

>>RUTH YODAIKEN

We'll go ahead and start. We've been waiting for a few minutes but because last time we ended a bit late we'll go ahead and start. You're here for the consumer and business empowerment panel and what we're going to talk about is how to have ways to empower consumers and businesses. Yesterday we heard a lot about cyber criminals and fraudsters trying to use email to bring malicious code into computers and we heard about the different ways they do that in terms of sending emails that contain these things in attachments or that get the consumer to do something that helps get the code into their machine, whether that is to click on a link or take some other action of downloading something. Okay? We heard that these do two things mainly. They damage the computer systems and they take information from them and they work to trick consumers into more elaborate phishing initiatives. They also compromise these computers, whether they are the individual computer -- they compromise these computers and try and make them part of a network used by cyber criminals and by fraudsters to perpetuate more crimes and frauds. Okay? So today, this morning, we heard about law enforcement and how they are trying to deter these criminals and trying to catch them once they have done things. We've also heard from industry about initiatives to try to prevent these emails from even reaching the consumer's box. The one thing that we've heard in the past day, this morning, is that, to a certain extent, a consumer can't do anything and it has to be other players that do the work. But to a certain extent, what a consumer does is key, to try and help stop malicious code from getting into the computer and server. So here to help us work out what we need to do, to do -- the Chairman said yesterday work on computer self-defense. Here to help us are four panelists. We have Linda

Sherry, with Consumer Action, we have Dave Lewis, Market and Product Strategy, StrongMail Systems and he'll talk to us about how to help consumers differentiate the ordinary commercial email that they would get from malicious email from spammers, who are trying to trick them. We have Jeffrey Fox, Technology Editor of Consumer Reports, and he'll talk to us about new data that Consumer Reports has gathered in terms of analyzing these tools that are out there for consumers to protect themselves. And we have Miles Libbey, Senior Project manager at Yahoo, Senior Product Manager at Yahoo! Mail. And he'll talk to us about email service providers and how they try to help consumers, what they do to work with consumers, so that consumers are aware of what's going on and can try to have better habits.

>>LINDA SHERRY

Thank you, Ruth and thank you for holding this important spam summit. Today I'm going to talk a little bit about some of the challenges that face consumers in trying to identify spam and malware, which are significant, we believe. The first of which might be complexity. These protective programs really require a very high level of expertise in some cases, just to purchase, download, install, and to run effectively and to update effectively. And we find little evidence of standardization among the different software companies. It seems like many of the companies have taken their own path in this in developing these products. There is substantial cost in protecting yourself from spam. First of all, when you purchase a computer, many people think perhaps that the protection should be built into the computer from a lot of these things. But software costs money. There are free options out there but I think somehow consumers don't necessarily know about them and there aren't a lot, actually, as I like online. And

consumers may really miss genuine opportunities to receive mail is one example. Very often we'll get something in junk mail or someone will email me back, because we hadn't emailed, we don't email a lot, they would say, you know, I don't know you. Well, you knew me 6 months ago when you signed up, you know. So this kind of thing is very difficult. So we can't get our message out. There is cost involved. If the fraud or malware damages your computer or you click on a phishing email and you get, or a lottery type of fraud, so there is cost that way, too. And we really wonder, we think everybody, all the players have to think about, it's there to make consumers responsible for all of these additional costs. The frustration of dealing with spam, to protect yourself, it takes a lot of time and effort. Just because spam stays out of your inbox doesn't mean you have to do something with it. You have to deal with it later. A drop box or perhaps backtrack with colleagues and other people to make sure that for some reason, their email didn't reach you. An email from home or that kind of thing. A lot of people just give up. Which is not good for the system. Email holds a lot of promise, it's already shown many of its promises, for communication purposes in the future and we don't want people to give up. Computer performance, one of my favorite points, and on some computers, when you're running the security software, the antispam software, the antivirus software, it slows that computer down, and nothing really -- you can Google, you can search on the internet if you're savvy and a lot of it still won't tell you why it's doing that. The frequent updates will stop you in your tracks when you're trying to work, the spam going on will slow things down. We find consumers will maybe turn them off, which is a terrible thing to do because then they are unprotected. The onus is unfortunately now on consumers to protect themselves. I don't really think that's fair, and I'll

say something else about that in a minute. But recognizing phishing and other social engineering tricks, we're leaving that up to the consumers. A phishing email looks like this, don't click on it. Find misdirected legitimate emails, that can be tough because somebody will say to you, your boss will say, I sent that you email. You feel so silly. To mark spam, that can even be a challenge. You might mark something, for some reason, Chico's has targeted me, I guess I checked the wrong box. I feel they are spamming me even though they are a company I go to, to buy clothing from. You have to check the junk mailbox. You have to read and understand the consumer education materials that come from providers or online help. That's a significant time -- dedication of time which many consumers don't have today. And some of it is written in such terms that the consumers themselves can't possibly understand it either. You have to be able to determine who are the trusted entities out there that I really want to do business with? Do I want an advocacy email from consumer action? Did I sign up for a newsletter, this kind of thing. You've got to remember all of these things and after a couple of years it can be a little hard. Navigating all of the marketing and privacy options that are out there. How many of us really take the time to look closely at the privacy statements. Even in this community of very knowledgeable folks, sometimes we just let that slip, you know. Sometimes when we're buying something, we don't notice that the default is set to the check that we can get their mail, just because we're engaged in a process and we don't think about that. It can be a real challenge to tell the difference between spam and legitimate email. If legitimate emails come too often, you know, they can seem like spam. Deception and fraud is really tough to tell sometimes because they have thought overtime about tricking you. That's where the social

engineering comes in. They know what buttons to push. These takeover email accounts, how do you know it's not coming from the person that consumer action took over our server once. People were yelling at us. Sneaky graphics and links. Your boss sends you, again, a word file. You click on it, you don't think twice. Somebody else sends you an attachment or a little movie that they say is funny and you maybe don't think twice and it's malware. What about unknown senders who might have something you're interested in. We want to tell you that you need to act today to help a really good law pass but if you don't remember us or you don't recognize the way we're sending you email, you may ignore a legitimate opportunity to make a difference. Aggressive marketing, which I already mentioned, just some companies don't seem to get it that people don't want to hear from you every day of the week. There is a technology divide and an overload for consumers. Whether they have PCs, window PC versus MAC. Turning on fire walls and setting security choices in the computer, very complex business. On-guard online does some great education in that regard. Making warnings and updates meaningful. This is very important. Some of those updates that pop up, they will say, it's not a real domain name. My brokerage, I just clicked on my brokerage the other day and up came, it's not a real domain name. I've gone there a hundred times and I know it is. But if I was an unsophisticated person, what would I think, you know. There are all these different browsers that people use. Several main browsers. They have different capabilities, you have to set the settings in a different way. You find them in almost a different place, the preferences. Just imagine trying to tell your mom how to set the preferences on her browser. You may have sophisticated moms but mom is like -- you know. Unsubscribing versus spam reporting. Should you

click that button to unsubscribe. Should you report it as spam? It's just a big question. And a lot of people don't understand that when you give your email to a company and you don't say specifically you don't want it or you don't check the privacy statements, they have a legitimate ability to use that information, and even to resell it if you haven't opted out. Consumer protection is a big issue with spam. Who are you complaining to? Who do you complain to? There is a bunch of different entities. I go directly to the FTC and get some advice or to a consumer group but there are different entities depending on what the problem is. This is a global problem. There are many different ways, when they were talking about send your I.D. and the little saying, unlike, how would I know what that meant? I have no way as a consumer. I'm glad the ISPs are working on this for me but I have no idea really what it means or how I can check it because it looks like gobbledygook to me. Spamex, they may want to try to protect consumers but when you have an opt out it doesn't do much. Coordination between law enforcement entities is always a problem especially when you talk about global an global compliance. How are we helping consumers get control of this? I think that all the parties need to act together on this. Here I'll put in a plug to the ISPs and the computer makers and the other companies involved, mailers, et cetera, reputational companies. Talk to consumer groups. They can be really helpful in this regard. You wouldn't think twice before you go out and hire a consultant, you know, a business consultant. But what about just donating to a consumer group to ask them to come and listen to your products? Find out what your products are. Vetting your products in advance. Help to support that time that the consumer staff organization staff member is taking to come and give you good advice good, solid advice on what consumers will recognize, like, or use.

Be consistent in your approach across the different industries in protecting consumers. The same strategy for actually creating software, creating ways to educate consumers. Very important, these terminologies, and I hear all of these acronyms today. I think of my mom. She wouldn't have the faintest idea what some of these things mean so let's try not to use the acronyms. Let's standardize the terminology. Find consumer friendly words. Default, please, please, always set your default to the absolute most consumer friendly level and then explain to folks, that if you're not getting a certain -- if your browser isn't showing you a certain little window it may be because the default is set not to have pop-ups. Not to allow pop-ups. Don't do it the other way around. Allow pop-ups and then leave it up to the consumer to figure out that they can turn off pop-ups. The same with companies that do marketing. I mean, to have the box checked to receive emails, et cetera, that's just -- it just doesn't make any sense. You want to always do it at the lowest common denominator. Please, please, please, do not blame the consumer for failing to protect themselves. It is extremely important that we realize this is complex. A lot of you work for technology companies. And consumers are just not equipped, they don't have the background you do. They haven't been looking at this every day of their lives, since 1995 or before. Let's don't blame them. Let's help them get where they need to be, and help us all refine and make sure that the future of email is strong and helpful to everyone. Thank you. (Applause).

>>RUTH YODAIKEN

Thank you very much. Do you want to go ahead, Dave.

>>DAVE LEWIS

I would like to add my thanks to the FTC for holding this summit. I would like to

present a different viewpoint on the issue. I think you'll find from all of us there are some common themes and I will address what Ruth said I will address but in a broader context. With that, I would like to move on. I'm talking after lunch, so I'm going to use some visuals that maybe will be a little more engaging. You might consider them cutis, but I don't intend to deliver a cutesy message. Hope to be providing a perspective based on research that we've done with the navel sender and provider coalition -- email sender and provider coalition to look beyond the approaches we've used in the past. The title, keeping the killer app off death row. Do I really believe that? If you believe some of the pundits, they predict the demise of email about as frequently as they predict the meltdown of the internet, you would be concerned. No, I don't think the killer app is at risk, being outdone by -- or frankly even overwhelmed by spam but I do think the killer app is at risk and it's at risk because we haven't really addressed the sub point in this title, which is balancing email security with the demands of a vibrant medium. That's the issue that as an industry we need to come to grips with. So killer app, a shackled prisoner, that's how I view it. A prisoner because the medium, at this point, is in a position to fulfill its potential. That's partly what I want to talk about. And how do we keep from killing him off? Intentionally or unintentionally. It's really the unintentional shackling of the killer app, the actions or inactions that we may take in the name of the consumer, in the name of security, that concern me, and the consequences that those might have on the future of the medium. And ultimately, how do we set that killer app free? How do we enable the medium to fulfill its potential that I think we wouldn't be at this summit if we didn't believe in the medium and believe in its potential. So I want to just quickly review some of the key stats around where we are. I think we still think about email like we did

when many of us first became engaged with the medium and it's grown up. Consumers are hooked on email, and there are some stats that suggest that. 75% of U.S. households according to Forester use the internet. 97% of them use email regularly. Importantly, it's becoming or already is the medium of choice. These are rather startling statistics. Something that, a survey that we conducted along with marketing Sherpa that found that consumers felt that email was for useful than postal mail and particularly among the younger age group, 18 to 34. It's more useful than phone, though not as much. Nobody wants to take away the cell phone from the younger set. And most importantly, it's the best way to receive service notices, bills, account statements, by 41%, and when you think about what we've heard in terms of the phishing attacks and such, 41% is a pretty good number. I think the key statistic here is that consumers felt it was the best way for companies to communicate with them, for the companies that they do business with, to communicate with them. 64%, 72 for the 18 to 34-year-old age group. When you look at the business view of email today, when I was in London a couple of weeks ago, some stats that hit me there, I think, I would like to know the U.S. equivalent, about 50% of the communications, personal communications are now down via email. About 70% in the UK on business-to-business, which is a pretty alarming stat. Obviously marketers are hooked on email. We know that. 95% of them use it, for some very unique benefits. The DMA published some stats about the contribution of email, which, when you look at its economic contribution, it's significant and particularly when you look at the ROI, that's what businesses look at in terms of what medium they use to communicate with their customers. But you need to look beyond the marketing applications and look at how companies are also using email for

nonmarketing things, in terms of getting service notices, statements, things like that, out to their customers. It's how all of us transact business with partners, suppliers, and everyone else. I think at the end of the day, the medium absolutely has the potential to displace the U.S.P.S. and God knows with some of the postal rate increases we've recently seen, businesses need an alternative to the U.S.P.S. Email is also what really holds together E-commerce. Without it, you wouldn't have the ability to conduct E-commerce on the internet. And I think lastly, many companies are now fully dependent on email. They have optimized their operations around it, they simply can't revert back. So my point is, email is business critical. So why, then, is the killer app a shackled prisoner? I think because, despite these adoption stats, despite the contribution that email is now making, it's a troubled medium for all the reasons we've talked about here. It's in trouble because we've failed to solve the spam problem. Nine out of 10 emails for those who track those stats, are purportedly spam. Consumers still distrust it from what others have said earlier. Companies distrust email, too. 20% to 30% of your email -- is falsely intercepted as spam, you can't rely on it to be delivered to customers, contrast that with the U.S.P.S. There is no way that email can displace the U.S.P.S. when you look at the reliability of the medium itself. Of course, I think ISPs distrust companies that send email. The necessary result of all of this, the potential of email for business communication and commerce is still unrealized. And ultimately, I think that it's in this position, it's being held hostage because of our own, as an industry, our own inability to solve the problems and to work together to solve those problems in some fundamentally different ways. That's what I want to talk about. What will kill the killer app? In my mind, and Trevor Hue alluded to this yesterday, the measures being taken to

compact those. What will kill it is our own failings. I think the risks come in two fundamental areas. A failure to solve the problem through self-regulation, will invite government intervention. Hope not, but that's a risk. And our failure to find the right balance between security, protecting consumers, and the legitimate uses of email, ultimately impairs the medium for communication and commerce. But what I personally believe is that we're very close, dangerously close, to both of those potential options. What I would like to really talk about is the ways in which we kill the killer app off death row and that gets to something that this panel is all about and that's empowering the consumer in my mind. There are two potential ways of preventing that outcome. One is to inject some new thinking into the debate. Second, is to engage all the shareholders in the system, and that includes consumers, in a way that really preserves and protects it. I think as part of that we need to redefine the roles that each of us play. Senders, receivers, or ISPs, and consumers. I think ultimately, we play all three because probably every one of us in this room, if we work for a business, are in all three of those categories. So part of that new thinking in my mind is balancing the scales. We need to start becoming as concerned about the vitality of the medium as we are about its security. You know, there is a lot of talk about all of the things that we need to do to protect the medium from malware and from phishing and everything else, but we need to be weighing those actions against the consequences that it will have on the legitimate conduct of commerce. And I think we need to redefine what protection means. Yes, we need to protect the consumer against what's harmful and what they don't want, but we also need to protect their right to receive what is safe and also wanted. Something that I think we haven't discussed much is that we need to protect the commercial interest of

legitimate businesses who now are highly dependent on email for their communications and their livelihood in transacting business. So how do we do that? I think it starts, and again, alluding to some of the comments that Trevor made, with some new thinking and redefinition of what constitutes spam. I see it as two classes. There is the evil, which is stuff that's dangerous and criminal and doesn't conform to regulation and makes every attempt to evade detection, and there is the stuff that is bad. Email that doesn't -- that does conform to regulation may well be authenticated -- both are undesirable. We need to find ways to combat both of them. Stopping evil, everyone in this room would recognize as important to the security of the medium and restoration of consumer trust, it's what we do in applying those same tactics to the stuff that is bad, that puts us on the slippery slope of false positives and the reliability of the medium and that's what we need to start focusing on as well. part of that is in redefining the roles of the stake holders and determining how those different stake holders address those two classes of spam. That, I think, leads to the role of the consumer. You know, there is a lot of stuff we all do and say in the name of the consumer. But I don't really think their voice has been heard in this debate. We use a lot of proxies through technology, and I come from a high-tech company, to determine what consumers want or don't want in their inbox but I honestly don't think there is a technology solution for making that determination. And we need to move beyond that. And part of our attitude, I believe, around consumers, is that they are uninformed, or worse, that they are disinterested and needy. And we've taken a very paternalistic attitude towards consumers. And the survey that the ESPC conducted earlier this year suggests something entirely different. And that's what I would like to partly focus your attention on because I believe that the

engagement of the consumer is really critical to solving the problem. We found that they are much more savvy managers of their inbox than we previously thought. They do use the tools that are provided to them. 75% of them have used email for over 5 years. They are not novices. 80% of them check it daily. They may decide whether to open them or not based on reported spam, subject line, without opening them, 80% use the spam button if they don't know the sender. What's more important here is their willingness and ability to play a much more proactive role and what we did find, 53% want to have trust tokens, they need that to be able to make further determinations and decisions about what's safe to open and what's not. 90% want an unsubscribed mechanism right on the interface. 80% want a fraud button and 66% are willing to provide more than just a binary response on hitting a spam button as to whether it's spam but they are willing to provide feedback to the concerned on why it was determined as spam. I'm not suggesting here that there is not some use ability issues around how one would I am complement these things at the ISP but we need start looking at the consumer as playing a more proactive role particularly when it comes to sorting out the good from the bad. That has a real game changing -- potential. Why don't we leave it at that. (Applause)

>>RUTH YODAIKEN

We've got Jeffrey Fox up next and he'll present some new data that's not been released yet.

>>JEFFREY FOX

Good afternoon. This is now 10 years that I'm giving the FTC free advice. And I'm happy to see that they are still inviting me back for more visits. They have even taken some of it. This presentation, I'm going to mention, there is new

material here. If you didn't see it, there are copies on the table and also, if any media want to use any of this information, there is a media contact on the sheet if anybody wants to use it. So this is a little unusual because this summit is being held 3 weeks before we publish our annual cover story and package on this whole subject, so it came kind of at an awkward time for us but we decided to release some information from the September issue, which won't come out for a few more weeks, and incorporate it into my presentation, which is somewhat of a break with our usual practice in order to help the Commission. As you can see, I used your logo. I'll give you a quick background on our involvement in cyberspace in the last few years. Starting about 5 years ago Consumer Reports in addition to TV, car testing, that everybody loves, began testing protection software, first antivirus, then antispam, and more recently antispyware. Now we test them all every year. 3 years ago, seeing there was no independent source of national data about the impact and cost of these various things we've been listening to since yesterday we undertook the job of doing it ourselves and presenting it on an annual basis so these are kind of like annual benchmarks. We do our state of the net every year in our September issue. This is a nationally representative sample. This was last year's. As you can see, some of the major problems here, totaled more than \$8 billion in losses to consumers, both in repairs. I think in 1 case, one million consumers had to throw their computer out prompted by virus and spyware infections. So we talk about losses to bank accounts, these pump and dump scams but there are other losses besides what we've heard over the last couple of days. The 2007 version of this will be coming out shortly. The following trends that I'm going to present do incorporate the 2007 data as well as the data from the past surveys. A couple of

key questions that we're able to address in the data here, are consumers receiving more or less spam these days? How is the software holding its on? That's not from the survey, that's from our tests. On the one hand, in terms of, we've seen all the data about the actual rise in volume. It's about 90 plus percent of the volume out there, just a tremendous amount of spam circulating around. But over the 4 years that we've been conducting our survey the number of people that say they are getting a lot of spam, has been dropping. We attribute that both to improved practices by consumers as well as better filtering by internet providers. This is the one finding in this presentation that doesn't come from the survey. This is a summary of our spam blocking tests over the last 5 years. We started -- this is our fifth year. These are the number of email programs that we test and the number of that were like high passes. Compelled in certain categories -- excelling in certain categories. Over the first few years, if you look in the column on the right, which is the products most people buy, the spam blocks that you use with your email program, 4 years ago, one out of nine was a high pass. It's been improving up to last year. Last year to this year we see a little bit of a drop back. This is based on ratings that haven't been published yet so I can't give you the names of the products, you'll have to wait another 3 weeks for that but it looks like the antispam products, this is an arms race and they may be losing ground. Some other results from our four year analysis, good years and bad news, consumers are getting smarter about protecting their emails in their computers, for example, fewer are clicking on links in spam. I heard a complaint yesterday from a marketer about, you know, clicking on subscribed -- that's old fashion, like superstitious. These days you can trust mail. But, in fact, there is nothing to stop a phisher, for example, from sending a routine looking

mailing and when you look on the unsubscribed link, sending you to a website for download. I for the most part do not click on those unless I'm absolutely 100% certain where it's coming from. Fewer consumers are replying to spam, trying to stop spam by replying to it. I think these are responses to all the education that the FTC and us and a lot of other parties have been doing, educating people about managing. More people are using a spam blocker. We're up to 2/3 of people are using spam blocking on their home computer. And we're seeing an increased use of fire walls also over a few years ago. However, there are still millions of broadband users who aren't using fire walls. It's not 100%. Our consolidation is broadband users are very vulnerable to hackers. There is still a significant number, in the millions, who are not using fire walls. So this is good but the job is definitely not done. Some of the badges, many are still engaging in behaviors that help the bad guys. I know these little green bars look small but if you look at the note under here, because we used a base of around 78 million internet households, even that little green bar still represents half a million consumers that are admitting in our national survey that they patronize, that they bought a product or service based on a spam. So you can see, that's where some of the money is coming from to fuel these things. You see it's gone down but it's still significant.

And this is very important. Despite all the savvy we saw in the earlier graphs about people not replying and clicking on links, this is 8% of all the households. 8% of all people, period, gave information to phishing emails. That's huge. That suggests that people -- we need more education in that. Here are some recommendations. A record to different stake holders in this situation. Just to everyone. Our survey ruts show that education is working. Slowly. To change a

behavior of millions of people is a low process. It's working. I think we should build on it. And based on that response for phishing scams, clearly we need to put phishing scams front and center on our education campaigns. Most people are pretty familiar with the click on link issues. Other suggested ideas -- I personally don't see a presence of this kind of education in the place that is my family and my friends frequent. They don't go -- most don't know about on-guard online. We need to be in stores, computer stores. Public service announcements, and other type things, I think we need to step it up and make people more conscious of this stuff. I think we even need perhaps to find some way to attempt to get people to keep their protective software up to date a lot of people don't know, if you don't renew the contract it becomes relatively useless. Some suggestions for making -- (inaudible) I think in light of all the crime we're -- we're not talking that much about -- the bad guys who aren't actually criminals, but we don't consider, you know, to opt out the empowerment, that's -- legitimize spammers --[inaudible] Yesterday Rick Lane of News Corp suggested civil penalties for spammers. We're suggesting something a little more ambitious, which is to establish a private right of action. From these presentations, the bad guys way outnumber the good guys and it's time to start, you know, beefing it up. I don't think we'll get all of that money from law enforcement. Corporations and knowledgeable individuals, we might as well add to the population. There are a lot of knowledgeable people out there. Of course, we want the FTC to get all the resources possible, now that it can do more with the act, which we've endorsed for the last couple of years. Software manufacturers, we think adjusting some issues, making it user friendly. I don't know if you can read this. This is my award notification final notice, which I really wanted to read. When I went -- this

was from outlook, when I went to look at the header on there, to get a little information about it, I find, you know, and I've got decades of computer experience, this is really gobbledygook. Clearly, the better, more useful information we could give about the emails in their box. Other recommendations, fire walls. If you've never had a fire wall -- ever had a fire wall yell at you, trying to contact the internet, you want to okay this for ever after? I don't know how many people have a clue about whether to say yes but it should really tell you whether -- word, quicken, tell you what it's trying to do. We think the fire wall, there should be more information, looking at patterns, people behavior patterns. There is more that could be done there. We publish, and you can see the address if you want to read about it, windows outgoing fire wall has a problem. I've notified some people about this. We're waiting to see if it's going to be addressed. They say they are in the process of addressing this. It may go away, if it does, we'll let people know but we found it very difficult to be used effectively out of the box. ISPs and the internet community. We need authentication and to continue to work on an email devised 30 to 40 years ago. Never designed for the current circumstances. That's pretty much it. (Applause).

>>RUTH YODAIKEN

For people who don't know and there will be more discussion on this later, the on-guard and online, which he referred to, is the website WWW.ongardonline.com. That's a collaborative effort that the FTC has worked on with other entities to try to put good consumer information out there.

>>MILES LIBBY

I'm Miles Libby, Yahoo! Mail. We try to empower consumers -- so we host a wide variety of consumers across the world. We have more users not only in the U.S.

but also throughout the entire world. That means we have users like windows mom to the absolute tech know geeks in China, Korea, everywhere. I think one of the reasons why we've had that market success is because we take a very consumer eccentric approach to spam. Operationally, we define spam as whatever consumers do not want in their inbox. Every morning when I wake up, one of the very first things I do after giving my kids some breakfast is go and check email. The number of messages that a user sees in their inbox that they consider to be spam. We track that on a daily basis. We've been using these number of messages, spasms, from senders as a primary spam catching technique for a very long time. It's a reputation system that folks have been talking about all afternoon. So we frequently find a very high agreement among the community, but sometimes you can see different groups of people disagree with what the community thinks. For instance, Linda was talking just a moment ago about her experience with the Chico mail. Perhaps most users might think that the mail they receive from Chico isn't spam but Linda disagrees. Any time she would mark that message as spam, we would create filters in the background just for her so that the mail from Chico will arrive in her spam folder ongoing, but, for instance, my wife and I receive that mail and she wants it in the in box, she can do so. We do that behind the scenes without trying to make the consumer go through some arduous process of setting up filters or what have you. We've also developed a very extreme distaste for false positives. So we typically try to deliver all the spam that we get, and we'll tag that and put that into the user spam or junk folder. That way, they will have a chance to see -- if we do have a fast positive, consumer can go and see that message. We can override the setting for that user or update the entire community's view of the center's

reputation. The behind the scenes feature, a lot of time is spent on developing some user facing antispam features that you can interact with. We'll talk about all of these, one of my favorites is a product called -- (inaudible) the idea is you can great up to 500 different email addresses. As you're transacting online or surfing, whatever, you can make an address, gift out to that person, and if that address starts to attract spam you can simply throw it away never to be bothered with it again. We think this is a really powerful tool that consumers can use to help themselves and keep their inbox free of clutter. One of the other things we've seen over the last couple of years. The web has spent a lot of time focusing on how the companies can prove that it's Miles, for instance, logging into Yahoo. One of the things we're proud of, an idea that flips it on its head. The idea, how can a user prove that they are actually on Yahoo. Any time you sign into the Yahoo system, it will allow to you customize that log-in page, whether it's a picture or a favorite saying. Every time I log into Yahoo, I see a picture of my kids and so we know that since the bad guys don't have the picture of my kids, I can absolutely prove that it's Yahoo talking to me. I can feel safe and secure and type in my log-in credentials. We also spend a fair amount of time trying to pepper in throughout our email experience different tips for avoiding spam. This could be in the form of a dedicated site like a security center or an antispam resource center or help pages, or even product navigation, trying to make sure users know what to expect and do and do not do on the web. So I've listed a couple of these things. Mar go before mentioned, she thought this spam button was the most useful technology invented in a long time. I agree with her. It's one of the things that we think is immense valuable feedback for us and I certainly encourage all users to use that button to their advantage.

Thank you very much. (Applause)

>>RUTH YODAIKEN

Okay. You talked about a bunch of things. Let's start on an issue that you raised, and we've all talked about -- you've all talked about to different degrees, we talked about the responsibility of the consumer versus the burden on the consumer. Linda, you talked a bit about how it's a lot for consumers to go and read the information they need to know, or to update their antivirus software, and Dave, you talked about how the consumer is really sophisticated and could give a lot of feedback, in terms of, not just this is spam, but a little bit more in terms of, well, really it's not spam, it's just a catalog that I just don't want to see right now and I'm trying to get it out of my inbox. Linda, we'll start with you and maybe walk down and see who wants to talk about the burden versus the responsibility.

>>LINDA SHERRY

Yeah. I've talked to various people. I kind of have my touchstones, my mother but other people that are not very technologically savvy. I've talked about for instance, filtering emails. They have no idea what that is really, a lot of them. So, for instance, if I wanted to make sure all of my Chico things go into one Chico's folder, I can do that and look at it or not look at it, or erase all in one fell swoop but for some reason these kinds of basic messages, about the tools that are out there are not reaching consumers. I that I perhaps, these are captive consumers. These are your customers. Either they own one of your computers or they use your ISP, and I'm just thinking that can't you build in sort of reports. You know how American Express gives you at the end of the year, will line up everything that you've spent in different categories and give you this lovely report. Couldn't you do this periodically with consumers? Instead of some

pointless little pop-up box, it's popping up a useful maybe PDF, they could click on it or something, report, that would basically say to them, give these people information, these consumers information about, what are they actually doing online? For instance, I mean, your fire wall is set at off. You never -- you've not reported any spam messages this quarter. You know, the following authenticated senders have sent you email this quarter. Give their names. Authenticated by -- give the little -- give the URL where they can go and see the authentications companies. You have received email from the following unauthenticated mailers this year. Let's empower consumers with information that they can really use that's quick, and not too long and involved, but something that they can actually kind of at a glance look at and learn to expect, and learn to look for periodically, and to use the information.

>>RUTH YODAIKEN

So create a dialogue. Dave, does that work a little bit with some of the stuff that we talked about?

>>DAVE LEWIS

It does. It does. I think the point I was trying to make relative to consumer empowerment is I think we've had a certain mindset around what the consumer needs and wants. And at least with the ESPC survey we're beginning to challenge some of those underlining, preconceived notions. I think the behavior of consumers, demands like Yahoo, AOL, use of the spam button, and what I talked about in terms of their desires to have additional tools at their disposal, that would allow them to manage their inbox, there are a high percentage of consumers that are willing -- they are not only able to use the tools but willing to use the tools. To your question about, what is the responsibility of the consumer

when it comes to these things? I think we should recognize the limitations of technology. That's partly what I'm saying here. Even from a high-tech company, I'm saying that. We need to hear that consumer voice more directly and in a less ambiguous way. My belief is that if that voice comes through, what we now see as bad mail, not the evil stuff, if those marketers run the risk of being blocked from the medium that their customers prefer, and they know why they are being blocked by that consumer, and frankly, those consumers may be more compacting than the ISPs themselves, you will affect behavior change. That's my point.

>>RUTH YODAIKEN

Let me ask a follow-up question on that. On that, in terms of -- aren't there already ways, in terms -- if you're business email is being blocked isn't that because a lot of consumers have reported it as spam?

>>DAVE LEWIS

Not always, that's part of the problem. In many ways these filters are based on a panel, based on more blunt instruments like content, that have been collected by spammers, so legitimate markers use it when their mail is intercepted, regulated to the spam folder. The filters being used are based on more than just what the consumer has to say and that's partly my point. Figure out what's malicious and let the ISPs deal with that but empower the consumers with the tools so they can more effectively manage those things themselves.

>>MALE SPEAKER

I think this speaks to the relationship between the consumer and the ISP. I mean, the consumer is the customer. They are paying the ISP to deliver, and I think the ISP know where their money is coming, from their paycheck comes

from. I would think it would behoove the ISP themselves, I don't know if you've done it to find out from their customers if this is what they want. Because I don't think that the ISPs are there primarily to serve the sender. I think they are there, who aren't paying them, they are there to serve the receivers, but the receivers are not being well served by the current system. The ISPs should demand how the market should work.

>>RUTH YODAIKEN

Miles?

>>MILES LIBBEY

We need to make sure we're use -- it means delivering the messages that the users do want in their inbox and that they don't want into their junk folder or not at all. You can use that seat back mechanism to help us say, I really want that Chico's mail in my inbox.

>>RUTH YODAIKEN

You've got a lot of stuff coming in, directed at the consumers. And you're blocking as much of it as you can that's bad and you rely on some consumer interaction, and when you get this important, you know, clicks from consumers to say this is spam, that helps you make your decisions about how to go forward, and there is a relationship there. Is there any need for a relationship that goes further back where you're contacting the businesses and giving them what I think to be hearing from Dave is a little more feedback on, you know, what's happening?

>>MALE SPEAKER

I think there has been a lot of collaboration efforts in the last several years with the ISPs and senders. In the last 18 months, I think a lot of ISPs have begun to

use feedback loops. A fair amount of time working on ways to standardize that feedback. The reporting feedback protocol and more and more ISPs are starting to use that to be able to send -- to send complaints back to the sender.

>>RUTH YODAIKEN

Okay. Jeff, I wanted to jump in and ask you a question. You had done a little work on some of the protective measures that consumers have in terms of, not just how they respond to email but how they try to keep their antivirus software going and so forth like that. Can you tell us a little bit about some of the choices that consumers need to make, and some of the factors they need to consider.

>>JEFFREY FOX

Yes, I spoke with an engineer who has been testing the software for years. A lot of consumers don't know that if they don't renew the annual fees that the thing becomes, you know, eventually ineffective and many people used to buying a word processor, which is basically good for ever. Another thing he suggested, because there are compatibility issues and conflicts on different products, at this point it's probably best for the consumer to go for a Suite and use the fire wall from the Suite rather than the operating system. It's not only simpler but pretty much guarantees everything will work together in a nice way. He has seen some cases where even one manufacturer themselves wouldn't allow their antivirus and their anti spyware software to operate side by side, as independent products. If you wanted both of those functions you had to uninstall each of their products and then get their Suite. In this case, they actually were willing to send the Suite as a replacement for free but it was kind of odd that even with the same manufacturer products wouldn't work together. A number of other problems, using anti spyware or antivirus, there are ways to use these things together but

you have to know which most people don't.

>>RUTH YODAIKEN

Let me ask anyone who wants to jump in, Miles, I thought of you because you guys actually tried to get your customers to update their antivirus and to use antivirus software. How does the consumer really know what they should be doing? Who should they turn to in terms of trying to figure out what protective measures they should be taking.

>>MALE SPEAKER

This is something everybody should share. Whether it -- I think we all have a role to play in helping to educate the consumers about what they should be doing or they shouldn't be doing.

>>MALE SPEAKER

I would agree with that completely. It is a shared responsibility. But you need to be balancing that as you balance, you know, security versus commerce issue. You need to be balancing the educational process that needs to occur with, you know, consumers continued trust and use of email as well. So you don't great an alarm.

>>FEMALE SPEAKER

Right.

>>MALE SPEAKER

I think it's how it's done. But fundamentally, I think one of the messages that we have not well communicated is that when it comes to protecting your identity, protecting your assets and all of those types of things, through email or through any other online activity, you as a consumer have a responsibility. And that message needs to be conveyed, too, along with how you exercise that

responsibility prudently.

>>RUTH YODAIKEN

Let me just ask you a question about, well, while we're on this, about the business consumer interaction and pointing out here that a lot of businesses are consumers. And from that end, are there special steps that businesses, as consumers, should be looking at? There was a lot of talk yesterday about servers, email servers being compromised, and businesses as well as consumers need to take what steps they can to make sure that everything is protected and that people use basic safe precautionary measures. I saw an article recently which talked about complacency of staff. Very often when you're in a business situation, the staff might say, well, our technology department is going to take care of that, so their habits in terms of email use and surfing and so forth, was different.

>>MALE SPEAKER

I think all of us are in all three roles in my mind. There isn't a sender, receiver, consumer role that any of us play. We're all kind of in all three camps in most instances. I think the biggest challenge we face, authentication is a good example, is on both the receiving side and the sending side, when you get down to the smaller entities, it's extremely tough. Okay? So, you know, we've got to maybe create some business opportunities around, taking it to the lower end of the market, where the fat part of the pyramid is and where the bigger risk is. In terms of finding ways in which to allow those things to be implemented because our company, for example, I mean, we authenticate out our email but we're not as careful on the inbound. So what does that permit to have happened? Things to sneak into our corporate environment, and, you know. Inadvertently access

critical data. The same is true with a lot of companies. You see the compliance more on the outbound sending of email than you do on the inbound. We need to look at it on both sides.

>>RUTH YODAIKEN

Anybody want to add anything on that? Miles?

>>MILES LIBBEY

Sure. I would recommend for businesses to authenticate your mail. Take advantage of all the feedback that is available, the ISPs, every time that a business sends an email, they are putting their reputation on the line, whether they know it or not so the feedback loops are a great way to start to get an understanding of how consumers view their mail and how they can take both reactive and proactive measures to protect that reputation. There lots of infrastructure hygiene that you can have but that would be a whole other panel, I would think. Like everyone else we have our own IT department. It's good to have centralized control to be responsive to the individual user. Some people don't want certain things. If you have a one size fits all, that will be a problem for your staff.

>>RUTH YODAIKEN

You work with organizations in terms of training and some issues they may face in terms of their system. Is there anything you want to add or is there anything --.

>>LINDA SHERRY

I think what happens with a lot of nonprofits, something bad will happen to a group, with, say, a small network, a virus will come in, it will shut down the computers. They will have to rush all over to fix it and then they will come down heavy with new rules which means nobody can check their Verizon email or

something from work. Then it does also cause sort of a backlash with staff. So it's a very key thing. People, you've got to train your employees not to be complacent about the fact, just because they are at work they think there is some excellent security system in place so they can go visit some, you know, questionable website. But on the other hand, you've got to somehow balance these things so you don't have a lot of disgruntled employees who can't do a simple thing on their lunch hour like check their web mail.

>>RUTH YODAIKEN

You raised this in your presentation. You talked about defaults, and how there is no standardization in terms of that. I know, Dave, you've also talked about defaults -- well, I'll use the term defaults, but in terms of companies and the different ways they try to reach their customers, and how everybody has got different practices, in terms of the bank saying I will only reach you this way or different businesses say I'm going -- you know, to help their customers recognize when it's really them or when it's not, and in terms of the setting, just a standard thing. Can you talk a little bit about that?

>>LINDA SHERRY

The first thing is, there are so many different places in the computer space and in the email space where you need to make settings. There is the browser, there is the computer. There is perhaps you've got to go on to the website of the Yahoo or whoever provides your email. So there are all of these different places and it's very hard for consumers to actually -- I think we need to really work hard to either give them a checklist of some kind or even, I was noticing even on-guard online, which has some great recommendations to people and very clear recommendations of how to change different settings, your fire wall, et cetera, on

your different systems but I was noticing there were plenty of them. How can we get to something that, if not standardized, at least in a central place where consumers will know about it, where they can actually go and have a centralized checklist to know what they need to do? The downside of not setting the default in a protective manner, Microsoft saw a few years ago when they had that virus come in that no one's firewall was on, and boom. The first thing they did was to do the service pack and then tell everyone, and then every new computer that was shipped out after that had the fire wall on by default. You know, you don't want to have to wait until something awful happens. There is always a way to set the default at the most protective level and let consumers know this is at the highest level. If you want to go down, you can, that's your choice but we don't recommend it.

>>RUTH YODAIKEN

So the difference being, instead of the way it is now, having kind of a government offered or consumer group offered information packet saying these are the things you need to look at, maybe still having that information, but that information would be more, your default from your companies are more and more set at a very high setting, and if you want to play around with this, these are the things that you should look at.

>>LINDA SHERRY

I think we have to set them at the highest protective level because what is the other option? Set it at the lowest and let the consumer set them higher if they want? I don't think we can necessarily -- the consumer doesn't have that much knowledge at this point in time and as far as working with all the different players and stake holders, I do notice and I'll say it again and I sound like a broken

record but the consumers groups are being left out of this conversation to some degree. I really think we need to get them to the table. We're at the table with phone companies, banks, et cetera, we need to get to the table with the ISPs and consumers.

>>MALE SPEAKER

I wouldn't agree with Linda on the default setting.

>>RUTH YODAIKEN

Why don't you tell us why.

>>MALE SPEAKER

The reason is, we underestimate the sophistication of consumers. That was the point of the study, is to really understand where they are at in their ability and their willingness to deal with some of these issues. But there is no denial that the structure of our industry itself inhibits a lot of the solutions that we all think need to be implemented. We're talking about a very fragmented environment on both the sending and receiving side. So it's difficult to be talking about more than just point solutions. That's why I think having things like some of the things mentioned in the last panel are important.

>>RUTH YODAIKEN

Okay. So we've got just a few minutes -- we don't -- I thought we bumped the time. Okay. Apparently we don't have any time for questions. Thank you all, thank you, panelists, very much. (Applause) We're taking a quick break. How long? Back at 3:00. Thanks.