Testimony of David Jevans

PHISHING EMAIL FRAUD

Greetings Commissioners:

I have been asked today to provide insight on the problem of email "phishing" fraud, and its impact on senior citizens as they get online and increase their use of the Internet. First, I'd like to start out with a definition of "phishing".

Phishing is a hacker term for a particular type of email fraud. This fraud is perpetrated by email scammers and spammers. Typically, a spam email is sent to random users of the Internet, pretending to be from a legitimate bank, Internet Service Provider ("ISP"), e-commerce company or government agency. This email looks exactly like an email that you would expect to receive, complete with the email address, logo and other branding elements of the legitimate website.

However, the email is not really from who it says it's from. It's from a fraudster who is luring the consumer to a fake website, in order to trick them into revealing their credit card details, bank account information, online banking password or other personal identity information.

Last summer, the FBI termed phishing "the hottest, and most troubling, new scam on the Internet." Indeed, reports of email phishing attacks jumped over 400 percent during the 2003 Christmas holiday season, according to the most recent analysis by the Anti-Phishing Working Group. Worse, the increasing realism of the phishing messages - including logos and professionally designed forms for entering credit card information and bank account data - have made them ever more successful, with an average positive response rate of between 1 and 5 percent of those who receive them.

Phishing attacks are increasing in frequency, scope and sophistication. Recently, Citigroup, Lloyds TSB and Barclays Bank have been subjected to phishing attacks that spoofed their identities in pursuit of customer's account, debit and credit card data. Within the last year, Wachovia, Bank of America, US Bank, Bank of Montreal, Westpac Bank, and the ANZ Bank of Australia, have been hit by phishing scams. Although financial services firms were obvious initial targets for phishing attacks, adept identity theives have expanded their phishing operations to exploit a number of Internet consumer brands and government agencies including Yahoo!, eBay, Paypal, Monster.com, Bestbuy.com, Microsoft MSN and even the FDIC.

The term "phishing" comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users. The first mention on

the Internet of phishing is on the alt.2600 hacker newsgroup in January 1996, however the term may have been used even earlier in the printed edition of the hacker newsletter “2600”.

"Ph" is a common hacker replacement for "f", and is a nod to the original form of hacking in the early 1970s, known as “phone phreaking”. This is in fact the origin of a lot of the "ph" spelling in many hacker pseudonyms and hacker organizations.

By 1996, hacked accounts were called "phish", and by 1997, there is evidence that “phish” were actually being traded between hackers as a form of currency. For example, people would trade 10 working AOL phish for a piece of hacking software that they needed.

Over the years, phishing attacks grew from simply stealing AOL dialup accounts into a more sinister criminal enterprise. Phishing attacks now target users of online banking, electronic payment services and online e-commerce sites.

Phishing scams are of particular concern to the Senior community. A recent survey by Nielsen/NetRatings indicates that those 65 and older are the fastest growing group online, increasing their presence on the Internet by 25% in 2003. These consumers are new to the Internet, as such, are not educated about the new dangers of phishing fraud.

Another significant demographic fact is that persons over the age of 50 control at least 70% of the nation's household net worth. It is estimated that the elderly will control approximately $10 trillion in assets within the next 10 years. Because phishing is a financial crime, seniors make particularly appealing targets. Fortunately, it is still difficult for phishers to target seniors specifically, however there are email databases available on the Internet that are used by spammers for sending spam. These databases often do categorize email addresses by the interests of each consumer. They get these categorizations by harvesting email addresses from newsgroups and mailing lists that cater to particular interests. Thus it is feasible for a phisher to obtain or derive a list of email addresses that could be used for more targeted attacks. However, they do not need to do so, as a spam-like broadcast of a phishing email to millions of email addresses will reach many seniors.

The senior population make appealing targets, and should be particularly careful of phishing attacks, because they potentially have the most to lose. If a banking or investment account were to be compromised, a phisher would have access to significant assets. Also, if personal identity information such as a social security number is obtained by a phisher, then the criminal can apply for bank loans or credit cards using the identity of the consumer. Because many seniors have good credit ratings and more sizeable assets, the phishers will be able to obtain larger loans and credit limits.

The challenge for seniors, and in fact for most consumers, is that phishing attacks are increasingly sophisticated, and difficult to discern from legitimate emails. I recommend

that consumers exercise caution when they receive any email that requests personal identity or financial information, or that takes you to a website that requests such information. Because the sender can be faked in email, consumers cannot trust that an email was sent to them from their bank, ISP or an e-commerce site just by looking at the "From:" field in the email.

Here are some recommendations for consumers to protect themselves:

- You should examine the web address (or "URL") of any web page that you are taken to by an email. If that web page address does not match the web address that you are used to, be very suspicious.

- In my experience, I have almost never seen a legitimate reason for a web site to ask for a Social Security Number. Any site or email that asks for this information should be regarded with great suspicion.

- Similarly, there is no reason for any site to request your ATM PIN. Any site that requests this is fraudulent.

- If you receive an email purporting to be from a company, bank, or even government agency that you do not do business with, and this email requests personal identity or financial information, be extremely suspicious. There have been instances in recent months where emails were sent out purporting to be from

the FDIC or from Regulations.gov government agencies. These emails have used scare tactics to frighten consumers into divulging personal information. Such phishing emails suggest that a consumer's bank account has been compromised by crooks or terrorists, and the consumer should enter their bank account information for verification, or risk having their bank account frozen.

- Consumers should use anti-virus software and keep it up to date. Use the software not only to protect from inbound viruses, but also to do a weekly scan of your hard disk for any viruses or Trojans that may have slipped through the anti-virus filter.

- Keep your computer's software up to date with the latest updates from Microsoft. There are new updates issued by Microsoft every week or two, and they are mostly to fix newly discovered security problems that phishers could exploit.

The "Anti-Phishing Working Group" has been organized to develop an acceptable solution to email phishing scams. This is an organization of over 180 members from financial institutions, ecommerce providers, ISPs, law enforcement agencies and software vendors. I am the Chairman of the organization, and a Senior Vice President at Tumbleweed Communications, a vendor of secure email and anti-spam technology. The goal of the Anti-Phishing Working Group is to provide resources, technology, vision and expertise to facilitate the rapid deployment of a solution to email phishing scams.

The Anti-Phishing Working Group has established the www.Antiphishing.org website as a repository of information about phishing. The site contains a news feed of articles about phishing, as well as an ever-expanding archive of known phishing attack emails and websites. Proposed technical solutions, lists of vendors and government agencies who can help combat phishing are also listed.

The working group members are exploring technology solutions to allow businesses to authenticate, or digitally sign, their emails to their customers. These techniques would allow consumers to determine that the sender of an email was really who they purported to be. Other technology solutions being tested include detection and scanning services to monitor attacks as they happen.

Members of the Anti-Phishing working group are working together to develop educational messages and best practices for consumers and companies. The Anti-Phishing working group is working with other organizations that are working on combating Internet fraud including the Bankers Information Technology Secretariat (BITS) and the Information Technology Association of America (ITAA). Consumers should also be aware that the Federal Trade Commission (FTC) and U.S. Department of Justice (DOJ) have advisory bulletins and other information available on their websites.