

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 name 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.

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.

#### STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LEAHY: