06.04.19

26 MALICIOUS BREWS—EPISODE TRANSCRIPT

- **GEOFF SISKIND:**

  It's daytime and two people are gazing into a shop window when they suddenly spot an absolutely stunning-looking, high-end coffee maker. It's truly a thing of beauty; shiny red with bright chrome accents. Looks like the kind of machine you'd find in a fancy Italian coffee shop. One of the onlookers is intrigued, and he goes in for a closer look.

- **GEOFF SISKIND:**

  But, just as he does, something unexpected happens: The coffee machine springs to life. Four legs emerge from out of the bottom of it, and then it hops off its display case, and crashes through the store window, and out on the sidewalk. The two people watching are stunned, and that's when they realize that, not only does the coffee maker seem to be alive, but it's coming for them, and it looks angry.

- **GEOFF SISKIND:**

  That ridiculous scene was from the 2009 animated feature film, G-Force, and the people I was describing in that scene weren't actually people at all; they were guinea pigs who were also secret agents. And I can't really tell you much more than that, because, truth be told, I didn't make it through the whole movie.

- **GEOFF SISKIND:**

  But why we're talking about that scene on Hackable? today, and I admit this might be a bit of a stretch, we wanna tease out the idea that coffee makers can actually be dangerous, and not just because they deal with hot liquid that can burn you, but because now they can also be hacked. Because, like a bazillion other things found in our homes today, even our coffee makers are now smart.

- **GEOFF SISKIND:**

  And that's what we're doing today on the podcast: We're hacking coffee makers as well as tea kettles. Two smart devices, pitted against each other in order to see which device is more hackable. Coffee versus tea: Who will win? Welcome to Hackable? - an original podcast from McAfee.

- **INTRO THEME:**

  This computer is on the job around the clock in case of attack. Their principle target is you. The design is complete, but will it work? Shake hands with danger.

- **GEOFF SISKIND:**

  I'm Geoff Siskind, and I'm here, as always, with Bruce "The Hammer" Snell. How are you, Bruce?

- **BRUCE SNELL:**

  (laughs) Good. How are you, Geoff?

- **GEOFF SISKIND:**

  I should also mention, because I'm now so obsessed with just giving you a nickname every time, you're also-

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  ... a cybersecurity expert.

- **BRUCE SNELL:**

  That's true. (laughs)

- **GEOFF SISKIND:**

  (laughs) Which is the real reason you're on the show. Not just for your- your- your hammer-like intellect, I don't know, but, um ... (laughs)

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  In just a few minutes, Bruce, uh-

- **BRUCE SNELL:**

  Blunt and forceful.

- **GEOFF SISKIND:**

  Exactly. In just a few minutes, we are gonna try something never before tried on live podcasting anywhere.

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  Which may or may not be true. But at least it’s...

- **BRUCE SNELL:**

  I mean, are we- are we- are we live, though?

- **GEOFF SISKIND:**

  ... Ish?

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  Here's the point: I'm gonna make a lot of claims that may not be true, but what I do know is that this podcast-

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  It has never been tried before on Hackable? before. We are gonna hack not one, but two devices at the same time.

- **BRUCE SNELL:**

  I'm on the edge of my seat.

- **GEOFF SISKIND:**

  I can tell. And- and so basically, what I have, the setup I have is downstairs in my home. I have two devices.

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  I have the smart kettle and a smart coffee maker.

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  Both are ready to go. It's coffee versus tea: the ultimate showdown, and we are gonna have one hacker hack one-

- **BRUCE SNELL:**

Uh-huh?

- **GEOFF SISKIND:**

  ... one hacker hack the other to see who will reign supreme.

- **BRUCE SNELL:**

  That's fantastic. I- I think it probably is the first time that's been done on a podcast. I think- I don't think that's an outrageous claim.

- **GEOFF SISKIND:**

  And I think it's not ju- I think it's the first time not just it's been on a podcast, (laughs) the first time it's been done in the history of the world.

- **BRUCE SNELL:**

  (laughs) In the United S-

- **GEOFF SISKIND:**

  I feel- I feel safe, uh, making that claim. Again, just- I-

- **BRUCE SNELL:**

  The- the first coffee versus tea hacking competition? I think you may be right.

- **GEOFF SISKIND:**

  When we went shopping for devices that we were interested in hacking for the show, to me, these are both a little bit goofy -

- **BRUCE SNELL:**

  Mm-hmm (affirmative)

- **GEOFF SISKIND:**

  Because I can't think of an occurrence where I would need to either set- turn my kettle on, like, via an app on my phone, or my coffee maker, given that-

- **BRUCE SNELL:**

  Uh-huh

- **GEOFF SISKIND:**

... the end result, which happens minutes later, I have to physically be near the machine to take the cup of coffee or pour the hot water from the kettle into a teacup.

- **BRUCE SNELL:**

  Yeah, I know. It's- it's all about the home automation, right? So, you- you wanna be able to set so that, you know, 10 minutes before you get out of bed, the- the kettle starts or the- the coffee starts brewing, so that when you're- when you get up and you are doing your morning routine, you've got everything already taken care of on that- that side.

- **GEOFF SISKIND:**

  I guess so. Uh, you see, my- my point I was driving home at you've now- you've now just totally ruined.

- **BRUCE SNELL:**

  (laughs) I'm sorry.

- **GEOFF SISKIND:**

  The point- the point I was making is- is that- is- is the- are these things a solution (laughs) looking for a problem, but maybe that was a problem.

- **BRUCE SNELL:**

  Well, I guess it is.

- **GEOFF SISKIND:**

  I guess I don't see it as a problem.

- **BRUCE SNELL:**

  Well, I mean, it ... Did- did you ever- you ever see Wallace & Gromit?

- **GEOFF SISKIND:**

  Yes.

- **BRUCE SNELL:**

  You know, he's always ... You know, Wallace always has these contraptions to- to make his morning easier, right? And that's- that's basically what these- these connective devices are doing.

- **GEOFF SISKIND:**

  Okay, so I basically have a Wallace & Gromit-style setup in my kitchen right now.

- **BRUCE SNELL:**

Yes, yes. Does that- does that make it more appealing now?

- **GEOFF SISKIND:**

  (laughs) I don't know.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  But I am curious about what's gonna happen, uh, on this historic episode of podcasting. (laughs)

- **BRUCE SNELL:**

  I'm so excited.

- **GEOFF SISKIND:**

  Where we are going to, once again, not hack one, but two, two devices-

- **BRUCE SNELL:**

  For morning beverages.

- **GEOFF SISKIND:**

  ... for morning beverages.

- **BRUCE SNELL:**

  Let's- let's- let's see what they've got brewing.

- **GEOFF SISKIND:**

  (laughs) I like it. Okay, very good. So, Bruce, here we go.

- **BRUCE SNELL:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  Uh, Pedro is bringing over the first hacker. He should be ringing my front doorbell any minute now to begin the hack.

- **BRUCE SNELL:**

Perfect.

- **GEOFF SISKIND:**

I- I will talk to you when we are done and we, my friend, will declare the winner.

- **BRUCE SNELL:**

(laughs) I'm excited.

- **PEDRO MENDES:**

[knocking] Geoff?

- **GEOFF SISKIND:**

Hello. How are you, Pedro?

- **PEDRO MENDES:**

Good, good. How are you?

- **GEOFF SISKIND:**

I'm- I'm- I'm fine.

- **PEDRO MENDES:**

You ready to be hacked?

- **GEOFF SISKIND:**

Sure.

- **PEDRO MENDES:**

Again?

- **GEOFF SISKIND:**

Always. Always.

- **PEDRO MENDES:**

Uh, this is Thomas Zook. He is from Packetlabs. Thomas, what- what- what do you do there?

- **THOMAS ZOOK:**

Uh, so, I'm a penetration tester.

- **GEOFF SISKIND:**

  Okay. And, Thomas, do you know what you've been called here to do today?

- **THOMAS ZOOK:**

  I believe we're gonna have some fun hacking you, Geoff.

- **GEOFF SISKIND:**

  Okay. So- so, we are having a- a beverage off, the great beverage off. Coffee versus tea. Thomas, you have to pick sides. Are you a coffee man or are you a tea man?

- **THOMAS ZOOK:**

  I'm gonna go with tea today, Geoff.

- **PEDRO MENDES:**

  Ohh, bold. Bold move.

- **GEOFF SISKIND:**

  Bold, bold move. I respect that. As a tea man, I- uh, I totally respect that. So, you know what that means? We have a coffee maker and a tea maker, both smart devices. You, my friend, my new friend, are going to hack the- uh, the tea maker. Are you up for that?

- **THOMAS ZOOK:**

  Sure. Let's get started.

- **GEOFF SISKIND:**

  All right.

- **PEDRO MENDES:**

  Can we come in?

- **GEOFF SISKIND:**

  Is it possible to do it just on the porch outside?

- **PEDRO MENDES:**

  Yeah, I guess. What if somebody calls the cops or something?

- **GEOFF SISKIND:**

  It's not- it's not that cold. 'Cause I- 'cause I'm gonna be- I'll be recording inside with the- doing the coffee thing.

- **PEDRO MENDES:**

  Yeah? Okay. Thomas, you all right with that?

- **THOMAS ZOOK:**

  Yeah, I think so. I've got a hoodie on and we can hide from the neighbors.

- **PEDRO MENDES:**

  A hoodie, of course.

- **GEOFF SISKIND:**

  Of course you have a hoodie. (laughs) Excellent.

- **PEDRO MENDES:**

  Then we'll get started.

- **GEOFF SISKIND:**

  Godspeed, my friends.

- **THOMAS ZOOK:**

  Thank you.

- **GEOFF SISKIND:**

  Okay. So, I'm- I'm back in my studio. I have Steve Povolny and Sam Quinn from McAfee's Advanced Threat Research team. Now, just to set things up, you know, I have Pedro and Thomas out on my front porch hacking the kettle. You guys, however, have a advantage or disadvantage, depending on, I don't know, juju, hacking juju, where you guys are actually-

- **STEVE POVOLNY:**

  (laughs)

- **SAM QUINN:**

  (laughs)

- **GEOFF SISKIND:**

You're doing this remotely and you guys are actually thousands of miles away, and I am video chatting with you, uh, and you are gonna be hacking one of these devices. So, in this case, it would be the coffee maker, I hope you're up for that, remotely. Does that- does that- is that possible?

- **STEVE POVOLNY:**

  Yeah. We'll show you a little bit how we're gonna plan on doing that, but you're correct; we're about 2,000 miles away and, uh, we're looking forward to the challenge.

- **GEOFF SISKIND:**

  So, not knowing anything about anything, how do you even start something like this?

- **STEVE POVOLNY:**

  Well, there's a couple of ways we could do it and we'll see which one is most effective. Since we are remote, we have a little bit more of a challenge, here, to get access to that local home network that you're running and the devices that are on it.

- **STEVE POVOLNY:**

  So, what we could do is, if we were, uh, within range of your Wi-Fi network, we could employ a brute force attack. We could try to find a device that had the credentials on it. But, because we're remote, we're going to try to leverage a feature in the router, actually, that you're using to control these, uh, smart devices and we're going to try to abuse the feature to give ourselves remote access, uh, to complete our attack over the internet. That will require us to be able to, uh, steal, or find, or- or brute force some credentials, uh, to gain access to that router, but, uh, we'll see if that's possible.

- **GEOFF SISKIND:**

  Okay. So- so, if I (laughs) understand this correctly, you're gonna abuse my poor router by trying to find my credentials somehow?

- **STEVE POVOLNY:**

  Yeah. I mean, when you say it that way, it just sounds so mean.

- **GEOFF SISKIND:**

  (laughs)

- **STEVE POVOLNY:**

  But, uh, we're- we're gonna log in totally legitimately, hopefully, uh, using illegitimately-stolen credentials.

- **GEOFF SISKIND:**

Okay. So, I'm gonna l- leave you to do your hacker things. Uh, I just wanna go downstairs and check up on Pedro and Thomas, who are on my front porch trying to hack my smart kettle. Can you hang on for a second and just, you know, talk amongst yourselves while I go- I go check up on 'em?

- **STEVE POVOLNY:**

  Yup. Say "Hi" for us.

- **GEOFF SISKIND:**

  Okay, I certainly will. (laughs)

- **PEDRO MENDES:**

  Oh, yeah.

- **GEOFF SISKIND:**

  Okay, you're smiling.

- **PEDRO MENDES:**

  Yeah. (laughs)

- **GEOFF SISKIND:**

  What does that mean?

- **PEDRO MENDES:**

  Well, mostly because your neighbors are giving us dirty looks.

- **GEOFF SISKIND:**

  Okay. (laughs)

- **PEDRO MENDES:**

  But also, uh, I believe it is, uh ... So, mission accomplished.

- **GEOFF SISKIND:**

  Really?

- **PEDRO MENDES:**

  Part one.

- **GEOFF SISKIND:**

  What do you mean? How? What have you- what have you done?

- **THOMAS ZOOK:**

  Well, I believe I've gotten your Wi-Fi password and we're logged into your network, here.

- **GEOFF SISKIND:**

  Through the kettle? Or did you-

- **THOMAS ZOOK:**

  Through the kettle.

- **GEOFF SISKIND:**

  ...What do you mean? Wha- how- so ... (laughs) It- it-

- **PEDRO MENDES:**

  Despite- I love the fact that, despite that this has been done to Geoff so many times-

- **GEOFF SISKIND:**

  (laughs)

- **PEDRO MENDES:**

  ... he is still shocked.

- **GEOFF SISKIND:**

  No, but how- no, okay, but how do you ... Guys, how did you do that? What- what happened?

- **THOMAS ZOOK:**

  Um-

- **PEDRO MENDES:**

  Well, because ... Hold on, hold on. We should say at this point, you know, 'cause I don't know if Thomas knows, you've had your stuff hacked so many times. Like, you have, like, pretty good security on your Wi-Fi and all that sort of stuff, right?

- **GEOFF SISKIND:**

Well, yes.

- **PEDRO MENDES:**

I mean, you have, like, a really unique password.

- **GEOFF SISKIND:**

Yes. I- so, I have a good password.

- **THOMAS ZOOK:**

Yes.

- **GEOFF SISKIND:**

But, Zook, just- again, you're just- you're just hacking the kettle and not my Wi-Fi router?

- **THOMAS ZOOK:**

Um, that- that's partially correct, yes. So, what I've done here is we've identified which network's your Wi-Fi network thanks to Pedro, 'cause he's been here, and what I did is, uh, we started checking what type of devices were connected to your, uh, Wi-Fi.

- **THOMAS ZOOK:**

And then what we did is we found- uh, we were able to identify the kettle through its MAC address, because vendors, they have, uh, a prefix to their MAC address that are consistent. So, we're able to link this to a specific kettle maker. Uh, and then what we were able to do is we were able to make a rogue access point with the same name as yours, and then we were able to send, uh, de-authentication packets to the kettle and force the kettle to connect to our Wi-Fi station.

- **THOMAS ZOOK:**

And from there, the kettle actually has a default password, so we were able to log into the kettle and we were able to ask it what password it has stored for your Wi-Fi network.

- **PEDRO MENDES:**

Okay. Hold on, hold on, Thomas, hold on, Thomas. Geoff has that look on his face.

- **GEOFF SISKIND:**

(laughs) I ca- I- I ... Let me say it back to you. I'm, like, 1,000% sure what I'm gonna say is wrong.

- **THOMAS ZOOK:**

Okay.

- **GEOFF SISKIND:**

  T- let me know and cut me off if I'm wrong.

- **THOMAS ZOOK:**

  Sure.

- **GEOFF SISKIND:**

  S- Pedro told you what my Wi-Fi network name was 'cause he's come over here and I've- I've- I've, uh, now clearly... was the wrong move, but I gave him (laughs) access to my network, and you figured out that, were somehow able to do that ... Okay, that's where I've- I've lost. So, what happens? So now you have the name of my Wi-Fi network, and what did you do next?

- **THOMAS ZOOK:**

  So, we decided to see what type of devices are connected to your network and check what vendors those devices are associated with. And...

- **GEOFF SISKIND:**

  And you did that- you did that without having my password?

- **THOMAS ZOOK:**

  Correct.

- **GEOFF SISKIND:**

  How'd you do that?

- **THOMAS ZOOK:**

  Anyone can do this. So, you-

- **GEOFF SISKIND:**

  Really?

- **THOMAS ZOOK:**

  Yes.

- **GEOFF SISKIND:**

  So, if I know- if I go to, you know, the- your ... I sit outside your house and I look, "Oh, there's, you know, Thomas's network," I can then check what devices you have?

- **THOMAS ZOOK:**

  Yes. That is correct.

- **GEOFF SISKIND:**

  Oh, that's crazy.

- **THOMAS ZOOK:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  Okay. So, now- now you've figured out what devices ... You've seen the kettle?

- **THOMAS ZOOK:**

  Yes, we have. Yes, we've identified the kettle.

- **GEOFF SISKIND:**

  Okay, what ha- what happened next?

- **THOMAS ZOOK:**

  Uh, we took a ... We basically did a quick Google search and found, "Is there any issues, any vulnerabilities with the kettle," and we were able to find out what the default password of the kettle was.

- **GEOFF SISKIND:**

  Ohh.

- **THOMAS ZOOK:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  Interesting. Which, I didn't change, 'cause I don't think I thought my kettle needed a password. (laughs)

- **THOMAS ZOOK:**

  No, most people would not.

- **GEOFF SISKIND:**

  Most people would not. Okay. So, and then- then you got into the kettle?

- **THOMAS ZOOK:**

  So, what we did is we set up our own Wi-Fi point that looked as if it was yours and tricked the kettle into connecting to it.

- **GEOFF SISKIND:**

  Ohh.

- **THOMAS ZOOK:**

  And from there, we were e- able to use the default password to ask the kettle what your Wi-Fi password was.

- **PEDRO MENDES:**

  Right. Because when you first installed the kettle, right, you installed the app for the kettle and everything, you put your password into that thing.

- **GEOFF SISKIND:**

  I guess so.

- **PEDRO MENDES:**

  So, the kettle has your password. But then Thomas was able to trick the kettle into connecting to us, and so he was able to then say, "All right, then, kettle, what password were you using to connect?" And there it was, wide open.

- **GEOFF SISKIND:**

  So- so you now- through hacking the kettle, you now have my Wi-Fi password.

- **THOMAS ZOOK:**

  Yes, I do.

- **PEDRO MENDES:**

  Well, do you wanna tell him what it is? I love this part.

- **THOMAS ZOOK:**

  W- um ...

- **GEOFF SISKIND:**

  Thomas? I hate this, but I'm gonna ask you anyway. Like, g- okay. Thomas, what is my Wi-Fi password?

- **THOMAS ZOOK:**

  It's a very secure password. How's that?

- **PEDRO MENDES:**

  Tell him. Just say it.

- **THOMAS ZOOK:**

  All right. It's [censored beep]. (laughs)

- **PEDRO MENDES:**

  Gotcha. Gotcha. How does it feel again?

- **GEOFF SISKIND:**

  Not great. Okay, so, you- ugh. So you, ahh, have my password. Now I have to find another really hard to crack password. So, now you have my password. Is that it?

- **THOMAS ZOOK:**

  Um, no, we can always keep going.

- **PEDRO MENDES:**

  Yeah. 'Cause you've got your other guy working, right? Yeah, on the coffee maker?

- **GEOFF SISKIND:**

  So, we're inside doing the coffee maker. It's starting to rain out here, but if you hug sort of close to the house, you should be fine. If just- I think it's just-

- **PEDRO MENDES:**

  Just for this next part. I mean, we've already done it. Can't we just come in and do the next part inside?

- **GEOFF SISKIND:**

  You know what? I'm gonna check in with you guys in a few minutes, okay? Just-

- **PEDRO MENDES:**

  Ugh.

- **GEOFF SISKIND:**

So, you guys do it and just ...

- **PEDRO MENDES:**

Fine. Sorry, Thomas. I swear to God...

- **GEOFF SISKIND:**

(laughs) Okay, Steve and Sam, I am back in the warmth of the studio. So, I have to say, Pedro and Thomas are- they're doing pretty well. They did this weird thing where they somehow tricked my smart kettle into giving up my Wi-Fi password, which seems super sneaky, but- uh, but they did it. How are you guys doing?

- **STEVE POVOLNY:**

Well, we- we have- we have the easier challenge. I think they're actually probably trying to, uh, de-authenticate the client and- and s- steal hard-coded credentials off of your device, which is actually, you know, a really creative and innovative way to get the network password off of that device, and- and certainly a vulnerability for that device.

- **GEOFF SISKIND:**

Yeah. I'm- I'm actually- (laughs) I'm a little blown away by the whole thing.

- **SAM QUINN:**

For us, we actually are going to employ a slightly different technique, as we discussed earlier. And what we found here is that the credentials that are used to set up this router, and specifically, the feature that lets us, uh, enable a- uh, a remote connection to it, those credentials were actually found in a recent public data breach, and we actually took the- the, uh, user's e-mail that set this up-

- **GEOFF SISKIND:**

What?

- **SAM QUINN:**

... and we were able to- to plug it into a site that lets us search through all of the breach history accounts and passwords, uh, retrieve the password for that, and sure enough, it hasn't been changed since then. And so we- we can just log in as if- uh, as if we're you, setting up this router and controlling it for the first time.

- **GEOFF SISKIND:**

So ... Ugh. So, the user who set it up was probably me, first of all, and then ... So, what you're saying, 'cause I probably set it up and I don't think I've touched it since I set it up years ago ... So- so, somehow, I was part of a breach after I set up my username and password for my router and you got that- you've got the information from the breach?

- **STEVE POVOLNY:**

Yeah. Exactly, Geoff. So, you- you can actually go out right now, anyone can, and there's a number of websites that let you just plug in your e-mail address. You can even, uh, uh, enter your password if you wanna find if that password has been in breaches, and you can determine whether that account is, uh, a part of a recent breach, and you can actually see the details for it.

- **STEVE POVOLNY:**

  So, we were able to do that, check the e-mail address. Um, we actually have downloaded all of the breach credentials and we found yours. You were- you are right; it was you that set it up. Um, y- you know, we were gonna come around to that eventually, so, tear the Band-Aid off now.

- **GEOFF SISKIND:**

  (laughs) Thank you.

- **STEVE POVOLNY:**

  (laughs) And, uh, you know, not only did we get the- the password for it, um, you know, but it was a fairly simplistic password that could've been brute forced, I think, with ease, too, so ...

- **GEOFF SISKIND:**

  Ugh. And, you know, I've- I've been on those, uh, password sites before and I think- I think I've s- actually seen the one you were talking about, and I just assumed because it happened a couple years ago that I probably had changed ... Ugh, but I guess I hadn't. Ugh. Okay, so, what's next, Steve?

- **STEVE POVOLNY:**

  So, Sam has actually already done a quick network scan, here, and found a smart coffee maker that is actually vulnerable to the attack we have in mind, here, and-

- **GEOFF SISKIND:**

  Okay.

- **STEVE POVOLNY:**

  ... he's going to go ahead and actually complete that exploit and show you what we're capable of doing, beginning to end.

- **GEOFF SISKIND:**

  So, hold on. Because of my unprotected router that I have in my house, Sam has gotten in (laughs) and he's able to scan the other devices and found my coffee maker?

- **STEVE POVOLNY:**

Yeah. Once he's on the network, we can just run a simple scan to enumerate the different types of devices. One of them found is a smart coffee maker. Uh, he's also found, uh ... Looks like you might have some surveillance cameras in your home. Is that accurate?

- **GEOFF SISKIND:**

  ...I have security cameras.

- **STEVE POVOLNY:**

  Yeah.

- **GEOFF SISKIND:**

  It sounds less creepy (laughs)

- **STEVE POVOLNY:**

  (laughs) Well, we'll be surveilling the security cameras. Uh, but, yeah, he's found a security camera and, uh, you know, we also see a couple of PCs on the network that are- are joined to your router. So, we can- we can probably do some damage with all those devices today.

- **GEOFF SISKIND:**

  Are you saying that you can go into my security camera?

- **STEVE POVOLNY:**

  Yup.

- **GEOFF SISKIND:**

  And can you see what my security camera can see?

- **STEVE POVOLNY:**

  We're gonna test that theory out. Um, y- don't tell us what it's pointed at and we're gonna try to-

- **GEOFF SISKIND:**

  (laughs) Okay.

- **STEVE POVOLNY:**

  We're gonna try to exploit the camera, pull a live feed through the coffee maker, through the router, over the internet, back to the comfort of our lab, and try to tell you what you're looking at from that- uh, that security camera.

- **GEOFF SISKIND:**

Oh, my God. Okay. Can you- can you do that now?

- **STEVE POVOLNY:**

Let's do it. Sam, why don't you go ahead and take over?

- **SAM QUINN:**

All right. So, um, I'm connecting to the, uh, coffee maker right now. I sent it a, uh-

- **GEOFF SISKIND:**

Okay.

- **SAM QUINN:**

... malicious brew cycle, which, uh, s-

- **GEOFF SISKIND:**

It sounds delicious.

- **STEVE POVOLNY:**

Those words have never been said before. "A malicious brew cycle."

- **GEOFF SISKIND:**

I know. (laughs) Brew cycle. Okay.

- **SAM QUINN:**

Uh, and I scheduled it for just a minute from now, so after a minute, your coffee maker will start executing this brew cycle, which is h- normally how it makes coffee, and will actually open up ports on your router and also send back the information to us that you have a coffee maker that's exploited and a, uh, webcam that we can view now from anywhere in the- on the internet.

- **GEOFF SISKIND:**

Now, it's- it just- I just wanna ... Uh, it's worth noting, as- if I'm understanding correctly, because I physically have this coffee maker in my house that you found a way to exploit ... It's like there is a spy physically inside my house that now you are manipulating to do your- your evil deeds.

- **STEVE POVOLNY:**

That's a good way of thinking of it. It's kind of like a Trojan horse, right? Once- once you're in, you're in, and you're- you're part of that trusted network now.

- **GEOFF SISKIND:**

Wow. Okay, this is, uh ... I am intrigued. I am intrigued by the malicious brew. So- so you set something, Sam, to go off in a minute, and then in a minute, the malicious brew is gonna happen. I think it's been a minute, now, hasn't it? Do we- do we-

- **SAM QUINN:**

Yup, and I actually have, uh, a live feed of your ... Looks like, um, your-

- **GEOFF SISKIND:**

What?

- **SAM QUINN:**

... your- your street, there. You have a- a red house across the way and a gray house with a little shed next to it.

- **GEOFF SISKIND:**

Can you show- can you show me the picture?

- **SAM QUINN:**

Yeah. Here you go. (laughs)

- **GEOFF SISKIND:**

(laughs) Holy (beeps). Holy (beeps). Oh, my God.

- **SAM QUINN:**

(laughs)

- **GEOFF SISKIND:**

Oh, my God.

- **SAM QUINN:**

And-

- **GEOFF SISKIND:**

You have ... This is the camera. I should just explain because I'm, uh, a little bit, um, tongue-tied. This is the camera I use as a security camera, just to see what's happening outside my front door, and y- you are able to get the live feed from thousands of miles away through my coffee maker.

- **SAM QUINN:**

Yup.

- **GEOFF SISKIND:**

  Oh, my God. You r- ohh. And you- if you- you could just put this anywhere online and anyone could now view-

- **STEVE POVOLNY:**

  Absolutely. Well, we were a little nervous of what you had- would be pointing your, uh, security camera at, so luckily it was just across the street, but-

- **GEOFF SISKIND:**

  In hinds-

- **STEVE POVOLNY:**

  ... I- I had visions of something much worse.

- **GEOFF SISKIND:**

  Well, in- in hindsight, uh, so am I.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  I'm glad it was facing out. Not that I- I- ... I am a f- decent, uh, citizen.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  So, I have nothing to hide. But, uh-

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  But still, that is- um, that is ... [phone ringing] Oh. K- okay, can you- can you- can you guys hang on one sec? That is Pedro calling me from my porch.

- **STEVE POVOLNY:**

  All right.

- **GEOFF SISKIND:**

  I'll be right back. Hold on a second. Hello?

- **PEDRO MENDES:**

  Hey. Geoff?

- **GEOFF SISKIND:**

  Pedro? How's it- oh-

- **PEDRO MENDES:**

  It- it's Pedro.

- **GEOFF SISKIND:**

  You guys ... Good. H- hi. You're s- still out there?

- **PEDRO MENDES:**

  Yeah, it's raining.

- **GEOFF SISKIND:**

  How's the- uh, how's the hack going?

- **PEDRO MENDES:**

  Okay, listen. Do you know off the top of your head, you know, roughly how many Facebook friends you have.

- **GEOFF SISKIND:**

  I don't know. Like, it's a bunch, I think. I don't, like-

- **PEDRO MENDES:**

  Okay. Do you wanna go check?

- **GEOFF SISKIND:**

  Yeah. What- have you-

- **PEDRO MENDES:**

  Just- just l- log into Facebook and-

- **GEOFF SISKIND:**

  Did you-

- **PEDRO MENDES:**

  ... and check how many friends you have.

- **GEOFF SISKIND:**

  Okay. Did you hack my Facebook account?

- **PEDRO MENDES:**

  Just do it.

- **GEOFF SISKIND:**

  Okay, hold on a second. Facebook.com.

- **PEDRO MENDES:**

  Did you put- did you put the http?

- **GEOFF SISKIND:**

  No, I d- (laughs) I did not. I just put in www.facebook.com. (laughs) Hold on a second. Username, okay, and my password. Okay, and it didn't ... Oh. I'm kicked back to the ... What's going on, Pedro? Pedro?

- **PEDRO MENDES:**

  Oh. Is- uh, is your Facebook password by any chance, um, [censored beep]?

- **GEOFF SISKIND:**

  (laughs) What have ... Hold on. I- I'm gonna come out there, okay? Can you-

- **PEDRO MENDES:**

  (laughs)

- **GEOFF SISKIND:**

Okay. Hold on, hold on, hold on. I'm coming out. I'm coming down, I'm coming down, I'm coming down. Hold on.

- **PEDRO MENDES:**

(laughs)

- **GEOFF SISKIND:**

(laughs) What happened? What-

- **PEDRO MENDES:**

Look how scared he looks. Look how scared he looks.

- **GEOFF SISKIND:**

I know. What- (laughs) what- so- so-

- **PEDRO MENDES:**

Yeah? Yeah.

- **GEOFF SISKIND:**

What did I just do?

- **PEDRO MENDES:**

Thomas?

- **THOMAS ZOOK:**

Um, I think you allowed us, uh, access to your Facebook password, Geoff.

- **GEOFF SISKIND:**

Okay, so, hold on. So- so, rewind for a moment. So, I have my smart kettle, I have it plugged in, I have it hooked up to my Wi-Fi. You come along and Pedro knows my Wi-Fi network name.

- **THOMAS ZOOK:**

Yes.

- **GEOFF SISKIND:**

Through that, you're able to figure out that I have a smart kettle. You then get into my smart kettle, find out my Wi-Fi password ...

- **THOMAS ZOOK:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  And then what's the Facebook connection?

- **THOMAS ZOOK:**

  Uh, so we just wanted to try and, uh, play a few little tricks on you, so we decided to, uh, use a tool to clone Facebook, and then I hosted that on my laptop, and what I did is I poisoned your DNS.

- **GEOFF SISKIND:**

  (laughs) Poisoned.

- **THOMAS ZOOK:**

  So, when you're making a request-

- **PEDRO MENDES:**

  You're g- you're gonna- you're gonna wanna clean that out, now, right?

- **GEOFF SISKIND:**

  (laughs) Definitely wanna clean that out.

- **THOMAS ZOOK:**

  Uh, so, what happens is, when you make a request to facebook.com, your w- uh, your computer asks, "What IP is that at?" And what I did is I said, "Well, I'm where you get that IP from and I'm that IP." So, what happens is you went to my computer hosting a fake website.com, uh, login page, and then you entered your credentials, thinking it was the real Facebook.

- **GEOFF SISKIND:**

  So, wait a second. So, I'm- I'm on my computer, typing in facebook.com-

- **THOMAS ZOOK:**

  Yes.

- **GEOFF SISKIND:**

  ... and it looked like facebook.com.

- **THOMAS ZOOK:**

Yes.

- **GEOFF SISKIND:**

  Somehow, through magic and juju-

- **THOMAS ZOOK:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  (laughs)

- **THOMAS ZOOK:**

  (laughs)

- **GEOFF SISKIND:**

  ... you managed to- to make that not facebook.com but make it thomas.com or what- I th- not actually thomas.com. But whatever- whatever your-

- **PEDRO MENDES:**

  Do you know how the internet works, Geoff?

- **GEOFF SISKIND:**

  I don't. I clearly don't. I think that's become very obvious. You managed to make this face Facebook page and I've now entered my credentials, and you now have not only access to my Wi-Fi network, but now access (laughs) to my Facebook page.

- **THOMAS ZOOK:**

  That's exactly what happened, yes.

- **GEOFF SISKIND:**

  Did you guys- did you- did you do anything? Did you-

- **PEDRO MENDES:**

  Well, I mean, the next stage would've been maybe your bank and then maybe your- you know, an e-mail client, your work client, your credit cards. Yeah, it could've just got better and better.

- **GEOFF SISKIND:**

I think this would be the point we call it. (laughs) This feels like, uh, "Thanks for coming out. Thanks for playing Hackable?."

- **THOMAS ZOOK:**

  Okay.

- **GEOFF SISKIND:**

  I think we're gonna call it here.

- **PEDRO MENDES:**

  Okay.

- **GEOFF SISKIND:**

  Um, this is good. Uh, I'm gonna go back upstairs and finish the coffee maker hack, um, but, uh, thanks, Thomas.

- **THOMAS ZOOK:**

  Uh, can I at least come in for tea?

- **GEOFF SISKIND:**

  It is- it is cold out here. Sure. Yeah, Thomas, you- you can come in.

- **THOMAS ZOOK:**

  Okay, thank you.

- **PEDRO MENDES:**

  What about- what about me? Geoff? Geoff, I d- why can't I come in, too?

- **GEOFF SISKIND:**

  Okay, Steve and Sam, I am back. So, it seemed that team Tea Kettle, uh, (laughs) they-

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  ... poisoned my network so that I actually went to a fake version of Facebook. Uh, I don't know if you could hear it, but basically, they tricked me into putting my password, and they now have that, and it could've been way worse. It could've been my bank or work accounts.

- **STEVE POVOLNY:**

  Yup.

- **GEOFF SISKIND:**

  So, that's horrible. Uh, Thomas is now downstairs having tea (laughs) and warming up.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  I don't like what they did, but let's- let's- let's finish up with you guys (laughs) to see if yours is more horrible than what Thomas was able to do. You guys (laughs) so far have managed to get into a device that wasn't even part of the competition, so it doesn't seem, like, fair. You went to my webcam.

- **STEVE POVOLNY:**

  Team Malicious Brew has another surprise for you, so-

- **GEOFF SISKIND:**

  (laughs) Team Malicious Brew. Okay.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  I- well, I am both excited to see what you have and- and, as I've learned from doing this show, uh, completely horrified and somehow vulnerable.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  All right. So, what- what else you got?

- **STEVE POVOLNY:**

  So, you know, it's- it's pretty common practice to show- you know, using a smart device, such as a coffee maker, to pivot to other IoT devices on the same network, and- and that's- uh, that's common practice. So, we've shown how we can, you know, e- exfiltrate data from that surveillance camera, that security camera.

- **STEVE POVOLNY:**

  But, you know, what about the really critical protected assets in your home? This is, you know, your working PC, or, uh, you know, if you're in a business, it's your- your critical servers. Um, a- and we wanna show how we can actually use the fact that we're already inside your network, we're that- that Trojan horse already, to compromise and run arbitrary code. We're gonna run some malware, uh, on a laptop that's fully patched in your home.

- **GEOFF SISKIND:**

  (laughs)

- **STEVE POVOLNY:**

  So, we should not be able to- uh, (laughs) to attack this thing. We're not gonna actually use any vulnerabilities, here; we're gonna use the fact that we've gotten inside your network using the smart coffee maker and we're going to compromise your main laptop, Geoff, and we're gonna run some code on it and show you what happens.

- **GEOFF SISKIND:**

  (laughs) Amazing. Okay, so, what- (laughs) what, uh ... Do I have to do anything?

- **STEVE POVOLNY:**

  No, that's the beauty of this; there's- there's no user interaction. What's Sam's gonna do next is he's going to serve as kind of a man in the middle. That's what we call this type of attack, where he's gonna actually-

- **GEOFF SISKIND:**

  Okay.

- **STEVE POVOLNY:**

  ... poison your network into thinking that your coffee maker is actually the router and your PC is- uh, is the coffee maker, and they're gonna ... By injecting into the conversation between those two, he's gonna actually control part of the software update process.

- **STEVE POVOLNY:**

  So, all we're gonna really ask you to do is, uh, you know, do your normal update on your- uh, on any- any software on your machine. I think you said you're running Notepad++, so if you just go ahead and do a normal update on that software-

- **GEOFF SISKIND:**

  Okay.

- **STEVE POVOLNY:**

... um, Sam is gonna actually be the man in the middle and he's gonna be able to, uh, execute some malware from- from that conversation between you.

- **GEOFF SISKIND:**

  So, Sam, you want me to- to update my- my software?

- **SAM QUINN:**

  Yes. Uh, go ahead and click-

- **GEOFF SISKIND:**

  Okay.

- **SAM QUINN:**

  ... um, "Update" and see what happens.

- **GEOFF SISKIND:**

  Okay, I will just- uh, I'll go to update. Okay. Uh, (laughs) oh my God. Okay.

- **SAM QUINN:**

  (laughs)

- **GEOFF SISKIND:**

  I'm guessing this is you.

- **SAM QUINN:**

  (laughs) It better be, Geoff. We hope so.

- **GEOFF SISKIND:**

  It- it better be, um, or I'm in a lot of trouble. (laughs)

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  Um, so, (laughs) a pop-up window. Uh, a window- sorry, a window has just popped up. (laughs) I guess what looks like ransomware where you have all of my- um, all of my files, uh, that you have, uh, captured, and, uh-

- **STEVE POVOLNY:**

  We're- we're only asking 30 bitcoin for this one, Geoff. Uh, we're usually a little bit harsher.

- **GEOFF SISKIND:**

  (laughs)

- **STEVE POVOLNY:**

  But, uh, no, we gave you a fake-

- **GEOFF SISKIND:**

  Yeah?

- **STEVE POVOLNY:**

  ... ransomware, uh, pop-up screen, but we did run a full executable.

- **GEOFF SISKIND:**

  (laughs)

- **STEVE POVOLNY:**

  We just set it to- of course, not to encrypt your files, 'cause we're- we're feeling really nice today and just gave you a nice splash screen.

- **GEOFF SISKIND:**

  Wait. Do you- so this ... You don't actually- you don't actually have my files but you could... Or you do?

- **STEVE POVOLNY:**

  Well, it depends. Are you willing to pay, or-

- **GEOFF SISKIND:**

  (laughs) I will pay you four doubloons. How does that ... Is that worth anything?

- **STEVE POVOLNY:**

  (laughs) All right. We'll- we'll- we'll take it. It's more than we usually get, so, uh, no. You're- you're good.

- **GEOFF SISKIND:**

  Perfect. Fantastic, fantastic. Oh, man.

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  Okay, so, are we done? Is this it? I- I'm impressed. Is there anything else you've got up your sleeve?

- **STEVE POVOLNY:**

  W- what else do you have in the home? No, I'm- yeah, I- I think we're gonna- we're gonna give you a little respite for today.

- **GEOFF SISKIND:**

  (laughs) Okay, let's- let's call it.

- **STEVE POVOLNY:**

  I think we'll call it.

- **GEOFF SISKIND:**

  Okay.

- **STEVE POVOLNY:**

  Uh, as long as team Malicious Brew, uh, gets the win, we'll call it a day, here.

- **GEOFF SISKIND:**

  Well, I have to say-

- **STEVE POVOLNY:**

  (laughs)

- **GEOFF SISKIND:**

  ... every part of my body wanted to call it a tie so that nobody would have their feelings hurt, but you you might have edged- you might have edged out team Tea.

- **STEVE POVOLNY:**

  But-

- **GEOFF SISKIND:**

You might- you- I- I- I'm g- I'm gonna say- I'm gonna- I'm gonna call it that you guys- that you guys won, because you did- you did two things and team Tea really just did one, I think.

- **STEVE POVOLNY:**

  Well, that's all the validation we need. (laughs)

- **GEOFF SISKIND:**

  Exactly, and also, it's- you guys are the ones I'm actually talking to, and then I'm probably gonna go downstairs and tell Thomas he won.

- **STEVE POVOLNY:**

  We expect nothing less.

- **GEOFF SISKIND:**

  Hope that's cool. Thanks, guys.

- **GEOFF SISKIND:**

  Whooo. All right. Bruce Snell, cybersecurity expert.

- **BRUCE SNELL:**

  Yes, sir.

- **GEOFF SISKIND:**

  We are back. The hacking competition, coffee versus tea, we have-

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  I don't know if we've declared a winner. I think they were both pretty cool.

- **BRUCE SNELL:**

  Yeah.

- **GEOFF SISKIND:**

  I think I told th- I kind of told the coffee guys they may have had an edge, but they were the last guys I talked to, so I- I j- you know.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  (laughs) I didn't wanna hurt th- that- that- that was- it was crazy, though. So, just to recap for a moment, team Tea gets into my system.

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  Hacks around my system, I don't know what they were doing.

- **BRUCE SNELL:**

  Ahh.

- **GEOFF SISKIND:**

  Do something where, basically, they were able to get on my computer, clone Facebook, have me sign up to my Facebook account, and steal my credentials.

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  Of which that could've been banking or anything else horrible.

- **BRUCE SNELL:**

  Yup.

- **GEOFF SISKIND:**

  Team Coffee, meanwhile, does some crazy thing where they hack in through my coffee maker and are able to access an entirely other device, my webcam.

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

They're now able to not only see live stream of what's happening on my webcam, but they're now sending me pictures, like, of my own webcam, and they're, you know, thousands of miles away.

- **GEOFF SISKIND:**

  And then, to make it even crazier, they then got on to my laptop 'cause it was on the same network and, through tricking me into updating a program, infected my laptop with ransomware.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  Had- you know, perhaps if I just (laughs) kept this going, if we had enough time, I-

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  I- I wouldn't even have a device to record on, 'cause they would've just destroyed everything at my house.

- **BRUCE SNELL:**

  That's true. That's true.

- **GEOFF SISKIND:**

  So, i- it- there's a time limit where I called it. I think within that time limit they both did some serious damage.

- **BRUCE SNELL:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  The cheesy polite person in me says- wants to just call it a tie so that everyone wins.

- **BRUCE SNELL:**

  That's 'cause you're Canadian.

- **GEOFF SISKIND:**

  It's 'cause I'm Canadian, but I might- I may say-

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  If you pushed me, sir, (laughs) I might say-

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  I might say the coffee thing was just, like, five to 10% creepier.

- **BRUCE SNELL:**

  I would have to go-I would have to go with coffee as well, although tea did get- team Tea did get pretty far into your network and they did a really good job. I think coffee, being remote, pushes it a little bit over the edge for me. Um...

- **GEOFF SISKIND:**

  Yes.

- **BRUCE SNELL:**

  'Cause, I mean, I- I like to think you would notice if somebody was sitting in your house trying to hack your- your kettle.

- **GEOFF SISKIND:**

  I- I'd like to think, too.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  (laughs) Um, but they could be ... Like, in this case, uh, they were outside my house.

- **BRUCE SNELL:**

  That's very true. They- they could be outside.

- **GEOFF SISKIND:**

So, Bruce Snell, cybersecurity expert.

- **BRUCE SNELL:**

  Yes, sir?

- **GEOFF SISKIND:**

  Short of just not having any devices and, uh, moving up to the woods and, uh, brewing coffee over a-

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  ... an open- open hearth, what can I do to protect myself?

- **BRUCE SNELL:**

  You know, it's tough, 'cause there ... I mean, you think about the tea hack, um, you know, the- the- the kettle had your password, your Wi-Fi password, sitting, you know, in- in memory, right? Or- or sitting in a- in a really easily-accessible l- location.

- **GEOFF SISKIND:**

  Yeah.

- **BRUCE SNELL:**

  Uh, so that- that's- that's a- a negative thing on the- on the security of that kettle. But it's- it's like any of these sort of devices, right? As you're- as you let these smart devices in, you have to make sure that there's been some attempt to- to provide security.

- **BRUCE SNELL:**

  In the past, we've talked about, you know, nanny cams and things like that. Like, they- for example, they took over your- your unsecured webcam the- from the- the coffee side. A lot of these devices come shipped with really poor security because people are just trying to get things out the door as quick as possible. So, you know, the odds of some random manufacturer from China or wherever producing a tea kettle that is unsecured is pretty high, right?

- **BRUCE SNELL:**

  The- now, if you're gonna go and you really decide that you really need a- a- a- a Wi-Fi-enabled tea kettle, start looking around for known manufacturers, right? So, I mean, I- I don't know who makes-

- **GEOFF SISKIND:**

Okay.

- **BRUCE SNELL:**

  ... (laughs) tea- electric tea kettles, right?

- **GEOFF SISKIND:**

  (laughs) Yes, yeah.

- **BRUCE SNELL:**

  Um, but, I mean, look for- look for people that have some skin in the game, right? Because, if you think about it, if a- if a large company's, uh, connective coffee maker suddenly gets hacked, they've got egg on their face, right? Just to keep the- keep the breakfast analogy going.

- **GEOFF SISKIND:**

  Okay. Yeah, I appreciate that.

- **BRUCE SNELL:**

  Um, so- so they're probably more-

- **GEOFF SISKIND:**

  (laughs)

- **BRUCE SNELL:**

  ... inclined to actually l- look for fixes and- and try and update and- and patch those devices.

- **BRUCE SNELL:**

  So, again, it's, you know, my- my favorite piece of advice, which is to make sure your devices are updated. Right? So, and that's really going to vary. I mean, there-

- **GEOFF SISKIND:**

  Okay.

- **BRUCE SNELL:**

  ... there should be some sort of ... You know, if we think about the tea kettle, um, there should be some sort of setting in the app that you're using to start it that says, "Check for updates." Right? Same with the coffee maker.

- **BRUCE SNELL:**

The other component is, start looking at, you know, making sure that they are secured with a l- legitimate password. Right? That you can change the password. And so if you're- if you're being able to access your tea kettle remotely, uh, make sure that it's, you know, not sitting there with an open port listening for anybody to come in and use password 123 or- or whatever to- to get in and- and start hacking around.

- **GEOFF SISKIND:**

  Okay. So- so if I have this right, when buying IoT devices or any device, look-

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  ... for manufacturers that have a reputation.

- **BRUCE SNELL:**

  Right.

- **GEOFF SISKIND:**

  That will fix something if it's wrong and might actually care to put something on the market that isn't wrong to begin with.

- **BRUCE SNELL:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  Or- or at least- at least they think is- is pretty secure.

- **BRUCE SNELL:**

  Right.

- **GEOFF SISKIND:**

  And, of course, update the devices in the app, and-

- **BRUCE SNELL:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

... always keep those up to date. And make sure that your IoT devices or any other devices are secured with a legit password and that that password can actually be changed.

- **BRUCE SNELL:**

  You know, and- and it's interesting, 'cause we've- we've hit this point that, as the average consumer is now being- is now being expected to be more savvy about security because, you know as you're bringing these devices in, you c- you can't go to your- your IT guy for your house. (laughs) Right?

- **GEOFF SISKIND:**

  (laughs) Yeah.

- **BRUCE SNELL:**

  And make sure that everything's kept up to date, right?

- **GEOFF SISKIND:**

  Yeah, yeah.

- **BRUCE SNELL:**

  Because typically, that's gonna be you, right?

- **GEOFF SISKIND:**

  Yeah.

- **BRUCE SNELL:**

  So, I think as we start moving in to buying more smart devices, we have to start adding in security to our general mindset.

- **GEOFF SISKIND:**

  Bruce, I just wanna bring up one more thing.

- **BRUCE SNELL:**

  Uh-huh?

- **GEOFF SISKIND:**

  The thing I- I know we've talked about on the show before that I am, like, bonkersly excited about-

- **BRUCE SNELL:**

  Mm-hmm (affirmative)?

- **GEOFF SISKIND:**

  ... and I'm also excited about this 'cause we're actually getting some action on it. It's the new Hackable? hotline toll-free number.

- **BRUCE SNELL:**

  Still so excited about this.

- **GEOFF SISKIND:**

  It's- I'm so excited about this. I'm excited because people are calling and people are- are ... We're gonna- we don't exactly know what we're gonna do with it, whether we're gonna do a special episode or just-

- **BRUCE SNELL:**

  Uh-huh.

- **GEOFF SISKIND:**

  ... use some of these calls on normal episodes, but I am thrilled that, uh, the phone is ringing. I- the first couple days, I was waiting by the phone. It wasn't ringing. Wasn't sleeping.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  Just pacing.

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  A lot of pacing. And- and now it's ringing. I don't really pick up the phone, but (laughs) it- it goes through a machine-

- **BRUCE SNELL:**

  (laughs)

- **GEOFF SISKIND:**

  ... and- and- and- and we get to hear the calls. But we are thrilled that people are calling. Please keep calling if you haven't already. Questions for you, Bruce, uh, if you have s- tech questions.

- **BRUCE SNELL:**

  Mm-hmm (affirmative).

- **GEOFF SISKIND:**

  Questions about the show, if you wanna suggest a hack, or just wanna say "Hi," or a joke. You like jokes.

- **BRUCE SNELL:**

  I do like jokes.

- **GEOFF SISKIND:**

  The number is 1-855-4, the number 4, and then the word "Hackable." Again, that's 1-855-4-HACKABLE. Please call it. It is toll-free and we would love to hear from you 'cause it's so much fun.

- **BRUCE SNELL:**

  Absolutely. Please, please give us a call.

- **GEOFF SISKIND:**

  As well, if you wanna find out more about the show, people can also go to our website, hackablepodcast.com. As always, this has been Hackable? - an original podcast from McAfee. Bruce, thank you, sir. It's been good.

- **BRUCE SNELL:**

  Thank you, Geoff. It's been a pleasure.