PLUGGING THE "PHISHING" HOLE: LEGISLATION VERSUS TECHNOLOGY

ROBERT LOUIS B. STEVENSON[1]

ABSTRACT

This iBrief analyzes the Anti-Phishing Act of 2005, legislation aimed at curbing the problem of "phishing." Phishing is the sending of fraudulent emails which appear to be from legitimate businesses and thereby fooling the recipients into divulging personal information such as credit card numbers. While this legislation may provide some assistance in the fight against phishing, it is limited by the global nature of the Internet and the ease with which phishers can hide and avoid judgments. This iBrief therefore concludes that although the Anti-Phishing Act can play a supporting role in the battle, technological solutions are the most effective means of reducing or eliminating phishing attacks.

INTRODUCTION

¶1 The Internet has created a marketplace for businesses and consumers to come together and interact in new and exciting ways. Unfortunately, it has also provided criminals and the unscrupulous with a new venue.[2] Nowhere is this more evident than in the recent emergence and growth of the phenomenon known as "phishing." The United States Department of Justice defines phishing as

> criminals' creation and use of e-mails and websites—designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords.[3]

---

[1] Robert Stevenson is a third year student at Duke University School of Law. He received a B.A. in Economics from Brigham Young University and is the founder of an Internet services company.

[2] *See e.g., House of Representatives Government Reform Committee, Technology, Information Policy, Intergovernmental Relations and the Census Committee Hearing*, 108th Cong. 35-36 (2004), [hereinafter House Committee Hearing] (Testimony of Bill Conner, Chairman, President and CEO of Entrust, Inc. stating that "[j]ust as the Internet has supercharged commercial transactions, it has also supercharged cybercrime.") *available at* 2004 WL 2137978.

[3] United States Dept. of Justice, *Special Report on "Phishing,"* p. 3 (2004) [hereinafter DOJ Report], *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf (last visited Oct. 19, 2004).

¶2 Studies indicate that the number of phishing incidents is increasing at an alarming rate. A recent report by the Anti-Phishing Working Group[4] ("APWG") found that phishing attacks have increased by an average of 30% each month since July 2004.[5] In January 2005, alone, more than 12,800 phishing emails and 2,560 phishing web sites, representing 64 hijacked brands, were reported and tracked by the APWG.[6] Perhaps the rapid growth of this new type of consumer fraud can be explained by the additional finding by the APWG that "data suggests that phishers are able to convince up to 5% of recipients to respond to them."[7] By contrast, the estimated response rate for regular spam is 0.01%.[8] Further research has estimated that the costs of these phishing attacks on consumers in 2003 ranged from $500 million to an amazing $2.4 billion.[9]

For other definitions of "phishing," *see also* The Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of Email Spoofing Scams*, Dec. 12, 2003 [hereinafter APWG Whitepaper] ("Phishing is the creation of email messages and web pages that are replicas of existing sites to fool users into submitting personal, financial, or password data.") *available at* http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf (last visited Oct. 19, 2004); *and* Financial Services Technology Consortium, *Project Proposal: FSTC Counter-Phishing Initiative*, 2004, p. 2 [hereinafter FSTC Proposal] ("'phishing' refers to the activities of criminals who imitate legitimate companies' e-mails, web sites, and phone calls or other communications to entice account holders to share highly sensitive personal data such as SSNs, usernames and passwords, and/or account numbers. Once acquired, perpetrators leverage the stolen authenticators to commit a myriad of subsequent crimes.") *available at* http://fstc.org/projects/FSTC_Phishing_Prospectus_Final.pdf (last visited Oct. 19, 2004).

[4] "The Anti Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing…There are currently over 706 organizations participating in the APWG." Anti-Phishing Working Group, *Phishing Activity Trends Report*, January, 2005, [hereinafter APWG Report] *available at* http://antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf (last visited March 6, 2005). The website for the APWG is http://www.antiphishing.org/.

[5] APWG Report, *supra* note 4.

[6] *Id.*

[7] *Id.*

[8] Laura Sullivan, *California; Internet 'Phishing' Scams on the Rise*, L.A. TIMES, Mar. 22, 2004, p. C2.

[9] *Good news: 'Phishing' scams net* only *$500 million* , CNET NEWS.COM, Sept. 29, 2004 (article summarizes studies from Truste, Inc. and Gartner, Inc.) *available at*

¶3 Phishing is a particularly invidious attack on the Internet community because it almost always involves two separate acts of fraud. The phisher first "steals" the identity of the business it is impersonating and then acquires the personal information of the unwitting customers who fall for the impersonation. This has led commentators to refer to phishing as a "two-fold scam"[10] and a "cybercrime double play."[11]

¶4 It is clear that something must be done soon to curb this alarming trend. The question, however, is what can and should be done to reduce or even eliminate phishing attacks.

¶5 On February 28, 2005, Senator Patrick Leahy (D-VT) introduced the Anti-Phishing Act of 2005 ("the Act") in the United States Senate.[12] The Act is virtually identical to the Anti-Phishing Act of 2004, which Senator Leahy introduced last year but stalled in committee without coming to a vote before the congressional session ended.[13] This iBrief provides an analysis of the Act and concludes that this bill would fill some gaps in the current law and would make prosecution and conviction of phishers easier. However, the Act suffers from the same inherent weaknesses as all legislation aimed at solving what is essentially a technological problem. Although Congress should enact this legislation, alone it is unlikely to truly stop the flow of phishing attacks. The only way to effectively eliminate the phishing problem is to focus on technological changes and have legislation play a supporting role.

I. THE ANTI-PHISHING ACT OF 2005

A. Content of the Act

¶6 The Act, if passed, will add two crimes to the current federal law:

1. It would criminalize the act of sending a phishing email regardless of whether any recipients of the email suffered any actual damages.[14]
2. It would criminalize the act of creating a phishing website regardless of whether any

---

http://news.com.com/Good+news+Phishing+scams+net+ionlyi+500+million/2100-1029_3-5388757.html (last visited Oct. 19, 2004).

[10] Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 12 (2004).

[11] Thomas Fedorek, *Computers + Connectivity = New Opportunities for Criminals and Dilemmas for Investigators*, 76-FEB N.Y. ST. B.J. 10, 16 (2004).

[12] S. 472, 109th Cong. (2005).

[13] S. 2636, 108th Cong. (2004).

[14] S. 472 at § 1351(b).

> visitors to the website suffered any actual damages.[15]

¶7 Senator Leahy described the effects of the Act in this way:

> The [Act] 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.[16]

¶8 The Act is also notable for what it does not contain. The bill provides no guidance or allocation of additional resources for its enforcement. This is in contrast with a recently proposed bill in the House of Representatives[17] aimed primarily at "spyware."[18] While the House bill adds no law related to phishing, it does provide for the appropriation of "the sum of $10,000,000 to the Attorney General for prosecutions needed to discourage the use of spyware and . . . phishing."[19] Because the House bill adds no new law directed at phishing,[20] this iBrief does not further discuss or analyze it. It is noted here only for the purpose of pointing out a possible deficiency in the Act.

---

[15] *Id*. at § 1351(a).

[16] 150 CONG. REC. S7897-02 (daily ed. July 9, 2004) (statement of Sen. Leahy). This statement was in support of the 2004 version of the Act. Because the 2005 Act is virtually identical to the 2004 version, statements supporting, analyzing, or criticizing one version are assumed to apply to the other version, as well.

[17] Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, 109th Cong. (1st Sess. 2005). This act is virtually identical to one that was submitted in the previous Congressional session but did not reach a vote. That act was the Internet Spyware (I-SPY) Prevention Act of 2004, H.R. 4661, 108th Cong. (2d Sess. 2004).

[18] "Spyware" is "software that 'aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge.'" H.R. REP NO. 108-698, at 3, (2004) (Report quotes from the Federal Trade Commission's definition of spyware available at http://www.ftc.gov/bcp/workshops/spyware/).

[19] H.R. 744, Sec. 3, 109th Cong. (1st Sess. 2005).

[20] There is some indication from the Report accompanying H.R. 4661 that its sponsors did not feel that any additional law specifically addressed to phishing is necessary since they write that "the [phishing] schemes themselves, and the uses of the information by the criminals who obtain it are not unique to the Internet, and almost all are illegal under existing Federal criminal laws dealing with wire fraud." H.R. REP NO. 108-698, at 4 (2004).

B. History and Status of the Act

¶9 There is little information indicating how the Act came into being. Senator Leahy, himself, at the time he introduced the 2004 version of the bill said only that "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."[21] For instance, Senator Leahy has attempted to address First Amendment concerns that some groups may have had regarding certain provisions within the bill since Senator Leahy also stated when he introduced the bill, "[t]here are important First Amendment concerns to be protected. The Anti-Phishing Act protects parodies and political speech from being prosecuted as Phishing."[22]

¶10 Beyond the congressional record, there is some indication that the Act had the support of some influential Internet entities including the Anti-Phishing Working Group, the Center for Democracy and Technology, and eBay.[23]

C. Analysis

1. Where the Act helps

¶11 The main area in which the Act will likely help in the current fight against phishing attacks is in allowing the prosecution of phishers without requiring a showing of specific damages to any individual. As explained by a member of Senator Leahy's staff:

> [p]hishing scammers already violate a host of identity theft and fraud laws, but prosecuting them under those statutes can be challenging . . . . To charge scammers now, law enforcers need to prove that a victim suffered measurable losses. By the time they do that . . . the scammer has often disappeared.[24]

¶12 This reasoning is bolstered by data compiled by the APWG finding that the average life span for phishing sites, measured by how long they continue to respond with content, is 5.8 days.[25] Accordingly, law enforcement personnel have, on average, 5.8 days from the time the phisher

---

[21] 150 CONG. REC. S7897-02 at S7898 (daily ed. July 9, 2004) (statement of Sen. Leahy).
[22] *Id.* at S7897.
[23] Winter Casey, *Lawmakers File Tech Bills To Spur Economic Growth*, TECHNOLOGY DAILY PM, July 9, 2004, *available at* 2004 WL 74915988.
[24] David McGuire, *Senate Bill Targets 'Phishers'*, Newsbytes News Network, Jul. 12, 2004, *available at* 2004 WL 55866572.
[25] APWG Report, s*upra* note 4.

first initiates the scam to track him or her down and compile sufficient evidence to bring charges.[26]

¶13 Additionally, removing the requirement to show damages permits businesses to more easily come forward as the prime complainant against a phisher that has "stolen" their web identity to scam their clients. Recall that a phishing attack involves two victims, the business and the consumer.[27] While the consumer's economic damages are usually fairly obvious, the reputational damages that a business incurs as the result of a phishing scam are often much more difficult to quantify.[28]

2. Where the Act falls short

¶14 Any legislation aimed at punishing Internet-related offenses faces three formidable hurdles: (1) difficulty inherent in finding the perpetrator of an on-line crime, (2) obtaining personal jurisdiction, and (3) collecting the judgment. Unless these can be overcome, the net impact of bills such as the Anti-Phishing Act will be limited, at best.

¶15 The first problem, finding the perpetrator, is illustrated by two related phishing incidents at the University of Michigan and Duke University. In the fall of 2002, the University of Michigan hosted a conference of the Palestinian Solidarity Movement ("PSM"). Shortly before the conference was to begin, an email was sent to "a large number of [the university's] faculty, staff, and students"[29] purporting to be sent by a member of a student organization involved with the conference and with the approval and assistance of university administration.[30] The email, which was not in fact authorized by anyone connected with the conference or the

---

[26] This is, of course, assuming that an actual person can be traced even if a particular phishing website remains "live." For a more in-depth discussion of the difficulties of tracking down Internet scammers and holding them legally accountable for their actions, *see* Michael Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 CHAP. L. REV. 39 (Spring 2004).

[27] *See e.g.* Kathy M. Kristof, *Avoid Letting Yourself Get Hooked by an Internet 'Phishing' Expedition*, LOS ANGELES TIMES, Feb. 1, 2004, C3 *available at* 2004 WL 55890852. (referring to phishing as a "two-tiered scam").

[28] *See e.g.* Karen Greenstein, *Defending Your Brand from Email Spoofs—Powerpoint Slides*, 784 PLI/Pat 271, at 279-80 (Apr. 2004) (listing the harms to a business caused by a phishing attack as (i) harm to reputation, (ii) impairment of legitimate communication, (iii) strain on the customer service department, and (iv) strain on the servers).

[29] Paul Courant, *Provost's Statement on Fraudulent ("Spoofed") E-Mail*, Oct. 3, 2002 [hereinafter Second Courant Message], *available at* http://www.umich.edu/courant2.html (last visited Oct. 21, 2004).

[30] *Id.*

university,[31] contained "many misstatements of fact"[32] and "violated norms of civility and respect."[33] Despite "pursuing a vigorous investigation"[34] into the source of the offending email that included the services of "campus information technology security experts"[35] the investigators were only able to conclude was that "the message originated in California."[36]

¶16 A university administrator in charge of the investigation explained the inability to track down the sender of the unauthorized email more precisely:

> It is important to recognize that when e-mail is sent from one point on the Internet to another, it can follow a complex path as it travels through multiple mail servers. In this case, the senders used an unsecured server known as an "open relay" in order to help hide their identity. Despite the best efforts of the investigating team, it is possible we may not be able to determine who really sent the messages.[37]

¶17 Two years after this event, an almost identical incident occurred at Duke University shortly before Duke hosted a PSM conference.[38] As of yet, investigators at Duke attempting to track down the source of the unauthorized e-mail were again only able to "determine that it originated in California."[39]

¶18 These incidents highlight one of the biggest roadblocks that any legislation in this area faces—finding the perpetrators. In order to punish phishers for their fraudulent actions, one must first locate them. Yet, the current state of Internet technology makes this extremely difficult. In a recent report to Congress by the Federal Trade Commission concerning the spam problem—the findings of which could apply equally as well to phishing—the situation was explained in this way:

---

[31] *Id.*
[32] Paul Courant, *Interim Provost Paul Courant's Message to Campus Regarding Violation of E-Mail Policy*, Sep. 26, 2002 [hereinafter First Courant Message], *available at* http://www.umich.edu/courant.html (last visited Oct, 21, 2004).
[33] *Id.*
[34] *Id.*
[35] Second Courant Message, *supra* note 29.
[36] *Id.*
[37] *Id.*
[38] Email from John F. Burness, Senior Vice President for Public Affairs and Government Relations, Duke University, to Members of the Duke Campus Community (Oct. 13, 2004, 15:24:00 EDT), *available at* http://www.dukenews.duke.edu/psm/bogusmessage.html (last visited Oct. 21, 2004).
[39] *Id.*

> The single greatest challenge for anti-spam law enforcement is to identify and locate the source of a particular spam campaign. Finding the wrongdoer is an important aspect of all law enforcement efforts, but in spam cases it is a particularly daunting task. Because the present email system lacks any mechanism requiring that a sender's identity be authenticated, spammers can and do conceal their identities with ease.[40]

Put another way,

> [the] Internet allows anonymous communications that are virtually impossible to trace through Internet nodes. Cyber-tortfeasors frequently use false e-mail headers and anonymous remailers to make it difficult to retrace the steps of wrongdoing. Computer records are easy to alter and it is likely that spoliation of electronic evidence is widespread.[41]

No threats of legal action can ever hope to effectively reduce the growing phishing problem until there is some way of finding the phishers.

¶19 The second hurdle, obtaining jurisdiction over the phisher, stems from the fact that "[c]ybercrime has always been a cross-border enterprise."[42] Even if the perpetrator can be located, it is very possible that the person is located in a foreign country outside of the legislation's jurisdictional reach. Indeed, "[c]ountries where cybercrime flourishes tend to have weak laws dealing with computer crime, law enforcement agencies that lack computer forensic capabilities and an underdeveloped apparatus for collaborating with law enforcement agencies in other countries."[43]

¶20 In fact, the APWG found that as of January 2005, only 32% of phishing web sites were located in the United States.[44] The three countries hosting the next largest percentage of phishing sites were China, South Korea and Japan.[45] Clearly, jurisdictional issues are a major hurdle in applying U.S.-based legislation to foreign phishing scheme perpetrators.

---

[40] FEDERAL TRADE COMM'N, A CAN-SPAM INFORMANT REWARD SYSTEM: A REPORT TO CONGRESS at 10 (Sep. 2004) (footnotes omitted), *available at* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf (last visited Oct. 21, 2004).
[41] Rustad, *supra* note 26, at 66.
[42] Fedorek, *supra* note 11, at 17.
[43] *Id.*
[44] APWG Report, supra note 4.
[45] *Id.*

¶21 The third problem is that even if the first two hurdles are overcome the perpetrator will very often be found to be "judgment proof."[46] This phenomenon is explained as follows:

> Even when a prevailing plaintiff wins a large punitive damages award, collecting it is a different matter. Collecting a punitive damages award is difficult because a number of wily Internet mice either fail to make an appearance, file bankruptcy, or simply disappear after the plaintiff obtains a judgment. Default judgments outnumbered cases decided by juries in the larger cybertort dataset. . . . The large number of default judgments in cyberlaw reflects the reality that it is easy for web sites to disappear or assets to be transferred.[47]

¶22 The Federal Trade Commission's own experience in attempting to enforce judgments against Internet scammers illustrates the problem:

> Indeed, the most egregious spammers, like other fraud operators, are likely to transfer assets offshore to place them beyond the reach of U.S. courts. . . . In the FTC's experience, attempting to reach the defendants' offshore funds necessitates a foreign action to enforce a U.S. court judgment. This is time-consuming, expensive, and, in many cases, futile, as many countries do not enforce U.S. court judgments obtained by government agencies.[48]

The House of Representatives itself has echoed these sentiments by acknowledging that "the vast majority of phishing would likely be unaffected by government regulation or civil enforcement."[49]

¶23 With these three formidable hurdles—finding the perpetrator, obtaining jurisdiction, and collecting the judgment—what options do we have to combat the ever increasing phishing problem?

---

[46] "Judgment proof" is defined by Black's Law Dictionary 439 (abridged 5th ed. 1983), as "[d]escriptive of all persons against whom judgments for money recoveries are of no effect; e.g., persons who are insolvent, who do not have sufficient property within the jurisdiction of the court to satisfy the judgment, or who are protected by statutes which exempt wages and property from execution."

[47] Rustad, *supra* note 26, at 67-68.

[48] FEDERAL TRADE COMM'N, *supra* note 40.

[49] H.R. REP NO. 108-698, at 5.

II. ANOTHER OPTION – FOCUS ON TECHNOLOGY

A. If not legislation, then what?

¶24 Phishing is a problem that exploits a weakness in the current state of technology and, in a manner of speaking, "uses it against us." It makes sense, then, that an effective solution to this problem should focus on repairing this weakness.[50] One commentator described the technological weakness in this way:

> When the Internet was used mainly to communicate and access information, the lack of security didn't much matter. Now that it's used for online transactions and critical information, the absence of security is truly a big problem. It's as if consumers and businesses that rely on the Internet have wandered into a dangerous neighborhood of cheats, pickpockets and thieves, and don't even know it.[51]

¶25 Now that consumers and businesses are becoming increasingly aware of the Internet's "dangerous neighborhood," what can be done about it? The House of Representatives has offered this useful suggestion: "[t]here is no silver bullet to end spyware or phishing but greater consumer awareness and use of available technological countermeasures clearly hold the greatest promise for curbing these abusive practices."[52]

¶26 Congress's first recommendation is to increase "consumer awareness." To be sure, "common sense and a healthy level of suspicion go a long way toward not becoming a victim of phishing."[53] Nevertheless, consumer awareness alone is not sufficient to solve the phishing problem. While it might be convenient to assume that only the gullible or Internet novices fall victim to phishing scams, the current state of technology and the phishers' ability to exploit it is such that even the most jaded and "web savvy" consumers can fall victim to a phishing scam.[54] Consumer awareness must be coupled with technological improvements.

---

[50] FSTC Proposal, *supra* note 3, at 3 (noting that "phishing relies on email, phone, and web technologies to bring forward its traps. Thus, countermeasures will necessarily have a fundamental technology basis rooted in the ability to authenticate emails and web sites.").

[51] House Committee Hearing, *supra* note 2, at 36 (Testimony of Bill Conner, Chairman, President and CEO of Entrust, Inc.).

[52] H.R. REP NO. 108-698, at 5.

[53] *Id.*

[54] For an in-depth look at many of the possible ways that current phishers are defrauding consumers, *see* GUNTER OLLMAN, NEXT GENERATION SECURITY SOFTWARE, LTD., THE PHISHING GUIDE: UNDERSTANDING & PREVENTING PHISHING ATTACKS (Sep. 2004) *available at*

B. The Recommendations

¶27 A number of Internet-industry groups and technology companies have come out with specific recommendations for changes and improvements in the current Internet technology that they feel would reduce or even eliminate the phishing problem. These groups include the APWG,[55] the Financial Services Technology Consortium,[56] Next Generation Security Software Ltd.,[57] Yahoo! Inc.[58] and Microsoft Corporation.[59]

¶28 Judging from the number of different sources that are making them, there seems to be no shortage of recommendations for how to make the Internet and email more secure. The real questions seem to be (1) which recommendations should be implemented, (2) how should they be done, and (3) when? It is the lack of a consensus on these details that has prevented us from already having the recommended upgrades.[60] Despite the current disagreement, the rising tide of phishing scams is prodding the various groups to work together to implement changes to alleviate the problem.[61]

¶29 Leading the charge in calling for technology changes to combat phishing has been the APWG. In December 2003, the group proposed four

---

http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf (last visited Oct. 19, 2004) [hereinafter NGSS Whitepaper]. *See also* Leslie Walker, *Internet Snagged In the Hooks Of 'Phishers,'* THE WASHINGTON POST, Jul. 29, 2004, E01, *available at* 2004 WL 82772584 (stating that "Verisign, Inc. reported that phishing attacks are increasingly sophisticated. Verisign analyzed 490 bogus e-mails and found most did not contain the misspellings often seen in first-generation phishing. . . . Today, even cyber-savvy folks can get stung because the bogus e-mails and Web sites look so official, down to perfect replicas of, say, eBay's logo and the real Bank of America Web site."); *and Deceptive E-Mail Could Cost Consumers $500 Million, Study Finds*, CMP TECHWEB, Sep. 30, 2004, *available at* 2004 WL 64588196 (stating that "[p]hishing attacks are hard to detect. . . . In a test of 200,000 E-mail users . . . fewer than 10% were able to distinguish phishing messages from legitimate E-mail all the time.").

[55] *See* APWG Whitepaper, *supra* note 3.

[56] *See* FSTC Proposal, *supra* note 3.

[57] *See* NGSS Whitepaper, *supra* note 54.

[58] *See* Thomas Claburn, *E-Mail-Authentication Problems Spawn New Apps*, INFORMATIONWEEK, Sept.21, 2004, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=47900731.

[59] *See* Thomas Claburn, *Standards Group Rejects Microsoft's E-Mail Authentication Plan*, INFORMATIONWEEK, Sept. 14, 2004, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=47205247.

[60] *See e.g.*, *id.*

[61] *See e.g.*, Claburn, *supra* note 58 (noting that "[d]espite disagreements about authentication standards, pretty much every commercial enterprise on the Internet concurs that something needs to be done to address domain spoofing and phishing.").

possible technological solutions aimed at preventing phishing scams.[62] These recommendations are:

1. Strong Website Authentication.[63]
2. Mail Server Authentication.[64]
3. Digitally Signed Email With Desktop Verification.[65]
4. Digitally Signed Email With Gateway Verification.[66]

¶30 The first recommendation, strong website authentication, "would require all users of legitimate e-commerce and e-banking sites to strongly authenticate themselves to the site using a physical token such as a smart card."[67] In essence, this means that anyone wanting to bank or make purchases online from such websites would first need to swipe a card in a device connected to their computer before being allowed to do so. The APWG notes that this approach is feasible only "for e-commerce and e-banking applications that do not have a large number of users, and where the risk of a phisher gaining access to a user's account are high."[68]

¶31 The second recommendation, mail server authentication, would require all email to pass through a gateway server for source verification.[69] The APWG notes that the benefits of this approach include the ease with which it can be configured and the increased ability for legitimate business email to be identified.[70] Potential drawbacks, however, include the facts that both sender and recipient gateways are required and that it does not accommodate e-mail forwarding.[71]

¶32 The third recommendation, digitally signed email with desktop verification, would have companies that feel they are vulnerable to phishing attacks attach a digital signature to all their outbound email. The digital signature would then be verified for authenticity by the email client used by the recipient.[72] In evaluating the pros and cons of using digital signatures, the APWG notes that this approach would make it impossible to forge the

---

[62] APWG Whitepaper, *supra* note 3.
[63] *Id.* at 5.
[64] *Id.* at 6.
[65] *Id.* at 7.
[66] *Id.* at 8.
[67] *Id.* at 5.
[68] APWG Whitepaper, *supra* note 3, at 6.
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.* at 7.

"From:" address without detection.[73] However, it would still be possible for a phisher to obtain a valid digital certificate for a domain that is deceptively similar to that of a target company (e.g. the phisher could use "ebay.custservices.com," which is an entirely different domain from "ebay.com").[74] Concerning the use of the recipients' email client to verify the validity of the digital certificates, the main drawback is that not all email clients currently support the secure email standard that would be employed.[75]

¶33 The fourth recommendation, digitally signed email with gateway verification, is almost identical to the third recommendation; however, "[i]nstead of relying on the end user's email client to verify the signature on the email, a gateway server at the mail relay level would verify the signatures before they were even received by the receiver's email server."[76] While this approach solves the problem of some recipients' use of email clients that do not support the digital certificate standard, it does not address the problem noted above regarding a phisher's possible use of a deceptively similar domain name.[77]

¶34 After providing a detailed and critical discussion of each recommendation the APWG concludes their analysis with the opinion that "a combination of signed email with desktop verification, and either gateway verification or mail server IP verification would solve all aspects of the phishing problem for both consumers and business users."[78] Whether or not that prediction would eventually prove accurate, technological changes of the type recommended by the APWG are generally agreed to be a much needed step in the right direction to address the rising phishing problem.[79]

CONCLUSION

¶35 Something must be done to stop the increasing flow of phishing scams on the Internet and technological changes must be at the forefront of any action taken. While the Anti-Phishing Act of 2005 will likely provide some additional assistance in the fight against phishing scams—and should, therefore, be passed into law—its usefulness is limited due to the global nature of the Internet and the ease with which phishers can hide and avoid judgments. Technological changes such as those proposed by the APWG

---

[73] *Id.*
[74] APWG Whitepaper, *supra* note 3, at 8.
[75] *Id.*
[76] *Id.*
[77] *Id.* at 9.
[78] *Id.*
[79] *See e.g.*, FSTC Proposal, *supra* note 3, at 5; Claburn, *supra* note 58.

therefore offer the most hope of providing a comprehensive and lasting solution to the phishing epidemic.