

Anti-Phishing Consumer Protection Act of 2008

What is phishing?

Phishing is a method of online identity theft that takes the form of fraudulent emails or fake websites, purporting to be from a legitimate business, but is actually used to deceive the recipient into giving personal or financial account information. In November 2007, the Anti-Phishing Working Group found that 178 corporate identities and brands were hijacked and used for phishing scams, which is the highest number ever reported.

Approximately 59 million deceptive phishing emails are sent per day and as many as 10 million of them are opened by recipients. As a result, between August 2006 and August 2007, more than 3.5 million Americans were victims of phishing scams and suffered losses totaling \$3.2 billion.

In addition to victimizing unsuspecting consumers, phishing scams maliciously exploit the trust legitimate businesses have worked so hard to establish with consumers. According to a 2007 Javelin Strategy & Research study, 80 percent of Internet users are concerned about being victims of online identity theft and many of these consumers are hesitant to conduct online transactions. From a business perspective, a 2006 Zogby Interactive poll of found that 78 percent of small business owners polled stated that a less reliable Internet would damage their business.

What does the legislation do?

The “Anti-Phishing Consumer Protection Act of 2008” would prohibit the practice of phishing as well as related abuses, such as the practice of using fraudulent or misleading domain names, which are commonly used by phishers, by defining them as deceptive practices under the Federal Trade Commission Act.

Additionally, the legislation seeks to solidify the integrity of domain name registration, a long-time goal for the Federal Trade Commission, by making it illegal for a domain name registrant to provide false or misleading identifying contact information in the WHOIS database when registering a domain name. Too often law enforcement officials have been hindered in their pursuit of phishers and other online scams because the person responsible is hiding behind the anonymity of false registration information—this legislation would put an end to that practice by requiring accurate registration information about those that own websites and domain name that are used to harm consumers.

A recent phishing scheme

Last month, the IRS issued another warning about phishing scams. This time involving real-looking e-mails aimed at getting recipients to offer up financial and personal data on fake IRS Web sites by saying the target is eligible for a rebate check. So the threat is real and all Americans that have an email address are constant targets.