's a hundred percent secure. So I want to change the question just slightly from are password managers safe, to are password managers safer than what you're doing right now. And for most people, yes is the answer. They probably are. But there's a lot of things to consider with password managers. For those who don't know what password managers are, is they substitute this crazy life that most people live where they have to remember dozens...actually, I saw a study not long ago that said the average person has more than a hundred passwords they have to remember. So that's crazy. Right? And of course you're supposed to use complex characters and letters and numbers and all that and no one does that because it's impossible.

BOB: So you do the the worst thing possible, which is reuse the same password over and over. So password managers give you a single password to rule them all for a piece of software that you purchase. And then that piece of software stores a bunch of passwords that are safer and it uses them when you have to use your online banking or open an app or use Facebook or any of

those tools. So in principle that's a good idea, but I think impulsively many people are horrified at the notion of putting one password on all of these things because of course what happens if the password manager gets compromised. Now the security itself that the password manager software uses is pretty good, although I can tell you that security experts have tried to hack into it and they have found some vulnerabilities in it. So again, it's not a hundred percent safe. So the security is pretty good. However, there are all these other weak points, one of them being you need to have a password to unlock the password manager. Any discussion like this is really a discussion about what's a good password? Kelly, what do you know about what a good passport is?

KELLY: So what I know about a good password is that, uh, it's supposed to be a string of random words that aren't connected to each other and spaces are really good. Um, and actually putting like random characters and numbers in like a lot of uh, websites make you do actually isn't as safe because it's like giving hackers a template for what your password must include. Is that right?

BOB: Oh, that's all correct. Yeah. That the old rules about passwords when something like this, first of all, use a mixture of upper case letters and lowercase letters, use special characters, use numbers and change them frequently. In fact, a lot of websites force you to do those kinds of things. Those all provide people with a false sense of security. And in fact, uh, there's general consensus now that forcing people to change their passwords on a regular basis, like every 30 days is a terrible idea because that just encourages you to use these conventions.
Like Kelly's password 1, one Kelly's password 2, Kelly's password 3, so that you have 12 months worth’s of passwords to get into your system. The organization in the United States, Uncle Sam that gives out advice for standards, NIST, actually last year published a brand new paper suggesting what the best techniques are for passwords.

KELLY: NIST stands for the National Institute of Standards and Technology. They set standards across all sorts of industries so we can count on products from different companies working together. Basic things like what precisely is a kilogram or how long is a second to more complex things like what's a good password.

BOB: What we've come up with is long pass phrases, random words, put together, kind of like word salad, that wouldn't make sense to anyone are actually the safest thing.

KELLY: So what if we forget our LastPass password or any other password manager main password.

BOB: Yeah. This is a really big risk with password managers. What is the recovery mechanism? And in some cases there is no recovery mechanism. There's no way to get your password back. The tools are designed such that no one can just call and say hi, I'm Kelly. I know I don't sound like Kelly, but I am Kelly and I forgot my password manager password. Would you give it to me? And that's for obvious security reasons, right? So that's again, that's a policy that makes sense

when you're talking about something that's this secure. But there are other problems too, like a, a virus that actually logs your keystrokes on your computer. So maybe a bad guy could essentially virtually look over your shoulder and see what happens when you type your password into the password manager. And then again, that hacker could get into your entire digital life. So there are scary things about these password managers, but again, the most important thing is not are these safe, but are they safer than what you're doing right now?

BOB: And if they are, you should look into them.

KELLY: Okay. So the thing is, is being so young when I use the Internet, was that there's probably so many things that I used a password for, like an old YouTube account or you know what? Probably an old Yahoo account that I made that I didn't need to make. You know what I mean? That I've used a random password for and when I was a kid, just use the same one over and over again.

BOB: So one really important concept with passwords is that they live forever. And there are these big databases in the sky of hacked passwords, billions of them that have been stolen through the years dating all the way back to like the MySpace hack and the LinkedIn hack. And of course the Yahoo Hack we've talked so much about. So bad guys have put all these in a big computer database and the, and the reason that reusing passwords is so bad is that when, when they sit down to hack into your account, they do what are called credential stuffing attacks.
And that means they just start running tens of thousands of maybe millions of passwords through a website to try to find one that matches. And so there are now billions of passwords that are no longer safe because they're out in the wild in these databases that hackers have. I was at an art exhibit in New York City a couple of years ago. It was actually put on about privacy. It was a great exhibit, really clever. Um, in order to attract people from the outside, they had a big LCD TV screen on the front window and they were sucking data out of people's smart phones as they walked by. You probably don't know this but your smartphone is constantly doing things like looking for wifi networks. And in order to do that, it has to broadcast some information about itself. And so if you walked by the storefront of this art exhibit, you would probably see something from your smart phone pop up on the screen. So that was unnerving. And that got people inside. Once inside they had all sorts of clever exhibits. But the one that caught my eye were these massive volumes sitting on a desk, it looked like a huge Encyclopedia Britannica. Inside were nothing but a list of the passwords stolen from the LinkedIn hack. And it was amazing because what you would see is people would walk up to these books, and the passwords were listed alphabetized. So you could start scanning through the pages and one by one people would go, oh my God, oh no. And of course run home to change their passwords because they would see in black and white, their password listed in this book. And that was a useful experiment to see how compromised your life might be. But I also think viscerally to you know, just to see this massive volume of compromised data, you know, really, really drove the point home.

Many of these passwords were things that people set when they were, you know, 13 years old and the first time they used MySpace, and your human tendency to set passwords is to use patterns. Our brains like patterns, we can't avoid them. So maybe you started using ex-girlfriend's names when you were a teenager or you started using parts of your address or a nickname you had or a pet's name obviously. And you know, you're smart enough to change it somehow, but you use a root of something that you can remember as part of your password. When hackers are using some kind of system to break into a password, it's very hard for them to break into something that's 12 random characters long. But if they can even eliminate some of the potential variables, mathematically that makes their task much, much easier. That's why you should never put your pet's name on social media unless you never ever even think of using a pet as part of your password. Because if someone can say, start with, you know, four of the 12 characters in your password, well their job is infinitely easier when it comes to hacking into your password.

KELLY: And those like little games that I would see on Facebook that was like the name of your hometown street and your dog, uh, and combine that with your dog's name and you'll get your like spirit name or whatever.

BOB: Right, right.

KELLY: And so everyone would post their like fun little name. And then I was like, I was thinking about this last night, I was like, oh my gosh, wait that, that you could just get someone's password through that or like a part of someone's password through that so easily.

BOB: Yeah, 100% to me. I mean that, that's it. That's a really common technique. The sort of social media backgrounding of someone if, if you want to target them. And also by the way, you know the other speed bump and it's not a very good speed bump into hacking into people's sites is often these questions like, well, we started with, what's your mother's maiden name? And then we moved into what your high school mascot's name, that kind of thing. So many of those questions, you know, those out of wallet questions. So many of them can be answered by social media. You know, how hard is it to figure out what your high school mascot was if I go to your social media page. So when you pick that one password to rule them all, you know this is the challenge. You have to pick something that you'll remember but nobody else can guess.
And ironically enough, Bruce Schneider is probably considered, he's the rock star of computer security. He's been around for a long time writing about all these things. He has a great website at schneider.com and one of the pieces of password advice that he's given out for years, believe it or not, is to pick a very, very complex password and write it down and put it on a piece of paper in your wallet next to your driver's license, which obviously doesn't sound safe, if someone stole your license, they would have your password. But again, this is a matter of managing risk and that technique is far safer than using a simple, easy to remember password. And I want to just add one thing about that, that big database in the sky of hacked passwords that criminals use. Within the last couple of years, companies have started to use that database for good. And I like this. They'll tell you when you log in that you're using a password that's

known to be compromised in the world and suggest that you change it. And there's even now an extension for Google Chrome that I quite like that watches as you go to all the sites you go to and pops up and says, Hey, the password that you entered onto the site, we know this is a bad password. So you know really you should change it. And I think that's a good idea. Knowing that you're using a password that hackers have in a big database, well obviously that's, that's the riskiest thing of all that you can do on the Internet, and you should change that.

KELLY: So Bob, what's the TLDR on password protection?

BOB: Well, the first and most important point is don't ask if password managers are safe, ask if they are safer than what you're doing right now. Be Honest. If you reuse passwords, if you have one or two passwords that you use everywhere, then that's a terrible idea. And using a password manager is an upgrade on your personal security. So you should definitely consider it. But if you are thinking that you're going to use a password manager and that's just going to be easy and you don't have to worry about anything ever again, that's a bad idea because security is not a one and done thing. It's it's an ongoing effort. So even using a tool like a password manager, you have to be ready to stay on top of it on a regular basis. I do also think, I mean if you're listening to this episode and you've even considered a password manager, then great. That means you care about your security and I'm very excited about that. At a bare minimum right now, do a little mental audit. Identify the things that are most important to you and would be most important to a hacker like your bank account, like your brokerage account, your work account, and one that people forget: their Gmail. Gmail is used as a backup account for almost everything. So your Gmail account is probably just as important as anything else in your life. It almost acts like a password manager for many people, but do a little audit and make sure at least at those sites you have really, really difficult challenging passwords. Like these pass phrases we have discussed. Go to these sites, update your passwords from four years ago when you never did and make it something stronger.

KELLY: If bad passwords were Sabrina Spellman messing up all of her spells and causing general witchy mayhem, then Bob Sullivan is Aunties Hilda and Zelda swooping in to give all of those words of wisdom. Thanks Bob. Next week, Alia and Bob talk about attention or lack thereof. Is technology making our attention spans worse? You don't want to miss it. If you have questions about your digital life, write to us or send us a voice memo at sobob@spokemedia.io or a DM on Twitter or Instagram @sobobpod, you may be featured on our next minisode. So Bob is a Spoke Media production. It's hosted by Alia Tavakolian and Bob Sullivan. It's produced by me, Kelly Kolff, with help from Reyes Mendoza and Carson McCain. This episode was mixed by Will Short. The songs you hear in this episode come from FirstCom. Our executive producer is Keith Reynolds. Thanks for listening.