“Tech Talk” TV Show

“Computer Viruses” Episode

The ceiling of a hospital is seen from the perspective of someone being carried on a gurney. Doctors and nurses are walking beside the gurney and holding up IV bags. From under the sheet a computer mouse dangles and sways. Text on the screen reads, “Computer Viruses *revisited*.”

Tech Talk intro plays

Susan McKinnell: Hello and welcome to Tech Talk from the University of Minnesota, your source of information about the world of technology that surrounds us. I’m your host, Susan McKinnell. Today, we’re revisiting a topic we focused on last year, but the topic, like the microbes from which it gets its name is always mutating and multiplying and in some cases becoming more virulent. We’re talking about computer viruses in all of their manifestations. Some of the terms you’ll hear include: patch, spoofing, virus definition and registry. Someone who knows a lot about these bugs is Brian Eckman, he’s a part of the University’s Office of Information Technology’s security team in the past half-year he’s identified sixty viruses that a leading antivirus program had failed to detect. Brian, you’ve even worked with the FBI and the Secret Service on some computer criminal cases, haven’t you?

Brian: Yes, I have.

Susan: Now, thanks so much for being here with us today.

Brian: Thank you for having me here.

Susan: I understand one of the things that you get to do is kind of play around with new viruses, test them out.

Brian: I do get to do that, yes.

Susan: And what exactly do you do with them?

Brian: I run them in a controlled environment to try to see what kind of damage they spread just in case I need to share that information with the University computer community to issue a warning.

Susan: And that’s how you’ve discovered these viruses that hadn’t been detected yet by the antivirus programmers.

Brian: Correct.

Susan: Because new viruses come out all the time, isn't that the case?

Brian: Oh, certainly; daily.

Susan: And so the antivirus software can't quite keep up with it.

Brian: That's correct, yes.

Susan: So, what do viruses do to our computers? Why do we need to make sure that our computers don't get viruses?

Brian: What a virus does, a virus is just a computer program that spreads itself. Nowadays, viruses programs are spreading themselves over the network which can cause a lot of excess network traffic. It can certainly slow down your computer's internet connection.

Susan: And when you say the network, you mean the internet.

Brian: Sure, for the most part, yes.

Susan: I mean for most home users that's the issue is that it spreads over the internet.

Brian: Yes. Correct.

Susan: And it slows down the traffic?

Brian: Sure.

Susan: And is that the biggest issue with most viruses?

Brian: No. Viruses often cause damage to your computer; they may delete files, they may delete critical system files so that your computer won't work properly anymore, as well.

Susan: That's a big issue. (laughs)

Brian: Sure.

Susan: But they also could delete files that you want to have for yourself, also; files with your own information.

Brian: Sure. For example, the Love Letter virus that came out a couple of years ago would delete all of the jpg's on your computer so if you use like a digital camera or you are scanning pictures, all of those photographs would have been overwritten by this virus and would be gone.

Susan: It deletes all of your pictures because jpg's are common picture files.

Brian: Sure, sure.

Susan: And, very simply, the virus itself just overwrites them?

Brian: Mm. Hmm. And overwrites those files with itself or some viruses will delete the files for example.

Susan: So viruses can do all sorts of things to our computers since they are simply computer programs.

Brian: Sure they can do basically anything to your computer that you can do to it.

Susan: How do viruses typically spread?

Brian: A common method is via email and those are certainly the ones we see the most of because they are very visible, you open up your email and there's the virus saying, you know, "here, click me."

Susan: (laughs) Which you're not supposed to do, right?

Brian: (laughs) Yes, exactly. They can spread themselves through flaws in software, for example, flaws in Microsoft Windows were how Blaster spread itself if you didn't apply the patch in time then it would, you know, silently install itself on your computer and then spread itself to other computers.

Susan: Blaster was a worm, I believe, that was spreading in August of 2000.

Brian: Blaster was actually the one, I think, in August of 2003.

Susan: 2003, that's right. Thank you.

Brian: Sure.

Susan: But did Blaster actually…how did that get onto people's computers?

Brian: There was a flaw in the RPC service of Microsoft Windows, and again, a patch had already been issued, but a lot of people didn't install the patch in time and so it would try to connect to the service on the computer and if it could make that connection then it would overflow what's called a buffer in the software and then use that overflow to install itself onto the computer.

Susan: Okay, I don't want to get too technical into how this actually works, but if a person hadn't installed the patch; the patch that would fix this problem with Windows, and they connected to the internet and without going to any specific website or checking your email or anything like that, because that virus was out there, it could still get on there.

Brian: Yep. You wouldn't even know it. You wouldn't even see any signs of it or…

Susan: That's why we really need to do some serious preventive maintenance.

Brian: Sure.

Susan: Now, before we get into that though I wanted to talk a little bit more about email because I understand that email viruses are getting trickier and trickier day by day.

Brian: Sure.

Susan: One of the things I've heard about is spoofing.

Brian: Spoofing. Email viruses often look on your computer's hard drive for email addresses to send itself to and nowadays they often take one of those email addresses and pretend to come from that email address. Whenever an email is generated you can say it comes from whoever you want to say it comes from and the viruses will do that in order to make it harder for you to find out where it actually came from.

Susan: So, if someone gets a virus, on their own computer, that virus might go through and grab all those email addresses that are on that computer and then send it out all over the place.

Brian: Right.

Susan: So I might get an email from my friend and it says it's from my friend but they never sent it.

Brian: Right. Exactly.

Susan: Absolutely. So, that can really…because, you know, people see emails from their friends or coworkers or whatever and they assume that it's okay, but it's not always the case.

Brian: Sure.

Susan: So, what's the main rule then with email attachments?

Brian: The main rule is with email attachments is don't open them unless you are actually expecting that type of attachment from that person. Email worms are very tricky nowadays to where they will actually try to hide what type of file they are. And so it might actually look like a text file or a word document or a picture depending on the email software that you use but it might actually be an executable attachment that could be a virus.

Susan: And “executable” being a small program.

Brian: Right.

Susan: So, even though it might look like a word document, it may be a program. Don’t open it unless you are really…

Brian: Unless you are expecting it from that person, sure.

Susan: Sounds good. Now, I wanted to talk about some other preventative stuff. What is some basic preventative stuff you can do to your computer to keep viruses off?

Brian: Well, certainly an important thing to do is to install and keep updated antivirus software.

Susan: Okay.

Brian: The rule used to be to update your antivirus software weekly, nowadays most antivirus software, you can set it to automatically update and if you can make that setting daily, I certainly would recommend it. There are often, you know, a dozen or more viruses that come out each day. So why have that exposure when you don’t need to?

Susan: Absolutely, let’s take a look; I know that on this computer we have some antivirus software on here. We have a very standard brand called Norton, but there are many antivirus companies out there.

Brian: Sure.

Susan: And any of them? As long as you’ve got antivirus software; that’s the main thing. And as long as they come out with updates on a regular basis.

Brian: Correct.

Susan: Okay.

Brian: A couple of important things with the antivirus is you want to make sure that it’s doing what is called a “real time” scanning as well.

Susan: Okay.

Brian: What that does is if the virus tries to write itself to your computer it’ll stop it and that is opposed to doing a scan after the fact which, you know, is helpful—to find the virus—except if the virus has already done it’s damage to your computer it’s kind of late.

Susan: If you've already lost all those pictures…

Brian: Sure. Exactly.

Susan: Okay. So you want it doing real-time scans and is it going to be scanning your email as it comes in and it's going to be scanning…

Brian: Yep. Anytime a file is written to your computer's hard drive it'll scan that file and make sure it's okay before it'll let that file run.

Susan: Great. Great. In order to do a virus definition update, let's go ahead and do that quick.

Brian: Okay. On this particular antivirus software, basically we just want to run the live update and we'll actually find out now that there is a more recent live update.

Susan: Really?

Brian: Yep.

Susan: We'll let that run for a minute. Usually and the live updates do go very quickly they take a few minutes, right?

Brian: Sure, a few minutes or even less.

Susan: So not a hard thing to do to keep everything running smoothly.

Brian: Okay, the other thing I want to talk about too, is we mentioned patches earlier. Now, and we mentioned Windows in particular, but it's according to the system that you're running. If you've got Macintosh you also need to run patches, correct?

Brian: Exactly, yep; Macintosh, Linux, Solaris, whatever you're running.

Susan: All those types of computers that we have out there.

Brian: Yep.

Susan: Now, in order to run patches on Windows; there's a Widows updatees, I know that on Microsoft, excuse me on Macintosh, there is also a Macintosh update. Let's take a look at the Windows update real quick. We go down here. When you run the windows update it just takes you to the Microsoft website, right? And then what would you do at this point?

Brian: Scan for updates and now Windows update is going to look for the critical updates, those are the security fixes that are very important and also look for other updates you may or may not want to install it’s really not terribly important that the other types of updates get installed.

Susan: I can see over here that there are three critical updates and one regular update, the main thing is to get the critical.

Brian: Yeah, exactly.

Susan: Great.

Brian: So now it says, “We have found three critical updates” we want to review and install the updates. And it’ll tell us for example that over here one is for internet explorer one of which is for excess data access components. So that all we need to do is click “Install Now.”

Susan: How often do you want to install these patches?

Brian: Microsoft has mostly switched to a monthly schedule of releasing patches, so certainly once a month. When something is patched that is very important, they may come out with an interim patch but once a month is generally enough.

Susan: So, if you hear about something in the news, and just to make it simple for our viewers, so that if you hear about any new virus, it’s a good idea go ahead and run both the patch and the live update, just to make sure.

Brian: Yeah. Certainly.

Susan: Great. Who is making these viruses?

Brian: The consensus is that most virus writers are between 14 and 34 years old, most of them are male—not all of them, generally they are considered not what you would call a social butterfly, they’re more apt to be loners, but that doesn’t mean that…

Susan: Those are the stereotypes, yeah.

Brian: There certainly are married virus-writers out there. There are virus writers in their fifties.

Susan: And why are they doing this?

Brian: Some for the fame of it, the notoriety of the bragging rights of you know, “Hey I created and unleashed this virus.” Some of which do it because they feel superior to others and well, “You deserve this.”

Susan: Mm. Hmm. They can make damage all over the place. Is it legal to make a virus?

Brian: To make a virus certainly is legal to spread it to others is where you cross the line into committing a federal offense, basically, breaking into other computers.

Susan: So, if I wanted, and if I knew how, If I wanted to write a virus on my own computer that would be perfectly legal as long as I didn't go sending it all over the place.

Brian: Exactly. Yep. You can't spread that…you can't break into other people's computers.

Susan: And that's where some of the difficulty in prosecuting these people is, isn't it? Because, sometimes the people who make them and the people who spread them are two different groups.

Brian: Oh, yes. Exactly, yes. Some people will write them and share them with a group of other people and it only takes one of those people to spread it to everyone else.

Susan: Kind of frightening. Thank you so much for being here with us today, Brian.

Brian: Well, thank you for having me.

Susan: At the beginning of this program, Brian mentioned that part of his job is to actually capture viruses on his computer and like a research scientist, put them in a controlled environment to see what they do.

Brian: My job involves incident response; part of what I do is deal with virus outbreaks or worm outbreaks. We sometimes see viruses that the antivirus companies don't know about yet so I run them in the laboratory environment to determine what those viruses can do and then I alert the university community and let them know to be, you know, aware for this particular virus that is out in the wild and on our network. What I do to run the virus is configure my computer so that it will not allow any outgoing network traffic so that I can't spread the virus to anybody else. And then I also have this program running in the background that monitors network traffic coming to and leaving my computer just in case the filters don't work properly we can catch it right away and stop the virus as soon as possible. So now that we have that filtering in place and we have the monitoring going on, we're going to use this program here which is going to determine what changes the virus makes to my computer; so, any new files that it creates, any files that it deletes, any registry changes that it makes are all going to be noted here by this program. And then also in the background I run this other program here, that tells me what the virus is doing over the network, for example, the virus is trying to spread to other computers via these different methods. So the program takes an inventory of the files on my computer, of the registry of my computer and then it runs the file that I tell it to run and then when it is finished it compares the difference between what has changed from the first time that I ran it. So now that the virus is done running, we can see that there's no real network traffic going on. We are going to go ahead and tell the program that the installation is complete and it's going to tell those changes that have been made to the system. So here are the changes that are made to the system. It'll give us a report that shows us here the registry settings that are changed, the registry settings that are created, the files that are created on the system. And then we can use another utility here that will tell us what network ports have been opened by this virus. There are a number of different ports that this virus has opened onto my computer and at least one of these ports is going to be what's called a "back door port" where an attacker could stumble upon this port and perhaps they know about where it is and they can use this port to download other software onto my computer a keyboard logger or some other type of virus. They can use it to do damage to the computer, to delete files, to add new files. So now that we've seen what the virus can do to our system, we can determine how big of a threat it is and issue a warning to the network administrators throughout the University of Minnesota to let them know what this does and how big of a threat it is to the University.

Susan: And if the warning to University community comes too late, Michael Waltonen is sent in to fix the damage. Michael is an onsite technician for the ResNet program, for student resident hall internet services. When a computer gets infected and refuses to do much of anything, they call for Mike. Mike, thanks for being here with us today.

Mike: Well, thank you.

Susan: First question, how do you know if you have a virus? Can you tell by what's going on with your computer?

Mike: Sometimes you can tell; sometimes you can't, it depends on the type of virus you do get. Different weird behaviors will happen, the Blaster virus that Brian was talking about earlier, you can see weird things where cut-and-paste will stop working but other things may work, sometimes a warning message saying your computer is going to turn off will pop up; that ones pretty obvious. Other times your computer will start running extremely, extremely slow for no real apparent reason, you didn't do anything and it'll just begin to do that.

Susan: Now, some of these things might happen, just if something is going on with your computer, maybe you've installed something new or something like that.

Mike: Sure. It's not necessarily a virus if you see performance changes in your computer that's…like with the virus that we have on this computer, here, that's definitely one sign that you have it, but it's not necessarily true for everything.

Susan: And also if you do see performance changes and you haven't done anything recently, then it is certainly the first place to check.

Mike: You can suspect it, it's not exactly "tell tale" but it is a possible sign to it.

Susan: Now you said that we've got a virus on here.

Mike: Yes, we do.

Susan: And what is it?

Mike: We have the Gaobot virus on this one.

Susan: Gaobot virus, G-A-O-B-O-T, I believe. Yeah, the one that's kind of hard to pronounce.

Mike: Mm. Hmm.

Susan: And what does this one do?

Mike: This one will try to spread itself to other computers around you and depending on the version, there are a very large number of variants of this virus, but some will try to attack other websites, every version of Gaobot will try to connect to internet chat servers and there are people on there who know how to communicate with the virus and will send instructions to it and they can send new programs to run your computer and have it do whatever they want it to do.

Susan: So, basically, with this virus people are trying to take over your personal computer for their own use.

Mike: Yes.

Susan: What about that "variant" stuff by the way? A new virus comes out and very quickly…what's going on with the variant thing?

Mike: A variant is, you essentially have the same virus on your computer but instead they'll change the filenames, change the locations of where things go, sometimes you get a few different small behaviors but for the most part it's the same virus, it just puts itself in a different place.

Susan: And my understanding is that this is frequently with the new viruses that come out, someone who hasn't created that virus picks it up, changes it a little bit and re-releases it.

Mike: Exactly.

Susan: So that's how you get all these different versions of the same thing.

Mike: Mm. Hmm.

Susan: Now, there was a "tell tale" thing that we noticed with this particular version of Gaobot, what does it do on this computer?

Mike: First off, this one will really slow your machine down but what happens is, if you decide you want to open your antivirus program here

Susan: Just to do a basic scan which you need to do frequently.

Mike: Right. We'll go in for a scan. We actually have Norton antivirus right here, but to go actually into it if you don't have it in your recent programs list…

Susan: It'll always be listed under your programs.

Mike: Yep. Those are your programs. And if you go in here, the program will open and the program will just shut down.

Susan: Oops. There it goes.

Mike: There we are.

Susan: So it doesn't really give you time to do anything.

Mike: Right. And this virus is looking for programs that are for tracking down what the virus is—usually diagnostic materials—or ones for going in and manipulating your system.

Susan: This is a very sneaky thing that a lot of these viruses, these days, are doing is that in some way inhibiting your own antivirus program, right?

Mike: Yes.

Susan: Mm. Hmm. Okay once you have a virus, or maybe you just suspect you have one because you can't get to your antivirus program to check it out, what do you do to get rid of it.

Mike. Depending on your internet situation, it depends on what you can do. Usually there are computer help lines that you can call and they can try to at least advise as to what to do, depending on the virus, it may be too complicated for you to do yourself, where there may be inherent danger of wrecking your computer, depending on where you have to go.

Susan: And where does that danger come in?

Mike: There are programs within your computer, there is one in particular called the registry editor, which holds a lot of values and locations essential to your computer telling it where to look for different things and certain files, or certain entries within this, if you delete the wrong ones, your computer may not start up again.

Susan: And that is called the registry right?

Mike: The registry.

Susan: And a lot of new viruses, these days, in order to get rid of the virus, in addition to having your antivirus program running, scanning with the latest definitions, you also need go in to edit this registry stuff as well.

Mike: You don't have to all the time, but it is advisable to go in and remove every piece of the virus that is in there.

Susan: And sometimes little bits are left in there and that's just not something the basic user should want to do.

Mike: No. I would advise definitely against doing something like that.

Susan: Okay. So I've got this virus, I can't edit the registry myself, should I be bringing this somewhere else to have someone take care of it or…?

Mike: It's a good idea to be doing that if…[with] some viruses people will just be able to tell you, "Yes, you can do it yourself. You just need to update your antivirus program." And then go ahead and scan for it and you'll find it and you're done. Other times what you have to do is have someone look at it and there are services that will do it for you for some fee whatever they set it to be.

Susan: Okay, so the first step is to call someone.

Mike: Right.

Susan: I know that here at the University we have a wonderful helpline service.

Mike: Mm. Hmm.

Susan: But fort he general public, what sort of place should they call?

Mike: For calling, it's usually very difficult to know who to call; usually it ends up being someone like the Geek Squad or something like that. I believe they do help you over the phone, briefly, at least to determine what the problem is and you can go from there, but…

Susan: So most likely it is a for-fee service of some sort.

Mike: It is a for-fee service, yes.

Susan: You might be able to contact the manufacturer of your computer, or Symantec or something like that.

Mike: They might be able to help you out, but most likely not. One piece of advice for people who don't want to pay for it, if they know people, like if they have friends who are involved in this stuff; they may be able to help you out with it.

Susan: This is always the first resource isn't it? To ask someone you know; a family member or a friend.

Mike: It is a problem, yeah.

Susan: Absolutely. Okay, now I noticed that with some antivirus programs that when you have the virus and you run the program it might delete the virus or the infected files but in other cases it might do something else with it, like put it in quarantine.

Mike: Mm. Hmm.

Susan: This makes me a little nervous because it sounds like the virus is still sitting there on my computer, it's just somewhere. What does it mean when it's in quarantine?

Mike: When it's in quarantine it actually will take the file and turns it into a form that Windows can't even understand, it's like its own new format that only your antivirus program understands it makes the virus not even runable.

Susan: So, that means that it really can't do any harm to my computer anymore?

Mike: Yeah. It's not possible to do anything.

Susan: Why does it put it in quarantine instead of deleting it?

Mike: It's possible that for some viruses actually add themselves to your files that you want to keep and quarantine is a place where you can put files; it's kind of like a pre-delete. It hangs on to them there in case they are files that you actually may want to keep, it will place them there.

Susan: Okay. So if it's in quarantine is there anything further that I need to do with it?

Mike: You can just leave it in quarantine. If you want to, you can delete it out of quarantine; if you really want to feel that it's gone, dead, no more, dead. You can go ahead and do that.

Susan: No more, it can't come back at all!

Mike: But it's not necessary, you can just leave it in quarantine, you should be safe.

Susan: Mm. Hmm. Okay. And just to come back to the Gaobot briefly and this version we have on here, if we can't run our antivirus program, the first step would be to call someone?

Mike: Right.

Susan: To find out what our next step is.

Mike: Right. Usually what they'll advise you to do is to reboot your computer in what is called safe-mode, which is Windows but it runs with limited portions of it actually active and many times the virus won't be able to be started when you do that and you will be able to run your antivirus program successfully that way.

Susan: Okay, and starting in safe mode; there are multiple places on the internet that give you instructions for how to start it up in safe mode.

Mike: Yes.

Susan: Great. Brian had several suggestions to prevent viruses on your computer: updating Windows patches and the other one he mentioned was, of course, having the antivirus program and making sure that it is updated with its definitions, virus definitions regularly. Do you have anything to add to that, any other preventive measures?

Mike: Other things that you can do it is, one, just use common sense, when you try to do it, when you get an email from someone and they have an attachment and you're not expecting it; don't open it.

Susan: Even if it says, "Looky here, these are wonderful pictures?"

Mike: Right. Right. One that we've had commonly on campus that we've had problems with is people are faking to be technical support for the University here and it'll say, "Please open attachment or we'll close your account in three days. Read details."

Susan: (laughs)

Mike: And everybody is opening it.

Susan: Because they think it's coming from the University technical support.

Mike: Right. It looks like someone who should be…

Susan: That is just evil.

Mike: I know!

Susan: So, basically you can't trust anything that comes in an email.

Mike: If there is an attachment, don't open it unless you are expecting it.

Susan: Mm. Hmm.

Mike: If you think you should be opening it, email the person back first, and say, "I got this attachment from you, should I actually be opening this?"

Susan: One last thing that I do want to get to; firewalls. Is that something we should be concerned about?

Mike: Firewalls are handy if it's a virus such as Gaobot which will spread just by you being on the internet.

Susan: Mm. Hmm. Like Blaster you don't need to have a particular email attachment or anything.

Mike: Right. Right. It'll just do it without your knowledge at all. What firewalls would do is they only allow communication from the internet to come in that you ask for. Like when you ask for a web page, you'll get the web page back off the internet. You asked for that, but if it's like the Blaster virus, the Gaobot virus, whatever other one, if they try to communicate without you asking for them.

Susan: Okay. And so firewalls will prevent that. All of the new operating systems come with a built-in firewall, correct?

Mike: Yeah. Windows XP and Mac OS X both have firewalls built-in.

Susan: So it's just a matter of making sure that you turn that on.

Mike: Right. It's either click a button that says start or checking a box for it and that's all.

Susan: Sounds good. Thank you so much, Mike. You've given us wonderful information today.

Mike: You're welcome.

Susan: Well that's our show on viruses we covered a lot of important points and here are some reminders For Your Files.

Brian Eckman said viruses which are computer programs that spread themselves can basically do anything to your computer that you can do to it, which means…

Brian: Viruses often cause damage to your computer; they delete files, they may delete critical system files so your computer won't work properly anymore.

Susan: Brian says there are a number of ways to keep viruses out; one is antivirus software.

Brian:…install and keep updated antivirus software.

Susan: Okay.

Brian: The rule used to be to update your antivirus software weekly, nowadays most antivirus software, you can set it to automatically update and if you can make that setting daily, I would certainly recommend it.

Susan: Brian had one other important comment about the antivirus program you select.

Brian: …You certainly want to make sure that it's doing what is called a "real time" scanning as well.

Susan: Okay.

Brian: What that does is if the virus tries to write itself to your computer it'll stop it

Susan: Brian also wanted us to know that it's essential that we update our operating system.

Brian: Windows update is going to look for the critical updates, those are the security fixes that are very important and also look for other updates you may or may not want to install…

Susan: If you get a virus, putting it in quarantine neutralizes it, but Mike Waltonen suggested using a firewall to keep the virus out in the first place.

Mike: …What firewalls would do is they only allow communication from the internet to come in that you ask for…

Susan: And one final tip from Mike about basic email security was…

Mike: … if there is an attachment don't open it unless

Mike: If there is an attachment, don't open it unless you are expecting it.

Susan: Mm. Hmm.

Mike: If you think you should be opening it, email the person back first, and say, "I got this attachment from you, should I actually be opening this?"

If you missed any portion of our virus program or want to see it all again, stop by our website. All of the programs we've done so far, including this one are right there for your viewing. Our address is techtalk.umn.edu. And if you have a question about viruses just post it on our website and we'll have one of our specialists answer it. Next week we're cooking up a special program on all that stuff that appears on your computer screens or your fax machines that you never asked for. Next week we'll be talking about spam in all its iterations. Thanks for watching. I'm Susan McKinnell.

Tech Talk is produced by Academic & Distributed Computing Services and the Digital Media Center, Office of Information Technology in cooperation with University Relations, University of Minnesota

Exexutive Producer
Robert H. Bruininks

Special Thanks to:
Steve Cawley
Sandra Gardebring
Shih-Pau Yen

Host
Susan McKinnell

Producer / Director
Susan J. Tade

Assistant Director
Richard Reardon

Associate Producer
J.B. Eckert

Technical Director
Steve Barbo

Audio
Laura Cervin

Floor Director
Dan Sagisser

Cameras
Pete Gorton
Jonathan Kranzler
David Lindeman

Lighting
Laura Cervin
Jonathan Kranzler

Set Design
Richard Stachow

Field Produceers

J.B. Eckert

Field Shooting
David Lindeman

Graphic Design
Nicky Torkzadeh

Effects Design
Paul Pecilunas

Make-Up / Prompter
Sharon Davis

Ms. McKinnell's wardrobe provided by
Herbergers

Web Development Team
Christina Goodland
Lance Cunningham
Ann Valenty

Thanks to:

CLA Studio B

NASA

Radio K

Bakken Library & Museum

KSTP Meteorology Department

Pavek Museum of Broadcasting

Antique Telephone Collectors Association