So with that, I'm going to introduce tonight's speaker is Dan Harpool. Dan has been with Complete Computing since 1989. He's currently the president and CEO of that company.

For the past six years, he's been the host of the Complete Computing show, saturday mornings on KARN in the Little Rock area but also on the web and on iHeart Radio. He's also served on numerous nonprofit boards and frequent speaker to diverse groups about computing technology, strategic planning and leadership.

So we are very grateful to have Dan tonight, and I'm going to turn it over to him so he can get started.

>> All right. Tricia, how long do we have to run, or should we run?

>> Tricia: Until 7:00. Thank you.

>> Okay. I'm going to set this so I don't go over and we'll have time for questions, although you can ask them anytime.

I apologize for the yellow hue. We took a major power hit here in Little Rock, and we're still getting some of the lights replaced. So can everybody see it okay?

I do a lot of Zoom, and I do the share my screen thing, but I like to do these where it's more like I'm in the room with you.

Sometimes there's a little delay with the hand gestures and all. And you do have a copy of the presentation, so I'm happy to be with you.

Thank you for all you do for our judicial system. You heard me speak earlier to the fact that I have a brother who's a federal judge and a nephew who is in the courts.

Tonight we're going to cover technology, just a little bit of fun to get us started since most of you have been working all day. Five computing trends in 2020. Tips for reducing cyber security threats.

I know we talked about superb security threats in prior times, but they are on steroids now.

The amount of spam, phishing, even video hacking. There's been a lot of zoom hacks that have gone on where we're doing a presentation like this and something we don't want in it starts to appear and so there's a lot of that going on.

You know, it's easy to -- and I hope you're staying safe. We talked about that earlier and hopefully we're all going to get past this year in the somewhat near future.

Predicting the future is easy. The hard part is getting it right. And so when people tell me absolutely categorically this is what's going to happen, I'm always suspicious and I'm careful.

You know, we've been trying to make Zoom and Teams and WebEx and all that be popular and be used for years, and it took, you know, a 100-year pandemic to get people to really get into this.

So it's hard to predict. Back in 1876, the president of Western Union said the telephone has too many shortcomings to ever be considered a means of communication.

In 1946, the president of 20th Century Fox said television will never hold an audience and people will not sit and stare at a plywood box.

Bill Gates, cofounder of Microsoft said, There's no reason anyone would need more than 640 kilobyte of memory. Your phone has probably anywhere from 64 to 512.

So I'd like this one. And Apple is already dead. That's the former Microsoft, the CTO of Microsoft in '97.

Bill Gates also said in 2004, two years from now, the spam problem will be solved. When we go look at fire walls and spam control software, 80 percent of the software that comes to your interface is spam if it's not blocked by something.

A couple more: No chance that the iPhone is ever going to get market share. That was Steve Ballmer in 2007, the year that the iPhone was released.

1958, Thomas Watson, founder of IBM, said there's a worldwide market for five mainframe computers.

And in 1977, Ken Olsen, the founder of DEC computing said there's no reason for anyone to ever have a computer in their home.

And at that time DEC owned the mini computer market. A few more real quick ones. Bob Metcalfe, who really was instrumental winter net and the founding of the Internet said I predict the Internet will soon go supernova and catastrophically collapse.

We have 4.5 billion people on the Internet, 3 billion people on smartphones, and we think we're going to be at, you know, 5 1/2 billion in a few years.

Here is the nice one. So for children of YouTube. There's not that many videos that he wants to watch. And then a guy I worked with at Motorola many, many years ago: Cellular phones will absolutely not replace local wired systems.

And in a way they haven't, but clearly we know where that's gone.

So what are five trends we ought to be paying attention to? One is hybrid architectures. In a way, we're using that right now.

There's an element of zoom on the web and on cloud. There's a local element with the device you're viewing. There's a broadband network that's allowing me to do this.

So the future of computing is hybrid. And we talk about edge devices. Edge devices are literally tablets, smart phones, computers, routers, switches, and these edge devices are already -- and Chromebooks. They are already a piece of the computing pie, more so than you just use it to get on the Internet or you use it to print a document.

We have systems today that we deploy where the computing power may be on the cloud, may be on the server, may be on the local device or a combination of all those things.

Cloud providers, of course we know it's been the year of cloud for 15 years probably, but now it really is the year of the cloud and has become that over the past few years.

Number 2 will be 5G. 5G is more than just cell service. You'll have up to 1.9 gigs per second of data speed, so even faster than wired in some; download speeds that are many times the speed of 4G. 5G can support more devices per square mail. It has intelligent capability. It will support IoT that we'll be talking about, better security, less delays in late he is any which we have a little of in here.

And services beyond the traditional smart phone. You may have your broadband to your home delivered by 5G in a wireless transmission type of setup and many more things.

The 5G challenges, though, one has been the pandemic. The rollout has slowed. Supply chains, availability of people, a lot of cities and municipalities didn't know it was going to require all the towers and all the devices it's going to require.

The higher frequencies do mean less coverage, so you may not have the same coverage in a building, and it's going to mean why you see all these towers being built that just look like telephone poles or light poles and not the traditional cell towers.

Right now there's battery drain and heat from these devices which they have got to overcome.

Millions of additional towers are required. Some areas won't have 5G for five or six years.

Some people tell me, "I already have 5G. My phone says right up in the corner 5G. Well, apple doesn't even have a 5G phone yet. What you are seeing is advertising from the carriers saying they have some 5G deployed. That's why you're not really seeing any performance differences.

Also, wi-fi 6. We also use wi-fi when we're not using cellular, in a combination of things. Wi-fi 6 is coming. It's unlicensed spectrum, unlike 5G. It's going to be faster, have less late he is any, provide better security.

You may remember, you know, when you get in a large sport event or other venue and all of a sudden you can't get texts or calls are delayed and you certainly can't use wi-fi. Wi-fi 6 is going to solve this. The.

The routers aren't yet. They were supposed to be out, and clearly your iPhone, your tablet, your Chromebook, your computer, your notebook doesn't yet have 6.

So we have these two things coming on edge computing at the same time. They are going to give us some of the tools we've been needing in terms of speed, latency and security.

Now, the next generation of networking will be cloud, local server, local edge device, combination of the two.

We'll have virtualized environments. Some of you may already have virtualized environments. For instance, the server that is serving this presentation is, one, a physical server with nine virtual servers running on it.

Some people run virtual computers. They want Windows 10, Windows 7, Apple operating system and maybe something else. One's physical computer, but the software plus the resources -- the memory, if you will -- lets them do that.

Only by adapting this streaming and getting edges devices smarter will we will be able to take advantage of all these new technologies. And they are coming fast and furious and, of course, a lot of you know, whether it be your veterinarian, your dentist, and maybe even in the court systems, certainly the legal world, running your computer software or server software on a local physical server.

Is becoming less and less popular. But because of security and hacking and performance and broadband not being available everywhere, we're using these hybrid systems, and that's all that really means is a combination.

And every service that Microsoft's rolling out has more and more elements of this.

Edge computing includes IoT devices: Nest thermostat, your camera, your Crock-Pot. Whatever you might have, every 127 seconds, a new IoT device is connected.

By 2021, there will be 35 billion of these IoT devices. The average home they think will have 50. We've got about 20 now in most homes.

And so, of course, this study said 10. This is going to bring the computing down to the closest point where you've got the most control, the most features. It's also going to demand, of course, more broadband, going to demand more security and unfortunately more management by the users.

So when you're looking at an edge device and you say, "Okay, today I have a laptop, maybe a Chromebook, maybe a tablet, maybe all of them. You know how powerful the new smart phones are and what they can do but, yet, the screens are still inadequate.

They run an operating system that's not universal to all devices. So stay with leadership brands.

You know, when tablets broke, I used to get a lot of calls. When they became popular, I used to get calls on the radio: Well, I bought a so-and-so, but it doesn't do updates. Or, I bought another one, and it doesn't connect with whatever.

We went from 154 tablet manufacturers down to 10 in three years and now you could argue we've got Samsung, Apple and Microsoft Surface. Amazon's even fallen by the wayside with the firewall system.

So those leadership brands, you won't pay any more, and you will definitely have updates that work, capability and opportunities for the future.

Also, consider the operating system. You know, a lot of people go buy an android-based tablet or an android-based phone but, yet, they live in the Apple world or vice versa. And, of course, in Microsoft, you have no mobile option in terms of a phone and they got out of the business.

Why have all those different operating systems to deal with if you can avoid it and go with the world you live in.

Now, in cybersecurity, I said earlier 4.57 billion. We're supposed to have 9 billion people on earth in somewhere around 2050, but that's only 59 percent of the population that's on the Internet right now.

2.2 billion computers in the world and 3.5 billion smart phones. So lots of great opportunity out there for this hybrid cloud/local/edge device world but a lot more room to grow and, of course, a lot more room for mischief.

So what are some of the things we need to think about with these edge devices? When you had an IT department maintaining your network, your firewall, all your devices, limiting what you could do, and some of you still do that work within the courts and places. But you didn't have to worry as much about it.

But today we're all carrying our own computers around in our smart phones, in our tablets and so there's a lot more room for mischief.

They think that the number of passwords used by humans and machines will grow to 300 billion. Some of you may have a couple hundred yourself. A lot of us do. Worldwide spending on cybersecurity will be 133 billion, even though it's only 48 billion a few years ago.

Arkansas organizations are being attacked. We have sheriffs' departments, cities, all kinds of people, schools, hospitals. You've read about some of these stories. Some have been in 2020 already; some would have been before then. A lot of them never get reported for various reasons.

You know the hack of Twitter by the three teenagers two weeks ago. They only gained $154,000, but they had the Twitter handles and passwords and e-mails for 450 very influential people.

And it came from a phishing scam to start with, phishing that run all the way from your preachers in Nigeria and he's stuck and he needs your money to very sophisticated like, you've got an Amazon delivery but we can't find your house, or things of that nature, bank statements that look very real.

These criminals encrypt the data when they use phishing to get ransomware. We probably work with 15 cases a month where everything is encrypted.

So if you've got your thumb drive connected, your external hard drive, you're connected to a server, you've got other things linked, all the files are encrypted. These come 90%, some say 95%, come from e-mail. So if you watch the unsolicited e-mails that request you to click on a link, the ones that want you to download a file or the ones that have the strange addresses at the top.

Which are normally pretty recognizable, you can avoid ransomware. Now that bitcoin is back up to a significant fee -- it's usually 25 to $30,000 if you have to unencrypt. The FBI advises you don't; I advise you don't. Why reward criminal behavior, and half the time, or more than half the time, they won't un encrypt your files anyway.

Sometimes we can use known encryption keys and we can fix the problem, but in most cases, it's most efficient just to restore and we'll talk about that here in a minute.

Courts, prisons, Department of Defense, Google, no one has been immune from ransomware. 95 percent delivered by e-mail. An organization will fall victim to ransomware every 11 seconds. Now, you tend to think, well, okay, that would be the court system, that would be the law firm, that would be the whoever.

But they do hit individual computers, and we get a lot of calls on this. And again, normally you clicked on a file, you downloaded a link. Just seeing an e-mail, getting an e-mail won't do it. But that's why it's so important.

I got one the other day, and you probably have heard of these where it looked like it came from me. It went to my employees. And if you looked at the address, it looked legit. It was my e-mail. But the verbiage was strange, and it made people question it. There's some of that going around, so you have to look at content, does it make sense, before you answer, click on a link, et cetera.

Again, restoring files is normally what you have to do in a ransom ware attack. So having a thumb drive, having an external drive, having a second drive on your computer, keeping the files on two computers is not enough. You need a cloud system.

And we've talked a lot in the past about those, but they run from carbonite to iDrive, Google Drive, One Drive. But most of the time, you need something with some management, something that if you forget, it takes care of it for you. Something that does only incremental backups so it doesn't take forever and so you need to -- there's a great review out in pc mag. Just type in acquiesces best cloud backups systems 2020 -- type in "Best cloud backup systems 2020," and they run from inexpensive all the way to things that run a little money.

Now, in the corporate world, the business world, we use devices that store it locally and also store it in the cloud. Let's say we have a natural disaster like they had on the East Coast and it may be days to get broadband back. You need to be able to get back up quicker than that.

Plus, if you have to download a lot of data, it's going to take a long time. So a twofold approach is still very legitimate. I wouldn't even guesstimate, but we do somewhere in the realm of about 100 backup disaster scenarios every quarter.

And some of them are people you'd recognize. We have one state agency lose all of their e-mail for two years. So the good news is we're not using the old digital tape, we're not using the old quarter-inch tape. We've got good reliable backup between the devices and the cloud.

So some of this may seem like a rerun or something you've heard before, but here are the tips for reducing your cyber security threats, and I'm sure all of you have seen more phishing. It's really been on steroids this year, and it's going to continue because, again, more people online, more people online longer times, periods. More people online that aren't particularly sophisticated about using technology.

Strong passwords, and that's more computers, Chromebooks, mobile devices, networks, IoT devices. Everything you have that touches the Internet or touches a network.

Now, most IoT devices like a nest thermostat, a camera, an alarm system, a Crock-Pot, whatever you might have, it relies on your wireless network's security. It doesn't have a lot of smarts, and we'll talk about that in a minute.

A strong password is 8 or more characters. Most people are moving it to 12, but a lot of systems don't allow 12, or they don't allow full strong password.

For instance, upper and lower case alpha characters and numbers makes a tremendous difference to this hacking software, what they call just brute force hacking, if you've got a strong password. Don't use the same password for

everything. When Mark Zuckerberg got hacked last year, every social media and e-mail account he had had the same password. So when they were in, they were in. Of course, there's a big difference between banking, insurance, personal, your work and some casual things that you might do.

Some people -- in fact, the man who came up with the strong password theory back a long time ago, 25 years ago, now thinks we're going to have to move to pass phrases. He thinks that people can't keep up with them, they don't use strong enough passwords, and software's getting smart enough to figure out some of these.

We'll see if that's where it goes. Don't use the same password for everything. Don't share your passwords.

A lot of companies, I mean even law firms and some people you would know share the same password so they don't have to reset them. They share the same password so if someone's out and not at work. That's really bad, bad policy.

Encrypt your wi-fi networks, and what that means is your wi-fi requires a username and a password. It's not like Starbucks, it's not like McDonald's, which is considered a hotspot. The FBI says don't use hotspots, period, end of question.

Naturally we use them. We know we do. But if you have a VPN, a virtual private network, on your phone, on your Chromebook, on your laptop, whatever you are using, you at least are getting a tunnel and that is protecting you.

There's been very few incidents of somebody's VPN being hacked.

A lot of people working at home, their employer, their system requires a VPN, but they don't always use it because VPNs can be slow on home connections.

You have a lot of download but not a lot of upload in the traditional small office home broadband setup, and that makes the VPN pretty slow. So usually people have to upgrade their broadband if they are doing a lot of VPN work and you've got a husband, a wife and kids at home, so to speak.

VPNs aren't expensive. If you use Norton security software, you already have a VPN built in. But if you want to see a good review of VPNs, go out pc mag and just put in "best VPNs 2020." They run from free TO very cheap to a lot more money, and what changes is how many servers of the VPN accessing to keep the speed up and to keep it from ever being down and features.

And you can usually do a trial on them. So if you are not sure you like the interface or not sure what you read, just do a trial version.

Again, you can get the same one that works on Chromebook, laptop, iPhone, android phone, whatever you have. It does make a huge, huge difference. That's why employers require them.

Now, if you have a firewall, a physical firewall like at a law firm or a court system, they are going to have clients that are already built for VPNs, and they work very efficiently. That's a better way to go if you can do that.

When you have your -- you're probably on wireless right now, most of you. So when you get your wireless router installed, make sure you know the admin password and you change it.

I constantly encounter people who have the same default password that every universe modem has, every Comcast router has, and it's very easy

for people to break in if they know that. So change that password. Turn off remote access.

Remote access doesn't mean you are turning off the ability to use it. It means you are turning off the ability for someone to manage it remotely. And you don't need that in the majority of cases.

Don't use your admin password for general casual access. Get a user name, create a username, have a strong password.

Set up guests for your friends, your kids' friends, a temporary user, and then you don't have to give them your password or change your password and they will still have access.

Turn on automatic updates on the device, on the router. Sometimes it's turned on by default, but sometimes it isn't. And you want to make sure that it's staying up to date, and if it has a firewall function, make sure it's turned on.

I see a lot of installers, that because it can cause an issue, like maybe your printer doesn't like the firewall or you go to one website that it blocks, then they will turn it off or they will turn it to the lowest setting. That's not good because then it leaves it open and it gives people the ability to get in.

We talked many times P antivirus software is still required. Even if you have a vpn, you have a firewall, you have windows and it's up to date, you still need the antivirus software, particularly with spam and phishing control.

And McAfee, Norton and the better ones do have that, and it does shut down a lot of it. The same thing is you want to turn on your pop-up blockers. Whether you use Chrome, Internet Explorer, Edge, whatever. Turn that to the highest setting possible.

Sometimes it will cause issues, but it will stop a lot of the nonsense. And they have gotten a lot better.

By the way, that's kind of unrelated, but on your SOCIAL media, if you haven't run the security wizard lately on Facebook, Instagram, whatever you've got, hopefully not Tiktok, but if you do, run those wizards. They will tighten your security up. They will ask you some important questions. Run it as tight as you can run it and to prove that you have to make a change. We talked about the firewall on high.

Run the security wizards. Pop-up blockers. If you suspect you have been a victim of a cyber attack or it's going on right now, something's taking over your screen, characters are being typed, you aren't typing, you're getting messages in your blocker or maybe even in your social media that's not what you think it should be, disconnect immediately from the wireless or the wired until you can determine what's going on.

So if they are getting data off your computer or if they are doing something else, broadcasting spam using your e-mail, you can stop it. One of the differences in the fire walls that are on, like, windows 10 and defender, they are just protecting you from inbound. It doesn't protect outbound.

If you get your e-mail out there producing spam, those 300 big spam blockers around the country will block you, and it's a big pain to get off those lists. Plus, you don't want to have it sent to people you work with, friends, et cetera.

I get a lot of people saying, well, I've been hacked. And, of course, hacking is rare. Very few people have the skill to hack, but they can go out and get software on the web all over the place to make it appear they are hackers and to do some of this mischief stuff.

Like, for instance, you know, your Facebook friends are getting requests and you didn't send the new request, you didn't change your profile. 99 percent of the time, it's because people didn't lock their pictures down and block their photo albums and anybody can take a picture, put it up there like it's you and then send out a bunch of friend requests.

Facebook needs to fix that if they haven't.

Delete unsolicited e-mails. Even with a good filtering system, you are going to get some unsolicited e-mails. One crazy one I've been getting lately is this big announcement that Kelly Ripa's leaving the network. I don't know if any of you have seen that.

Or, you know, you know the other kinds that you get about people stranded that need your help, or you just got a $50 million bequeath in London, if you just fill out some information from a lost relative. Those are phishing e-mails. Don't click on the links. Don't download anything.

And even if you think it's a legitimate download, you've been waiting for this PDF, but it comes in as an exe, or you've been waiting for some other kind of file and it comes in with the wrong extension or doesn't look right, call the source, verify before you download it because once you download it or click on it, just like when we clicked into the zoom session, it's already a done deal.

I get a lot of those where I will call up and verify, and very often it turns out, no, I didn't send you an e-mail. Or, I didn't send you a file. So it's just very important to use your best judgment.

This is a little bit of the same thing. Look at the sender address. If you ever got those, FedEx is trying to verify your delivery, Amazon's trying

to verify your delivery. If you look up there, there's characters before www.Amazon, there's characters after the dot-com, there's characters in the middle.

They are usually fairly easy to spot. But if you are busy like we all are and it looks legit and the logo looks good, you might fall for it.

It's really important, if you're the tech guru in your household, that may include your husband, your kids or whoever it might be to spread these little tips around because people, particularly kids, yeah, they are wizards in tech, they think, and they can do Tiktok and they can do this and that, but most of them are not really in tune to these risks and the stuff that can go on and happen.

Same with smart phone. Turn on that aggravating number that requires you to, you know, or any other security that you've got on an app, turn that on because it will work. Remember how the FBI couldn't even get in to some of the phones because they had turned on the code and at that time it was a four-digit code, but it isn't easy to crack, and it does work.

Have it set where, you know, it goes in screen saver after a certain amount of time and that will save you a lot of grief if somebody gets ahold of that device.

So that's, again, where it's going is more cloud, the cloud isn't enough because of security, because of performance, because of cost. So we're going to have these hybrid systems that use a combination of computing devices to carry us through to the next piece of the future.

We're going to utilize wi-fi 6 and 5G to move us to steroids, which is going to help us be more productive, but it's also going to lead to more nonsense and more complexity sometimes.

And ultimately, IoT won't just be your nest thermostat, it won't just be your camera. It will be sensors in your clothes, it will be sensors in the doors and all kinds of other things connecting us to the world. So it will be more important than ever to make the right choices.

Maybe you are a gallant person and an early adopter and you don't care, but if it's for your work and it involves security, then you are going to have to pay attention and be careful as you move forward.

Some people that we think are going to own it are going to die and not succeed. How can windows and Microsoft never have gotten more than 2 percent of the mobile phone market with their power and clout?

You all remember blackberry. You all remember MySpace before, or probably. So it's hard to pick winners and losers, but market share, innovation, adaptation will help you.

So questions about any of that, or not? Can be technology in general.

>> Tricia: Hey, Dan, we have a question. What is your opinion about software like LastPass that will remember all of your passwords?

>> Dan: Great question. Dashlane is the one that wins the best awards. But I will tell you that it can be aggravating.

For instance, it loads up your passwords, it looks on your computer. You delete the ones that are old and you don't know are on there. They are saved in another file. They are saved in possibly browsers. But it can lock you up and cause problems if you change passwords.

But there have not been hacking incidents with them, and DashLane is the one that's won the most awards. The free version lets you do 50 passwords.

>> Tricia: Okay. Next question: How secure is auto-generate passwords?

>> Dan: People recommend it, and there's not been hacking incidents of those software programs to date. The problem is they can generate such a secure password that you'll put it on a Post-it note or you'll use it for everything or those general security things we talked about.

Clearly it's going to do a better job probably than you are going to do because you are going to be tending to use an address, a birthday, a name or something within that combination that makes it easier for people to detect.

And by the way, related to that, this never comes out in any documents I see, but when you set up security questions and they ask you for three, or some let you do your own, don't use things that people can figure out like where you grew up, where you went to school, your mother's maiden name.

What I can do is get that data, I can purposely mess up your password because I don't know it. I can log on until it gives me the ability to reset with security questions. I can answer those security questions, and I'm in. And that's happened in some of these Twitter hacks.

So take the opportunity to use the obscure ones or create your own, if you are creating those questions.

One more question. Should we allow "Save passwords" when asked?

>> The Dan: The answer is no. Because if somebody gets your computer -- and I'll tell you, perfect example: If you do use DashLane, even the free version, you watch that

thing load up all OF the passwords that you currently have and all the ones you used to have and how quickly it can get them from cookies, from buried files, from the configuration files.

You'll find out how many passwords are saved on your computer, and I do recognize that can create a problem if you've got lots of passwords.

>> Tricia: How do you change if you already have saved passwords set up?

>> Dan: You can go in on windows, and you can go into your control panel. And you'll see a choice for controlling credentials. And that's another place where you can see passwords that you've put in, in the past, and you'll probably be surprised how many there are. And if you're having a real problem logging on with a safe password, that's a place that you can reset it.

But that's also a place for someone who gets ahold of your computer can get those passwords.

>> Tricia: What might come after 5G?

>> Dan: Well, they haven't even thought about it. The reason is heat and coverage and battery life are already big challenges with 5G. Now, that isn't why Apple is late and why they won't have their 5G out on time in September, but those are major problems that they are already dealing with.

But, yes, there will be something, no doubt about it. If you were at 3G, you may remember in the early iPhones, couldn't get on the Internet, you couldn't really connect with a lot of corporate systems. 4G was a major leap forward, and 5G is an even bigger leap forward.

It will probably only be the major carriers that -- well, it will be the major carriers. It will be T-Mobile, sprint, it will be Verizon, it will be AT&T. They can afford to play in the game.

>> Tricia: Where would I find instructions for resetting passwords and such for my wireless router?

>> Dan: Okay. Find your brand, and if it's provided by the carrier, like Comcast or AT&T, you can go out to their sites and there will be instructions on how to log into.

Basically it is a matter of putting the IP address, the Internet Protocol address, into your browser, like you've probably done for other things. And it's going to pop up an administrative panel and you are going to type in the administrator name and password.

By the way, those, the default settings for the passwords are all over the Internet. So if they haven't set a unique one and given you a unique password, then you are going to find that out pretty quick.

Did I lose you? I can't hear you.

>> Tricia: Sorry about that.

>> Dan: There you go.

>> Tricia: If you click on an e-mail to read because you can't tell what it is but don't click on a link or download anything, can it still harm your computer?

>> Dan: No. At this point in time, there have not been incidents where it gets launched, malware or phishing or anything from just being in your inbox. Now, my personal preference is just to delete it without even trying to click on it and see what it might be because it will come at some point in time where those will be a problem.

But I understand if you can't really determine what it's about.

Now, another way to do that is if you have an e-mail client on your phone or your computer but you also have an ability to log onto the web and check your mail, maybe Gmail. If you go do it on a web browser, you can usually see more of the

content in the preview, and it's not generally going to be able to do any harm as long as you don't download it.

Tricia: Okay. Is Tiktok really bad?

>> Well, the main thing, and you've heard all the press about it, is there's a lot of evidence, credible evidence, that it collects everything you do on it. So not just the silly video that you shot but where you're located, what router you're going through, your password and username which, of course, they already possess that. So that's what all the fight's about because they believe the Chinese government is getting all that data.

So we'll see soon what's going to happen with all of that.

>> Tricia: Is it true -- I'm sorry.

>> Dan: Go ahead.

>> Tricia: Is it true your iPhone can't be hacked?

>> Dan: It's not true, but it is rare. And usually when it is hacked, it's malware that came through an application. There are about 700 known apps in the android world that have malware on them. In fact, you can go Google it and you can find out, do I have any of these apps on my android phone. It's been far less of those problems in the Apple world. Mainly because it's a closed system and they control their developers.

Plus, 75 percent of the phones in the world, smart phones in the world, are android. So it's pretty secure as long as you keep your operating system up to date. But if your phone gets so old that you can't do updates or you're so full, you don't have space, then it's time to do something about that.

iOS 14 is coming even without the new iPhone 12. So we will have another upgrade coming soon.

>> Tricia: Is using your hot spot on your phone a bad idea?

>> Dan: It is without a VPN. So, you know, what happens is you establish that hot spot and, of course, it's providing you with wi-fi. And as long as you're using a VPN to go do other things, then, you know, you're protected. And there's been very few incidents of hacking --

And there's been very few incidents of hacking of cell systems. It's not impossible but it's not very common. The biggest problem is people getting software on there to clone the phone, but that's not a common thing.

>> Tricia: That's all the questions I see so far on my end.

>> Dan: You know, the other thing just to consider is nothing is better than keeping your software or your devices and everything up to date. You may recall windows 10 in May, we had the 2004 build. I see computers every day in windows that are 18.04 or 18.03, which is now 19 months old.

So be sure you are getting updates. Sometimes check manually and just see and you'll find out maybe one didn't happen because your broadband was tied up, your computer was not on the battery. Just make sure. You should be up to date.

And the easiest way to do that in windows is just get your command prompt up down in your search bar and just hit winver, one word. It will come up and tell you, you're in windows 102004, which means you're up to date. And there's not only performance improvements, there's a lot of security improvements in the last -- in fact, we have seen a big decrease in malware since windows 10 became mature.

So it has been doing some good in terms of stopping some of this stuff. Now, if you're, of course, over in the mac world -- and maybe some of you are -- same thing: Keep it up to date. It's a myth that an mac can't be hacked. They do

get hacked. It's just less because there's not near the popularity or the payload for them to hack a Apple computer.

>> Tricia: One more question. Is it safe to have banking in credit card apps on the phone?

>> Dan: As long as you have good strong passwords for those applications. And I would go in to where you can tune, remember every app, you remember does it have access to location, does it have access to microphone, does it have access to camera.

I'd turn off everything until you find out it won't function, and sometimes it won't function very well. But keep your device up to date. Have that security code on your phone in case you lose it, and you should be okay.

There's not been a lot of incidents. Usually it's been somebody obtained somebody's password.

Which, by the way, if you are going to trade your phone in, pass it down, keep it as the spare, you know, just be sure and wipe that phone completely before it's out of your possession because there have been people gain access that way.

>> Tricia: I don't see any more questions yet.

>> Dan: You know, you probably notice that it's great we didn't have to have masks on, but you probably notice I've been violating the rules. I've had a big allergy attack earlier this morning from a job I was on with a bunch of dust and so I've been rubbing my face.

It's so hard to adjust to all the new rules, isn't it? By the way, that's a good one. You can wipe your devices. Say somebody used your phone. You guys are probably on some computers that -- I'm on way too many keyboards, to be honest.

Just don't drench pep, don't spray them down to where they are wet. Just use a wipe with a reasonable amount. If you want to go out for your particular device, all the manufacturers have put bulletins out about the safe way to sanitize your device. So that's worth knowing in this world of COVID.

>> Tricia: I want to give my old laptop s to goodwill but don't know how to erase the hard drive.

>> Dan: You can go to the web and get a free software download KillFdisk. And there's a windows version, there's a dos version. It's like BleachBit that got so famous during the, you know, Clinton era, and will wipe it where it is not recoverable.

Now, some people are so paranoid, they will take the hard drive out and they will put a new hard drive in it. But there's other products out there, but we use it. It works great. And it will have no operating system on it, so they are going to have to install windows or whatever they use.

>> Tricia: Is it true that on your cell phone, people can see through your camera when you're not using it?

>> Dan: There are apps where that's possible. And what I do on my apps, number one, I don't put stuff on my phone that I don't really need. And if I try something and decide I don't need it, I delete it.

But once again, by app, you can go out and turn off microphone, camera, location, and that will stop any opportunity of that happening.

It didn't used to be you could tune it per application, but now you can.

That's another good thing to do once in a while is go into your settings, cellular, and see what's using data. So if you see something that you barely

use and it seems like it's consuming a lot of data and there's a good chance the microphone or something is turned on and it's out there.

It may not be collecting data, but it's certainly using data. That's what the new iOS, by the way, 14 for the apple is going to have a lot of more granular security controls than the prior versions have had, and it applies to iPads, too, of course.

>> Tricia: That's all the questions so far.

>> Dan: You know, one other thing. People say, I don't have my tech support around or they are not available. It's something I haven't encountered. Go to the manufacturer website, the software vendor site. Those kinds of sites that use your information, there's a lot of bad information out there.

And some of it's not purposeful, but just try to go to the real source before you, you know, change a security setting, make a big change. And naturally, like always, if you are really going to reinstall all your software, you're going to make big changes on your phone or your Chromebook or whatever you have, make a backup.

When there's a problem, that will save you and you don't have to format it, reinstall, find all your license codes, and that has really improved the process a lot from where we didn't used to have that ability.

Well, we've got some questions here. What's the most important thing you can do to thwart cyberthreats?

How are the majority of cyber attacks delivered?

And what is the first thing you should do when you suspect or know you have encountered a cyber threat or been the victim of a cyber threat?

>> Dan, we want to thank you. You're always a great presenter and you have such a wealth of knowledge to give us.

>> You get us all moving on what we need to be smarter about and so we really appreciate that very much.

>> One other note. Remember, you may not be able to catch my radio show every Saturday, but out on Spotify, tune in and all the big podcasts, iTunes, all of them. I do a weekly podcast of the show, and I do special podcasts like wi-fi security, tuning up for better performance, things of that nature.

So you can kind of keep up that way as things break and happen. And number one rule of tech problems: Stay calm. If you stay calm -- and I know sometimes it's the worst time and crunch time. But if you stay calm and you think of this question: What has changed? Generally you can work your way through it and you can solve it. Thanks for all you do. Hope you stay safe and good luck with the rest of your conference.

>> Thank you, Dan, so much. Everybody.

>> Bye-bye.

>> Thank you. Give him an air clap and we appreciate you very much.

>> Thank you.

>> Dan: Have a great evening.