"How To Improve Your Cybersecurity" Excerpt Transcript

Excerpt from Jan 5, 2018 episode of Science Friday.

IRA FLATOW: This is Science Friday. I'm IRA FLATOW. All of these wireless, geeky gadgets are fun, aren't they? But how can you guard against hackers who might be trying to break into your WiFi-enabled refrigerator, or dryer, or whatever, and commandeer your system?

We're going to talk about how you can beef up your digital security, and avoid getting hacked. Let me introduce my guest. Micah Lee is a software developer. He's also a security engineer at The Intercept based out of Berkeley. And Jason Koebler is editor-in-chief of Motherboard, based in New York. He's here in our CUNY studios. Welcome to both of you.

JASON KOEBLER: Hey. Thanks for having me.

MICAH LEE: Thank you.

IRA FLATOW: All right. Let's get into some of those details. But first, Jason, I want to get into this flaw in the chip we've been hearing about. Intel announced a flaw in a chip that could make hardware vulnerable to hackers. And it's almost just about every computer.

JASON KOEBLER: Yeah, so it is every computer that has an Intel chip going back to at least 1995. So we're talking about billions of devices. This vulnerability has been called Spectre and Meltdown. And basically what it does is it allows hackers to gain access to the kernel of the device which is the system memory that usually a user wouldn't interact with. And it allows the hacker to basically knock down the wall between the system memory and the user's memory so they can access pretty much anything on your device.

This is a bigger problem for infrastructure companies and big– like, ATMs and things that aren't regularly updated. If you have an iPhone or a Mac, Apple has already pushed a software update that helps protect yourself against this.

And I think this will probably come up a lot during this conversation. The best thing you can do to protect yourself is to make sure you're updating your software and hardware as often as possible. So if there are new firmware updates– something pops up on your computer says, update this– you should probably do it, even if it seems pretty annoying.

IRA FLATOW: And there get to be many of them coming in. Let's talk also about the very basics of security being a good password. We have a question from Twitter. Farmer Bonnie asks, is it true that we no longer need to substitute upper lower case, numbers, and special characters to make our passwords more secure? Jason?

JASON KOEBLER: Yeah, I think that this is– common wisdom was always, you want a super complicated password that has special symbols, upper case, lower case. The problem with that is, it's really hard to remember a password when it's gobbledygook. So what we recommend is you get a

password manager, such as LastPass or 1Password.

And what this does is, you have one master password. And then this password manager enters the login data for all the services you use. So it's impossible to remember 300 different passwords, but the password manager remembers it for you.

So what we recommend when creating a master password is not to make something super hard to remember, but to make something that's secure. And what that means is, make something that you'll remember. It could be a string of words. It could be a sentence from your favorite novel or poem. Something that you'll remember is long, not easily hacked, but doesn't need to be a lot of symbols.

IRA FLATOW: Let's talk to Micah. Let's talk about two-factor authentication. It's a good way to protect your account? Should we all be using that?

MICAH LEE: Yeah, two-factor authentication makes your life slightly more annoying, but it makes your accounts way, way, way more secure. And so the reason is– OK, so this is how two-factor authentication works.

Normally when you log into an account– like your Gmail account– you use your username and a password. And two-factor authentication means you need something else besides just your password. And so a lot of times this is your phone.

And most people have probably experienced it– even if you didn't really intend to enable it– for your bank, or for maybe a couple of other services, where– when you try logging in– it has a security check and sends you a text message with a couple of numbers. And you have to type those in. That's an example of two-factor authentication.

But it's the best way to protect yourself against spear phishing or against– if your password is somehow stolen, making it so that attackers still can't access your account.

IRA FLATOW: But here's a question I have for you. Let's say– I don't want this to happen to anybody. You're in a car accident. You go to the hospital. You have your cell phone and left it at home, or it's in the car.

And you need to log into your bank account to pay the medical bill, right? And you can't, because you don't have your phone with you anymore. You're trying to log in, and it's sending the second thing to your phone that you don't have.

MICAH LEE: Yeah, this is exactly why it makes your life harder.

JASON KOEBLER: Yeah, I think that that possibility or hypothetical– it is an annoyance at times. You could be overseas is one thing. Like you're on vacation. You're at an internet cafe. You don't have

access to your phone.

What I will say is, it is the best thing you can do beyond updating your software and doing a password manager. If your password is stolen– someone tries to log into your Gmail from Romania– you'll get a text message. Say, why is someone trying to log in from my Gmail in Romania? And you say, don't allow it. And I think that is–

IRA FLATOW: Yeah, it's worth the hassle.

JASON KOEBLER: It's worth the hassle, yeah.

IRA FLATOW: Here's a tweet from Bobby Arndt who says, are you still safe if you open a phishing email but don't click the link? How can you recover your security if you accidentally click?

MICAH LEE: So you should be safe in under almost every circumstance. But there are maybe a couple of circumstances where a malicious email might just directly hack your email program that you're using. But for the most part, you should be safe if you get an email and don't actually click links or open attachments.

And if you do click links, it really depends– I mean, a lot of this depends on what the type of attack is. But in a lot of cases, you can click a link and you'll be fine as long as you don't fill in your username and password.

So the way that a lot of phishing attacks work is, you get an email and it looks exactly like it's from PayPal. And it says, we think your account is compromised. Login to confirm that you, you know, something. And it looks very scary, but it looks like an official PayPal thing.

So you click a link. You get to a website that looks exactly like PayPal, even though it's actually a fake website. And it's asking you to login with your username and password. And as long as you don't type in your username and password, you haven't yet been hacked. But this is also an example why two-factor authentication could totally protect you.

IRA FLATOW: I see. And a lot of times when you mouse over that little link, you can look at what the link says. It has nothing to do with PayPal, or any of that stuff.

JASON KOEBLER: They're getting a lot more sophisticated, though. Yeah, some of these are pretty– they're pretty impressive.

Micah Lee is software developer and a security engineer at The Intercept out in Berkeley. Jason Koebler is editor-in-chief of Motherboard based here in New York. Thank you both for taking time to be with us today. And happy holiday season to you.

JASON KOEBLER: Thanks for having me.

MICAH LEE: Thank you so much.