56th Annual Meeting of the International Whaling Commission; to the Committee on Foreign Relations.

ADDITIONAL COSPONSORS

S. 1411

At the request of Mr. KERRY, the names of the Senator from Vermont (Mr. LEAHY) and the Senator from Rhode Island (Mr. REED) were added as cosponsors of S. 1411, a bill to establish a National Housing Trust Fund in the Treasury of the United States to provide for the development of decent, safe, and affordable housing for low-income families, and for other purposes.

S. 1890

At the request of Mr. ENZI, the name of the Senator from Maryland (Ms. MIKULSKI) was added as a cosponsor of S. 1890, a bill to require the mandatory expensing of stock options granted to executive officers, and for other purposes.

S. 2313

At the request of Mr. GRAHAM of Florida, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of S. 2313, a bill to amend the Help America Vote Act of 2002 to require a voter-verified permanent record or hardcopy under title III of such Act, and for other purposes.

S. 2338

At the request of Mr. BOND, the mane of the Senator from Indiana (Mr. BAYH) was added as a cosponsor of S. 2338, a bill to amend the Public Health Service Act to provide for arthritis research and public health, and for other purposes.

S. 2340

At the request of Mr. BINGAMAN, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of S. 2340, a bill to reauthorize title II of the Higher Education Act of 1965.

S. 2412

At the request of Mr. BOND, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 2412, to expand Parents as Teachers programs and other programs of early childhood home visitation, and for other purposes.

S. 2526

At the request of Mr. BOND, the name of the Senator from Virginia (Mr. WARNER) was added as a cosponsor of S. 2526, a bill to reauthorize the Children's Hospitals Graduate Medical Education Program.

S. 2568

At the request of Mr. BIDEN, the names of the Senator from Delaware (Mr. CARPER) and the Senator from Illinois (Mr. FITZGERALD) were added as cosponsors of S. 2568, a bill to require the Secretary of the Treasury to mint coins in commemoration of the tercentenary of the birth of Benjamin Franklin, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LEAHY:

S. 2636. A bill to criminalize Internet scams involving fraudulently obtaining personal information, commonly known as phishing; to the Committee on the Judiciary.

Mr. LEAHY. Mr. President, today I am introducing a bill, the Anti-Phishing Act of 2004, that targets a large and growing class of crime that is spreading across the Internet.

Phishing is a rapidly growing class of identity theft scams on the Internet that is causing both short-term losses and long-term economic damage.

In the short-term, these scams defraud individuals and financial institutions. Some estimates place the cost of phishing at over two billion dollars just over the last 12 months.

In the long run, phishing undermines the Internet itself. By making consumers uncertain about the integrity of the Internet's complex addressing system, phishing threatens to make us all less likely to use the Internet for secure transactions. If you can't trust where you are on the web, you are less likely to use it for commerce and communications.

Phishing is spelled ''P-H-I-S-H-I-N-G.'' Those well-versed in popular culture may guess that it was named after the phenomenally popular Vermont band, Phish. But phishing over the Internet was in fact named from the sport of fishing, as an analogy for its technique of luring Internet prey with convincing email bait. The ''F'' is replaced by a ''P-H'' in keeping with a computer hacker tradition.

Phishing attacks usually start with emails that are, in Internet jargon, ''spoofed.'' That is, they are made to appear to be coming from some trusted financial institution or commercial entity. The spoofed email usually asks the victim to go to a website to confirm or renew private account information. These emails offer a link that appears to take the victim to the website of the trusted institution. In fact the link takes the victim to a sham website that is visually identical to that of the trusted institution, but is in fact run by the criminal. When the victim takes the bait and sends their account information, the criminal uses it—sometimes within minutes—to transfer the victim's funds or to make purchases. Phishers are the new con artists of cyberspace.

To give an idea of how easy it is to be fooled, we have reproduced some recent phishing charts, with the help of the Anti-Phishing Working Group. These are just two examples of a problem that affects countless companies. The website on the right is an actual website of MBNA, a well-established financial institution and credit card issuer. On the left is a recently discovered phishing site that mimicked the MBNA site.

As you can see, the two websites are practically identical. Both have the MBNA logo, and both have the same graphics, in the same layout. But if you end up going to the website on the left, when you enter your account information, you are giving it to an identity thief.

As another example, the next two websites both appear to be from eBay. Again, the one on the right is from the genuine website. The one on the left is a fake website that is controlled by a phisher. As you can see, if you end up at the website on the left, it would be next to impossible to know that you are not at the real eBay website. Informed Internet users can avoid this problem if they simply use their web browser to go to the website, instead of using a link sent to them in an email, but far too many people do not do this.

This is a growing problem. Phishing is on the rise. In recent months there has been an explosion of these types of attacks. As you can see from the next chart, these attacks are growing at an alarming rate. Roughly one million Americans already have been victims of phishing attacks.

And phishing attacks are increasingly sophisticated. Early phishing attacks were by novices, but there is evidence now that some attacks are backed by organized crime. And some attacks these days include spyware, which is software that is secretly installed on the victim's computer, which waits to capture account information when the victim even goes to legitimate websites.

Phishers also have become more sophisticated in how they cast their huge volumes of email bait on the Internet waters. Security experts recently discovered that vast networks of home computers are being hijacked by hackers using viruses, and then they are rented to phishers—all without the knowledge of the owners of these home computers.

Some phishers can be prosecuted under wire fraud or identity theft statutes, but often these prosecutions take place only after someone has been defrauded. Moreover, the mere threat of phishing attacks undermines everyone's confidence in the Internet. When people cannot trust that websites are what they appear to be, they will not use the Internet for their secure transactions. So traditional wire fraud and identity theft statutes are not sufficient to respond to phishing.

The Anti-Phishing Act of 2004 protects the integrity of the Internet in two ways. First, it criminalizes the bait. It makes it illegal to knowingly send out spoofed email that links to sham websites, with the intention of committing a crime. Second, it criminalizes the sham websites that are the true scene of the crime.

It makes it illegal to knowingly create or procure a website that purports to be a legitimate online business, with the intent of collecting information for some criminal purpose.

There are important First Amendment concerns to be protected. The Anti-Phishing Act protects parodies and political speech from being prosecuted as Phishing.

We have worked closely with various public interest organizations to ensure that the Anti-Phishing Act does not impinge on the important democratic role that the Internet plays.

To many Americans, phishing is a new word. It certainly is a new form of an old crime. It also is a serious crime, and we need to act aggressively to keep phishing from infecting the Internet and from eroding the public's trust in online commerce and communication. I look forward to working with others in the Senate in addressing this growing threat to the Internet, with effective and responsible action.

Again, this is called the Anti-Phishing Act. It targets a large and growing class of crime that is spreading across the Internet.

Phishing is a rapidly growing class of identity theft scams. It causes both short-term losses, but long-term economic problems. In the short-term, these scams defraud individuals and financial institutions.

To give some idea that this is not a minor matter, some estimates place the cost of phishing at over $2 billion over the last 12 months. You can imagine the outcry in this country if they said we had $2 billion worth of bank robberies in that same period of time. But it is not only the economic loss that undermines the Internet itself; it makes consumers uncertain about the integrity of the Internet's complex addressing system. It makes us all less apt to use it for commerce and communication, because if you cannot trust where you are on the Web, you are not going to use it for commerce or communication.

Incidentally, fishing is spelled P-H-I-S-H-I-N-G. Those who are well versed in popular culture might think it was named after the phenomenally popular Vermont band called Phish. But phishing over the Internet was named for the sport of fishing, as an analogy for its technique of luring Internet prey with a convincing e-mail bait. The ''F'' was replaced by ''PH'' in keeping with computer hacker tradition.

Phishing usually starts with e-mails that are, in Internet jargon, ''spoofed.'' They appear to come from some trusted commercial entity or financial institution. The spoofed e-mail asks the victim to go to a Web site and confirm their identity, in effect, their Social Security number, credit card numbers, and so on. What it does is, the victim thinks they are going to a trusted institution, perhaps one they have dealt with for years. Instead, it takes them to a sham Web site that is visually identical to that of the trusted institution, but it is run by a criminal. When the victim takes the bait, when they send their account information, of course, the criminal uses it. Sometimes they use it within minutes. They can transfer the victim's funds or make purchases. These phishers are new con artists of cyberspace.

I will give you an idea of how easy it is to do it. Here on this chart we have the genuine Web site. We actually had to mark them as ''genuine Web site'' and ''fake Web site'' because they look so identical. I am a heavy user of the Internet, and I could not tell them apart. On the other side, of course, is the fake Web site. They both have the MBNA logo. That is a trusted financial institution. They have the same graphic layout.

Suppose you were a customer of MBNA and they asked you to put your user name in, your password, and so on, and you go on there and they would continue to ask information. You would have given up your account number, whatever ID number you use, and it could be 20 minutes later, when you go on the right site and you want to withdraw some money or make a cash transfer, you may find it is all gone in that short time.

In fact, we also have a chart for eBay. I wasn't going to show it, but it is worthwhile, I think. We will show the two from eBay. Again, I have had them marked ''genuine Web site'' and ''fake Web site.'' Here is the genuine one. For those who use PayPal, it is increasingly used if you are using eBay. Anybody who has done that is well aware of PayPal. It is something you could be safe with, you know where your money is going, you know who is handling it, and you know you are going to get paid for something you might have sold.

Look what we have here. When you look at it, it is hard to tell the difference. Of course, the internal address is different. What do you do? You send money, you pay money, you are supposed to receive money. You are not going to do it. Somebody else is going to do it and they are going to walk off not only with your money but with your trust of the Internet.

That is why it is important that we do this, that we have some way of criminalizing this. We have in every one of our States businesses that thrive and survive because they can use the Internet. This is trying to stop them. Again, we must address this growing threat to Internet users.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 402—EXPRESSING THE SENSE OF THE SENATE WITH RESPECT TO THE 50TH ANNIVERSARY OF THE FOOD AID PROGRAMS ESTABLISHED UNDER THE AGRICULTURAL TRADE DEVELOPMENT AND ASSISTANCE ACT OF 1954

Mr. HARKIN (for himself, Mr. COCHRAN, Mr. ROBERTS, Mr. DASCHLE, Mr. CRAPO, Mr. FITZGERALD, Mr. CONRAD, Mr. COLEMAN, Mr. LEAHY, Mrs. LINCOLN, Mr. KOHL, Mrs. CLINTON, Mr. JOHNSON, Mr. DORGAN, Mr. LUGAR, and Mr. DAYTON) submitted the following resolution; which was considered and agreed to:

S. RES. 402

Whereas, in the aftermath of the Second World War, many countries did not have sufficient cash to buy the agricultural commodities needed to feed the people of those countries, especially in war-torn Europe and Asia;

Whereas, during the term of President Dwight David Eisenhower, it became apparent that the abundance of food available in the United States could be used as an instrument in building a durable peace after the Second World War;

Whereas a concessional credit program was established under title I of the Agricultural Trade Development and Assistance Act of 1954 (commonly known as ''P.L. 480'') (7 U.S.C. 1701 et seq.), signed into law on July 10, 1954, to allow for sales of agricultural commodities from the United States to developing countries for dollars on generous credit terms or for local currencies, with proceeds to be used by participating governments or nongovernmental private entities to encourage economic development;

Whereas since the enactment of the Agricultural Trade Development and Assistance Act of 1954, the title I program has facilitated sales of agricultural commodities from the United States, totaling an estimated $30,000,000,000 to nearly 100 countries;

Whereas the Food for Peace program was established under title II of the Agricultural Trade Development and Assistance Act of 1954 (7 U.S.C. 1721 et seq.), to provide humanitarian assistance to poor and hungry people in developing countries, based on legislation originally introduced by Senator Hubert Humphrey;

Whereas during the half-century since the establishment of the Food for Peace program, the United States Agency for International Development and the Department of Agriculture have worked together to provide 107,000,000 tons of food aid to developing countries, helping an estimated 3,400,000,000 people through 2003;

Whereas the government of the United States has depended on the commitment, skill, and experience of dozens of private voluntary organizations based in the United States, as well as the United Nations World Food Program, to carry out the Food for Peace program on the ground in developing countries; and

Whereas a number of countries that were early beneficiaries of both programs have emerged as democracies and strong commercial trading partners, including South Korea, Taiwan, the Philippines, Thailand, Malaysia, Singapore, Mexico, and Turkey, in part as a result of development projects and food distribution programs conducted using agricultural commodities from the United States: Now, therefore, be it

Resolved, That the Senate—

(1) on the 50th anniversary of the date of enactment of the Agricultural Trade Development and Assistance Act of 1954 (7 U.S.C. 1691 et seq.) on July 10, 1954, recognizes the United States Agency for International Development, the Department of Agriculture, and associated partners for—

(A) providing emergency food assistance to address famine or other extraordinary relief requirements;

(B) forging linkages between the abundance of food produced under the agricultural system of the United States and people in need of assistance throughout the world;

(C) undertaking activities to alleviate hunger;

(D) promoting economic, agricultural, educational, and community development in developing countries;

(E) identifying the private partners capable of carrying out the mission of the programs established under that Act;