Speaker 1 (00:04):

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 (00:31):

And I'm Allison Pennisi. And you 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 listen to 'Prep Talk' on your favorite podcast provider. You can also follow us on our social media, on our Twitter @nycemergencymgt, Facebook, Instagram and much more.

Omar Bourne (00:48):

Allison, I can hear that you have company with you and for our listeners, we are continuing to social distance and so Allison is recording from home and she has two special guests that we can hear in the background. And that's okay.

Allison Pennisi (01:03):

Yeah, I think they might be interested in this topic that we're going to be discussing today. It's October, which means it's Cybersecurity Awareness Month. Each year, the Cybersecurity and Infrastructure Security Agency, or CISA recognizes October as National Cybersecurity Awareness Month. It's a time to emphasize the importance of cybersecurity and sharing practical tips that people can use to ensure their security online. Omar, as you were just saying with more people working remotely because of the pandemic, cybersecurity is of the utmost importance.

Omar Bourne (01:37):

That is correct. And when we talk about cybersecurity, we're talking about helping to prevent, detect or respond to cyber attacks, any malicious attempts to access or damage a computer system. We have a special guest with us today, Toney Lewis, he's the director of information technology here at New York City Emergency Management. Toney, you've been on the show before talking about cybersecurity, you are back so welcome back.

Toney Lewis (02:07):

Thanks for having me.

Omar Bourne (02:08):

Let's get right into it. Toney, now last year, 2019, it was stated that the US business sector had 17% increase in data breaches. And this can be found on the website cisa.gov, www.cisa.gov and the report was done by the Identity Theft Resource Center. My question, with this increase in the amount or number of data breaches, what are some tips for businesses so that they can beef up their cybersecurity?

Toney Lewis (02:46):

Remote working means that people are juggling work and personal activity simultaneously. Downloading homework assignments for kids, ordering Amazon deliveries, all while managing multiple video meetings and accessing dozens of cloud services for work. Our personal and work roles are blended more than ever. In this new normal, we have to look at how we can protect our accounts, our devices and how we connect to the internet.

Allison Pennisi (03:14):

As we have mentioned, more and more people are working remotely due to the pandemic. I myself am working from home as we are on this podcast. How can individuals make sure their home network is not vulnerable allowing for a breach into their work system?

Toney Lewis (03:29):

Great question. People must know how to secure their networks. One way of doing that is changing the default passcode for your Wi-Fi or your router. You should use a passcode that's hard to guess. Take advantage of the guest feature on your router for friends. This puts their internet traffic on a different network. You also want to ensure that your router software and any internet connected devices are updated routinely.

Omar Bourne (03:53):

I want to get a little deeper into passwords. What should we remember? And you mentioned a couple of these tips, making sure they're strong, but what else can we remember when creating passwords? I know the one, two, three, four, five is a no no, that's the easy option. We don't want that. What other tips can you give to people to ensure that their passwords are strong?

Toney Lewis (04:16):

Strong passwords are the key. The longer, the better. Should be a mix of letters, upper and lower case, numbers and symbols, and no ties to your personal information and no dictionary words. And the good news is that you don't have to memorize an awful string of characters to do this. You only need a few tricks. Don't use words that are easy to guess, like password. That's always on the top 10 list.

Omar Bourne (04:42):

That is funny. That is hilarious.

Toney Lewis (04:45):

Don't use something that's easy to identify, especially if someone knows you like your birth month and year. And do use a phrase and incorporate shortcut codes or acronyms. An example of that is to be, or not to be, that as the question, you can substitute the twos, the T-O tos with number twos and the question, you can substitute that with a question mark.

Allison Pennisi (05:12):

Those are really helpful tips. I would have never thought of using a phrase like to be, or not to be that is a question and using that as a way to create a very complex password. Thank you for that tip. I think our listeners would really appreciate, would sincerely appreciate that.

Omar Bourne (05:29):

Allison, You sound like you're you're tipping your hand here.

Allison Pennisi (05:32):

I am tipping my hat. I'm tipping my hat in my mind.

Omar Bourne (05:39):

Is this going to be a future password for you here? That's what it sounds like.

Allison Pennisi (05:44):

I'm going to plead the fifth.

Omar Bourne (05:46):

There's another good, that's another good one.

Allison Pennisi (05:50):

That is another good one. I have to, okay. I'm going to move onto my question because I'm going to tell everybody my passwords at this point. We're going down a rabbit hole. Toney, we talked about complex passwords, obviously really critical. We spoke previously about having your Wi-Fi password also changed for your home network, but what can I do to protect my devices? I have a laptop, I have smartphones, all of these different things. Not that our listeners need to know every device I have, but we're in a world where everything is interconnected right now. What can I do to protect my devices during cybersecurity awareness month and beyond?

Toney Lewis (06:31):

Attackers can take advantage of bugs in software to attack your device. Again, it's important to keep software in your device updated. That helps prevent these types of attacks. Also using security software goes a long way in protecting you from attacks like ransomware or other malware.

Allison Pennisi (06:51):

And for our listeners, we know cyber attacks can lead to loss of money, theft of personal information, as well as a damaged reputation and safety. It also disrupts businesses and infrastructure. It really does run the gamut. Toney, can you tell our listeners, what are the most common types of cyber attacks? And how do they occur?

Toney Lewis (07:10):

One of the most common types of cyber attacks is called phishing and phishing is a social engineering attack or an attacker uses social skills to obtain information about you or your company. They may use email or malicious websites to get personal information from you by posing to be a reputable website. With the right information, they can deploy malware to your device or even compromise your banking account. A common form of malware is ransomware. And this is when an attacker installs software on your device that prevents you from using your files until a sum of money is paid.

Omar Bourne (07:46):

The advice then for our listeners would be kind of just to verify. How can we make sure that we don't fall victim to these types of attacks?

Toney Lewis (07:56):

Good question. One of the ways is not putting a lot of information about yourself on the internet. Another way is when you receive emails that are unsolicited, asking you to take action, you should always examine them closely, try another source to contact them. In other words, if they email you, pick up the phone and call the company that you think the email is from and verify that it's accurate.

Omar Bourne (08:22):

Trust, but verify, as we always say. And what if for whatever reason you do fall victim to a cyber attack? What should you do?

Toney Lewis (08:34):

If you believe your account or device has been compromised, you should report it to the appropriate people at your company or your financial institution. It sometimes may be necessary to contact the police. Change your passwords and watch out for other signs of identity theft, such as suspicious charges on your credit card.

Allison Pennisi (08:53):

Toney, I actually want to turn a question about social media. Millions of people use social media, New York City Emergency Management and several other local state and federal government agencies use social media as a means to connect with the public and keep them informed. On an individual level, even for a business, what should we all remember when using our social media channels when it comes to cybersecurity and safety?

Toney Lewis (09:22):

Don't provide too much personal information. This can help attackers perform a social engineering attack. Social media can also be a gateway for malware so be aware of before clicking links and also be aware of catfishing. This sounds kind of funny, but this is when someone fakes their identity and it's commonly used for dating, but it can also be used when someone wants to reveal your personal or financial information.

Omar Bourne (09:49):

That's probably the best advice that we've received. Be careful be aware of catfishing, Allison.

Allison Pennisi (09:57):

Well also to even the think before you click, because there have been times and I know we've talked about different types of cyber attacks that can occur. There are times that you may think that you're receiving a legitimate email or a legitimate message thinking it's from someone you know or an organization that you know, and if you just do a little bit of extra due diligence or just take a pause, you may find that it's not the person or organization that you think it is. Very helpful advice. And I've seen this happen time and time again and it's very helpful to share this information with our listeners.

Omar Bourne (10:34):

And sometimes it does come from someone that you know. I've received Instagram invites from friends and I'm like, but don't I have this person added already? And then you receive a note maybe a few minutes later stating, "Oh, don't accept that friend request. That wasn't me, I've been hacked." As you said, you really have to think before you click.

Allison Pennisi (10:56):

Toney, where can our listeners learn more about cybersecurity?

Toney Lewis (11:00):

You can find more information at Emergency Management's website, which is on.nyc.gov/cybersecurity. And you can also find information at cisa.gov. C-I-S-A dot G-O-V.

Omar Bourne (11:16):

We know it's October, it's cybersecurity awareness month, but cybersecurity is a year-round day-to-day endeavor. For our audience, for our listeners, Toney, again, why is it so important that people have to take cybersecurity seriously?

Toney Lewis (11:37):

Think of it as a chain and the weakest link compromises the chain. Here at Emergency Management we have various systems and firewalls to protect our data and our systems, but all it takes is someone to come on our network and to click a link that downloads malicious software. That could compromise our whole network. Cybersecurity is everyone's responsibility because the attack vector is from the top, the experts in IT and in cyber command all the way down to the end user.

Allison Pennisi (12:14):

Speaking with Toney Lewis, director of information technology at New York City Emergency Management. Rapid Response is up next but first, here is a message from New York City Emergency Management and the Ad Council.

Speaker 5 (12:27):

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 6 (13:28):

You're listening to 'Prep Talk,' the emergency management podcast. It's time for 'Prep Talk' Rapid Response.

Allison Pennisi (13:39):

It is Rapid Response time. And if you are a first time listener, it's simple. Omar and I will ask questions and our guest will give the first answer that comes to mind. Okay Toney, first question, what is the one emergency item that you cannot live without?

Toney Lewis (13:57):

My power station. It's just like a huge charger that can power my devices if there were a power outage.

Omar Bourne (14:04):

I like that answer, Toney and it's fitting for a tech guy. You want to make sure that you can stay connected so the battery powered power source. Very good answer. I am going to keep it in the vein of cyber and tech here, but we're going to talk movies. What's your favorite cyber related movie?

Toney Lewis (14:24):

Oh, that's an easy one, The Matrix.

Omar Bourne (14:26):

Ooh, can't go wrong with The Matrix. Another question here, cyber related. Cyber security tip, you're talking to me, you're talking to Allison, what's the one thing about cybersecurity you would want us to know?

Toney Lewis (14:40):

There's three things that can help prevent an attack, protect your accounts, protect your devices, protect your connection to the internet.

Allison Pennisi (14:49):

All great answers. Last but not least, sum up the work you do in one word.

Toney Lewis (14:53):

Troubleshooter.

Allison Pennisi (14:55):

I like that. That's a first too.

Omar Bourne (14:58):

That is a first.

Allison Pennisi (14:58):

'Prep Talk' first. Speaking with Toney Lewis, director of information technology at New York City Emergency Management. Thank you for joining 'Prep Talk' for this very special episode on cybersecurity. For our listeners, if you want to learn more about how to stay cyber safe, you can visit cisa.gov or you can visit New York City Emergency Management online to learn more about how to stay safe. And as a reminder, cybersecurity is everyone's responsibility.

Speaker 1 (15:33):

That's this episode of 'Prep Talk.' If you like what you heard, you can listen anytime online or through your favorite RSS feed. Until next time, stay safe and prepared.