Speaker 1:	00:01	Welcome to "Prep Talk," the Emergency Management podcast. Find out what you need to know about preparedness. Get all the latest tips from experts in the field. And learn what to do before the next disaster strikes. From the Emergency Management Department in the city that never sleeps. Here are your hosts, Omar Bourne and Allison Pennisi.
Omar Bourne:	00:27	Hello everyone. Thank you for listening. I'm Omar Bourne.
Allison Pennisi:	00:30	And I'm Allison Pennisi, and you are our listeners, and as always we thank you for joining us. We want you to come back as often as you can. So feel free to add "Prep Talk" to your favorite podcast provider. You can also follow us on social media, on Twitter @nycemergencymgt, Facebook, Instagram, and much more.
Omar Bourne:	00:47	On this episode we will be talking about cybersecurity.
Allison Pennisi:	00:51	That's right, Omar. Cybersecurity involves preventing, detecting, and responding to cyber attacks, which are malicious attempts to access or damage a computer system. We will be speaking with representatives, from New York City Emergency Management and from New York City Department of Information Technology and Telecommunications, on how New Yorkers can take steps to prevent cyber attacks, as well as the government's role in protecting New Yorkers from these cyber threats.
Omar Bourne:	01:18	But before we dive in, you know what time it is. Let us get you updated on the latest news in the emergency management field.
Speaker 2:	01:28	Here's your "Prep Talk" Situation Report.
Allison Pennisi:	01:36	This is the situation report. Let's get started.
Omar Bourne:	01:37	Thank you, Allison. Now October is National Cybersecurity Awareness Month, and the Department of Homeland Security wants you to secure your personal information online. This year's theme is "Own it, Secure it, Protect it." Now you can take a number of steps to protect your personal information online. Some of these include keeping software and operating systems up to date, using strong passwords, so Allison, no 12345 passwords. None of that. Limiting the personal information you share online, and using anti virus solutions, anti malware, and firewalls to block threats. So for more information, you can visit

niccs.us-cert.gov. That's niccs.us-cert.gov to find out how you can protect your personal information online.

Allison Pennisi: 02:45 Okay, thanks Omar. A United Nations climate panel recently released a new report on the state of the climate. And it turns out the report claims sea levels are rising at an ever faster rate than previously thought. Kind of scary. The report warned that if steps aren't taken to reduce emissions and slow global warming, seas will rise three feet by the end of the century. The report claims DARA effects will be felt on both land and sea, harming people, plants, animals, food, societies, infrastructure, and the global economy. In fact, the international team of scientists projected for the first time that some island nations will probably become uninhabitable.

Allison Pennisi: 03:27 The Intergovernmental Panel on Climate Change, or IPCC, increased its projected end of century sea level rise, from its previous projections, because of the increases in melting of ice sheets in Greenland and Antarctica.

Omar Bourne: 03:41 Thank you, Allison. Now this story comes from CNN. Officials from the Department of Education and the United Federation of Teachers in New York City are urging thousands of former students, staff, and teachers to apply for the 9/11 Victim Compensation Fund and World Trade Center Health Program. Now letters from the Department of Education are being mailed to anyone who was a New York City Public School student enrolled near the World Trade Center on or after September 11th, 2001. DOE and the UFT will also host a joint information event on October 28th to inform students, staff, and teachers of their rights. Back in July, President Trump signed legislation into law authorizing the extension of the 9/11 Victim Compensation Fund, which ensures compensation through 2090.

Omar Bourne: 04:42 The World Trade Center Health Program provides no cost, 9/11 related medical care to eligible members. Now a recent study published in the medical journal JAMA, J-A-M-A, Network Open found out both immediate, and repeated exposures to the dust during the months of cleanup following the attack, was associated with elevated cardiovascular disease risk that lasted for up to 16 years.

Allison Pennisi: 05:13 Thanks, Omar. The US Department of Health and Human services has earmarked funds to aid the development of new technology that could bolster emergency preparedness. Now this two-year, $4.9 million agreement will create technology that could create blood products available to save lives during a radiological or nuclear emergency. So the goal of the project is

		to develop human induced pluripotent stem cell derived platelets to treat blood conditions in which the body has an abnormally low number of platelets. Now, according to officials, improving the availability of platelets could also save lives. Now the deal is between the US Department of Health and Human Services, Biomedical Advanced Research Development Authority, and Platelet Biogenesis, Inc. And that's your situation report.
Omar Bourne:	06:04	Still to come, we will be talking with Eric Smalls and Toney Lewis from New York City Emergency Management, and Lois Last from the New York City Department of Information Technology and Telecommunications. But first, here is a public service announcement from New York City Emergency Management and the Ad Council.
Speaker 7:	06:24	Your daughter doesn't want to talk about why her room is a horrible mess. Your son doesn't want to talk about why he's wearing mismatching socks. Your spouse doesn't want to talk about their bad haircut. Families don't have to talk about everything, but they should talk to plan for an emergency. Pack basic supplies in a Go Bag: water, canned food, flashlights, batteries, medical supplies, IDs, and some cash. Talk about where you'll meet in case you lose one another. And of course, don't forget to pack the dog treats. Talk to your family and make an emergency plan. Go to nyc.gov/readyny, or call 311, to make your family's emergency plan. Brought to you by New York City Emergency Management and the Ad Council.
Speaker 2:	07:25	You are listening to "Prep Talk," the Emergency Management podcast.
Omar Bourne:	07:31	You are listening to "Prep Talk," and we are back. Joining us are Eric Smalls, assistant commissioner of technology at New York City Emergency Management. Also from New York City Emergency Management is Toney Lewis. He is the security engineer. And last, but not least, is Lois Last. She is the user experience senior director at NYC Gov Lab & Studio at the New York City Department of Information Technology and Telecommunications. Thank you all for joining us today.
Eric Smalls:	08:06	Glad to be here.
Lois Last:	08:07	Thank you.
Toney Lewis:	08:07	Thank you.

Allison Pennisi:	08:09	All right, so the first question is about cyber attacks. We know they can lead to a loss of money, theft of personal information, as well as a damaged reputation and safety. It can also interrupt businesses and infrastructure, and it affects both individuals and businesses. So what are the most common types of cyber attacks or cyber threats and how do they occur? Eric, let's start with you.
Eric Smalls:	08:32	That's a good question. I mean there are several, but one that comes to mind, because it's very tricky, is a man in the middle attack. And that's basically when you have a bad actor. They pose as a legitimate website. It could be your banking account, or just somewhere where you keep private information, and as you're typing your information in, they're collecting and actually going to the real website as you, and basically taken advantage of that information.
Toney Lewis:	09:03	One of our biggest concerns are phishing attacks, and that's a social engineering email attack where people are harvesting log on credentials or attempting to install malware. And the reason why it's a concern is that we have a variety of defenses, but by the time a phishing email reaches you, that means that all of our defenses have failed. So you're the last line of defense.
Lois Last:	09:27	One thing I've learned doing user experience for government services is that we are in the business of persuading people to do things the right way, to do the right thing. And I've found through doing a lot of user research, and creating a lot of products, people given the choice between doing the right thing and the easy thing, they often go with the easy thing. So our biggest challenge, our biggest opportunity is how might we make the right thing to do, also the easy thing to do.
Omar Bourne:	10:00	Easy thing. I like that.
Lois Last:	10:02	And we try to, through various methods, persuasion, and testing, and trying to figure out what generates trust, whether it's a website certificate or our logos and branding. We really try all the time to continuously improve the trust that we have with official government services, and try to educate people about things that are not official, and how to spot them.
Omar Bourne:	10:32	I am happy that you brought up education because with more people now connected to the internet through their smartphones and similar devices, what steps can be taken to protect individuals or their businesses? And if someone, or a business, is a victim of a cyber attack, what should they do?

Eric Smalls:	10:57	It's interesting that you mention mobile devices. Mobile devices take up 50% of internet traffic nowadays. But for personal use, users should, or New Yorkers or people in general, should just make sure that you have an antivirus program on your computer, and make sure that it's actually updated, and that you set it to scan on a daily basis. This is critical because a lot of times you can have applications run dormant and just waiting for a particular time to execute. So antivirus is a key tool to have in your toolbox.
Omar Bourne:	11:35	And we mentioned passwords, and I guess it shouldn't be a tricky situation, but it seems like it is. I mean we've done stories in the past where people have passwords that are basic passwords: 12345; or it's their date of birth; or a family members name. So how can people really understand that easy, as Lois says, is not always the best way. You got to create strong passwords. What advice do you have for people?
Eric Smalls:	12:17	I'd say that passwords are as important as your lock in your front door. Right? You wouldn't secure your front door with a screen door that someone can just easily just pick or kick open. You want to have a real door with a real lock. So you creating a complex password is you actually secure in your perimeter, you're securing your private information. So if it's easy for you, that means it's easy for someone else. And nowadays they have things called dictionary attacks. Right? So there's just a software out there that people write, and it just runs through all little basic passwords that you said. 123, ABCD, that's a given.
Eric Smalls:	13:02	The common thing today is use phrases, use complex phrases, and make sure that you change it up, you have a capital letter, you have a special character. So you can change Es for 3s, and in 0s for Os. And the systems nowadays can even detect against that. But you really want to make it a long complex password. Just don't think of one word, make it a phrase. And in that phrase have your capital letters and your special characters mixed in there. Make it hard for them. Secure your front door.
Omar Bourne:	13:36	And I like that. Secure your front door. I really love that analogy. And what if, because I guess with complex passwords, people feel as if they're going to forget it, right? So write it down.
Eric Smalls:	13:50	Nope, don't write it down.
Omar Bourne:	13:51	No? Don't write it down.
Eric Smalls:	13:51	Make it a phrase that you know.

Omar Bourne:	13:53	Okay.
Eric Smalls:	13:53	Make it a saying that you have that only you, something that you go by, or make it a phrase from your favorite movie or something like that, and just make sure you mix up the letters. Just make sure you have your special characters injected someplace in there. As Lois mentioned, my experience is that people always want easy. And so you can make a password easy. You can make a password, a phrase, easy. Because it's something that you know, it's something that you live by, and only you know that. You don't share that with people so you don't have to write it down. Just make it a phrase or a term that you know, because that would be easy for you.
Lois Last:	14:32	Great. Yeah, that's interesting, Eric. You're talking about complexity and complexity, for users, is increasing. Sometimes I think exponentially. For me, the passwords, the passphrase is one of the best things you can do. As long as it's a, like you said, personal one or something, we'll often take a title of a book on the shelf, that makes it easy to remember. Or something, part of the oatmeal box or something, that we know but it's very, very unusual. I often do that, but in terms of this increasing complexity, I find myself, and I find other people asking me about systems that handle passwords. Can we offload this to secure systems, be it apps, like 1Password, or be it Safari's, iCloud password systems? And increasingly I find this to be the case. Now I don't know if this is a good idea or not. But it's gotten to the point where I used to keep a database at home of all my passwords, and it was secure, and password protected, and all this stuff. And even that is too hard. So I'm offloading it to systems. I would like to know what you think about doing that.
Eric Smalls:	15:49	Yeah, definitely. I think it's a great idea. I mean the analogy that I like to use is that as we have more and more devices. You have the internet of things. Everything now is connected to the internet. And there's more passwords to remember, and it's almost impossible to create a separate, to remember a separate phrase for everything. And that's where these password managers, what you're referring to is a password manager. And they are paid, they're solutions that you can pay for. I think if you want to be most secure, you should definitely try to pay for a service. The free stuff you may not get, they might not be as robust. But they're definitely, they help. And those systems, those password managers, actually create those complicated passwords in there. And then you only have to remember one password. And that's that complicated phrase that we talked about earlier.

Lois Last:	16:38	Great. And also as mobile technology evolves, my favorite password of course is my face. Where I just hold up my phone, it looks at me, and it knows who I am. So maybe over time this increasing complexity will be offloaded by smarter devices as well.
Allison Pennisi:	16:59	Okay. So strong safe passwords, making things complex but still easy because cybersecurity as we were saying is actually easy. So the City has plans to address the growing need and defend against cyber threats. So what is an example of how City agencies are working together to address cybersecurity and cybersecurity emergencies?
Eric Smalls:	17:22	So the City has New York City Cyber Command and that's really their core responsibility. Their responsibility is to prevent, detect, and respond. And Cyber Command actually works with over a hundred city agencies. They are responsible for monitoring, and basically, alerting the IT units of vulnerabilities that we may not have. So they definitely assist us in protecting the city.
Toney Lewis:	17:56	And we work with Cyber Command directly. They provide us tools to monitor programs that run on our network. For instance, that you may have a program that you use daily, like Microsoft Word, and use it to create documents. If they detect that that program is doing something abnormal, we'll get a notification. Cyber Command does things like phishing tests against our users. And all of this are things that compliment internal tools that we have.
Allison Pennisi:	18:24	Okay, this is great. So strengthening interagency tactics and techniques for handling security threats. So we say this all the time, emergency management is a shared field. And even in the field of cybersecurity, this is a shared responsibility. So this is really wonderful to hear.
Omar Bourne:	18:40	I want to switch gears a little to talk about social media for our listeners. Again, this is Cybersecurity Awareness Month. We were talking about how you can Own it, Secure it, and Protect it. Now, 3.4 billion people, worldwide, use social media. That's an increase of 9% from 2018. So there's a lot of people, Allison, that's using social media today, right?
Allison Pennisi:	19:09	And we are among them.
Omar Bourne:	19:10	Yeah, exactly. So to our guests, what are some simple tips that people can take to own it, to secure their social media?

Toney Lewis:	19:24	Attackers are monitoring your social media. They're looking at Facebook. They're looking at Instagram. They're looking at your Twitter. Looking for information that they can use to compromise. So you want to be careful about what you share online, and how widely or publicly you share it. So attackers can't use your information against you. Example of that may be, Omar may post to Twitter that he's recording "Prep Talk" today. And I may get Allison's number from a public number, and call her, and say, "Hey, I heard Omar's recording 'Prep Talk' today. Can you tell me where's that's going to be recorded at? What time?" And being that I have the correct information, that he is recording "Prep Talk," you may be more likely to give me additional information.
Omar Bourne:	20:12	Wow. Wow. Yeah.
Eric Smalls:	20:14	And they do that too with, it's not only just with social media, but in general with phone calls. If somebody calls you randomly... Don't offer up information about people. Because they might start the phone call, or they might send you an email saying, or they might send you a DM saying, "I work with such and such." and you say, "Oh, is it this person or is it that person?" So you're giving them information. Don't provide additional information to people on social media and email, or especially on the phone, because then what they do is they take that information you tell them, and then they call somebody else that's sitting next to you. Because they have an idea of what the telephone number in your agency or in your business is. And then they call the next person, and then because they have that little bit information, just like they did with social media, nowadays they're putting the pieces to the puzzle. And because the person sounds credible, the next person might provide additional information.
Eric Smalls:	21:08	On another note, another way that you can secure your social media presence is remember that there's no delete button on the internet. Once you post it, it's there forever, no matter, you could try to take it down, but are systems that's crawling the internet and just capturing information. So be deliberate. Own what you do. Make sure that it's purposeful. Another thing you should do is you should update your privacy settings. A lot of social media companies now are getting scrutinized and they have to put the power back into the people's hands. So there might be settings that you can elevate your privacy, but they're not going to be on automatically. You have to go in there and you have to like turn them on.

Eric Smalls:	21:57	Another thing you should do is if you feel like something's happened, report it. Every social media has a button someplace or something that says, report suspicious activity. Or if someone puts a, posts something that's incorrect about you, take action. Own it. Make sure that... Don't let that stuff get away, because once it's out there... Put the onus on the company to keep your information accurate.
Lois Last:	22:27	And I would say be aware that personal information, of course, maybe you don't want to share, but even some seemingly innocuous information can come back to haunt you. One of the most common forms of social engineering is the affinity scam. Where you post something seemingly innocuous, I love golden retrievers group, or something that you're a part of, your kids go to this school district. Or something where someone contacts you and says, "Oh, I love golden retrievers too." "Oh, we're also in the Eastern Queens area."
Omar Bourne:	23:05	Right.
Lois Last:	23:05	And by using these affinity things, people's defenses are often naturally reduced. Because just this natural tendency of, "Oh it's somebody like me. We're in the same type of group."
Omar Bourne:	23:19	Right.
Lois Last:	23:19	So even innocent seeming information can actually be used. And this is often used in social media, cyber attacks, and also financial fraud as well.
Allison Pennisi:	23:33	A lot of these steps I think for social media also apply to other parts and aspects of your life. We were talking offline about how there are times where companies will have correspondence that goes out and says, "You haven't paid this bill." Or it's seemingly that company. You find out later that that's fraud. And I think it's important, and we've talked about this is you should probably contact those organizations or institutions directly and say, "I received this correspondence. I want to make sure it's legitimate." In addition to spam that you get in the mail, there's spam that you get on social media, through the internet, through your email, to just be mindful of the content, and don't take things at face value I think is really the big lesson here. And oftentimes people, as Lois just mentioned, your defenses are reduced. So one question I do have is about New York City's NYC Secure Initiative. It also includes a mobile app. So new Yorkers can protect themselves through their smartphones from cyber threats. Let's talk about that.

Lois Last:	24:42	Well this is great. It provides security for your device, and it also monitors network safety. This is an app you can download for free, and it will tell you if the, for example, WiFi network, you know you connect to WiFi, everybody does it. You're in the coffee shop. You're in the airport. Well, this app will tell you if it's a secure network or not.
Omar Bourne:	25:11	Right.
Lois Last:	25:11	And I find it extremely useful, when I come into JFK airport for example, we've all heard the horror stories of there being rogue WiFi networks, and you went and made a banking transaction in public or something. So this is really, really helpful and it runs in the background, and it just alerts you. I have used it on many occasions, and it's free for all New Yorkers.
Eric Smalls:	25:36	And that's to the testament of the New York City Cyber Command because this is their initiative. Their initiative is actually to protect the city as well as government agencies. And the one thing I like, what they're trying to do is they have a big picture idea where they're literally trying to make New York City the hub of cybersecurity. They're trying to build a culture of cybersecurity and make it number one in the world actually. And that secure app is one of the things that they rolled out. Another thing that we have in the city is LinkNYC, and that's also secured in the same manner. But you can log onto LinkNYC, and it's WiFi for the city, free WiFi. But it also has a component in there where it has a micro VPN where you are, even though you're on this LinkNYC network, it's still secure. So the city's Cyber Command, through the mayor's initiative, is actually a great thing that they did.
Allison Pennisi:	26:49	So we were talking about building a culture of cybersecurity and I love that you said that. And we talked about NYC Secure and this mobile app. What about the other mobile applications that have been developed by the city? What is going on in terms of privacy, and if you are including personal information? For example, New York City Emergency Management and Department of Information Technology and Telecommunications have developed both Ready NYC, which is our ready New York program on a mobile app, and Notify NYC, which is the city's official emergency communications program. Also now available on a mobile app.
Lois Last:	27:27	Well one of the great things about developing a native mobile app, on iOS or Android, is we get to take full advantage of the devices' security features. So for example, on iOS with the facial recognition, this is your gateway to the app. And so we've been

		able to create these apps, taking full advantage of software developed by others, to bring the information and services to the people of New York city. Notify NYC for example, is a great mobile app you authenticate via your device. And then you have all of the push notifications, if you want, and all the notifications about citywide events, local events down to the zip code level, borough, borough quadrant, and so on around you. So you can actually get all the advantages of Notify NYC, in a secure way, so you can set your own settings, but it's on your personal device and is isolated to that personal device. That information is not stored in a place where it's going to be identified with you.
Omar Bourne:	28:38	A wealth of knowledge here today. We're talking cybersecurity. It is Cybersecurity Awareness Month. For our listeners. What's one last tip that you want people to know when securing their information? Eric?
Eric Smalls:	28:55	So the one thing that comes to mind is, they call it MFA, multifactor authentication. Even though you have a password, someone could sniff it, someone could be sitting over your shoulder, you're on the bus and you're typing in the password. Multifactor authentication requires you to add a secondary password that actually changes like every 60 seconds. So it's never the same. So even if your main password is compromised, this secondary device, the password, makes it harder for attackers. And that goes back into the theme of "Secure It." We want to secure our information. So back to the other, we mentioned earlier about social media, all of the social media accounts you should enable multifactor authentication. Whenever possible activate it because is only going to assist you, make you more secure.
Omar Bourne:	29:44	Wonderful. Toney?
Toney Lewis:	29:46	Protect your mobile device. We're not just using mobile devices for Facebook or Twitter. We're banking. We're paying our bills. We're looking at our insurance. So don't leave your device unintended in public places. Don't download apps from untrusted sources. And don't root or jailbreak your phone.
Omar Bourne:	30:05	Lois?
Lois Last:	30:06	Start with skepticism. Anytime somebody contacts you, assume that this could be a fraudulent contact. Until you are sure, don't give any information out.
Omar Bourne:	30:20	I like that.

Allison Pennisi:	30:21	I like that skepticism like a true New Yorker. [inaudible 00:30:24] [crosstalk 00:30:25]
Allison Pennisi:	30:28	All right. It's rapid response time and if you are a first time listener, it's simple. Omar and I will ask our guests a few questions, and they will give the first answer that comes to mind.
Speaker 2:	30:39	It's time for "Prep Talk" Rapid Response.
Allison Pennisi:	30:45	Okay, let's get started. What is the one emergency item you cannot live without? Lois?
Lois Last:	30:50	Extra water at home.
Toney Lewis:	30:52	Fire extinguisher.
Eric Smalls:	30:54	A plan.
Omar Bourne:	30:56	So the water. Every episode someone says water.
Allison Pennisi:	30:59	Someone says water or their phone. Actually, I'm surprised that nobody has said their phone in this episode.
Omar Bourne:	31:06	A question to Eric. I'm going to start with you. What is your favorite cyber threat related show or movie, or favorite cyber-related moment?
Eric Smalls:	31:16	I would say "Die Hard 4: Live Free or Die Hard."
Omar Bourne:	31:20	You're Bruce Willis fan. [crosstalk 00:00:31:22].
Allison Pennisi:	31:25	I actually know exactly what he's talking about. So Eric is my spirit animal right now.
Omar Bourne:	31:29	Toney?
Toney Lewis:	31:29	I guess I would have to go with "The Matrix."
Omar Bourne:	31:31	Ooh, Keanu Reeves, Keanu Reeves.
Eric Smalls:	31:35	Okay. Oh. That's a good one.
Omar Bourne:	31:35	Yeah.
Allison Pennisi:	31:35	That's a good one.

Eric Smalls:	31:35	That's actually a good one.
Omar Bourne:	31:35	That's a very good one. Lois?
Lois Last:	31:37	I'm going to go with the episode of "Brooklyn Nine-Nine," where they figured out somebody's password from their touchscreen by where the fingerprints were.
Eric Smalls:	31:46	Okay.
Allison Pennisi:	31:46	Wow.
Omar Bourne:	31:47	Wow.
Allison Pennisi:	31:48	Okay. Where is one place you would like to visit?
Lois Last:	31:51	I'd like to go back to Singapore.
Toney Lewis:	31:53	I've always wanted to go to London.
Eric Smalls:	31:56	Egypt, see the pyramids.
Omar Bourne:	31:58	All great answers. I haven't been to any of those places.
Allison Pennisi:	32:00	Neither have I.
Omar Bourne:	32:02	Yeah. Yeah. What is currently on your playlist, Eric?
Eric Smalls:	32:07	I don't really have a playlist. I'm boring. I listened to tech stuff, TED Talks, and stuff like that. I guess that's my playlist.
Omar Bourne:	32:14	Yeah, that's good. Toney?
Toney Lewis:	32:16	I'm currently listening to Ari Lennox.
Omar Bourne:	32:21	Okay. Lois?
Lois Last:	32:21	I've been listening to an REO Speedwagon song called "Roll With the Changes."
Omar Bourne:	32:26	Oh yeah.
Lois Last:	32:26	It somehow seems appropriate.
Omar Bourne:	32:30	So we also do karaoke on the show. So if you want, feel free.
Lois Last:	32:34	Be careful with putting me in front of a microphone.

Allison Pennisi:	32:38	She tells us this now, right?
Omar Bourne:	32:40	Yeah. Yeah.
Allison Pennisi:	32:41	Okay. Sum up the work you do in one word.
Lois Last:	32:45	Connect.
Toney Lewis:	32:47	Preparation.
Eric Smalls:	32:48	Fulfilling.
Allison Pennisi:	32:50	All great answers. And to our listeners, October is Cybersecurity Awareness Month. But cybersecurity should be something you think about all year long, and cybersecurity is a shared responsibility. We thank our guests for this very informative discussion on how to be cyber aware and how to protect themselves. For our listeners, you can visit NYC.gov for more tips and information on how to be cyber smart.
Omar Bourne:	33:17	And remember, "Own it, Secure it, Protect it."
Allison Pennisi:	33:22	Love it.
Speaker 1:	33:27	That's this episode of "Prep Talk." If you like what you heard, you can listen any time online or through your favorite RSS feed. Until next time, stay safe and prepared.